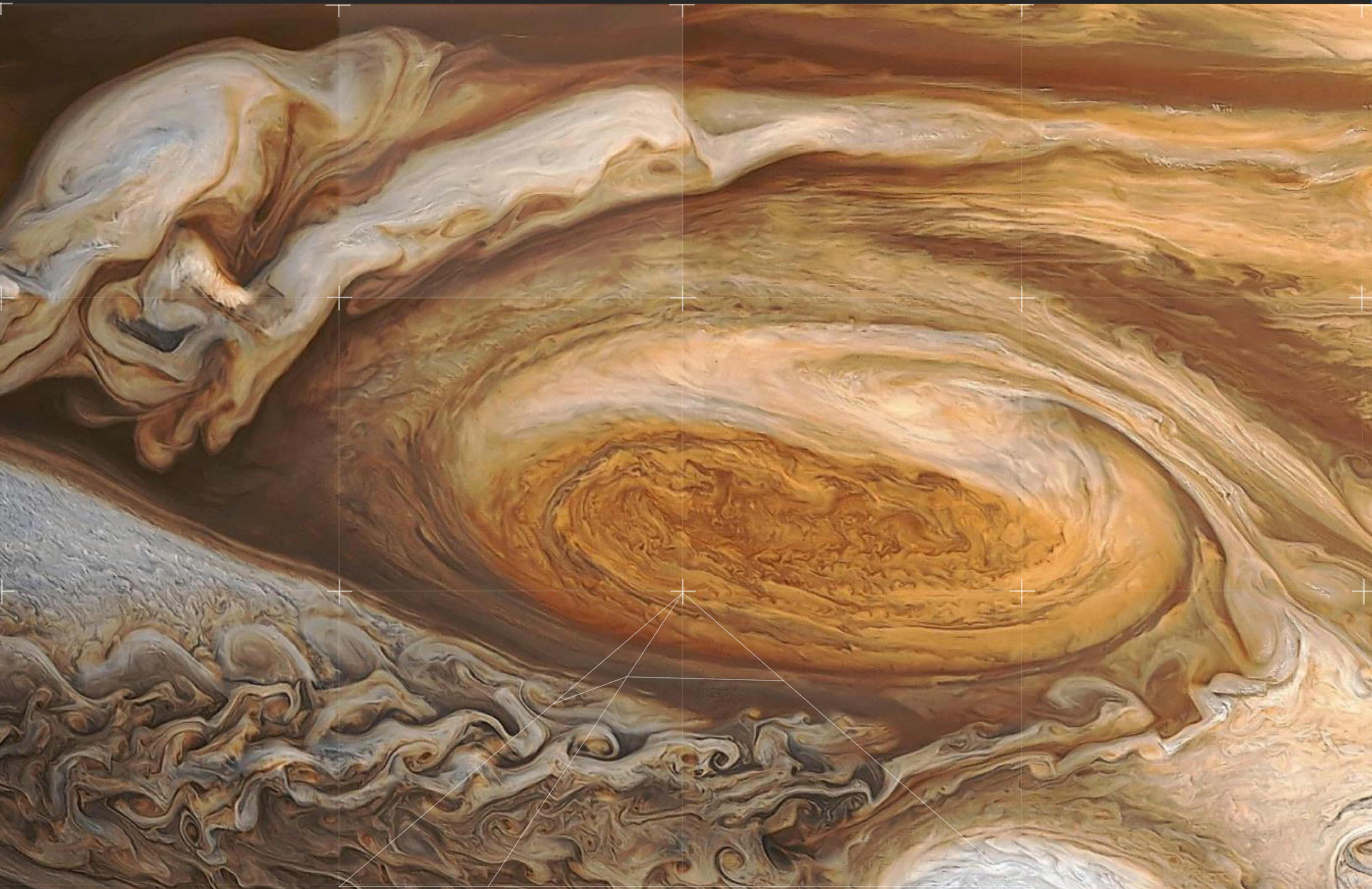
HYPERSPHERE

Technical Whitepaper



The HyperSphere – a Real-time Cybersecure Privacy Network with Embedded DyDAG Blockchain for Global e-Commerce

Evgen Verzun & Richard K Williams

www.hypersphere.ai

synopsis

A fully decentralized autonomous real-time cybersecure privacy network with enterprise-grade certificate authority (user identity), privacy protections (including pseudonymity), and energy-efficient network-native embedded blockchain for global e-commerce is described. Unlike the cyberattack vulnerability of financial and blockchain transactions executed over the Internet using TCP/IP, the HyperSphere employs a new communication protocol with military-grade hypersecurity– the Secure Dynamic Network & Protocol (SDNP). The SDNP protocol combines autonomous dispatcher-based packet routing and fragmented data transport of anonymous data packets over a meshed network with hop-by-hop dynamic encryption and state-based concealment techniques to repel packet hijacking, man-in-the-middle attacks, and metadata surveillance of network traffic. The HyperSphere cloud comprises an *ad hoc* dynamic array of cloud portals called 'HyperNodes', downloaded software hosted on global server clouds, local ISPs, and personal devices, representing a heterogeneous hybrid network of its users, i.e. the 'people's network', whereby HyperNode users participate as *resource providers* to execute transactions, perform computing, and transport data for HyperSphere merchants and service providers.

As compensation, HyperNodes participating in the successful completion of HyperContracts mint network-native eco-friendly digital utility token useful in purchasing HyperSphere services and tradable in digital currency exchanges. The process of minting is network-native, using (OSI Layer-3, Layer-4) data transport in the cloud to generate cryptographically unique HyperNode hop codes (HHCs)– hashed data required as Proof-of-Performance to adjunctively generate new digital currency using one-trillionth (10^{-12}) the energy required by Bitcoin mining.

All token transactions are recorded on multi-tree (non-communal) perpetual blockchains called *dynamic* directed acyclic graphs (DyDAGs) with ownership established through a private identity-trust-chain linked to a user's identity and root CA-certificates. Transactional integrity, privacy, and blockchain security are protected by numerous innovative mechanisms limiting access to a blockchain on a need-to-know basis, including blockchain replicant blockchain observer segments (RBOS), one-time transaction token (OT^3) proxies, blockchain defragmentation, pseudonymous transactions, auxiliary sidechains (for documentation), and more...

In the HyperSphere, merchants and service providers are able to access vast global resources at superior cost efficiencies to securely and privately conduct e-commerce including cloud communication, cloud computing, disaggregated cloud storage, cloud connected (IoT, V2X) devices, and e-services including financial transactions and blockchain-as-a-service (BaaS). The HyperSphere and SDNP protocol stack, licensed to the non-profit HyperSphere Foundation, represents an extensive portfolio of inventive matter including US and international patents, issued and pending.

Table of Contents

The HyperSphere – a Real-time Cybersecure Privacy Network with Embedded DyDAG Blockchain for Global e-Commerce

Evgen Verzun & Richard K. Williams

Abstract– An innovative and highly advanced cybersecure 'privacy' network for global e-commerce, realtime communication, and cloud computing– the HyperSphere, is introduced. Featuring military-grade 'hypersecure' data transport, enterprise-grade certificate authority (identity verification), and network-generated eco-friendly cryptocurrency, the HyperSphere mitigates security, transactional, and privacy risks of the Internet while enabling a self-contained economic environment for commercial and private transactions and e-services using its own network-generated cryptocurrency. The HyperSphere comprises a global dynamic *ad hoc* heterogeneous network of 'HyperNodes', software downloaded onto servers, PCs, and smartphones delivering resources to merchants and businesses while earning HyperNode owners (resource providers) payment in network utility tokens. HyperNodes operate metamorphically, changing adaptively into authority nodes, task (process) nodes, or name-server nodes as required to execute HyperContract tasks and services, and to apportion HyperNode payments ratably in accordance with its contributions. Unlike conventional PoW, HyperSphere employ lightweight multi-tree blockchains comprising *dynamic directed-acyclic-graphs* (DyDAGs), introduced herein for the first time, uniquely designed for rapid execution, robust dynamic security, cloaked distributed consensus, attack resilience, and inherent privacy protection. Using replicant blockchain observer segments (RBOS) and a cloaked jury-of-peers with limited access to blockchain provenance, the HyperSphere is able to mitigate double spending, prevent fraud, and repel attacks while prohibiting backtracing and privacy leakage. In the HyperSphere, network security is wholly unique: Using hypersecure technology originally developed and deployed in professional communication, the patented "secure dynamic network and protocol" (SDNP) offers anonymous packets of fragmented data dynamically routed over an ever-changing 'meshed' network, minimizing propagation delays while confounding surveillance, thereby rendering packet sniffing, hijacking, network surveillance, and man-in-middle attacks meaningless.

Index Terms– Network, real-time, security, cybersecure, privacy, blockchain (BC), decentralized, dynamic, cryptocurrency, digital currency, utility token, trust-chains, e-commerce, e-services, cloud computing, disaggregated data storage, real-time communications, cloud connected devices, Internet-of-Things (IoT), Internet-of Everything (IoE), OSI model, data packets, artificial intelligence (AI).

I. Introduction

THE advent and recent rapid expansion of digital signatures [1], distributed ledgers [2], blockchains [3] [4], and cryptocurrency [5] comprise the adaptation and repurposing of *cryptographic transactional technology* [6] to everyday business and personal life, a surprising (and largely unexpected) info-tech development with potentially profound commercial [7], personal, and sociological ramifications [8] [9]. Advocates purport crypto-based commerce represents a uniquely transformative technology promising transactional integrity of credible business contracts and personal agreements without requiring a legal authority or governmental agency to participate in an exchange. These so-called "smart contracts" or crypto-contracts digitally facilitate, verify, and/or enforce the negotiation or performance of a contract [10] without third parties, thereby allegedly protecting privacy and personal information of its participants.

The potential application of crypto-contracts is diverse and may include electronic notary services [11], electronic purchase agreements and supply chain management [12], bank-less money transfers [13]; blockchain recording of property deeds [14]; and lawyer-less execution of wills, trusts, and estates [15] [16]. By removing the need for a central bank or certification authority to achieve 'trusted' transactions and contracts [17] [18], transaction speed and efficiency improves while contractor expense is reduced (or eliminated altogether), driving down transactional costs while improving business profitability. Specifically, decentralizing legal [19] and financial [20] authority and processes offers the potential benefits of fostering competition, improving service, lowering fees, and inviting innovation in risk adverse industries.

In financial services for example, blockchain technology offers a compelling option to replace monopolistic, autocratic, arcane, and even obsolete federated practices of big banks with flexible decentralized alternatives. By eliminating reliance on a central authority, blockchain technology can improve the integrity and transparency of financial transactions involving secure payments [21] [22], money transfers [23], e-commerce [24] [25], and insurance [26].

Ironically risk adverse industries such as banking, reticent to adopt new technologies or embrace blockchains, remain notoriously vulnerable to cyber attacks, putting at risk client information, personal identity, wire transfers, online transactions, and theft of account assets. Although financial institutions offer comfort that most (but not all) financial transactions are insured, the ultimate cost of bank crime, fraud, and theft is invariably born by the consumer, camouflaged as inexplicable service fees and rising expenses.

Aside from its potential benefit to the financial services sector, blockchain technology is already proving useful for tech startups, facilitating both a channel for marketing and a flexible means for fundraising. Decentralized blockchain based contracts represent a potentially powerful disruptive market force, enabling small and medium sized businesses (SMBs) to effectively compete against much larger corporations [27] by facilitating supply chain management and contracts [28][28]; audit-ready records; process automation [29] [30] and by connecting entrepreneurs to clients and capital funding [31]

Evgen Verzun is a founder & architect of the HyperSphere and CEO of Listat Engineering, Silicon Valley and Europe (e-mail: e@ hypersphere.ai).

Richard K Williams is a HyperSphere co-founder & author; and the CEO, President and CTO of Adventive Technology Ltd. in Hong Kong, Taiwan, and Silicon Valley (e-mail: r@hypersphere.ai).

31 Jul 2018, HyperSphere technical whitepaper, version TWP 1.8

[32]. Decentralization also addresses concerns that large corporations could control access of big data [33], insuring that no one company has exclusive access to or control of market data. As such, blockchains offer the potential for *democratizing* business.

As an alternative to venture capital and debt financing, blockchain-based cryptocurrency offerings including both private placements and public ICOs (initial coin offerings) have been used successfully for fund raising for startups, for funding product development, and for marketing [34] [35] [36]. One advantage of cryptocurrency offerings over venture capital is that the issuer needn't relinquish control or ownership of the company to fund development or growth.

In their exuberance, some blockchain advocates believe since a blockchain comprises an immutable ledger, that blockchain technology should be used to combat fraud, security and privacy attacks. The implication of this premise is that the blockchain itself is secure and immune to hacking. But is this accolade meritorious, or is the blockchain just replacing today's vulnerabilities with newer ones?

II. Network vulnerabilities & deficiencies

Despite its limitless potential, the ultimate commercial and sociological destiny of blockchain technology depends on reaching widespread acceptance and user adoption. Successful market penetration relies on several factors– utility, convenience, cost, and most significantly on "trust", i.e. user perception of blockchain security and privacy. Because blockchain transactions occur over the Internet, network security and personal privacy represent real threats and valid concerns for blockchain transactions, the same as any online activity.

Amid an incessant barrage of news reports of data breaches, cyber-attacks, and surveillance reports, the Internet's lack of security and deficient privacy provisions are notorious. Confounded by the cavalier treatment of client personal information by social media, merchants, credit bureaus, insurance agencies, and financial institutions, the Internet not only provides a platform for cyber criminals to hone their trade, but also represents a convenient medium for 'profiling' targets, i.e. collecting information in order to maximize cyber attack damage. To perform a proper risk assessment for blockchain technology, we must first look at the kinds of security methods employed to protect banking, Internet, and e-commerce transactions, and the types of attacks these known security measures can reliably repel.

With a proverbial plethora of 'experts' and vendors claiming to hold the secret keys to mastering security and insuring privacy, one must question why the number, frequency, and magnitude of cyber-attacks are growing, not diminishing. The answer is at least in part, network vulnerability is a multi-factor problem with varied root causes including reliance on antiquated systems, unsecured communication links (intrusion points), the willful release and promotion of personal data and private information on and by social media, target behavior predictability, and in general a pervasive (if not religious) over-reliance on encryption as the sole means for securing data and transactions.

Because security and privacy attacks come in many forms, no unified taxonomy can be employed to arrange or classify the subject matter. That said, it is convenient to group attacks into several classes of vulnerabilities (A) trust attacks, (B) network attacks, (C) data breaches, and (D) blockchain attacks.

A) Identity Fraud & Trust Attacks

Trust attacks can be considered *an attack of imposters*, where perpetrators (or their devices) pretend to be someone they are not, usurping the identity, authority, and access privileges of their target to engage in illicit transactions or to install malware into devices disguised as valid applications or utilities. Oftentimes trust attacks are performed immediately following network and communication attacks in order to capitalize on stolen information before anyone notices. Spying and personal profiling are also often used to gather information as a prelude to imposter exploits including the use of network attacks and packet sniffing, or through physical device interventions using malware including spyware, key loggers, login exploits, etc. The monetization of identity theft also represents another type of trust attack, using fake credentials to divert funds (wire fraud) or fraudulently pay for purchases (transactional fraud).

1) Money Wire Fraud

Surprisingly, because of their antiquated methods, financial institutions are particularly susceptible to trust attacks. For example, present day bank wire transfer systems such as the widely used Society for Worldwide Interbank Financial Telecommunication (SWIFT) [37] employ half-a-century old technology– systems predating the smart phone, the Internet, and even the personal computer. These outmoded methods are wholly incapable of supporting the rigorous demands of today's international commerce, contending with modern cyber-attacks, and even in preventing financial accidents.

In particular, SWIFT and other bank wire transfer systems lack the ability to detect misdirection of wire transfers except by manual checking. They also lack the capability to trace and recover misdirected funds once they are wired. In such attacks, perpetrators typically schedule their attacks for long weekends and holidays when bankers are not working. By the time employees return to work, the wire is unrecoverable. In recent SWIFT attacks, cyber criminals absconded 2B$ USD worth of wire transfers, highlighting the extreme vulnerability of such systems [38] [39]. More recently, Deutsche Bank reported accidentally sending $35B to a clearinghouse [40], lacking proper safeguards to detect or prevent the erroneous transfer. Despite the frequency of successful cyber attacks, bank fraud, and undetected human errors, the global banking industry's response has been simply to bandage, rather than to replace its existing systems.

2) *Transactional Fraud*

Banks face additional vulnerabilities in executing electronic payments as well, including both online purchases and credit card transactions involving point-of-sale (POS) terminals. Early attempts to unify merchant and credit card industries in adopting a common platform such as the Secure Electronic Transaction or SET protocol [41] [42] failed because of specific encryption vulnerabilities and high computational costs. With consolidation unviable, the payment processing industry bifurcated into two separate classes, one class dealing with online transactions, and a second dealing with credit card and point-of-sale transactions, each with their own distinct susceptibilities.

For online transactions, security today employs an XML-based protocol known as '3-D Secure' [43] [44] [45] to ensure process integrity. Surprisingly, this protocol relies on secure socket layer (SSL) cryptography [46], a method banned [47] by Internet Engineering Task Force (IETF) for well-known and highly publicized vulnerabilities [48]. One such scheme, the "Padding Oracle On Downgraded Legacy Encryption," or POODLE attack [49] comprises a fairly simple man-in-the middle exploit requiring only 256 SSL-3.0 requests to reveal each successive byte of encrypted messages.

Point-of-sale (POS) transactions, in contrast, execute and process credit cards transactions in accordance with the Payment Card Industry Data Security Standard with the acronym PCI DSS [50] [51]. POS transactions face numerous attack risks including the need to secure memory (data at rest), communication (data in transit), application code (software), and configuration information. POS attacks include skimming, using physical or software-based card readers to steal data contained within a credit or debit card, or by subverting the data transmission process between the POS and the issuing bank.

One unique aspect of credit card processing is the large number of stakeholders involved in every transaction, comprising in-part: consumers, merchants, the acquiring bank, card issuer, card brand companies, payment processors, payment gateways, software vendors, and hardware vendors. A large stakeholder population also opens numerous avenues for criminal attacks and fraud as well as inviting delayed transaction times and high processing costs (typically 4-5% of a payment). POS data in transit employs Transport Layer Security (TLS/SSL), an upgrade to SSL-3.0 certificates [52] allegedly offering improved resiliency to attack. Despite its extensions (improvements to patch vulnerabilities), the protocol is still subject to two-step POODLE attacks (degrading the security through friendly transactions before attacking) and even worse, to the notorious Heartbleed bug [53] [54], and to a UNIX specific vulnerability Shellshock or BashBug, a particularly insidious infection that creates a UNIX shell functioning as a command language interpreter. If exploited successfully, the hack could allow an attacker to gain control over the targeted computer [55] [56]. Although patches have been employed to plug known TLS vulnerabilities, the possibility of new and undiscovered transport vulnerabilities looms ever present.

> This [bug] is a serious vulnerability. Some might argue that it [Heartbleed] is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet [53].
>
> Joseph Steinberg
> *Forbes,* 10 Apr 2014

3) *CA-Certificate Fraud*

Since the Internet is intrinsically unsecure, imposters can misrepresent their identity to commit fraud and malfeasance with anonymity and impunity. To mitigate imposter fraud when using the Internet– trust, security, and identity are established cryptographically using 'digital certifications', electronic documents issued by *Certificate Authorities* or CAs.

Through public key infrastructure (PKI) based cryptography, CA-certificates promise confidentiality of message content, establish content integrity to detect and thwart tampering, and authenticate the identity of the communicating party or device. In public key cryptography, messages encrypted with the public key can only be decrypted (read) using the private key, but messages encrypted with the private key can be decrypted with either the public or private key [57]. The key owner keeps the private key secret, and distributes the public key freely, enabling a variety of authorization strategies to be realized over an unsecured network, theoretically without the need for securing the network itself.

Establishing trust over a PKI involves exchanging a CA-certificate through a handshaking process the first-time devices connect. For example, the secure browsing protocol 'hypertext transport protocol secure' or HTTPS [58] relies on digital certificates to ensure that a browser downloads files and images only from trusted CA-certified secure 'ports'. During handshaking, the requesting browser contacts a web server on a secure network port and sends a certificate signing request or CSR. In computer networking a *port* is a network connection's terminus and an associated gateway into a computer or mobile device operating system. Not to be confused with physical device ports, a network port is a software-based logical construct identifying a specific service or process, e.g. IETF designated port 443 for secure HTTP connections. In response to the CSR, the host server's port responds to the user's browser with a X.509 public key certificate [59] containing a public encryption key, the host server's identity, and a digital signature.

This digital signature comprises a cipher of the public key created by encryption using the corresponding private key. The browser, then checks whether it can open the file thereby confirming the host server holds the corresponding private key. Once verified, the host server will be considered trustworthy in all subsequent communiqués. The X.509 certificates may be self-signed or may be issued from a respected third-party certificate authority such as Comodo, IdenTrust, Symantec, DigiCert, and others. It is presumed that if a commercial CA issues the root certificate, all the intermediate digital certificate issuers are also trustworthy, with trust established during the certificate authentication procedure. In a man-in-the-middle trust attack (see **Figure 1**), an imposter inserts a node into the communication network between communicating parties and attempts to subvert the certificate authentication procedure by introducing false credentials into the exchange.

Aside from using digital signatures, another cryptographic tool used in various CA certificate authorization protocols is the cryptographic hash function [60], a mathematical operation that unidirectionally maps data of arbitrary size into a fixed-sized encrypted output. The hash process allows two ciphertext files of differing origins or heritage to be compared without knowing or revealing their plaintext sources. The hash process is highly non-linear, where even a miniscule perturbation in source data results in a profoundly different hash. By comparing hash files, it can be concluded with high confidence that if the hash files match, the source files must be identical. Moreover (with minor exception), it is impossible to recover the source input from the hash output. CA exchanges involving both encryption and hash files therefore afford greater security than digital signatures alone. Regardless of the certificate verification procedure used, trust is established by the integrity of a Certificate Authority revealing its true identity during the CA handshaking procedure. Since browser sessions trust previously established CA-certificates implicitly, i.e. without repeating the CA handshaking procedure, an imposter or hijacker once infiltrating a client's trust zone can conduct valid transactions with all of a client's related devices undetected. As such, self-signed CA-certificates are considered risky because the issuer may in fact be a fraud, criminal, bad state actor, or digital miscreant. To reduce CA-certificate fraud risk, a 'trust chain' [61] [62] is established between the client and a respected Certificate Authority through a cascade of intermediate CA-certificates.

Since only the 'root certificate' issued by the respected third-party CA is self-signed, the risk of undetected fraud is reduced. The root CA issuer is responsible for performing identity checks on all CSRs to confirm their integrity. Fraudulent CA-certificate issuers, once identified, have their root certificate revoked, thereby canceling the validity of all certificates they issued, and all progeny thereof. The revocation process can be painful, disrupting valid clients and applications while failing to stop the malware's spread [63].

Metaphorically speaking, the Internet's abject reliance on certified trust is a double-edged sword, efficiently and expeditiously establishing connectivity for trusted transactions but unable to detect or discern when a security or trust fraud risk is present.

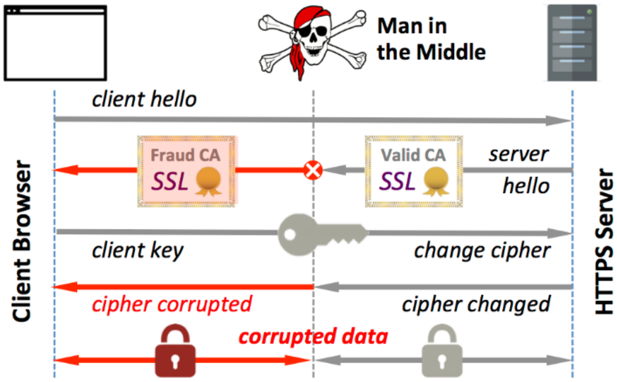


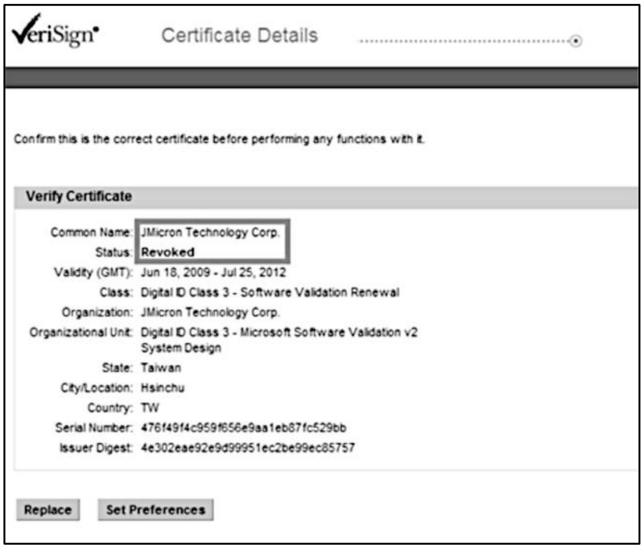
Fig.1: Man-in-the-Middle trust attack of certificate authentication

In essence, through trust chains frauds once detected can be expunged from engaging in Internet transactions. Frauds that go undetected, however, enjoy *carte blanche* access privileges, representing significant risk to personal and corporate finance, personal privacy, and even to national security. For example, a tally of digital certificates stolen from the Dutch "trusted" Certificate Authority DigiNotar jeopardized over 500 domains, including "the CIA, MI6, Mossad, Microsoft, Yahoo, Skype, Facebook, Twitter and Microsoft's Windows Update service" [64].

According to one IT security expert report [65] "That's where the problem lies. There are hundreds of such trusted CAs in our browsers, and each of them can produce certificates for any website on the Web. That means if any of them gets hacked, and their private key released into the wild, a hacker can create a certificate for any website they want, and all browsers will see it as valid." Worse, they can make fake certificates for any use, including signing email, encrypting VPN connections, installing software, and more.

So why steal a CA-certificate? Generally, trust attacks can be sub-categorized into three broad classes (a) malware diffusion including spyware and denial-of-service exploits (b) economic frauds, and (c) cyber warfare [66]. According to Hackmageddon's cyber attack statistics for March 2018 [67], the underlying motivation for these attacks comprised 76.5% for cybercrime, 19.4% for cyber espionage (commercial and governmental), 3.1% for cyber warfare (active attacks), and 1% for hacktivism (digital anarchists).

Malware diffusion using valid digital signatures is surprisingly prevalent. In fact, the pervasive infectious outbreak of the notorious cyber weapon Stuxnet occurred using valid signatures of at least two companies operating in the Hsinchu Science and Industrial Park in Taiwan [68]. The certificate (see **Figure 2**), likely stolen using a dedicated Trojan horse such as Zeus, facilitated a zero-day exploit that infected computers across the globe. Zero-day exploits are especially dangerous because the malware goes live immediately active upon infection, i.e. on 'day zero', giving its target no time to develop a patch to prevent damage and to stop infection of other devices. While documentaries like "Zero Days" (2016) sound like sci-fi and spy novels, the story is based on actual events.



Certificate Details

Confirm this is the correct certificate before performing any functions with it.

Verify Certificate

Common Name: JMicron Technology Corp.
Status: **Revoked**
Validity (GMT): Jun 18, 2009 - Jul 25, 2012
Class: Digital ID Class 3 - Software Validation Renewal
Organization: JMicron Technology Corp.
Organizational Unit: Digital ID Class 3 - Microsoft Software Validation v2
System Design
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: 476f49f4c959f656e9aa1eb87fc529bb
Issuer Digest: 4e302eae92e9d99951ec2be99ec85757

Fig.2: Stolen CA-certificate used to sign the Stuxnet malware pandemic

Because they are immediately infectious, zero-day exploits can infect a device's operating kernel even without a digital signature. In September of 2013, cyber criminals deployed malware using a digital certificate signed by Adobe impacting three MacOS and Windows applications. In response, Adobe had to revoke the certificate and update all of its clients' software. Six months later, a new variant of the Zeus Trojan designed to avoid detection was discovered, signed by a stolen digital certificate belonging to Microsoft. In 2015 two more respected Taiwan high-tech companies had their digital certificates stolen, including one taken from the tech giant Foxconn used to orchestrate the Duqu 2.0 hacking of the Russian security firm Kaspersky [69]. In each instance, the perpetrators used a different certificate, suggesting the ease by which illicit CA-certificates can be obtained. Even risking detection, the zero-day exploit used a signed certificate to ensure re-infection of patched or cleaned (wiped) devices.

CA-certificate theft can occur is numerous ways– through spying, network attacks, or by malware. "If a computer is infected by a backdoor Trojan, the attacker may gain full access to the compromised computer and will be able to control it. The attacker will therefore be able to steal any information found on the computer" [70]. Aside from Zeus (also known as Trojan.Zbot) other malware designed to steal both private keys and digital certificates include Downloader.Parshell, Infostealer.Snifula, Backdoor.Beasty Trojan.Spyeye, W32.Cridex, Trojan.Carberp & W32.Qakbot, to name a few.

As an alternative to theft, fake code-signing CA-certificates can be created through counterfeiting [71] and purchased online over the dark Web for nefarious campaigns. To create a counterfeit certificate at the behest of a client, unscrupulous shop owners use digital identities stolen from a legitimate company (or its employees) to order a valid CA certificate from a respected CA-certificate issuer. In most cases, duped business owners and CAs are completely unaware that their data was or is being used in these illicit activities.

Regardless of how fraudulent CA-certificates are obtained, cyber criminals use them to diffuse malware [72] and to commit illicit transactions over the Internet, sometimes even disguised as beneficial antivirus software [73].

4) Malware Infections

Malware infections deliver and install malicious code into target devices in order to commit crime, gather information (see **Figure 3**), or deny services. In the early days of computing, memory devices such as floppy disks, CDs, and USB-drives carried viruses. Ever since the 1988 Morris worm attack [74], the first recorded malware exploit delivered over the Internet, the cloud has become the medium of choice to infect computing and mobile devices. Not only did it result in the first felony conviction for cybercrime, it exposed the intrinsic vulnerability of the Internet and email to attack– alarming users while inspiring hackers.

While fairly easy to detect and expunge, the Morris worm revealed the potential chaos an effective denial-of-service attack could render. Thirty years later, network infectious agents have evolved significantly in capability and in stealth, employing a wide variety of attack vectors including email [75]; web browsers (HTTP-exploits) [76] [77]; file (FTP) downloads [78] [79]; ad-blockers [80], system cleanup software [81]; software updates [82] and installers; java scripts [83]; Acrobat and PDF readers [84]; media files and Flash players [85], and personal messengers. Most network delivered malware exploits also employ fraudulent CA-certificates (described previously) in order to establish trust, avoid detection, and gain access. Others gain access through adware [86], when a user connects to a malicious URL [87] [88], or in typosquatting [89] when a user mistypes the name of a valid URL and is diverted to a hostile site.

Installed malware operates in various ways. In denial-of-service attacks, fork bombs, ransomware [90], lethal viruses, and many zero-day exploits, the target knows immediately of the infection because of overt system failures or messages. In interactive exploits like phishing, login exploits, keyloggers, and scareware, a user is tricked to willingly enter personal private information, unknowingly revealing it to a nefarious party. In spyware, rootkit, eavesdropping, data scrapers, and backdoor attacks, the malware surreptitiously invades the target using evasion methods to 'cover its tracks', avoiding detection and erasing all evidence as to its presence and its source.

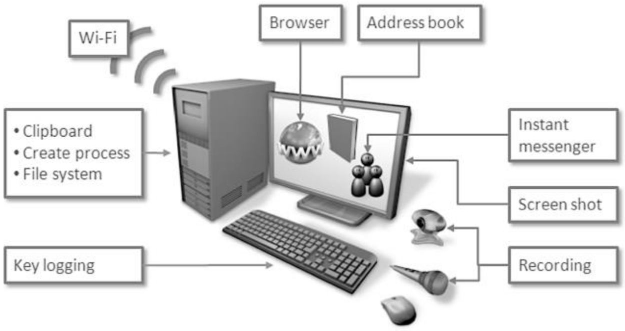


Fig.3: Spyware personal data collection

Still another class of time-delayed malware including time bombs and logic bombs waits unnoticed till the conditions arise to release its payload, either to damage the target device or to launch a pandemic against other devices. More advanced attack vectors called Frankenstein malware exploits [91] deliver hostile components in a series of innocuous looking "benign binaries" disguising their true malicious intent. After delivery, the component pieces are collected and reassembled, i.e. 'stitched' together to activate the attack.

With the rapid growth of mobile devices and apps, cyber criminals are turning their attention to attacking smartphones and tablets, in part because they offer less-sophisticated means to detect or prevent intrusion, and because they tend to contain significantly more personal information than the data commonly stored in PCs. For example, researchers recently identified an Android Trojan in the wild (dubbed KevDroid) disguised as anti-virus application [92]. The most recent instantiation of the malware features severally disturbingly sophisticated capabilities, including the ability to:

- Record phone calls & audio
- Steal web history and files
- Gain root access (take control)
- Steal call logs, SMS, emails
- Detect (and relay) a device's location (every 10 seconds)
- Collect a list of installed applications

These capabilities allow a criminal, gang, or crime syndicate to track a person's whereabouts; monitor their voice, text and email communications, engage in fraudulent bank transactions, and commit extortion or blackmail. As such the loss of privacy through a security breach could seriously endanger a target, reaching far beyond the realms of cybercrime. As an open source platform, Android suffers the lion's share of malware attacks for any mobile operating system [93] [94]. While the vast majority of these attacks are delivered through network connectivity, either WiFi or wireless communication networks, as a multisource market, unscrupulous mobile phone makers and OEM manufacturers may also install data tracking, back doors [95], and malware [96] to surveil client behavior. Although iOS and iPhones are less susceptible to unwanted incursion, a variety of attack vectors and iPhone attack stratagems have been reported [97] [98].

In any device, be it computer or smartphone, protecting the device from malware requires careful diligence to avoid infection. Best practices against cyber attacks involve:

- Communicating using secure networks and protocols
- Accepting CA-certificates only from trusted sources while rejecting unknown vendors and self-signed certificates
- Communicate using only "secure" network ports such as HTTPS (port 443), SMTPS (port 465), IMAPS (port 993), FTPS (port 989 for data, port 990 for commands), and TELNET over TLS/SSL (port 992)
- Limit web browsing, downloads, and financial transactions to trusted URLs (having a Seal of Approval from respected Certificate Authorities).

While these practices are prudent, in reality they offer only limited protection. Because of the porosity of the security protocols available over the Internet, there is no certain means to guarantee transactions are truly secure or private. Even using trusted Certificate Authorities offer no certain way to ensure trust, or that a fraudulent CA-certificate has not corrupted the trust chain. Similarly, because of intrinsic SSL and TLS/SSL vulnerabilities described previously, even secure ports are not robustly secure and may be hacked.

Assuming that Internet-based attacks cannot be prevented, virus checkers and firewalls are sometimes used to combat cyber insurgencies. For global businesses today, however, there is no realistic means to facilitate a firewall to cover an international footprint without employing cumbersome high latency virtual private networks (VPNs). Even worse, virus checkers are often only able to detect an attack after the infection has occurred. Advanced attacks like Frankenstein binary-fragmented malware avoid detection altogether. As such, preventing cyber attacks over an open public network such as the Internet remains the focus of numerous research efforts [99] [100]. Network carried malware constitutes a serious impediment to trusted commerce and growing risk to personal privacy and safety.

B) Network Attacks

Network attacks represent the *unauthorized access* or surveillance of communication and computer networks to gain information; redirect packet traffic; interfere with (or impede) bona fide business, or to commit fraud, theft, and malfeasance. Denial-of-service (DOS) attacks may be considered a type of network attack. Network attacks also frequently play a role in trust attacks including wire fraud, transaction fraud, CA-certificate fraud, and malware diffusion. Network sniffing, snooping, and spying may participate in profiling, privacy attacks, and identity theft. Network attacks can best be understood by considering the communication protocol's "layer" on which a specific attack targets.

1) Open Source Interconnectivity (OSI Model)

The term "layer" refers to the name given to a class of functions in the 7-layer OSI model [101] [102]. OSI, an acronym for Open Source Interconnection, is a conceptual abstraction and hierarchical construct used to codify packet-switched communication between and among network-connected electronic devices. Standardized in a 1984 ISO publication entitled the "Open Systems Interconnection Reference Model", the OSI model facilitates interoperability of diverse systems and components without regard to the component's implementation, underlying technology, or manufacturer, so long that the model's protocol is observed.

Packet switched technology describes communication segmented into data packets traversing the network in discrete packets rather than comprising a continuous analog signal or transmission (such as radio broadcasts). As such, the OSI model does not apply to circuit-switched telephony such as POTS (the plain old telephone system), even though in rural areas packet switched and circuit switched networks may co-exist and require certain limited-function bridging capability. The flexibility and universality of the OSI model, arguably rescued from irrelevance by the widespread adoption of the

’transmission control protocol’ or TCP/IP *protocol stack* [103] [104], is largely responsibility for the success of the Internet. Today, as a decentralized open-source network, the Internet seamlessly connects a myriad of devices including computers and servers; mobile telephony (such as smartphones and tablets), data storage (drives), and cloud-connected devices used in smart homes, smart factories, etc. referred to as Internet-of-Things or by the acronym IoT [105] [106].

Network connectivity is now migrating into commercial and private transportation including cars, trucks, tractor-trailers, ships, trains, and even commercial aviation. Networks include vehicle-to-vehicle (V2V) awareness and safety features, vehicle-to-infrastructure (V2I) connectivity for telephony and infotainment, vehicle-to-device (V2D) as passenger hotspots, vehicle-to-pedestrian (V2P) for pedestrian safety, and vehicle-to-grid (V2G) for traffic flow management. Collectively, the foregoing may be considered as V2X, meaning vehicle-to-everything [107].

The concept of ubiquitous connectivity has since expanded into the broader topic of Internet-of-Everything (IoE) [108] to include people, data, processes, and things, for example including machine-to-machine (M2M), business-to-business (B2B), and business-to-consumer (B2C), etc. Because of the Internet’s layered protocol construct, it is unnecessary to know the details of a how a connected device operates to support it. In the OSI model, a network and its corresponding activities are partitioned into platform independent abstraction layers [109] [110].

In operation, each layer relies on processes performed by the layers below it, and performs services for the layers above it. As such, a particular layer doesn’t care how lower layers execute their tasks so long that data is exchanged with the layer directly below it in accordance with its protocol. Similarly, the same layer is not concerned with how upper layers utilize or create data so long that it supports them, delivering and receiving data in accordance with the protocol. In this manner, a predetermined division of labor and functional communication is realized for each layer without requiring detailed knowledge of any other layer.

Using abstraction layers in an open architecture promotes fair competition, giving SMBs unbridled commercial access to the burgeoning Internet and World Wide Web while thwarting any one company, technology, or government from dictating policy or usurping control. No registration or central authority approval is required to connect to the Internet. Simply by adhering to agreed abstraction layers in accordance with the open systems interconnection OSI model, a device can reliably negotiate and subsequently communicate with other network-connected devices with no knowledge of the other devices.

In detail, the seven OSI layers collectively comprise a ‘protocol stack’ representing the physical interface, either electrical signals, electromagnetic waves, or light, along with data processing hardware and software used to interpret and use the signals. In operation, data is passed to and from a network-connected device, which in turn may utilize its own separate and unique abstraction layers dedicated to realizing applications in computing [111], databases [112], robotics [113], IoT [114], security, or as general hardware abstraction layers (HAL) [115]. The Internet’s protocol stack can also be linked to business services [116], or to other non-tech industries, financial transactions, banking, shipping, and more.

F	#	Layer Name	Function/Feature
Application	7	Application	APIs, BC, PKIs, login Telnet, file transfer FTP, trust CA-cert/L7, email IMAP, SMTP, computing DCOM, networking DNS, DHCP, NTP, TLS/SSL
	6	Presentation	Cryptographic encapsulation, compression, trust CA-cert/L6, encoding, translation, images EBCDIC/ASCII, PDF, MPEG, document security
	5	Session	Session initiating, authentication, trust CA-cert/L5, authorization, full/half duplex, session restoration, SOCKS, tunneling PPTP
Internet	4	Transport	Transport reliability and handshaking (TCP/UDP), port addressing, transport security selector (SSL/TLS)
	3	Network	IPv4/IPv6, IP routing, IP addressing, traffic control, time to live, ICMP, PIM multicast
Physical Medium	2	Data Link	Media Access Control (MAC) connectivity in accordance with Ethernet, WiFi, 3G/LTE, 4G, 5G, DOCSIS3 protocols, security WEP, WPA2
	1	Physical (PHY)	Signal transmission as symbols (or bits) including timing control, synchronization, digital (electronic), radio, microwaves, light

Table 1: 7-Layer OSI protocol stack for Internet communication

As described in **Table 1**, the 7-Layer OSI model includes two lower layers for connecting a device to a network over a physical medium, two middle layers for controlling packet routing over the Internet, and three top layers for managing network applications. During communication between two devices, data from the application layer is encrypted then passed down the stack, encapsulated into an IP datagram with transport instructions and IP address routing, then transmitted over the PHY layer to the second device using the Data Link Layer-2 specific protocol. Once delivered to the packet’s destination IP address and port, the packet is validated, decrypted then passed to the application layer for execution. Although the 7-layer abstraction model is generic, its most common realization is the TCP/IP network stack, an acronym for transmission control protocol / Internet protocol.

As shown in **Figure 4**, even though the only physical connection occurs on the PHY Layer-1, each communicating device pair operates virtually on a layer-by-layer basis, where transport Layer-4 communicates to the other device’s transport Layer-4, session Layer-5 communicates to it corresponding Layer-5, and so on, embedded in structured data packets. Each layer exhibits its own security vulnerabilities [117], especially Layer-7 data comprising a packet’s payload, the contents of which may include user ID information, passwords, login files, executable code, and blockchain data or cryptocurrency.

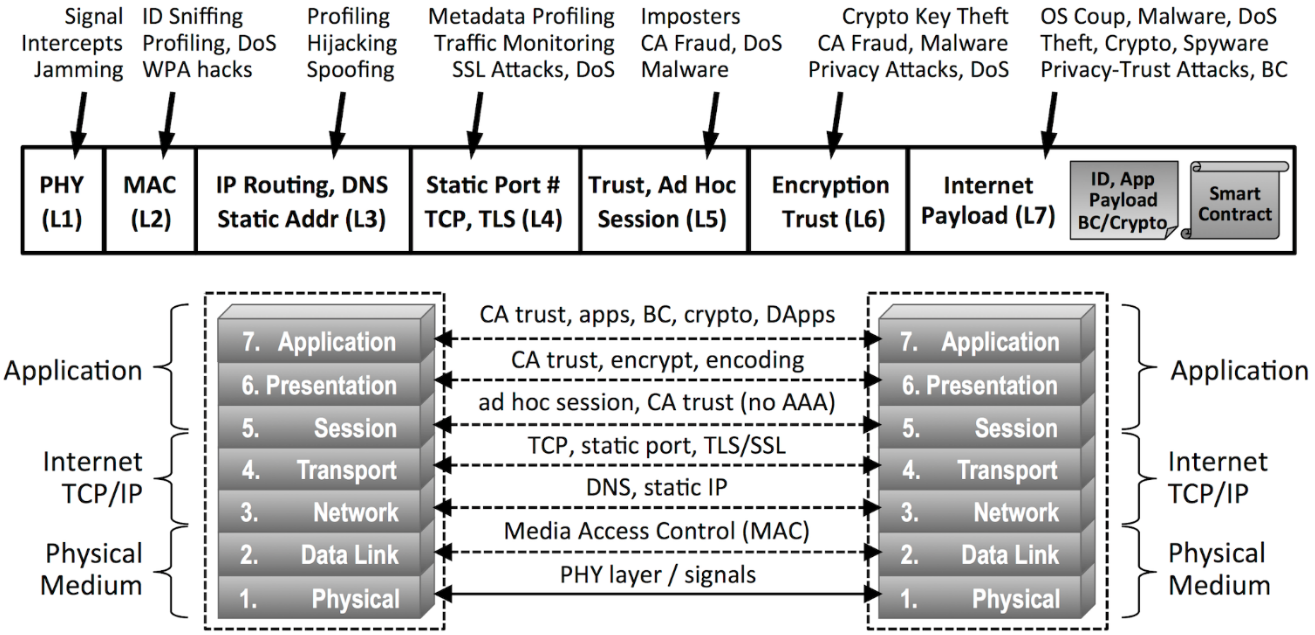


Fig.4: OSI representation of the Internet's TCP/IP communication stack and data packet with corresponding vulnerabilities

2) *PHY & Data Link Layer Vulnerabilities*

The PHY Layer-1 and Data Link Layer-2 provide the physical means by which any device can be connected onto a private or public packet switched network such as the Internet The vulnerability of this "Last Link" connection to the device depends on the type of network connection used and whether the link is public or private. For example, if network access is made through an Ethernet cable plugged into a cable modem (CM) located in a personal residence, intercepting the signal can be challenging, especially if the CM communicates over fiber with the cable modem terminating system (CMTS) in the company's hub office using an advanced protocol such as DOCSIS-3 rev-C. On the other hand, if a caller's Last Link connection involves a public WiFi "hotspot" or a cellular network, many means exist to intercept microwave signals and reconstruct information from the transceiver packets [118] [119], especially if an older router or a low performance (2.5G or 3G) legacy cellular connection is used [120] [121].

For example, in *packet sniffing*, a cybercriminal monitors data traffic to analyze or steal data [122]. Referring to the data packet shown in **Figure 4**, the observable data contained in intercepted IP packet includes the Layer-2 MAC addresses of the sender's device; the Layer-3 source and destination IP addresses of both communicating parties (essentially their identities); the data transport protocol (UDP, TCP) employed; and the Layer-4 port number of the sending and receiving devices describing the type of service being requested. Collectively, this data is referred to as 'metadata'.

The IP datagram also contains the Layer-7 Internet payload, either in encrypted or unencrypted form. The payload often carries personal information and may contain valuable private assets such as account numbers, passwords, login information, cryptocurrency, and CA-certificates. If the file is unencrypted, a cyber-pirate can easily read the payload's contents. If encrypted, payload security depends on the level of cryptography used. Since computing capability is growing steadily, many cryptographic methods previously secure are now easily broken using 'brute force' attacks. For example, to ensure rapid processing required by low-latency high-speed wireless routers, WiFi encryption standards WEP, WPA, and are necessarily lightweight having low cryptographic strength and, as such, are easily broken. In 2017, WiFi's most popular encryption WPA2 was broken using a Key Reinstallation attACK, (or KRACK attack) [123]. Uninformed users relying solely on WiFi encryption for insuring wireless privacy and security are naively unaware of the risks they are taking using public hotspots.

In general, packet sniffing is more dangerous executed locally over the Last Mile (the connection between the cloud and the local router), or over the Last Link (the connection between the local router and the client's device). Local attacks are more effective because (i) packet traffic is limited, (ii) device MAC addresses are available within the same subnet, and (iii) the attack can be combined with *spying* methods. For example, if a hacker packet sniffing WiFi traffic in a café (in person or via a hacked security camera) sees someone taking out their credit card to make an online purchase, they can capture and record all the WiFi packets during the observed transaction, and later extract the credit card data to commit transactional fraud.

Other packet sniffing attacks may involve pattern recognition, looking for packet sequences indicative of an ongoing session (a communication dialogue) occurring between two parties where the sniffed data involves an entire sequence of packets, i.e. packets repeatedly using the same IP addresses. In *sidejacking*, packet sniffing is used to steal cookies from a previous web transaction. Such cookies often include login credentials in unencrypted form. Once such attack called Firesheep involved using a public WiFi network to commandeer a stranger's Facebook session, gaining access to sensitive data and sending viral messages and wall posts. In an *evil twin attack*, an imposter launches a rogue WiFi access point to fool wireless users into connecting a laptop or mobile phone to its tainted hotspot by posing as a legitimate provider.

The access may be used for monitoring packet traffic or to request fraudulent credit card payments. WiFi based local area networks (LANs) employing the Address Resolution Protocol are subject to a combined Layer-2 plus Layer-3 attack vector called ARP *spoofing*, where a perpetrator sends fake messages to a LAN associating their MAC address with the target's IP address. Confused, the router mistakenly forwards a valid message intended for a victim's IP address to the attacker instead. The attacker can behave as a passive gateway, only sniffing the data, or as a man-in-the middle attack modify the data before forwarding it without the target detecting any intrusion.

Aside from piracy, local intrusions are able to launch effective *Layer-2 denial-of-service* attacks employing the aforementioned ARP spoofing, rerouting all messages to a non-existent MAC address or alternatively by launching a distributed denial-of-service (*DDOS*) attack by overwhelming a router with fake messages from multiple senders, also known as a 'MAC flooding attack'. By creating excessive traffic congestion, a perpetrator is able to overwhelm its resources preventing bona fide communications, transactions, and commerce– possibly even crashing a device's physical port connection (referred to as a Layer-1 DoS attack). In fact, denial-of-service attacks can be perpetrated on any of all seven OSI layers [124]. DoS attacks can also be executed in blockchain attacks (described later) to prevent peer repudiation of fraudulent cryptocurrency transactions or double spending.

3) Network & Transport Layer Vulnerabilities

While local attacks focus on PHY and Data Link physical medium vulnerabilities, cloud attacks involve Network Layer-3 and Transport Layer-4 vulnerabilities. Network based attacks are often generically referred to as *Man-in-the-Middle* attacks because the attacker interjects themselves into the middle of a transaction, either as an imposter using IP spoofing, by packet hijacking, or combined with a trust attack using a fraudulent or stolen CA-certificate.

In network vernacular, identity deception is referred to as *IP spoofing* [125] an imposter deception in which IP datagrams are routed to the wrong IP address without the target realizing the misdirection. Imposter exploits can be executed as Layer-3 attacks comprising IP address spoofing or DNS server spoofing or combined with Layer-2 MAC address deception in ARP spoofing (described previously). In DNS server attacks, DNS address request replies are modified to redirect traffic to the wrong IP address, useful for packet hijacking and virus propagation. In IP address spoofing, the content of the IP source address in the IP header is falsified either to intercept traffic or to launch a reflected DDoS attack.

In 'reflected' distributed denial-of-service attacks, the target receives more requests than it can process. To avoid detection of the attack's source, the identities of 'botnet' antagonist devices generating fake requests are disguised by IP spoofing. Botnets comprise a group of malware-infected servers controlled by a central cyber attacker. The service attack can be further exaggerated by amplification [126] whereby domain name servers (DNS) and network time protocol (NTP) are tricked into collectively and concurrently sending message requests. Smurf attacks comprise an ICMP (ping) request sent to every node in the subnet using the target's IP address whereby all the replies are directed toward the target.

The term 'amplification' is apt, as each malware server creates one to two orders-of-magnitude more traffic than it sends itself. DDoS attack mitigation is difficult, requiring the use of deep packet inspection (DPI) to rapidly identify the sincerity of an incoming request before allowing packet routing to occur into a subnet [127]. Although compute intensive, DPI has been used in a cluster of scrubbers to repel a DDOS attack up to 470 Gbps. Because of the magnitude of massive DDoS attacks, it is unclear what role AI can play in discerning and repelling such affronts [128] [129].

IP address spoofing can also be executed as part of a trust attack involving Layer-4 SSL certificate or Layer-7 CA-certificate. Disguised as a source known to the receiver, an anonymous perpetrator convinces the target that the false IP address is valid by exchanging a stolen CA-certificate. Once the parties exchange CA-certificates, the victim sincerely executes transactions with full trust of the imposter, which may include theft of cash or property, encouraging fraudulent transactions, or delivering malware. In another method, after the fraudulent certificate is exchanged, the session is rerouted to a malicious server.

Alternatively, the exploit may include the delivery of spyware, traffic monitoring, or data forwarding as part of target profiling as a prelude to a more significant cyber attack against the target or against the company or its successful business partners. In *packet hijacking* shown in **Figure 5**, a cybercriminal introduces a malicious pirate node into network communication between two parties, intercepting all packet traffic without either party knowing their messages are passing through an undetected intermediary. A hijacking exploit requires only a single act of deception to establish a pirate node as a valid participant.

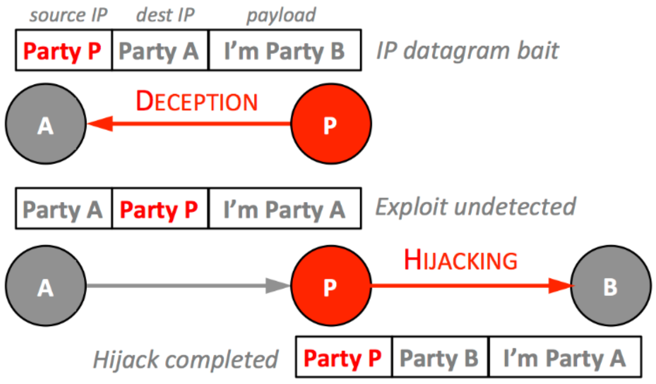


Fig.5: Internet IP packet hijacking exploit

In this exploit, the pirate node having an IP address |Party-P| sends a message to party-A as bait, claiming to be party-B. To do so, the IP datagram header uses the destination IP address of |Party-A|, but replaces the packet's source IP address with |Party-P| for |Party-B|. If party-A doesn't realize the IP address of the incoming packet is the pirate and not party-B (and why should it?) then the attack is halfway home. Because in standard Internet routing a receiving device always replies to the source address of incoming packets, if the incoming packet fools its recipient, party-A will naturally reply to party-P thinking it is communicating with party-B's server.

The pirate node then faithfully forwards the received packet contents to party-B identifying itself as party-A but using its pirate IP address |Party-P| as the IP source address. Party B then replies to the party-P pirate address convinced it is party-A rather than an imposter. At this juncture both parties send and receive messages to one another not realizing all traffic is actually passing through an intermediary, the pirate server. The pirate can then (at a time of its choosing), execute nefarious actions either by using the information passed in the packets' payloads to commit fraud, theft, or insider trading. More aggressive cybercriminals can, at the risk of discovery, overtly change the content of the messages.

An audacious variant of this stratagem has been perpetrated using faux cell phone towers to monitor and intercept wireless network communications [130] [131]. Numerous other attacks on wireless telephony and 4G LTE data communication affecting security, user privacy, and disruption of services have been recently identified [132]. The attack vectors relate to three critical procedures of the protocol, namely attach, detach, and paging operations. For example, in an *authentication relay attack* an adversary is able to spoof the location of a legitimate user to the core network without possessing appropriate credentials.

Network attacks can also be executed over the Transport Layer-4. These attacks may comprise an attack of SSL vulnerabilities (described previously), or may employ *port interrogation*, i.e. constantly sending information to various port numbers of the same IP address in order to construct a profile of the device, to identify open ports, or to discover backdoors. Transport layer stratagems can also be used to launch effective local *denial-of-service (DoS) attacks*, by attacking a specific vulnerable port with requests [132]. In fact, so common are DoS attacks on port-80, the unsecured HTTP daemon in charge of background process servicing web browser port requests, that port-80 is now being officially decommissioned as an approved port by ICANN [133], the agency in charge of Internet names, numbers, and reserved port registration.

Other port assaults involve combinational exploits involving both Layer-4 and Layer-7. One class for example attacks the Border Gateway Protocol (BGP). The role of the BGP is to determine packet routing based on paths, rules, and policies of a network administrator [134]. Running as a service over a TCP connection [135] on port 179, the BGP is a simple finite state machine that keeps track of each peer-to-peer session by a state variable tracking where the process is– either in idle, connect, active, open sent, open confirm or established states.

Packet propagation employs a routing table and a set of rules to decide how and where to forward a packet. If the routing instructions are corrupted reliable delivery is affected. The BGP process faces a number of vulnerabilities, including configuration errors, fraudulent instructions (original or modified), compromised routers, routing by miscreants, as well as packet sniffing and content injection. The goal of a BGP attack includes disruption of communication, deception, and unauthorized disclosure.

Another Transport-Application Layer combinational attack involves Regional Internet Registries or RIRs. One such stratagem involves using 'zombie blocks,' using unused and forgotten blocks of Internet addresses to execute nefarious transactions free of monitors. Rather than hijacking the packets themselves, the perpetrator hijacks IP space itself simply by changing the WHOIS file in the RIR registry to their own name server. The commandeered IP space can then be used for SPAM, DoS attacks or deceptions. A similar ruse involves routing packets into bogon (fake) IP space, to an IP address that should never appear in an Internet routing table. Combined with packet hijacking, messages and data can be redirected to a 'black hole' never to be seen again. Another Transport Layer-4 attack involves interfering with the TCP handshaking procedure [136]. Using this attack vector, TCP connection packets are overwritten with fraudulent data as part of a Telnet or FTP exchange. In such scenarios, the problem of identifying fraudulent FTP and Telnet transactions is handled only by the transport-layer 'transmission control protocol' (TCP) and nothing else.

Cloud related attacks could also involve *surveillance*, the monitoring of network traffic by nation-states for national security purposes, by corporations for protection of intellectual property, and by crime-gangs and cartels for competitive advantage over competing organizations. In contrast to spying– covertly obtaining privileged and sensitive information, *surveillance* is openly observing the actions of an individual or a group in order to understand or manage them [137] [138]. Surveillance may be limited to gathering metadata or involve the more aggressive practices of hacking, code breaking, and CA-certificate fraud.

4) Application Layer Vulnerabilities

The upper "application" layers of the OSI model collectively comprise the Session Layer-5, the Presentation Layer-6, and the Application Layer-7. In operation the Session Layer and the Presentation Layer collaboratively work to support distributed processing capabilities to Application Layer-7. Unlike Layer-4, whose job is to deliver packets of bits to ports and services without regard their content, the Session Layer-5 is responsible for preserving the embedded 'structure' of this raw data during transport using an abstract "transfer syntax". Layer 5 also manages creating, releasing, and aborting connections, as well as hosting dialogue-control facilities of synchronization and checkpointing. Presentation Layer-6 is responsible for converting the Session layer's transfer syntax into concrete 'application syntax' specific to the operating system of each host device, e.g. Windows, UNIX, MacOS, and Linux, including Linux derivatives Android and iOS [139]. An attack on one or more of these layered operations is considered an *application layer attack*.

Unlike physical-medium and network layer attacks, application layer attacks generally involve first executing a trust attack using a stolen or *fraudulent CA-certificate* to establish communication or system privileges. Because these upper layers rely on certified trust of communicating parties established through a cryptographic CA-certificate (or a trust chain of multiple CA-certificates), without first procuring a fraudulent digital certificate, an upper layer attack will likely not prevail. Once, however, the attacker has procured and exchanged fake certificates with its target, the upper layer attack can proceed, generally starting with Layer-5 and working its way up the protocol stack.

In a Session Layer-5 attack, a fake CA-certificate is used to authenticate the attacker's identity and to open a valid session using a *fraudulent session* token thereby bypassing the Layer-5 security provisions. The fake session token can be stolen in several ways including a man-in-the-middle attack, session sniffing, or a blind hijacking, i.e. injecting malicious commands into the data stream. Another certificate theft method employs a Trojan horse to "manipulate calls between the main application's executable code (e.g. the browser) and its security mechanisms or libraries" [140]. In an SSH downgrade exploit, the attacker tricks the client and server to use a less secure protocol before continuing with their attack.

The malicious session can then be used to gather information or to commit fraudulent transactions. Opening a fake session may also be employed to execute a *Session layer malware attack*, delivering system malware including zero-day exploits, time bombs, viruses, or worms (described previously). Without a successful Layer-6 incursion to steal cryptographic keys, however, a successful Layer-5 campaign will still not enable a privacy attack, because *sans* crypto keys a datagram's secure Layer-7 payload will remain as illegible ciphertext.

Presentation Layer-6 attacks generally involve *stolen security credentials and encryption keys* often using the same fake CA-certificate used to fool Layer-5 authentication. Because virtually every Internet data packet relies on encryption to ensure security and privacy, an attack on Layer-6 and Layer-7 delivered cryptographic keys renders most communiqués exposed to spying and criminality. Aside from defeating security and disabling all privacy protections, the exploit may also involve Presentation Layer-6 malware attacks, installing malicious code in the form of innocuous looking utilities including PDF readers, media players, ad-blockers, disk defrag utilities, etc. One particular strategy for crypto key theft involves apprehending the distribution of one or more crypto keys from a third party crypto key server when a connection is first made. For example, some allegedly 'secure' personal messengers distribute keys openly over the Internet. If the keys are intercepted, the security of "end-to-end" encryption is compromised.

Application Layer-7 attacks employ a diverse range of stratagems involving fake identities (CA-certificate fraud and trust attacks), malicious code (malware and spyware), and a variety of denial-of-sever attacks. Most Layer-7 attacks start with deception– using a digital signature, fake SSH keys [141] or fake CA-certificate to gain access and system privileges. Once a cyber attacker uses fraudulent security credentials to pass authentication and gain access to the system or cryptographic keys, the only protection remaining for Layer-7 applications are the security provisions built-in to these apps. Many apps however, offer limited or no security provisions, instead relying wholly on the protocol stack to secure their content and integrity.

Layer-7 malware attacks [142] [143] can be used to subvert, cripple, or destroy a system with viruses and worms (such as Stuxnet), to gather information using spyware [144], phishing, key loggers, and Trojans, to bypass security by installing backdoors, to overtly take control of a system such as ransomware [145], or to surreptitiously gain control of files and processes. Other attacks involve zero-day exploits [146] or to use fileless malware infections [147]. Data drive attacks can also be used to steal personal information, steal credit card and banking data, or perform theft of cryptocurrency. Downloading of personal photographs and private documents may also be used to perform extortion or blackmail. The attack can also involve installing content or software of unknown content or purpose, generally activated through some active process or application [148] [149]. In some cases, cyber criminals may utilize special software called 'crypters' to protect their malware from antivirus utilities [150]. Similar cyber attack methodologies are adaptable to cell phones [151] [152] including back doors, ransomware, botnets, and spyware [153]. Attack vectors include downloads from malicious websites; encrypted malicious payload downloads; and stealth malware designed to circumvent detection including anti-security, anti-sandbox, and anti-analyst techniques.

Another means by which cyber criminals are able launch an effective application layer attack is through root access, to gain access to system administration rights of a device, server, or network [154]. Root access can be gained through covert means such as Trojans [155] or by injecting malicious adware [156] to infect a large population, to steal information, and to earn money as credit for fraudulently installing apps. So rather than gaining unauthorized access to one user's account, by hacking the system administrator's login, significant access and privileges become available to the cyber pirate without the knowledge of those using the system. Since the system administrator acts as a system's police, there is no one to catch their criminal activity – in essence for systems or networks with corrupted administration there is no one able to police the police.

Such attacks on personal computers, servers, and on mobile phones are referred to as *pirate administration* or infiltration attacks. The task for cyber criminals is made easier by the practice of jail breaking or 'rooting' [157], where a user modifies the operating system of a mobile phone to give themselves administrative privileges. The phone, once rooted, loses its defensive abilities against malware [158]. In extreme cases, the attacker can usurp complete control of the device.

This scenario is especially worrisome in IoT and V2X transportation applications, where an effective cyberattack could take control of an autonomous vehicle, intentionally or inadvertently causing life threatening conditions or accidents.

Denial-of-Service attacks, while possible to execute on any layer, are most commonly executed on Application Layer-7 because of the myriad of diverse applications on which the attack can be executed [159] [160] including HTTP, FTP, IMAP, Telnet, SMPT/POP, IRC, XMPP, SSH, etc. Especially popular vectors include HTTP attacks on web server processes and web application attacks on CPU processes. What are the motivations for a denial-of-service attack? Motivations for DoS attacks (not ranked in any specific order) include the following [161]:

- Anti-competitive business practices
- Anger, criticism, or anarchist activity
- Punishment as a response to an action or inaction
- Gang, mob, cartel, or government cyber-warfare
- Extortion involving a DoS threat
- Misdirection to cover other criminality

A DoS attack can also be used in cyber espionage training and in cyber-warfare (sometimes provoking reciprocal attacks). Moreover, like any crime, many DoS attacks remain unexplained.

C) Data Breaches

According to the United States Department of Health and Human Services, a data breach is "a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." [164] While a data breach can occur by hacking network communication (described previously), most breaches occur using methods designed to *steal or corrupt stored data files*. Stored in corporate or government databases, online in cloud storage, or in massive storage farms or server farms, such data may involve active records, regular backup files, archival data, or catastrophic recovery files.

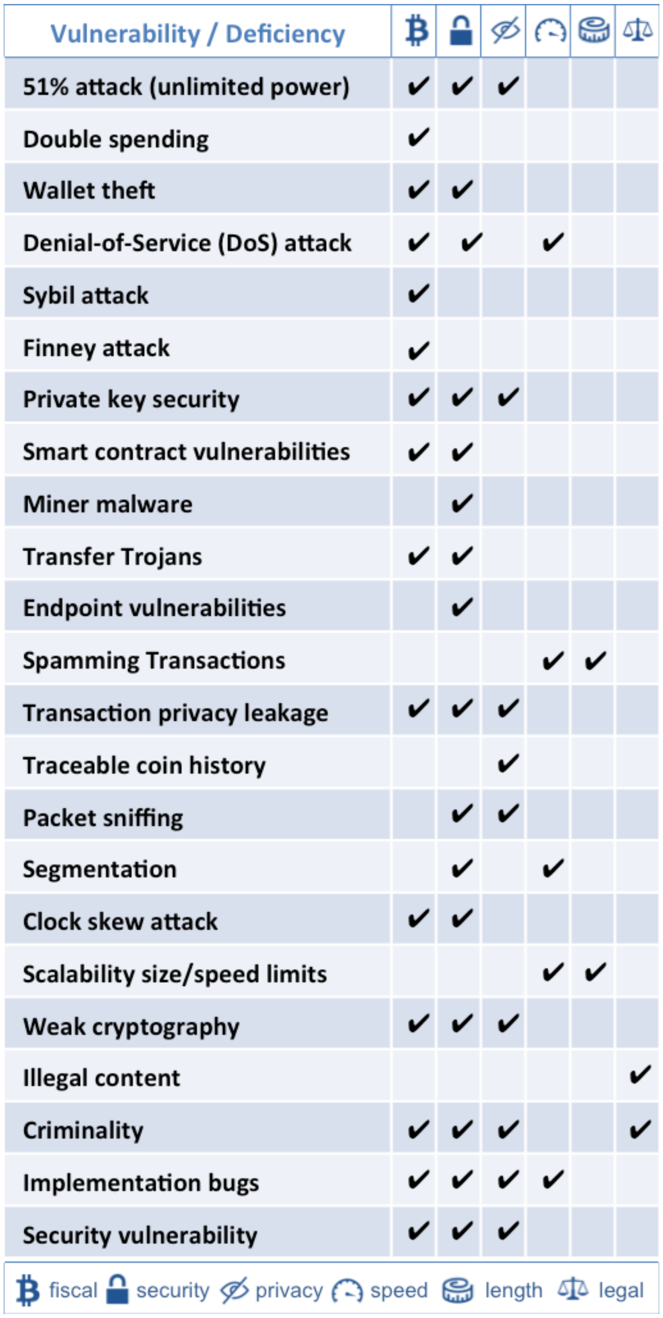
Data breaches impact every aspect of modern life, both personal and public [162]. Attacks may be made on financial records, business transactions, trade secrets and intellectual property, client lists, personal information, social security and tax records, government employee records, active military personnel records, veteran associates records, insurance records and personal health information, files for social media platforms, and personal cloud storage containing, pictures, and other private information. The motive of such attacks can be for financial gain, for espionage, or for FIG (fun, ideology, grudge) [163]. In identity theft, for example, social security information, driver's licenses, passports, addresses, email addresses, phone numbers, etc. are stolen and then used to create fake IDs to commit fraud or theft, to circumvent homeland security authorities, or are sold to spammers for marketing campaigns. Incalculable personal and commercial harm has resulted from security breaches involving access to or theft of commercial and personal private data. Several notorious cases [164] include the 28.6M files stolen from the Department of Veterans Affairs in May of 2006. Sony experienced a data breach affecting 77M PlayStation users in 2011. In October of 2013 Adobe Systems revealed 130M user records were stolen. Two months later, Target Corp. reported 130M user records were stolen. In September of 2014, Home Depot suffered a data breach of 56 million credit card numbers. Adult website Ashley Madison had the records of 37M of its clients stolen in 2015 followed by blackmail threats to expose the site's customer's identities unless payment is made. The US government's civilian workforce database was hacked in June of 2015 exposing 22M employees' personal records. In September of 2016, Yahoo finally reported that 500M accounts had been breached nearly two years earlier.

The year 2017 was a particularly a bad year for data breaches. In March, WikiLeaks started publishing the contents of Vault 7, top-secret files detailing capabilities and activities of the United States Central Intelligence Agency (CIA). In July, the largest known data breach in history, the hacking of the consumer credit reporting giant Equifax was reported exposing the personal identity and information of 145.5M consumers. In October, 235 GB of classified military documents of the USA and South Korea were stolen. Meanwhile, the WannaCry ransomware attack [165] crippled computers in 150 countries, with an economic impact exceeding $4B.

While many of the data breach and data-storage attacks involved theft of large blocks of memory *en masse*, others attacks were more targeted, suggesting spying and profiling were employed to maximize the attack's value or impact. A particularly nefarious database attack is *identity usurpation* where perpetrators corrupt or erase a target's identity in a database altogether as though they never existed and usurp their personal identifiable information (PII) [166] Although hardcopy, backup storage, and unrelated data bases can be used to reestablish a person's identity, the recovery process could be arduous and the financial impact to a person or business devastating.

In another class of data breach, *transactional record attacks* are also possible. For example, an effective transactional attack on a bank's database could transfer or misdirect funds from one bank account to an offshore account then erase all records of the illicit transfer. Without hardcopy backup, a victim would have no means by which to prove the theft occurred or that they ever even owned the money. The same class of database attack could, at least theoretically, be launched against insurance databases, against corporations, or against government agencies such as veteran's administration, the social security agency, or federal banks. Blockchains, if secure, may reduce transactional record fraud by producing indelible ledger chronicling a sequence of transactions.

Since numerous commercial databases involve proprietary interfaces and allegedly 'secure' protocols, many database companies promote a false narrative that their database is incorruptible despite overwhelming evidence to the contrary. Like trust attacks and network attacks, data breaches are made possible because of an overreliance on cryptography. To break into a database, there is no need for a perpetrator to crack the encryption; just steal the account password or circumnavigate the security gates. For example, in one database exploit called SQL *injection*, an attacker adds Structured Query Language (SQL) code to a web form input box to gain access to resources or make changes to data. Through automation, it is believed professional hackers, so called 'black hats', are developing freeware hacker tools for SQL injection [167] to steal passwords, inject worms, and access data, potentially exposing 60% of all Web applications using dynamic content. This vulnerability cannot be avoided because user access to virtually all databases and storage files today occurs over the Internet, an intrinsically unsecure communication medium.



Vulnerability / Deficiency	₿	🔒	⊘	⏲	🪙	⚖
51% attack (unlimited power)	✓	✓	✓			
Double spending	✓					
Wallet theft	✓	✓				
Denial-of-Service (DoS) attack	✓	✓		✓		
Sybil attack	✓					
Finney attack	✓					
Private key security	✓	✓	✓			
Smart contract vulnerabilities	✓	✓				
Miner malware		✓				
Transfer Trojans	✓	✓				
Endpoint vulnerabilities		✓				
Spamming Transactions				✓	✓	
Transaction privacy leakage	✓	✓	✓			
Traceable coin history			✓			
Packet sniffing		✓	✓			
Segmentation		✓		✓		
Clock skew attack	✓	✓				
Scalability size/speed limits				✓	✓	
Weak cryptography	✓	✓	✓			
Illegal content						✓
Criminality	✓	✓	✓			✓
Implementation bugs	✓	✓	✓	✓		
Security vulnerability	✓	✓	✓			

₿ fiscal 🔒 security ⊘ privacy ⏲ speed 🪙 length ⚖ legal

Table 2: Blockchain & cryptocurrency vulnerabilities and deficiencies

D) Blockchain Attacks

Blockchain and cryptocurrency-based e-commerce comprise a decentralized transactional process using cryptographic digital-ledger technology (DLT) recordkeeping and distributed consensus validation. Using cryptography to protect blockchain content, transactions are broadly purported to constitute reliable, secure, unhackable processes applicable for commercial, legal, and personal transactions. Moreover, because they employ immutable digital ledgers not controlled by a central authority, blockchain records are not subject to backdating, record tampering, or post revision.

Blockchain transactions are often characterized by the term "trustless" systems, a somewhat confusing reference to the lack of a central authority needed to validate transactions. More accurately, blockchains don't eliminate trust– they shift reliance from a single party to a group of interconnected computer nodes acting as a jury-of-peers [168] distributing control and eliminating single point system failure risks. Despite these beneficial features, in practice numerous attack strategies have been devised to corrupt blockchain transactions and steal cryptocurrency, to launch security and privacy attacks, or to engage in criminality or other malicious online activities [169]. Other attacks seek to exploit blockchain's decentralized trustless consensus as a weakness. **Table 2** provides a sample of blockchain vulnerabilities and deficiencies.

As shown, cyber assaults on blockchains and cryptocurrency primarily involve financial fraud, security breaches, and privacy attacks. The attacks can be perpetrated on the network Layer-3 using sniffing and other means to capture cryptographic keys, using a DoS attack, or directly corrupting the blockchain transaction itself. Blockchain attacks can be grouped into several broad classes including (1) blockchain fraud, (2) cryptocurrency theft, (3) malware attacks, (4) privacy leakage, (5) blockchain illegality, and (6) smart contract fraud.

1) Blockchain Fraud

Generally, for economic gain, blockchain fraud comprises any method obfuscating illicit cryptocurrency activity while intentionally subverting timely validation of bonafide transactions. These blockchain attacks typically utilize two specific types of online malicious activities: double-spending and record hacking. In *double-spending* fraud, cryptocurrency is intentionally spent twice where only one transaction is valid. To complete the illicit transaction, the perpetrator must avoid detection using various means such as system disruption, misdirection, or disguise. In a 51% attack [170], for example, a group of miners controlling a majority of the network's mining hashrate or computing power intentionally impede the peer consensus process preventing confirmations of bonafide transactions in lieu of preferentially enabling illicit ones. The 51% majority attack vulnerability highlights a significant weakness of proof-of-work (PoW) consensus protocols [171] [172] used to validate transactions in decentralized processes. Specifically, because parties with the most computing power can unapologetically usurp control with no vested interest in protecting the integrity of the cryptocurrency against fraudulent transactions or out-of-sequence spending, perpetrators controlling peer consensus are able to commit fraud with impunity.

Blockchain fraud enables double spending through a variety of mechanisms [173] [174] including race attacks, Finney attacks, Sybil attacks [175], timejacking [176], and variants thereof. Even without majority control, mining monopolies [177] can constrain rapid resolution of transactions improving their odds of launching undetected frauds, especially when the number of newly generated coins rewarded to miners declines as a particular currency such as Bitcoin matures, and traders become more desperate (the so-called Tragedy of Commons). Considering the benefits of mining monopolies, it is not surprising that PoW based cryptocurrencies are less decentralized than previously believed [178].

In blockchain *record hacking*, a perpetrator corrupts a blockchain by either inserting unverified fraudulent blocks into the blockchain, or by creating a hardfork in a blockchain for nefarious purposes. Once the blockchain is corrupted, unless it is rejected before the next transaction, the damage is nearly irreversible. The design-around of a corrupted block is to launch a hardfork prior to the offending event while rolling back (cancelling) the main blockchain branch and revoking all subsequent transactions. Such a remedy is unpopular, extremely problematic, and possibly illegal in specific jurisdictions because the cryptocurrency, once spent, is unrecoverable.

Advocates of the hardfork sanction hold the position that a perpetrator's benefit should be expunged, i.e. to unwind the theft, but in so doing it penalizes coin holders having executed legally valid transactions subsequent to the fraud. Opponents of the fork include those penalized by the action and philosophical blockchain purists adhering to the principle of *caveat emptor*, that blockchains should remain irrevocable even when fraud occurs. One notorious and legally contentious example of such blockchain fraud occurred in the summer of 2016 involving the DAO cryptocurrency running on the Ethereum blockchain [179]. DAO lawsuits persist.

Oftentimes record hacking involves a concurrent DDoS attack to prevent detection and transaction repudiation [180] [181]. In fact, it has been reported that 74% of all Bitcoin-related sites suffered a DDoS attack [182]. It is profoundly ironic that blockchain technology is promoted as a method to stop denial-of-service attacks [183] when it can't protect itself from them.

2) *Cryptocurrency Theft*

One of the present-day risks of e-commence based on decentralized currency is the possibility of theft without any recourse to recover stolen assets. The thefts, totaling hundreds of millions of dollars, have occurred by attacks on robbing cryptocurrency mining companies [184], mobile wallets [185], end-points (devices), and even over WiFi [186]. Other attacks focus on digital currency exchanges and web hosts. [187].

Many cryptocurrency thefts involve simple password hacking through malware and spyware (see next section), misplaced trust through fake CA-certificates, cryptographic key theft, packet sniffing, reliance on unsecure third parties, use of fake currency exchanges, or engaging in unsecured online transactions [188] [189]. In short, an unsecure Internet is not able to protect cryptocurrency from online theft [190].

One method to execute online theft employs phishing for cryptocurrency wallets using a login exploit. In this attack, a cybercriminal redirects the login window to a fake website where the victim willingly enters their password and login information, unknowingly passing it to the hacker who subsequently uses it to log into the real site to steal their funds. Such exploits depend on a fake SSL certificate. While preventing login exploits over the Internet is not certain, the risks can in part be mitigated by employing site-specific unique passwords, multi-factor authentication, and by carefully checking all site's SSL certificate for signature authenticity. More importantly, the majority of funds should be stored offline in 'cold storage'.

3) *Malware Attacks*

Malware attacks on blockchains represent another risk to digital currencies. A recent paper presented at the RSA conference revealed 146 different types of malware designed to steal Bitcoins [191]. These techniques include Trojans, viruses, and spyware designed to log personal keystrokes, steal cryptocurrency wallet passwords, capture screenshots, or even stream video-screen images live to a hacker. If a target's computer is infected, their CPU can be commandeered to mine new cryptocoins with the high electrical power consumption and utility bills paid for by the unaware victim. Malware infections can also sequester devices for use in botnets– massive networks of malware-infected computers used to execute attacks on blockchains, cryptocurrency wallets, and the devices storing them.

Other attacks involve viruses designed to search out the wallet.dat files containing the private cryptographic keys used to protect the wallet and its contents. Although the wallet can be encrypted, if the infection includes a key logger, typing the password even once gives the hacker the ability to open the wallet, steal (relocate) the cryptocurrency to their own accounts, or to change the password to remove owner access. Once transferred, coin traceability is altogether lost.

Another form of malware intercepts cryptocurrency transfers. The virus surreptitiously infects a computer waiting silently until the infected device copies a Bitcoin address whereupon the malware immediately becomes active to launch its attack by redirecting the coin transfer to the hacker's Bitcoin address [191]. A particularly aggressive attack involves ransomware, malware demanding payment in Bitcoin or other cryptocurrency in exchange for unlocking an infected computer or its files.

An endpoint attack uses malware specifically focused on interfering with devices participating in a cryptocurrency exchange such as the purchaser, the merchant, and the cryptocurrency wallet holding the coins to be exchanged. As such the attack is performed on the terminus devices, not the nodes carrying the transaction through the network. Best practice for mitigation of malware, while imperfect, involves using firewalls, antivirus software, and offline operation of a dedicated personal computer.

4) *Privacy Leakage*

Although originally believed to deliver transactional pseudonymity protected by cryptographic hash methods, in

2013 blockchainologists confirmed their ability to extract the private information from an encrypted blockchain including names and account numbers [192] [193]. This process, referred to as ‘deanonymisation’ [194] executes a detailed analysis of a cryptocurrency’s blockchain using a combination of data-driven pattern recognition (to extract commonalties in blocks), and analysis of test transactions (to uncover addresses). Since a full blockchain contains blocks detailing every prior transaction, there are risks not only that digital assets may be stolen but also that personal privacy and private financial information may inadvertently be leaked. Private information leakage through a blockchain can be leveraged by astute cybercriminals to profile targets, steal cryptocurrency, engage in identity theft, or to launch personal attacks. Blockchain records can also be employed to identify and selectively target more successful cryptocurrency traders.

The vulnerability of a blockchain to deanonymisation depends on management policies and personal behavior, especially in address reuse [195] and web purchases using cryptocurrency [196]. For example, in the case of online purchases using cryptocurrency, third-party trackers providing online analytics and advertising possess sufficient information to “uniquely identify the transaction on the blockchain, link it to the user’s cookie, and further to the user’s real identity.” Moreover, if a purchaser executes multiple online transactions on the same blockchain, the user’s entire cluster of addresses can be exposed including all transactions even if the user employs blockchain anonymity techniques. The analytical risk is indelible and perpetual, meaning an attack can be mounted retroactively.

As industries migrate to blockchain records, the risk of personal privacy attacks through blockchain exploits becomes increasingly a matter of concern [197], especially as it might expose consumers to identity theft who are wholly unaware that their personal information is being stored in a blockchain. This conundrum has inspired intense research to address the issue of blockchain privacy leakage and how to mitigate it, including proposals to bind physical entities to virtual identities as proxies [198] in an effort to improve accountability while preserving anonymity. Present proposals, despite their creativity, are unconvincing, lacking any credible implementation, testing, or real-world deployment. Transaction resolution speeds of these privacy-protected blockchains are expected to be unusably slow.

5) Blockchain Illegality

Because blockchain can embed any type of data into its blocks, a blockchain could be contaminated with illegal or objectionable material that may be illegal in specific countries or jurisdictions [199]. In a decentralized system, *arbitrary content* files embedded into a blockchain are not reviewed or approved by any administrator prior to inclusion. As such, there exists no means by which to manage a blockchain’s content, to decide what is appropriate, or to identify and reject objectionable, questionable, or illegal matter. A number of risks result from blockchain’s ability to indefinitely store arbitrary content, including the risk of copyright violations, stolen intellectual property, malware, privacy violations, politically sensitive content, religiously offensive material, as well as illegal and condemned content [200].

Copyright violations involve the distribution, illegal downloading and unauthorized use of copyrighted material involving original works of authorship, including musical, dramatic, literary, artistic, and other intellectual works. Similarly, stolen intellectual property involves the unauthorized disclosure, distribution, or use of intangible creative or inventive assets not already made public, including unpublished pending patents, trade secrets, confidential work product, business plans, private contracts, and other private works of creativity. In any case, since it is impossible to recall or retract publicly distributed blockchains it is difficult to ascertain the economic damage caused by the unauthorized release of IP and creative works on the blockchain. Since most users are unaware of illegal material contained within a blockchain, some countries have begun to prosecute infractions based on the download and use of the unauthorized material rather than seeking remedy from the perpetrator who uploaded the stolen material.

Another risk of the arbitrary content field in a blockchain is the introduction of malware. According to INTERPOL, “the design of the blockchain means there is the possibility of malware being injected and permanently hosted with no methods currently available to wipe this data,” permanently impacting global *cyber-hygiene* [201]. Malware infected blockchains may involve zero-day exploits, time bombs, Trojans, or difficult-to-detect molecular viruses. Once infected, blockchain malware is impossible to expunge, representing an ever-present transactional risk and a continuing annoyance of triggering anti-viral software alerts.

The injection of politically sensitive or religiously objectionable material into a blockchain strongly depends on the country or community affected by the material. Political or religious views held sacrosanct in one country may be considered sacrilege in another. Illegal content relating to religiously offensive content or pornography also vary country-to-country. Since there is no arbitrator to ensure the cyber-hygiene of a blockchain, the unknowing import of cryptocurrency containing illegal or banned material into a country may result in unexpected or severe legal consequences. The illegal use of blockchains may also include blackmail, extortion, trafficking, or comprise threats to a sovereign nation’s national security and stability.

6) Smart-Contract Fraud

Smart contracts represent a significant potential for both beneficial and malicious use of blockchain technology. Smart contracts comprise digital code comprising an executable computer program indelibly stored in a blockchain [202]. Operating as a sequential state machine [203], the smart contract executes a sequence of verifiable tasks and distributes cryptocurrency rewards to a pool of miners based on a negotiated value for each job. Although the concept of smart contracts [204] dates back to 1996, it was nearly twenty years before Ethereum offered the first smart-contract based [205]

[206] blockchain-as-a-service (BaaS).

By enabling other companies to utilize its platform and blockchain, Ethereum has differentiated itself from conventional cryptocurrencies focused on trading [207]. Although BaaS adoption is slow and market penetration limited, in part due to distrust in new technology and bad press from reported cases of fraud, a number of exciting potential use cases have emerged [208], mostly in financial technology (fintech) including securities, trade financing, derivatives trading, financial data recording, insurance, and mortgages. Other possible non-financial applications include digital identity, record keeping, supply chain management, land title recording, clinical trial management, and medical research.

Proponents of BaaS suggest that smart contracts can be used to prevent fraud in business [209] [210] while opponents are quick point out that smart contracts have been shown to be susceptible to Ponzi schemes and other fraudulent exploits [211] [212]. In practice, smart contracts today remain illusively problematic, facing a myriad of issues including their intrinsic lack of privacy [213], the inability to expeditiously repel attacks [214], and a propensity to duplicate errors using flawed drafting techniques and error-filled code propagating vulnerabilities, reportedly in 44% of 19,000 Ethereum smart contracts studied [215]. Ironically, blockchains promoted as a solution to preventing distributed-denial-of-service attacks [216] are unable to combat DDoS attacks on Bitcoin exchanges [217] relying on blockchain technology.

7) Other Deficiencies

Referring again to **Table 2**, blockchains suffer numerous other inherent deficiencies affecting their performance. These weaknesses, once identified, invite cybercriminal attacks. Notable deficiencies include elongated blockchains, slow transaction resolution, high mining costs, and environmentally irresponsible consumption of electrical energy, especially using coal-powered generation with a large carbon footprint.

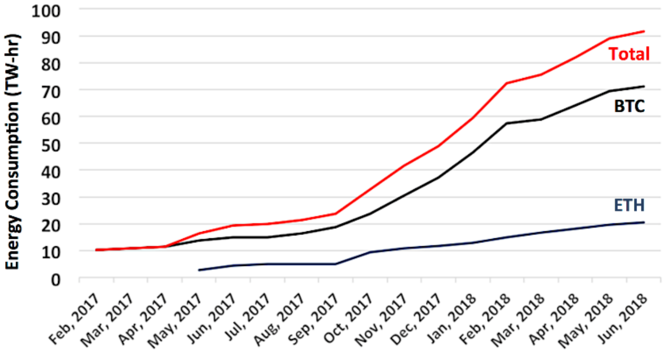


Fig.6: Bitcoin and Ethereum mining energy consumption

Environmentalists warm cryptocurrencies (as realized today) as an unsustainable and flagrant waste of our planet's natural resources. **Figure 6** illustrates this problem, depicting the growth in electrical power consumption for two largest cryptocurrencies. Although the consumption is only estimated, as of May 2018, consumption was estimated to be 64.5 TWh for Bitcoin [218] and 18.3 TWh for Ethereum [219], together representing approximately 83 TWh, greater than the annual energy consumption of all but the top-40 biggest energy consuming countries on planet Earth [220]. This consumption [221] [222] has spawned a firestorm of controversy about energy waste balanced against the potential yet unproven benefits of cryptocurrency[223] [224] [225].

The issue of energy waste is not likely to be resolved by present day cryptocurrencies such as Bitcoin, Ethereum, and their hardforks, since they all rely on a consensus protocol referred to as Proof-of-Work (PoW). By design, PoW was never intended to be energy efficient. To the contrary, PoW was originally invented to protect computer networks against denial-of-service attacks by forcing the attackers to spend money, i.e. waste energy, to qualify in connecting to the network. The idea behind the PoW strategy was simple– if an attacker must waste money to hack a network, they will redirect their mischief or malfeasance elsewhere [226]. Despite the fact that the idea of using a blockchain to realize a cryptocurrency has already been proposed years earlier, it wasn't until the groundbreaking papers (mysteriously published under the pseudonym Satoshi Nakamoto) suggesting the use of PoW consensus to realize digital cash [227] [228], that the first cryptocurrency Bitcoin became available 'in the wild'.

Another feature of cryptocurrency is its inescapable reliance on blockchain technology to ensure a trusted pedigree required to prevent fraud and double spending in a decentralized currency system. To enable verification of the Bitcoin family tree, traceability extends to its origins including every mining event producing new coins, every coin transfer, and every hardfork and softfork stemming from the main blockchain. The resulting impact of this thorough record keeping is three-fold, namely (a) the blockchains become excessively long, (ii) the resolution speed (time needed to confirm the coin's veracity) becomes slow, and (iii) if the trade takes too long, its payee will not do a thorough job on confirming the coin's validity.

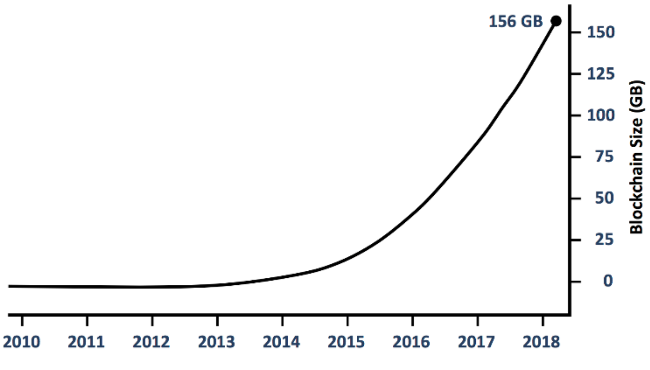


Fig.7: Bitcoin blockchain size (length)

Incomplete checking invites fraud and double spending exploits. The longer a blockchain exists in the wild, the more elongated it becomes and more protracted its checking time becomes. As shown in **Figure 7**, the size of Bitcoin blockchain is now 156.4 GB long [229]. The memory requirement for Bitcoin is now becoming prohibitive, in that it is too large to carry or conveniently use. With every global transaction the length of the blockchain grows incrementally increasing in size typically between 0.5 to 1.0 MB with each new blockchain entry depending on the type of transaction executed [230]. The maximum incremental size of each new block is preset to be 1-MB maximum as part of the bitcoin protocol [231] and even now remains a topic of controversy [232].

The other major concern with cryptocurrency today is one of scalability. Using Proof-of-Work consensus, the more people who use a PoW cryptocurrency the longer the blockchain becomes and the more difficult it is to use. For example, hypothetically should Bitcoin become a global currency studies reveal it would become nearly useless [233] adding hundreds of gigabytes to the blockchain every day. For the sake of argument, assuming it requires 150 minutes to fully validate each 8-MB block, if the Bitcoin became a global dominant currency its block size would necessarily swell to 2.4 GB, taking over 51,000 minutes (over 2 years) to validate [233]. While alternative consensus protocols such as Proof-of-Stake [234] have been proposed, they primarily address issues regarding blockchain attacks rather than improving speed performance. Even so, such consensus methods remain exclusively the focus of whitepapers and academia.

> "Cybercrimes are becoming larger and more dangerous every year, and in the near future the situation will only worsen. I think that we should quickly limit the possibility of their commission. …Over time, we can, for example, build a 'block system' in which any serious action will require confirmation from users. Such a system would be almost impossible to crack. However, to work, we will gradually have to rebuild the entire Internet." [253]
>
> Steve Wozniak
> *RBC interview*, 5 Apr 2018

E) New Technology

The advent of new technology impacts cybersecurity and blockchain adoption, creating new use cases while simultaneously engendering new vulnerabilities.

1) Internet-of-Things (IoT)

The Internet-of-Things (IoT) represents the potential for the biggest single adoption use case of communication since the introduction of the Internet itself. Unlike computers and mobile devices that include a user interface (UI/UX) for human interaction, Internet-of-Things are devices that operate autonomously (or at least semi-autonomously) using a network communication link generally comprising wireless communication over Bluetooth, Zigbee, or WiFi. Because IoT devices are generally low cost, their communication links are relatively primitive and vulnerable to attack [235] [236]. Proposals to secure such devices include deployment of a protective shell or 'overlay,' a dedicated shell operating on an IoT dedicated component which limits dumb IoT devices' access to the home network and personal information [237].

2) AI and Quantum Computing

Artificial intelligence and quantum computing represent two new fields with potentially profound impact on security, privacy, and cryptocurrency. Artificial intelligence and machine learning offers the prospect to adaptively analyze network and device attacks and react with new algorithms to dynamically close the vulnerability [238] [239] [240] [241]. The same AI technology is however being weaponized by cybercriminals to improve cyberattack effectiveness [242]. Similarly, the potential impact of quantum computing on security is a proverbial double-edged sword, enabling cryptographers the ability to improve the complexity and efficacy of new encryption methods and algorithms [243] while simultaneously representing a risk that cyber hackers can employ the technology to break previously 'unbreakable' ciphers [244].

F) Internet-of-Everything

The 'Information Revolution' is a textbook example of interdisciplinary synthesis– the unexpectedly synergistic and symbiotic integration of numerous unrelated innovations of disparate technologies to engender an unexpected outcome, greater than the sum of its parts. Elements of the revolution include the advent of computing, communications & networking, mobility, and cryptography.

Computing, evolving rapidly in the 1980s, includes the development of microprocessors, personal computers (PCs), robust operating systems (UNIX, LINUX, MacOS, and Windows), high-capacity non-volatile memory (hard-drive, flash), and efficient voltage regulation (switching regulators) needed to eliminate heat. With accelerating growth in the 1990s communication and networking included the advent of packet switched communication and routers (Ethernet, WiFi); email; cable and optical fiber communication; widespread adoption of TCP/IP and the 7-layer OSI (open source) protocol stack; the Internet; HTML; the browser; and the World-Wide-Web. Starting at the turn of the century, mobility became important with the rise of high bandwidth cellular networks (3G/LTE, 4G, and soon 5G), color LCD screens, mobile devices (notebooks and smartphones) and the widespread adoption of the lithium-ion battery (Li-ion) used to power the devices. The last decade has emerged as the era of 'connectivity'– the Internet-of-Everything. IoE includes the advent of IoT devices, autonomous vehicles, robotics, drones, and more, all relying on distributed control combined with ever-evolving computing and communication fields.

Decentralization of distributed systems, however, depends wholly on 'trust' to ensure the stability and integrity of the interconnections, the security of communication, and the privacy of information carried over public infrastructure. Electronic trust today relies completely on cryptographic communication, digital signatures, and CA-certificates to establish identity in a permissionless network. The widespread emergence of cryptography also has driven steady adoption of digital ledger technology, blockchains, and enabled the realization of cryptocurrency, a fungible medium of exchange for commerce not controlled by a central authority or relying on fiat currency. Together these diverse technologies, enabled through a guiding principle of interoperability, gave birth to the

Internet and the Information Revolution, interconnecting a diverse range of devices including smartphones and tablets, personal computers and servers; cryptocurrency miner servers, gaming consoles; smart TVs; connected cars; factory-robots; power plants; home appliances; and wirelessly-controlled light bulbs. The global adoption of the Internet Protocol as the basis for cellular, WiFi, Ethernet, and cable TV connectivity has unified communication globally.

Moreover, through the open-source use of TCP/IP and the OSI's seven abstraction layers, technologists are able contribute independently and individually toward realizing and enhancing global interconnectivity, i.e. the Internet of Everything (IoE), without demanding they become Experts in Everything (EiE). The impact is profound– crossing the boundaries of geographies, countries, languages, and cultures. Today, the Internet and cloud communication has been elevated from simple technology into a fundamental human right. Our addiction to being "connected", however, is not without risk.

Misappropriating the "Architect's" self-absorbed diatribe from the sci-fi futurist epic *The Matrix*, trust (hope) in our technology to safely interconnect us all "represents the quintessential delusion, simultaneously the source of our greatest strength and our greatest weakness" [245]. Truly, interoperable connectivity of the Internet, mobile devices, and IoT, net-connected communication empowers individuals, businesses, computers, and machines to interact for personal, commercial, and humanitarian purposes. But increased network connectivity dares cybercriminals to respond in kind [246], investing effort, time, and money to perfect an ever-expanding repertoire of new malware and cyberattack stratagems (see **Figure 8**).

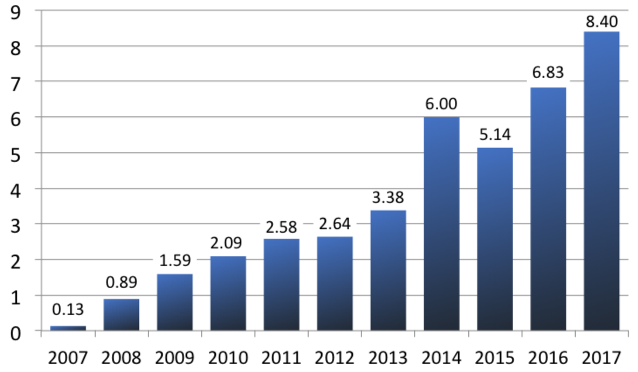


Fig.8: Number on new malware specimens discovered annually (millions)

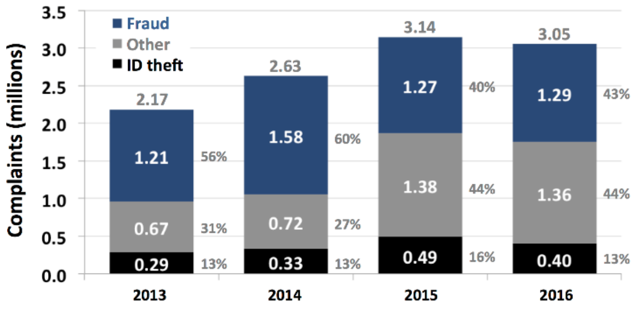


Fig.9: US reported cybercrime complaints by year

Malware today is delivered through a myriad of channels and attack vectors including email, Java, PDF readers, browsers [247], cell phone operating systems [248], and even blockchains. As shown in **Figure 9**, fraud remains a major component of cyber attacks today [249], along with theft and spamming (other). One strategic response to the hacks is to employ cryptographic technology [250]. Through cryptography, secure communication can be performed over an unsecure medium. Unfortunately, the same technology has been harnessed for criminality and nefarious purposes. Interoperability has greatly simplified the challenge for hackers and cybercriminals attempting to invade as many devices and systems as possible with the least effort.

So, what is the right level of encryption? Too low of a level of encryption (weak encryption) can easily be broken by cyber criminals to execute network interventions, privacy attacks, and theft. Supporting too high a degree of encryption (strong encryption) enables criminals, gangs, cartels, and terrorists to operate nefariously in plain sight without detection. In short, when relying solely on cryptography, there really is no right level of encryption. Part of the problem is that with encryption alone, a bad actor is able to disguise their digital identity. Much the same as using a payphone, over the Internet there is no way to confirm the other party's identity. Although CA-certificates offer protection against amateur imposters, professionals are able to steal or fake them with alarming consistency (see **Figure 10**) [251]. Given the diversity of software and hardware methods now available to attack today's communication devices and networks, clearly no single security method is sufficient as a sole defense or to ensure trust [252]. According to Steve Wozniak, in order to ensure security and privacy, "we will gradually have to rebuild the entire Internet," [253].

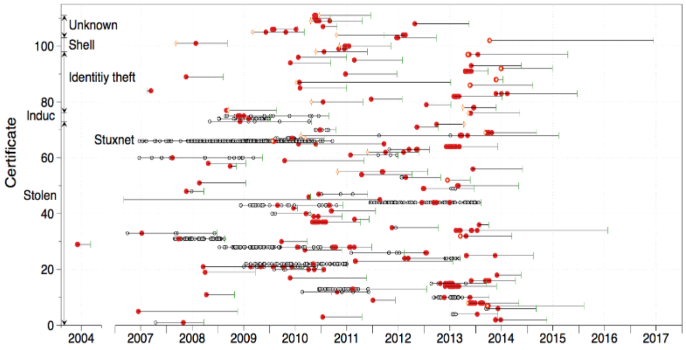


Fig.10: Lifetime of stolen or fraudulent CA-certificates [250]

G) Web 3.0, Internet of Blockchains

In 2007, the original use of the term Web 3.0 described a vision of a 'semantic web interface' [254] [255] [256] where machines readily interpret information semantically and contextually, finding, combining, and acting upon information on the Web. More recently, however, the term Web 3.0 has been recast to mean the Internet of Blockchains [257] [258] [259] representing a decentralization of the World Wide Web, i.e. replacing authority mediated read-write access and concentrated control of a digital oligarchy with a more "liberated, egalitarian, and fraternal Internet" [260]. The migration toward a trustless system, one not subject to the exclusive profiteering, corruption, and manipulation of oligopolies and powerbrokers, is expected to be highly disruptive across all industries. To date, the Web 3.0 ecosystem comprises over 3,000 variegated cryptocurrencies and tokens with over 900 decentralized apps.

While the question remains whether there is any need for so many cryptocurrencies (and even if it is sustainable) [261], the market's trend toward decentralization (reducing controlling influences) and disintermediation (removing go-betweens) is unstoppable. Affected industries already include online storage services, messaging, social networks, video and live streaming, music, and security services with its impact on more regulated industries such as housing, insurance, banking, and government services to invariably follow.

While decentralization is a powerful enabler for democratizing business and improving capital efficiency across industries, the blockchain is not a panacea for today's network security and privacy issues. Although it is trendy to aggrandize blockchains as a replacement to the Internet with compelling titles like "Blockchain technology will power Web 3.0 …*as the new Internet*", "Is Blockchain the Next Internet?" or "Blockchain Is the Internet," [262] [263] [264] [265], blockchain technology is in fact not the network of the future, destined to power the next generation web. In fact, a blockchain is not a network at all. In that context, a Bitcoin network [266][267] does not refer to blockchain communication or protocols, but that Bitcoin processing occurs via applications communicating over the top of the Internet to form an application layer-based peer-to-peer 'overlay' or OTT network on which to execute transactions.

Without the Internet [268] (or alternatively a peer-to-peer network [269]) to transport it, blockchains have no ability whatsoever to communicate, interact, or transact with other devices. And although the data carried by a blockchain can be useful in network management [270] [271], a blockchain is simply a payload– a data file carried in an IP datagram to be used on the Internet's OSI Application Layer-7 [272] [273] or a related host processor. Similarly, comprising only a passive string of serial data, a blockchain is not an application, an operating system, a computational engine, or computer architecture. Just as blockchains need the Internet for their transport, they likewise rely on specific hardware-hosted applications to execute tasks without which blockchains would be completely passive, incapable of autonomously performing any tasks whatsoever. Metaphorically, a blockchain ledger is analogous to viral RNA– it carries information but without processor support, it has no capability to use the information for itself or for the behest of others.

Another recently popularized misconception is that blockchains represent a new class of 'protocols' promising to revolutionize communication and computing. While blockchains are processed by applications that follow specific transactional rules, they themselves are not protocols, but merely data. In networks and computing, a protocol describes action– formal descriptions of digital message formats and rules required to exchange messages [274] [275] [276] [277]. Examples include TCP/IP, HTTP, VoIP, FTP, etc. (where the acronym "P" stands for protocol). This distinction is further complicated by publications describing so-called "fat" protocols [278] [279] [280] [281] making extraordinary claims of blockchain superiority over TCP/IP, asserting the blockchain "pushes more of the value capture down the stack to the protocol layer."

Mixing network operations with unproven economic theory have met with industry skepticism [282] [283], especially considering the fact that without the Internet's TCP/IP protocol stack, blockchain transactions wouldn't even be possible. More accurately, all blockchain transactions occur on Application Layer-7 [284] [285]. As such the terms "application" and "protocol" layers in blockchain vernacular do not relate to the OSI protocol stack but exclusively to blockchain functionality [286] [287] [288].

Another popular *blockchain-tech* buzz is that blockchain technology will secure the Internet from security and privacy attacks [289] [290] [291]. This assertion too, is erroneous. Although a blockchain may contain data used to validate a transaction, this functionality is not executed by the blockchain, but by a resident host processor. The blockchain cannot protect the Internet because it relies on the Internet. Likewise, the blockchain cannot protect an operating system it depends on. It is a contradiction-in-terms to expect a blockchain to defend the operating system of a network server when the blockchain uses the very same operating system for all its transactional execution. If the computer host or its OS becomes infected by malware, the blockchain will correspondingly be subject to risk and attacks, including data corruption, transactional tampering, and cryptocurrency theft.

And despite claims to the contrary, with nearly one hundred and fifty reported blockchain attack mechanisms able to pervert or impede bonafide transactions and even corrupt the blockchain itself, blockchain integrity and security today is routinely compromised. Only if the network used to transport blockchains is secure and every participating device free of malware, can a blockchain's integrity (and its associated transactions) be trusted.

Unfortunately, the Internet is not a secure network. And as such, blockchain transactions today are (and will continue to be) placed at risk unless a 'secure transport medium' and a 'trusted identity validation mechanism' become available. These security, trust, and privacy issues, compounded with slow transaction speed, long blockchain lengths, large data storage requirements, and large-energy waste [292] limit the ultimate potential of the blockchain and cryptocurrency in their present incarnations. What is needed is a decentralized alternative to the Internet and the blockchain that ensures security, identity, privacy and transactional integrity via convenient embedded cryptocurrency featuring rapid transactions and small lightweight blockchains.

III. The HyperSphere

To overcome the deficiencies of the Internet in securing communication, ensuring privacy, and supporting trusted business and e-commerce, we introduce a new, innovative, and highly-advanced cybersecure 'privacy' network for global e-commerce supporting realtime communication, data storage, cloud computing, cloud-connected devices, and e-services– the HyperSphere.

A) Overview of HyperSphere Features

The HyperSphere is an open-source hybrid-cloud platform amalgamating the global functionality of the Internet with the best features of mission critical professional communication, private networks, VPNs (virtual private networks), dynamic realtime networks, global telephony, military-grade cybersecurity, enterprise-grade certificate authority, trusted transactions, intrinsic privacy protections, and private blockchains. The HyperSphere is wholly unique in its novel method of realtime data routing, traffic management, cryptocurrency generation, and blockchain transactional execution.

During operation, tasks are performed autonomously and adjunctively [293], unassisted by network operators. Routing occurs dynamically based on network conditions without relying on pre-defined (static) routing tables. Instead, the HyperSphere represents a fully decentralized system employing dynamic meshed routing [294] [295] designed to minimize network propagation delay [296] to securely and rapidly execute transactions. Combining beneficial features of high-reliability fixed and backbone networks [297] [298], dark-fiber and backhaul [299] [300], wireless [301], and *ad-hoc* peer-to-peer communication [302], with an AI-based de-centralized marketplace, the HyperSphere dynamically analyzes and ascertains the best match between network performance and a client's performance and cost objectives. Because the network's nodal density increases with its number of users, 'the more people who use the HyperSphere– the better it performs', quite the contrary of fixed network clouds.

The HyperSphere is especially unique in its generation and use of its network-native (embedded) cryptocurrency. In the Internet, conventional cryptocurrency is "mined" using costly and energy-wasting Proof-of-Work puzzle solving such as nonce-hash [303] [304] [305] or prime number [306] [307] challenges with uncertain payment and ever-diminishing fiscal returns to its miners. In stark contrast, cryptocurrency generation in the HyperSphere is "minted", created adjunctively as data packets traverse the cloud as shown in **Figure 11**.

Unlike the uncertain return of PoW miners, in minting HyperSphere resource providers *receive guaranteed compensation for supporting completed transactions*, paid in accordance with pre-negotiated HyperContracts. Because the coin generation occurs adjunctively with network operation, virtually no additional energy is spent on minting cryptocurrency beyond the energy spent completing useful work needed for communicating or computing tasks.

Other than being energy efficient and ecologically responsible, dynamically generating network-native blockchains by data transport in the cloud prevents counterfeiting.

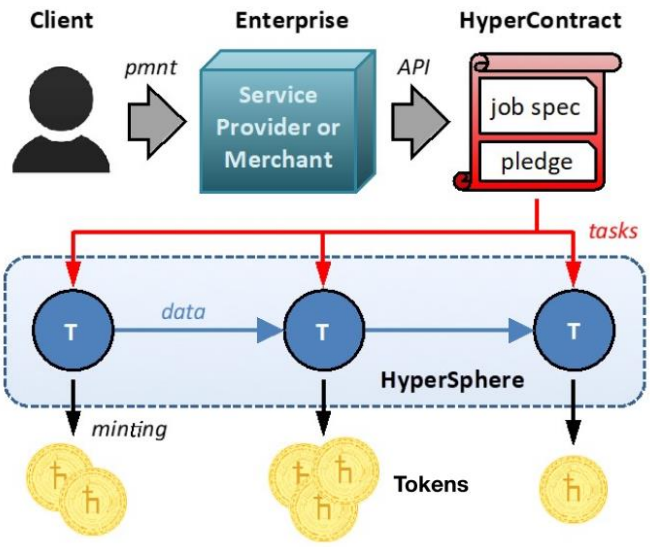


Fig.11: Tokens minting by HyperNode resource providers

Producing cryptocurrency using dynamic blockchain synthesis comprises a process of inter-nodal data transport that cannot be imitated outside of the HyperSphere. And because the cryptocurrency is network native [308][309], it can be transferred and retained in HyperWallets and reused in the HyperSphere without exposing blockchains to the Internet's hacking, theft, fraud, and online transaction risks.

HyperSphere access is entirely software-based with no need for specialized hardware. User interfaces for smartphones, notebooks, desktop PCs, gaming platforms, smart TVs, IoT etc. include support for major operating systems including Windows, MacOS, Linux, Unix, iOS, and Android. Businesses, corporations, research institutes, and universities can facilitate HyperSphere access to their private servers and networks via personal devices, i.e. enabling convenient, cost-effective Bring-Your-Own-Devices (BYOD) connectivity, while supporting corporate IT department security provisions and control. A cluster of devices can also operate as a private network [310] within the HyperSphere, i.e. as a publicly hosted private-network. HyperSphere users may engage in transactions in several ways including in the roles of:

- *Resource providers*– By downloading HyperNode portal software into one or more devices, individuals, companies, and institutions provide resources to the HyperSphere and earn tokens as compensation.
- *Merchants & service providers*– By creating a HyperSphere API-generated application or user interface, merchants and service providers can offer communication, computing, storage, cloud-connected devices, or e-services and products to their clients (even if their customers are not HyperSphere clients).
- *Users*– As clients of merchants and service providers, users can utilize the resources of the HyperSphere, paying them in fiat currency or using earned or commercially acquired tokens.

Hierarchically, rather than employing software running on the Internet as over-the-top (OTT) applications [311] [312] [313], the HyperSphere co-exists with the Internet, sharing resources, physical networks, last mile carriers, and data links. In this sense the HyperSphere essentially operates "on-the-side" (OTS) of the Internet representing a partially overlapping heterogeneous peer network. Furthermore, the HyperSphere is agnostic to last mile connectivity between the cloud and a user's device, seamlessly compatible with any medium including WiFi [314], Ethernet [315], DOCSIS-3 [316], wireless (3G/LTE, 4G, 5G) [317], etc.

Aside from its superior security and its embedded native cryptocurrency, as a 'privacy-network' the HyperSphere uniquely employs network-specific pseudonymous identities [318] [319] [320] [321] to protect personal account information. Using digitally signatures via CA-certificates to privately execute transactions, open HyperContracts, deliver network resources, or trade cryptocurrency, HyperSphere users are thus able to engage in e-commerce without exposing their true identity to potential attacks.

As a further precautionary feature, consensus verification of blockchain transactions employs a unique innovation– a replicant blockchain observer segment (RBOS), a limited length blockchain mirror used to validate transactions while preventing blockchain backtracing and privacy leakage. Another inventive element, a one-time-transaction token (OT^3) employs a single-use temporary transactional payment mechanism to prevent a payee's third-party transaction processor from gleaning private information from a payor's blockchain. In e-commerce, the HyperSphere offers numerous benefits over the Internet including:

- The ability to anonymously, securely, and privately transport realtime audio and video content: functionality needed by service providers offering communication and secure messenger services.
- The ability to anonymously, securely, and privately transport high-integrity data files including email; databases; private media content; and software: functionality needed by providers of secure email, database services, customer contact management, and online collaboration platforms.
- The ability to anonymously, securely, and privately dispatch; manage; and collate the execution of distributed cloud computing supporting researchers and online cloud computing providers.
- The ability to anonymously, securely, and privately transport, store and recall data in disaggregated form, functionality needed for big data analysis and by purveyors of online and cloud storage services.
- The ability to anonymously, securely, and privately transport command-and-control (C&C) instructions for cloud-connected devices while preventing security and privacy attacks on such autonomous devices: functionality and privacy features important to IoT device users and service providers.
- The ability to securely and pseudonymously execute financial transactions, payments or money wires using cryptocurrency intermediaries comprising network-native dynamic blockchains.
- The ability to anonymously, securely, and privately execute a wide variety of e-services for merchants including support for banking and fin-tech, medical apps, government, etc.
- The ability to facilitate the use of pseudonymous data to facilitate personalized AI-based recommendations without revealing a user's true identity or enabling the unauthorized access or sale of personal or private information. In the HyperSphere, a user owns their personal data, not the merchant or the network.
- The ability to form a merchant-operated hypersecure private overlay network securely deployed *within* the public HyperSphere cloud, i.e. using fully sandboxed processing to protect corporate and personal privacy and data integrity.
- The ability to dynamically tunnel past a Last Mile subnet to circumvent denial of service attacks or to access the Internet without exposing a user's identity to unsecured networks or clouds (an *ad hoc* Last Mile tunnel).
- The ability to securely accept, transfer, and hold various forms of cryptocurrency (including Bitcoins, and Ether) in private HypWallets using personal CA-certificate identity-based ownership validation and network-based anti-theft provisions.
- The ability to provide Blockchain-as-a-Service (BaaS) to HyperSphere merchants and startups supporting blockchain synthesis, processing, transactions, user tokens, etc.
- The ability to support cryptocurrency and token offerings as a platform for a variety of blockchain based companies, services, and startups.

The foregoing features as articulated describe but a few of the HyperSphere's innumerable beneficial hallmarks.

B) HyperSphere Design Architecture

Consistent with the HyperSphere Foundation's mission to establish and host the world's premier trusted network, the design objective of the HyperSphere is to facilitate an open source platform for e-commerce supporting a global community of users while both protecting user privacy and ensuring transactional integrity. To that end, the HyperSphere design methodology is based on five fundamental precepts comprising the attributes of…

- Identity
- Security
- Privacy
- Integrity
- Responsibility

As a computer network and communication cloud adhering to these core principles, the HyperSphere's design offers vastly superior operational command and control compared to Internet, peer networks, and corporate clouds. In fact, by its very nature the Internet relinquishes control to unknown devices connected to it. Internet servers and routers determine packet routing, the security methods employed (or ignored) in data transport, and even who can access or surveil a packet's contents or metadata [322].

As such, any bad actor can through a variety of means subject other users to theft, privacy invasion, and other malefactions without consequence, all protected by anonymity of the cloud. Metaphorically speaking, in this regard the Internet operates as a 'payphone', meaning anyone can communicate anonymously without disclosing their personal identity information to the network or to other users. Worse yet, with no ability to confirm identity or confidently establish trust, imposters can with relative ease use the Internet to usurp another user's ipseity without detection. In many cases, Internet attacks can be launched from IoT devices– the least secure components in a network [323]. In this way, a refrigerator, smart TV, thermostat, or dimmable 'smart' light bulb can compromise the integrity and security of an entire network and its users, becoming the attack vector of choice for discerning cybercriminals.

The HyperSphere, by contrast, explicitly controls network access by identifying and authorizing every user and attached component. Through software-based network portals called *HyperNodes*, the HyperSphere manages process and call initiation, controls the handling of different data types (voice, text, video, software…), directs data packet routing, selects security concealment algorithms and security credentials, and validates processes. It also carefully scrutinizes embedded cryptocurrency transactions, manages network operation to ensure high quality-of-service (QoS) [324] [325], and carefully verifies connected device and user identities. In the HyperSphere, security and privacy are addressed through separate mechanisms. Rather than augment the Internet's TCP/IP communication, HyperSpheric security is achieved by utilizing its own dedicated communication protocol– the Secure Dynamic Network & Protocol or SDNP. As such, the HyperSphere is not subject to traditional Internet security vulnerabilities and deficiencies.

Previously deployed over private networks for municipalities and emergency services in Germany, the UAE, and by various shipping port authorities, SDNP communication operates using proven field-tested technology with over than fifteen years' experience in professional and mission critical communication. Its use in supplying communication services [326] for US Army soldiers during the Iraq War confirmed the protocol's capability of delivering military-grade security over private professional networks [327] compliant with FIPS140-2 standards [328] [329]. The HyperSphere's design objectives as described here represent a public network open source deployment of that same technology combined with enterprise-grade certificate authority and embedded network-native cryptocurrency. A brief overview of these objectives and how the HyperSphere addresses the issues, follows here below:

1) *HyperSphere Identity*

In contrast to the Internet, in the HyperSphere no user is anonymous– every user, personal or corporate, holds a corresponding unique HyperSphere identity, privately protected from other users' inspection. This personal or corporate HyperSphere identity permanently interlinks a user's devices, HyperNode cloud portals, accounts, and wallets to an *identity-trust-chain* comprising HyperSphere network-generated CA-certificates. The Internet depends on third-party certificate authorities subject to theft and fraud.

In contrast, the HyperSphere generates its own *network-native* CA-certificates. As shown in **Figure 12**, this means all identity-trust-chains exclusively employ CA-certificates signed by the HyperSphere's master certificate, rejecting all self-signed or third-party certificates as untrusted.

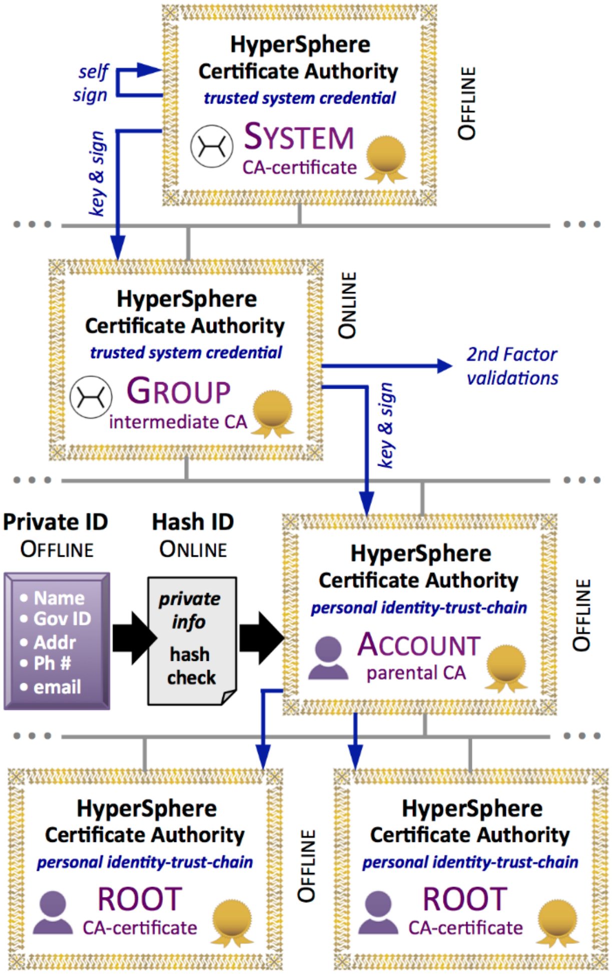


Fig.12: HyperSphere system, private account & root CA-certificates

By interlinking a user's CA-certificates to a corresponding identity-trust-chain, stolen or fraudulent certificates will not match other instances of the user's CA-certificates, and the fraud will be detected, rejecting all transactions involving the fraudulent certificate.

2) *HyperSphere Security*

While the HyperSphere's enterprise-grade certificate authority for identity verification is important, alone it is inadequate to prevent network incursions. In order to protect data, maintain transactional integrity, and prevent cryptocurrency theft or fraud, the HyperSphere employs military-grade 'hypersecure' data transport and multi-tiered security features made in accordance with its patented Secure Dynamic Network & Protocol (SDNP) [330].

Although encryption is employed in packet transport operations, the SDNP process does not depend exclusively on encryption to achieve its superior security protection. Instead, hypersecure communication combines the principles of *fragmented transport of anonymous data packets* together with *dynamic routing and concealment*.

In accordance with its protocol, SDNP data transport in the HyperSphere is secured by (i) limiting the quantity of data traveling through any single node in the network, (ii) obfuscating the packet's true origin and destination, (iii) concealing the content of data packets, and (iv) limiting the time in which to break the security provisions and launch an attack before everything changes (e.g. new security credentials, algorithms, packet routing, format, and more).

The last described security method of limiting 'time', more accurately described as *dynamic routing and concealment*, is especially frustrating and costly to cybercriminals because it constrains the useful duration of any successful hack to a mere fraction of a second, after which the attackers must start all over again. Changes in routing and concealment methods change perpetually, meaning even in the unlikely event a cyberattack breaks into a packet, they will be unable to ascertain where the next successive packet is or how it is being routed. In the HyperSphere's meshed network, it is unlikely two successive packets will ever traverse the same nodes.

And since SDNP data packets carry fragmented data, even if an attacker is able to break a packet's cipher (requiring the perfect execution of a century worth of brute force decryption in one tenth of second), without the other corresponding pieces a decrypted packet's fragmented contents are incomplete, meaningless, and utterly useless, discouraging further attacks on the HyperSphere's cloud and network traffic.

3) HyperSphere Privacy

Privacy is the right to control what information you share and with whom you share it. A secure network does not automatically guarantee privacy– ensuring privacy is more stringent and demanding than simply facilitating security. As such, the HyperSphere does not rely solely on its SDNP secure network capability to guarantee private communiqués and files remain so. Instead, a *privacy network* must, in addition to preventing hacking and surveillance, control access to personal content and private information on a need-to-know basis utilizing 'verifiable identity' to limit access.

Authorization by verifiable identity is especially critical in preventing imposters from capitalizing on anonymity to obfuscate their true identity, misrepresent their purpose, or secretly engage in malicious attacks against a person or enterprise. In order to function as a privacy network, the HyperSphere utilizes the principle of confirming user and device identities during the connection process, i.e. using network-native CA-certificates to establish trust of persons or devices *before granting user access* to privileged information. Beyond hypersecurity, the HyperSphere's privacy provisions protect personal identity and private information through a sophisticated combination of identity-trust-chains and verified CA-certificate lineage not possible over the Internet.

Shown in **Figure 13**, these safeguards include digitally signed authentication of devices, HyperNodes, accounts, blockchains (BCs), HyperContract transactions, and wallets, employing issuing (leaf) certificates distinct from its intermediate IM parents. Beyond a strong cryptographic defense, the foregoing methods uniquely employ HyperSpheric network-native CA-certificates and identity-trust-chains not subject to counterfeiting.

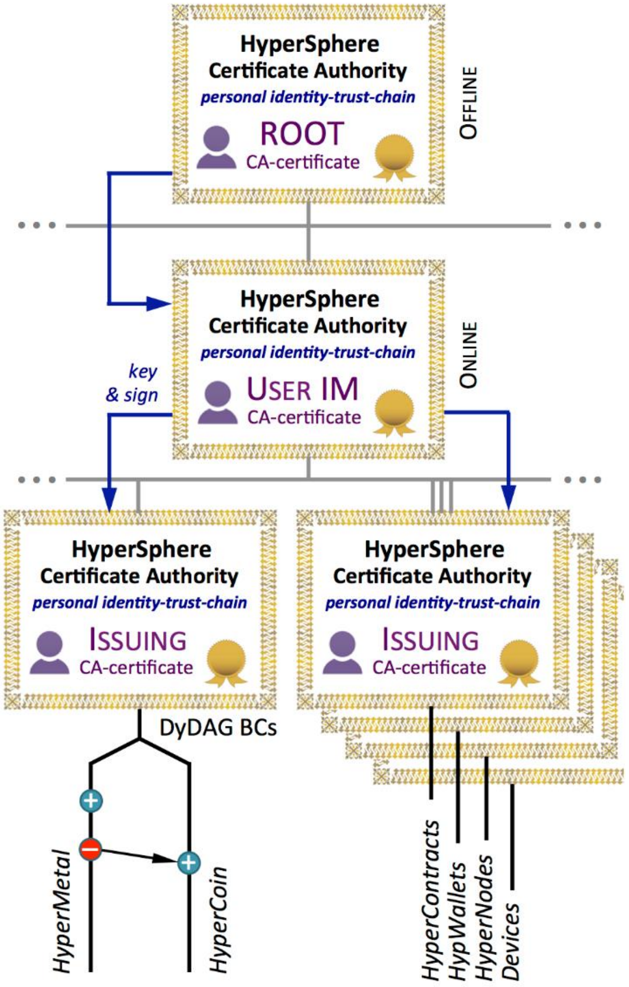


Fig.13: Personal account CA-certificates including root, intermediate (IM), and issuing (leaf) certificates for blockchains, devices, wallets …

One downside to identity-based privacy protection is that, without some means of backup, damaged or lost root CA-certificates may become permanently unrecoverable– a problem which the HyperSphere addresses with an innovative solution, the Quantum Sequential Key or QSK, described later in this manuscript.

4) HyperSphere Transactional Integrity

As a privacy network for hypersecure global e-commerce, transactional integrity depends on secure network operation, user authentication/verification, identity-trust-chains, assured HyperContract execution, and verifiable cryptocurrency transactions. Ensuring transaction integrity in the HyperSphere involves several important mechanisms including (i) preventing the creation of fraudulent (fake) cryptocurrency, (ii) preventing blockchain attacks intended to perpetrate double spending and theft, (iii) avoiding destabilization of cryptocurrency value impacting the HyperSphere's utility and cryptoeconomics, and (iv) ensuring expedient transactional processing and resolution.

5) HyperSphere Responsibility

The final consideration of the HyperSphere is its principled dedication to personal privacy, fiscal, ethical, and ecological *responsibility*. As a fully decentralized network using fragmented data transport with no network cryptographic master keys, HyperSphere operation naturally protects its user's confidentiality and personal privacy. Because of its dynamic meshed transport, privacy attacks using packet sniffing, surveillance, and metadata monitoring are completely unproductive.

In the HyperSphere, a user, not the network, owns their private data. Unless a user grants rights to a service provider to access or distribute it, merchants have no capability to obtain, know, share (or steal), a HyperSphere client's personal information. Moreover, by using pseudonymous leaf CA-certificates, clients can engage in e-commerce without revealing any personal data whatsoever or risking identity theft. Combining identity-based CA-certificates with advanced multifactor and biometric authentication, a user's accounts, blockchain, wallet, and personal data are not subject to inspection, data collection, attack, or usurpation.

Although the HyperSphere is committed to protecting personal privacy in the lawful use of its network, the HyperSphere condemns all acts of criminality, financial and business fraud, privacy attacks, theft, and terrorism. As an ethical communication network, the HyperSphere supports law enforcement in accordance with legal jurisdictions of the session's terminus HyperNodes, i.e. wherever a transaction between parties originates or terminates. Because of fragmented data transport across a meshed network and stateless node operation, no useful content or metadata is available except on the terminus nodes.

Environmentally, the HyperSphere represents the world's first and most eco-friendly method of cryptocurrency generation. Unlike PoW cryptocurrencies wasting vast amounts of energy, consuming precious resources, and exhibiting large carbon footprints only to solve useless puzzles and games, the HyperSphere's cryptocurrency is highly energy efficient, using data transport through its network as a symbiotic mechanism to generate new cryptocurrency. As such, the HyperSphere's Proof-of-Performance adjunctive synthesis and lightweight blockchains consume one-trillionth (10-12) the energy of Proof-of-Work cryptocurrencies such as Bitcoin, Ethereum, and their sidechain derivatives. In comparison to existing (and hypothetical) token and cryptocurrency generation schemes, the HyperSphere's adjunctive method of token minting represents the world's first ecologically friendly and environmentally sustainable cryptocurrency.

As a final point, the potential of the HyperSphere is not limited to commercial and personal profit-minded projects, but extends to all socioeconomic groups. For example, the HyperSphere can be adapted to support research, to facilitate funding of a new generation of entrepreneurs, and to facilitate a variety of charitable and philanthropic projects, including its potential role in will and trust execution and estate planning.

C) HyperSphere Operations

As an autonomous hypersecure communication platform and computing cloud, the HyperSphere efficiently and securely enables personal and commercial financial transactions over a fully decentralized cryptoeconomic system without the need for banks or central authorities to ensure financial transactional integrity. To facilitate and maintain such a high degree of autonomy, the HyperSphere employs a variety of control elements and transactional methods, many of which are reported here for the first time. Elements of HyperSphere operations enumerated below include:

(1) Multi-tree DyDAG blockchains
(2) Decentralized control
(3) HyperSphere merchants and service providers
(4) HyperSphere resource providers (HyperNodes)
(5) HyperContracts
(6) Embedded cryptocurrency (tokens)
(7) HyperSphere marketplace (AI-based)
(8) HyperSphere accounts (HyperNode owners)
(9) Replicant Blockchain Observer Segments (RBOS)
(10) One-Time Transaction Token (OT^3) proxies
(11) SQK, a sequential quantum key

The unique functions and beneficial features of these inventive elements are described in this section. For a more technical description see the Technology section of the paper.

1) Multi-tree DyDAG blockchains

To ensure the security, integrity, and speed of cryptocurrency generation and blockchain transactions, a blockchain must be limited in size and length, and therefore involve limited membership to avoid uncontrolled growth and prevent intrusion from unknown users. Existing blockchain technology used by Bitcoin, Ethereum, etc. employs a single public 'communal' blockchain with global permissionless participation [331] [332] [333].

Communal permissionless blockchains are also subject to privacy leakage, theft, content contamination, and illegality [334] [335] [336]. The resulting public blockchain is too cumbersome, slow, and vulnerable to attack [337] [338] to meet the HyperSphere's design goals and operational objectives. To circumvent long blockchain weaknesses and vulnerabilities, the HyperSphere employs a completely new blockchain structure and control system for distributed ledger processing, cryptocurrency transactions, and traffic management– the dynamic directed acyclic graph, or 'DyDAG', developed and introduced here for the first time. Adapted for dynamic realtime processes from static graph theory, DyDAG mathematics, graph theory, and control algorithms are employed extensively throughout HyperSpheric operations including governance of dynamic meshed data routing, HyperContract execution, rapid blockchain transactions, HyperSphere cryptocurrency generation, and e-commerce.

Contrasted against conventional single-chain ledgers, DyDAG blockchains shown in **Figure 14** are personalized and multi-tree, thereby limiting blockchain length, reducing storage demands, and accelerating transaction resolution rates. Beyond these obvious performance benefits, DyDAG blockchains are robust, ensuring tamper-proof consensus for transaction validation.

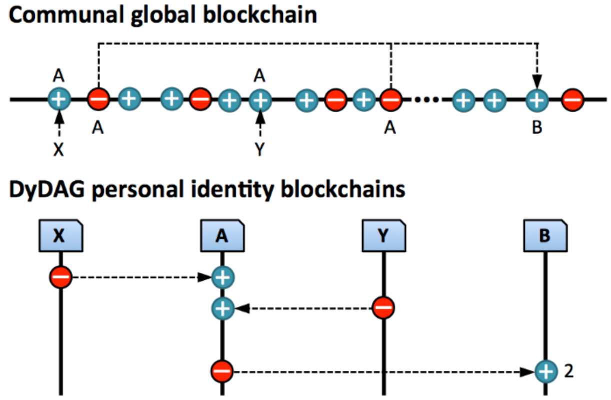

Communal global blockchain
A
A
A
A
B
X
Y
DyDAG personal identity blockchains
X
A
Y
B
2

Fig.14: Comparing communal global (heavyweight) blockchains to identity-based multi-tree DyDAG blockchains

Unlike the global communal permissionless unitary (single-chain) blockchain in conventional cryptocurrency, the various trees in the HyperSphere's DyDAG blockchains are 'individual' (not communal), with each blockchain having personal or enterprise ownership through an identity-trust-chain. DyDAG blockchains include both transitory blockchains or tBC, i.e. limited–life, ledgers used for contract execution, and perpetual (i.e. permanent) blockchains BC used to immutably record financial transactions and enshrine legal records.

Like unitary blockchain implementations, all transactions on DyDAG blockchains are time stamped, immutably chronicling a record of sequential transactions not subject to backdating and revision. Unlike communal unitary public blockchains, however, since each DyDAG blockchain tree is personalized and owned by different individual or corporate entities, a mechanism is required to interlink transacting blockchains and entities. As depicted, this link is realized by adapting the dual-column credit-debt ledger concept of general accounting for blockchains where every credit corresponds to a debit on another blockchain.

In the HyperSphere, all blockchain-to-blockchain asset transfers are executed through HyperContracts specifying the participants including buyers, sellers, jurors, and alternate jurors. At contract completion all credit-debit transactions are recorded, and time stamped as debits on the payor's DyDAG blockchain and as credits on the payee's private blockchain. In the case of public blockchains, the modified DyDAGs are then published on the HyperSphere using pseudonyms to protect the owner's true identity from hackers and thieves.

Although these pseudonyms do not reveal an owner's true individual or corporate identity, in criminal investigations or in cases of civil litigation, a pseudonymous blockchain owner is traceable to their true identity. The HyperSphere is also capable of supporting private blockchains. Unless a buyer waives built-in protective provisions, tokens recorded on private blockchains are not directly transferable to the HyperSphere's cryptocurrency. Instead such tokens should be exchanged through an independent digital currency exchange into fiat currency subsequently used to purchase HyperSphere embedded tokens.

2) Decentralized Control

No person, group, or corporation owns or controls the HyperSphere, its network, or its operations. Instead, the HyperSphere Foundation functions as a non-profit decentralized organization aggregating resources of its corporate, private, and research constituents. Comprising an autonomous network of participating members with virtually no fixed operating costs, merchants and service providers contract and pay resource providers on an *as needed* basis, with the HyperSphere Foundation having no material interest in any HyperSpheric transactions.

In this manner, the HyperSphere's network is made of its resource providers– a heterogeneous community of devices earning income for their owners mutually interested in protecting privacy for themselves and the HyperSphere's user base. Not to be confused with decentralized applications [339], as a fully distributed network, packet routing and network security are executed dynamically without central authority. Operationally functions are shared among nodes dynamically dividing the tasks of traffic management, packet concealment algorithms and methods, and in the issuance of security credentials and cryptographic keys.

In fact, because network encryption and packet concealment are state based, no master keys exist whatsoever. Instead dynamic security is 'state based' occurring dynamically hop-by-hop as data packets traverse the HyperSpheric cloud.

3) Service Providers & Merchants

As an e-commerce platform, the HyperSphere enables merchants to engage in realtime cybersecure network communication and cloud computing with no capital investment in hardware, infrastructure, R&D, or cyber-security developments. Rather than depending on privately owned or contractually obligated leases of servers, VPNs, or dedicated dark-fiber channel capacity, HyperSphere merchants and service providers use HyperContracts to solicit and contract independent resource providers (HyperNode owners) to facilitate network communication and execute their transactions.

Using artificial intelligence and machine learning, the decentralized HyperSphere Marketplace then solicits and procures the necessary HyperSphere resource providers to complete each contract. HyperContracts can be 'hard coded' by HyperSphere contract software engineers or generated automatically or quasi-automatically through API interfaces and templates, including the use of 'HyperSphere services', utilities created and digitally signed by the HyperSphere as system validated transactional processes and executable code.

These HyperSphere services, as shown in **Figure 15**, render certain commonly performed processes such as token sales, asset transfers, point-of-sale transactions, and installing HyperNodes onto devices, creating HyperNode clusters, signing HypWallets, etc. By utilizing easy-to-use pre-written executable code, merchants and service providers can prepare customized APIs without the need to hardcode interfaces from scratch, and conveniently decide to pledge compensation by tokens

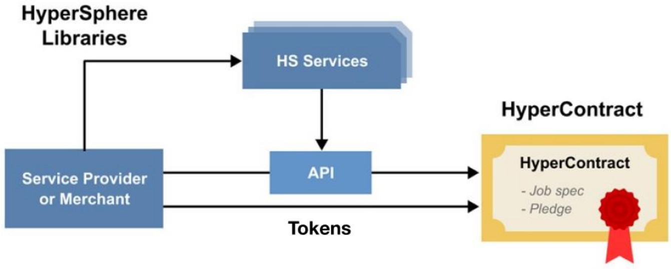


Fig.15: HyperContract automated API generation process

4) *Resource Providers (HyperNodes)*

HyperSphere resource providers deliver communication, computing and storage capability to merchants in accordance with performance requirements stipulated in HyperContracts– electronic contracts offered by merchants describing tasks, deliverables, and compensation. A HyperSphere resource provider is any network-connected communication device hosting operation of a HyperNode– a software-based portal for accessing the HyperSphere. HyperNodes may be downloaded from a trusted app store or from the HyperSphere's website. For identity validation, HyperNode owners use digitally signatures to ensure ownership by a specific parental CA-certificate and identity-trust-chain.

In operation active HyperNodes participating in completed transactions immediately earn tokens in accordance with their contributions. Contribution value and compensation depends not only on market demand, but also on intrinsic capability, speed, reliability, etc. of the HyperNode's host device. HyperNodes are not limited to operation on a single hardware host but may comprise clusters of devices forming a shared account linked to a specific perpetual blockchain and parental CA-certificate. Specifically, in the HyperSphere, resource providers are subdivided into four tiers of HyperNode owners based on their performance, speed, capacity, and uptime capability of their hosts, namely:

- 1st Tier: High-speed, high-capacity global server networks with high availability and extensive node populations, such as Azure, AWS, GWS, IBM Cloud Services, etc.
- 2nd Tier: High-speed, local server clouds with substantial node populations including ISPs, cable networks, bitcoin miner farms, local telco's, etc.
- 3rd Tier: Medium-speed, AC-powered computers and CPUs, maintaining semi-stable cloud connectivity, e.g. PCs, gaming consoles, smart TVs, routers, etc., *and*
- 4th Tier: Mobile and IoT devices with uncertain or variable cloud connectivity including notebooks, tablets, smartphones, games, appliances, etc.

Merchant access to and pricing of a specific tier of resource provider is determined by the cost and performance requirements stipulated in a merchant's HyperContract and by the market dynamics of supply and demand. During execution of a HyperContract, pledged payments (made in tokens) are recorded on the account owner's corresponding blockchain. Upon HyperContract completion and confirmation by a jury-of-peers, the HyperNode mints tokens in accordance with the HyperContract's pledge.

5) *HyperContracts*

Transactions in the HyperSphere occur using digitally specified procedures called HyperContracts issued by HyperSphere merchants and service providers to solicit and contractually stipulate deliverables from HyperNode resource providers. Every HyperContract comprises a *job specification* and a token *reward pledge* describing the compensation reserved, i.e. pledged, for payment to resource providers participating in the contract's successful execution (including jurors and backup nodes). To provide both transparency and to confound blockchain attacks, the jury-of-peers used for consensus-based validation includes both public and cloaked members, observers unknown by the transacting parties until after the consensus option has been rendered.

To solicit job resources and encourage participation, a HyperSphere merchant or service provider attaches a reward pledge to the HyperContract along with the job specification. The pledge, once attached, is temporarily sequestered, i.e. locked from use on the merchant's blockchain and essentially held in digital escrow pending contract completion or failure, thereby ensuring payment with the proviso that the contract is executed.

The merchant next delivers the proposal to the HyperSphere Marketplace, a decentralized market using AI-based algorithms executed by HyperNodes. The bidding process is iterative using various silent auction methods, continuing until all the required resources including participants, jurors, and backups are committed. The accepted contract is then executed as specified. Remuneration is likewise paid in accordance with contractual obligations.

6) *Embedded Cryptocurrency (tokens)*

The HyperSphere's embedded cryptocurrency and utility token, is a fully fungible medium of commerce with capability of

- Being traded, i.e. bought or sold, in independent digital currency exchanges,
- Being minted by resource providers (HyperNodes) as earned compensation for completing tasks and fulfilling HyperContracts, or
- Being used to engage and pay resource providers (HyperNodes) for completing tasks and fulfilling HyperContracts, the cryptocurrency being recycled into new tokens (having new digital cryptographic identities).

As shown in **Figure 16**, tokens can be generated in two ways, either through *minting* or by recycling (melting). In this process, the payment pledge of a HyperContract is ratably apportioned among participating HyperNodes then used to synthesize new tokens. After contract execution and consensus, the pledge is unlocked and recorded as a debit on the HyperNode owner's personal blockchain. In the case of token recycling, the pledge is entered onto the blockchain and held until HyperContract completion. Thereafter, the token is melted, i.e. reissued with a new cryptographic code, recycling the old coin into a new one. In either minting or recycling, participating HyperNodes automatically generate new tokens at the time of contract completion. Once generated, tokens can be sold, transferred, or moved into wallets.

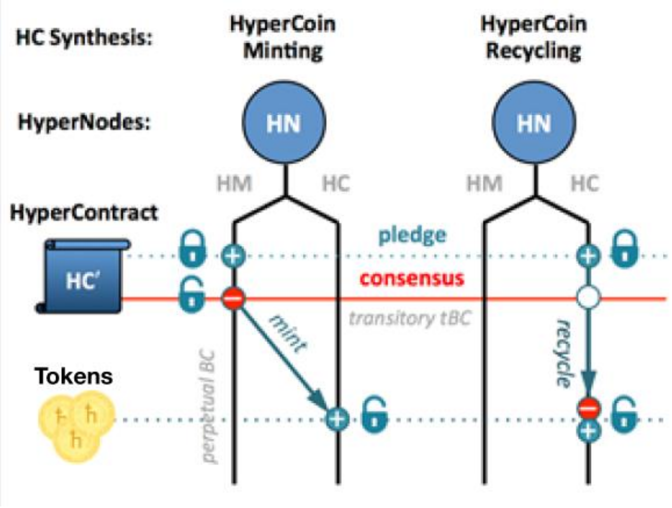


Fig.16: Tokens synthesis methods including minting and melting

7) *HyperSphere Marketplace*

To match HyperSphere merchant and service provider's requirements to resource providers willing to meet the terms and deliverables specified in a HyperContract, the HyperSphere utilizes the HyperSphere Marketplace, a decentralized capital-efficient electronic marketplace.

In operation, the HyperSphere Marketplace solicits resources and negotiates terms mutually acceptable to all parties. HyperNodes participating in the contract resolution process (jurors) are by definition not a party to the HyperContract. After negotiation is completed, the broker nodes are appended to the HyperContract for their role in brokering an actionable agreement. Token compensation is only paid upon successful execution of the HyperContract.

8) *HyperSphere Accounts*

HyperSphere accounts refer to the device assets, devices, and HypWallets owned by a particular parental CA-certificate. In particular, HyperSphere accounts of a specific owner include their devices, their registered HyperNodes or HyperNode cluster, their token perpetual blockchain and their HypWallets. Any number of intermediary CA-certificates may be used to digitally sign and verify ownership of these elements.

All HyperNode income earned by a HyperSphere account owner will reside on their personal token blockchain unless transferred into one of several HypWallets. Additionally, HypWallets may hold cryptocurrency other than embedded tokens including private company tokens using the HyperSphere as a Blockchain-as-a-Service (BaaS). Aside from minting tokens, all asset transfers in and out of a HyperSphere account occur through OT^3 proxy mediator.

9) *RBOS– Replicant Blockchain Observer Segments*

To manage transactional integrity while preventing personal identity theft or leakage from an account owner's blockchain, the HyperSphere uses a unique and inventive method referred to as a *replicant blockchain observer segment* (RBOS), introduced here for the first time. Comprising a limited length copy of a host's blockchain, the RBOS is sufficiently long to authorize a transaction but too short to enable backtracing of prior history or inadvertently result in privacy leakage.

An example of the use of an RBOS for juror consensus in HyperSpheric transactions is shown in **Figure 17**. Any given transaction can employ more than one RBOS to support any size jury-of-peers. After a transaction's completion, its corresponding RBOS is destroyed and the hashed blockchain recorded, protecting privacy while ensuring transaction integrity and traceability while preventing double spending.

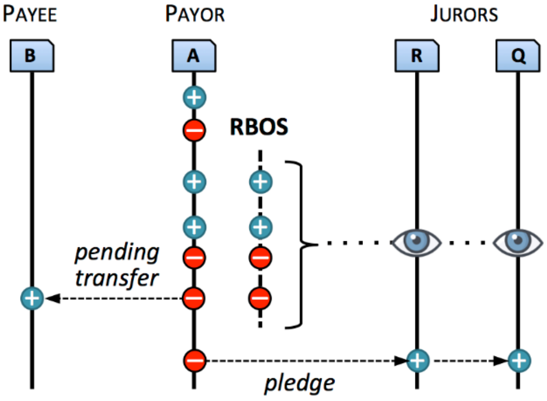


Fig.17: RBOS transactional verification facilitates reliable juror consensus while protecting a payor's privacy against BC backtracing

10) *One-Time Transaction Token (OT^3) Proxies*

As described previously, all asset transfers in and out of a HyperSphere account are executed using a special transitory blockchain referred to as a one-time-transaction token or OT^3 proxy. The proxy exists only during a transaction after which the mediator and its records are irrevocably dissolved. In particular, to prevent theft or backtracing during sale of tokens or when using tokens as payment for online or point-of-sale purchases, no direct blockchain access to the owner's blockchain is allowed. Instead, a two-step transfer process is employed where first the blockchains are moved onto a One-Time Transaction Token mediator or OT^3 proxy then in a second step the cryptocurrency is transferred from the proxy to the merchant or buyer in exchange for goods or currency (crypto or fiat).

During all OT^3 proxy mediated transactions, the first step requires the payor, the token holder, to request moving a specified number of tokens from their account or HypWallet to the OT^3 proxy. Shown in **Figure 18**, his process commences by the requestor opening an OT^3 transfer HyperContract. The HyperContract then identifies a jury-of-peers and creates a replicant blockchain observer segment (RBOS) from the owner's token blockchain (or HypWallet) of sufficient length to verify the payor holds adequate assets to execute the requested transaction.

Once verified, the requested tokens are debited from the owner's perpetual token blockchain and credited onto the transitory OT^3 blockchains. Because the payor cannot see the cloaked jurors, they are unable to execute a 51%, botnet, or Sybil attack to engage in double spending because they don't know the jurors who are checking the RBOS blockchain. Similarly, the payor cannot subvert or corrupt the RBOS data.

The next step is to confirm the sincerity of the payee, either the merchant selling goods and services, or the token purchaser. This can be accomplished in person for POS transactions, through an escrow agent (for real property) or by time-locking the OT^3 proxy's release till the transaction settles, e.g. until the validity of a cryptocurrency payment can be confirmed. After the transactional integrity is confirmed the OT^3 proxy transfers the token digital code to the merchant or buyer, and the proxy is closed. In this manner through the OT^3 proxy neither party directly interacts and is unable to commit fraud or backtracing.

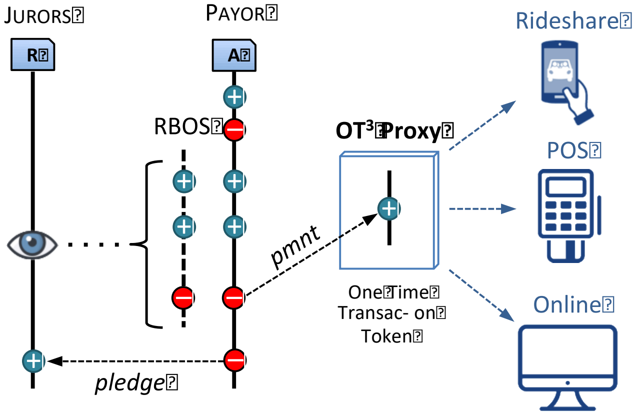


Fig.18: OT³ proxy based HyperSpheric e-commerce

The proxy mediator also speeds transactional resolution because the slower blockchain verification and transfer process can precede the actual e-commerce transaction. Lastly, the OT^3 proxy limits the total assets at risk for transactional fraud because the HyperSphere account holder never exposes their personal token blockchain or HypWallet.

11) SQK, a Sequential Quantum Key

To recover lost root CA-certificate and restore corrupted account identities, the HyperSphere includes, as a last resort, a unique cryptographic device introduced herein as a sequential quantum key or SQK. The SQK, properly decoded, gives its owner the ability to open and restore their root CA-certificate to reclaim rightful ownership of corrupted accounts.

Built on the principle of the *quantum observer effect*, which states that by very act of watching, an observer affects the observed reality, in a sequential quantum key, not only must the contents of the key be faithfully reproduced, the sequence in which each cell is viewed and entered must be executed in a precise way (metaphorically as a multidimensional Rubik's cube). If the sequence is executed incorrectly, the proper combination will never appear. The observer effect makes brute force attacks extremely difficult while allowing users to separate passphrase archiving and sequencing in unrelated media content.

D) HyperSphere Technology

The HyperSphere's technology platform is uniquely without peer, combining patented and inventive (patent-pending) communication, network, security, certificate-authority, blockchain, and cryptocurrency knowhow and capability into a single unified platform. In broad terms, these topics can be organized into three broad topics, namely (i) the Secure Dynamic Network & Protocol (SDNP), (ii) HyperSphere identity & certificate authority, and (iii) network-native DyDAG blockchains & cryptocurrency described here below.

1) Secure Dynamic Network & Protocol (SDNP)

In order to protect data, maintain transactional integrity, and prevent cryptocurrency theft or fraud, the HyperSphere employs military-grade 'hypersecure' data transport and multi-tiered security features made in accordance with its patented and patent pending Secure Dynamic Network & Protocol (SDNP) [330] [340] [341], Hypersecure Last Mile Communication [342], and HyperSphere operations [344]. Although encryption is a methodological element of its data packet transport operations [345] [346] [347] [348], the SDNP process does not depend exclusively on encryption to achieve its superior security protection.

Instead, hypersecure communication combines the principles of *fragmented transport of anonymous data packets* together with *dynamic routing and concealment*. Features of SDNP communication include:

- Hypersecure cloud communication among HyperNodes using anonymous fragmented data transport and dynamic routing over a distributed meshed network [349] [350] for secure reliable [351] [352] communication; not subject to packet sniffing and metadata surveillance,
- State-based communication packets [353] [354] [355] comprising dynamically changing payloads transported over a stateless [356] meshed network, retaining no record of calls, packet content, routing, source or destination addresses. As a stateless network, the network is unable to recall or inspect information or metadata even one nanosecond after transport through a communication node has been performed,
- Fully decentralized network operations including hop-by-hop dynamic security, state-based security credentials and cryptography and tunnel-protocol [357] data transport (not SSL/TLS), to prevent packet hijacking, man-in-the-middle attacks, and network usurpation
- Anonymous nodes having dynamic *ad hoc* IP addresses and ports, unrecognized by DNS servers with no fixed correlation to devices or user identity, to prevent identity tracing and packet hijacking,
- Tri-channel network communication performing the communication functions of name servers, signaling servers, and media servers using metamorphic HyperNodes able to dynamically transform to match job requirements,
- Network-generation of cryptographic and numeric seeds used in cryptocurrency minting performed adjunctively with data transport through the cloud, comprising unfakable blockchain generation and reward apportionment demanding

no additional power requirements beyond supporting network operations.

Unlike SDNP deployments over private networks hosted on dedicated hardware, decentralized communication over public networks with no fixed infrastructure requires a different approach. In SDNP private professional network communication, network nodes manage data transport and network traffic by executing single-purpose dedicated functions of name servers, signaling servers, or media nodes. In the HyperSphere, however, every device-installed node must be capable of executing any of the aforementioned communication functions, and more...

Accordingly, the HyperSphere employs an entirely new class of multifunctional network application software referred to as *metamorphic HyperNodes*– network nodes able to dynamically adjust their operations on an impromptu basis to execute required SDNP network functions, manage data storage, control connected devices, and orchestrate cloud-computing activities. As shown in **Figure 19**, metamorphic HyperNodes may function as either (i) HyperSphere 'name server' or NS nodes for identity management, (ii) HyperSphere 'authority' nodes for signal server, routing, and contract execution, or (iii) HyperSphere 'task' (or service) nodes performing media transport, distributed computing, and data storage services.

HyperNode interconnectivity occurs multidimensionally over stratified virtual-network layers dynamically formed by the nodes operating on that stratum. For example, at any given moment, the collection of metamorphic HyperNodes interacting as task nodes forms the HyperSphere's 'task layer' used to carry data packets and execute cloud-computing related functions. Similarly, an assemblage of metamorphic HyperNodes interacting as authority nodes forms the cloud's 'authority layer', a virtual-network layer used to instruct task nodes as to packet routing, to execute network command-and-control, and to access the name server layer needed for identity management and account verification.

By stratifying HyperSpheric operations into distinct virtual-network layers following strict rules defining all multi-dimensional layer-to-layer transactions, metamorphic HyperNodes achieve the same degree of security on a public cloud as that realized by SDNP private clouds employing single-function segregated node types. To prevent any one HyperNode from concentrating too much information or decision authority, a HyperNode's participation in a particular HyperContract is restricted to operating on a single virtual-network layer.

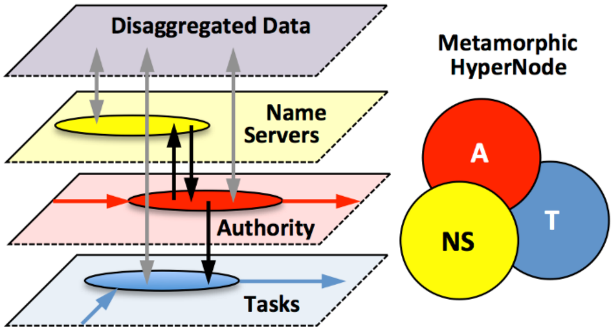


Fig.19: Metamorphic HyperNode operations for task |T|, name server |NS| and authority |A| functions including data mgmt

In other words, virtual-network layers function independently on a mutually exclusive basis, limiting a HyperNode's participation to only one of the three network functions for a specific HyperContract. Specifically, during HyperContract solicitation and negotiation, the cloud's decentralized AI-based HyperSphere marketplace evaluates and assigns each HyperNode its specific role as a task node, authority node, or name-server node. In response, the HyperNode transforms, i.e. morphs, into that specific type of HyperNode, operating only that corresponding virtual network layer for the duration of the HyperContract.

To confound packet surveillance and prevent network usurpation, layer-to-layer multidimensional interactions among the HyperSphere's virtual network layers are limited in scope and content. For example, although the authority layer interacts with the task layer by directing network traffic, the task layer cannot pass packet content up to the authority layer. While the authority layer interacts with the name server layer in planning and directing packet routing among cloud connected nodes, the task layer carrying data packets has no access to the name server layer and therefore has no way of knowing who is communicating.

Another virtual-network layer in the HyperSphere comprises the disaggregated data layer. The disaggregated data layer holds data in diffuse form, spreading data over multiple devices in a redundant array. Only by locating, collecting, assembling, and decrypting the disaggregated data is it possible to restore original saved information. Without knowing where various snippets of information are held and how to reassemble them, data theft is impossible. Stored and accessed multidimensionally, disaggregated data storage is literally 'hidden in plain sight', undetectable and unobservable except to its owners or authors.

Disaggregated data in the HyperSphere comprises two types– temporarily held *cached data* used in stateless transactions, and cloud-based *non-volatile data storage* or 'storage drives', needed to retain files for extended durations or in perpetuity. Unlike interactions with task, or name-server virtual-network layers, HyperNodes cannot access the disaggregated data layer in its undifferentiated state. Instead, access is gained only after metamorphic HyperNodes transform into single-function |A|, |T| and |NS| nodes, limited to their corresponding virtual-network layers. As a communication network SDNP operation is unique in its approach to protecting metadata and insulating payload content against surveillance or attack. In accordance with its protocol, SDNP data transport in the HyperSphere is secured by (i) limiting the quantity of data traveling through any single node in the network, (ii) obfuscating the packet's true origin and destination, (iii) concealing the content of data packets, and (iv) dynamically changing packet routing.

In regard to the first point, by splitting content into pieces (fragmentation), SDNP payloads are by design 'incomplete' containing no useful information. Rather than transporting complete documents or media files in jumbo packets, the HyperSphere employs the opposite philosophy– sending small amounts of data over multiple paths.

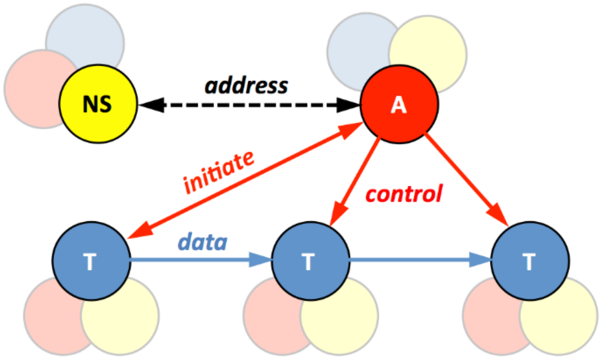


Fig.20: Meshed data routing using metamorphic HyperNodes.

Through dynamic fragmentation, the many packets' payloads each comprise partial content. Examples of partial payloads include a single pixel of a photo, incomplete ASCII codes, unintelligible media files (e.g. an audio snippet containing only a portion of a sound), or software fragments. When transporting packets over constantly changing routes (dynamic meshed routing), no single communication node carries successive packets of related information content.

By preventing the aggregation of data packet identity, ownership, routing, content and other metadata, SDNP packets

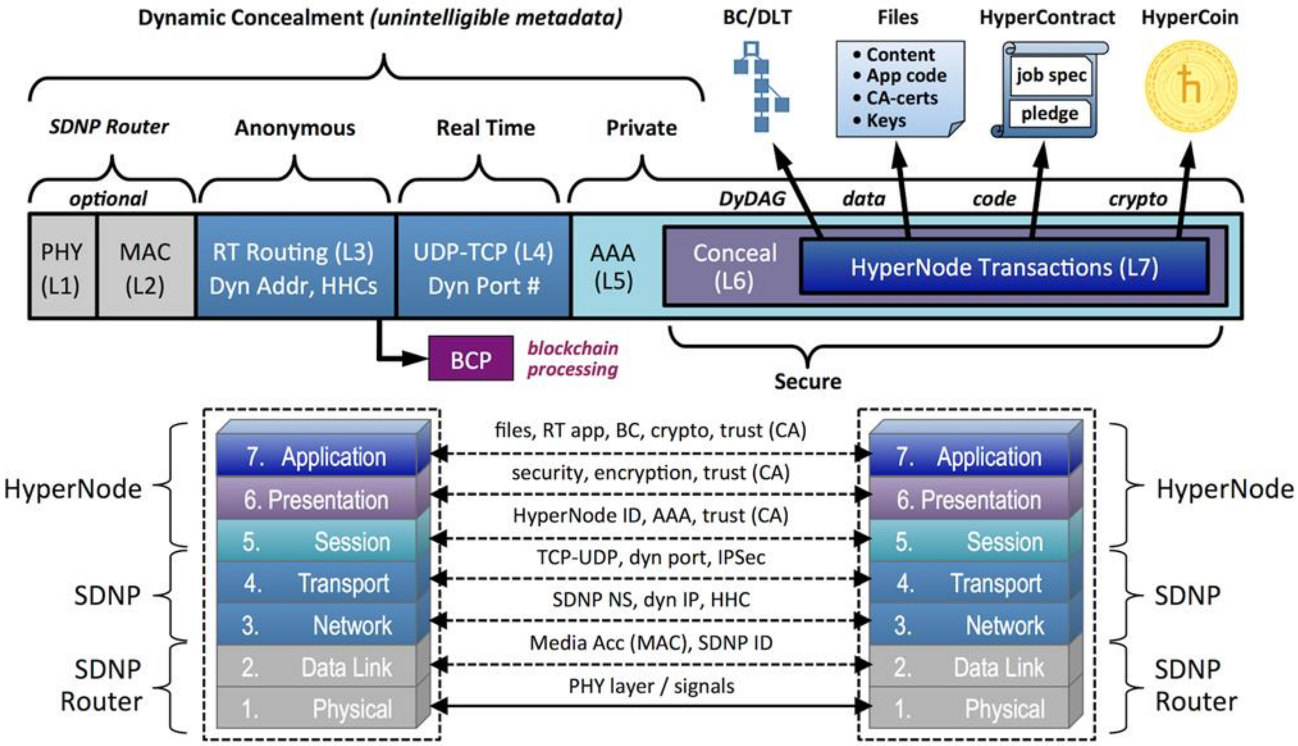


Fig.21: SDNP data packet construction, features, and protocol stack

evade advanced analytic cyberattack methodologies. **Figure 20** illustrates an example of dynamic meshed data routing where each metamorphic HyperNode performs tasks relegated to a single virtual-network layer, i.e. |T| nodes on the task layer, |A| nodes on the authority layer, and |NS| nodes on the name server layer.

In an example of a data messenger phone call, a caller initiates a call by contacting node |A| and identifying the phone number of the person to be called. The |A| node in turn contacts the |NS| node to identify the current IP address of the device and of the |T| nodes to carry the call. The |A| node then instructs the |T| nodes as to packet routing on a hop-by-hop basis. As a stateless network, the data packets are discarded immediately after processing retaining no record of the call or its contents.

As to the second novel feature, obfuscating the SDNP packet's true origin and destination, the HyperSphere employs anonymous data packets– IP datagrams specifying only single-hop source and destination IP addresses but not disclosing a packet's point of origination or its ultimate destination. This feature is depicted in SDNP packet construction and its 7-layer OSI model [358] in **Figure 21**.

As represented in Network Layer-3 of the SDNP protocol stack, not only are SDNP-packet IP-addresses dynamic (changed frequently), HyperSphere routing does not involve the Internet's domain name servers (DNS). Instead the SDNP name server function linking dynamic IP addresses to a user's identity, phone numbers, physical devices, MAC addresses, etc. is realized in a fully decentralized manner via the SDNP's name-server virtual-network layer, accessed through metamorphic HyperNodes and stored on the disaggregated data layer.

Without meaningful packet routing addresses, there is no way for hackers to use sniffing or surveillance to determine which packets are related to one another. To further confound metadata surveillance and DOS attacks, SDNP protocol for Transport Layer-4 employs *ad hoc* dynamic port addresses having no particular assigned port number or defined service (such as email, FTP, etc.) by which an attacker can analyze packet content contextually [359].

To maximize quality-of-service (QoS), the transport protocol employs both TCP and UDP transmission methods depending on the nature of the payload. While the Transmission Control Protocol (TCP) is employed for high reliability payload delivery such as code and content delivery, User Datagram Protocol (UDP) is employed for realtime (RT) communication such as voice, live video, and other realtime services. Moreover, RT datagrams will be routed by authority node's signal server function over the network's shortest propagation delay paths while TCP routing for high integrity delivery focuses on maximizing reliability, likely routed over entirely different meshed routes than UDP packets. And rather than using end-to-end SSL [360] or TLS transport security (notoriously vulnerable to attack), SDNP transport security is preformed by tunneling protocols such as IPSec and others, executed on a hop-by-hop basis in the cloud [361].

In so doing, unauthorized reconstruction of disaggregated digital content, conversations, media, or transactional sessions is prevented. As described, SDNP network operation confounds single-point attacks by limiting the content carried by any single node in the network, both by fragmenting the data and by only routing single packets through the same task nodes– quintessentially following the old adage "don't put all your eggs in one basket!"

The third attribute of SDNP network operation, concealing the content of data packets, employs a dynamic concealment methodology using *state-based* security methods and credentials. State-based security means that the security methods and credentials used to protect SDNP datagrams change with its state. A security 'state' is a condition existing at the moment of a data packet's creation, e.g. network time, location, security zone, etc. Packet concealment in the HyperSphere comprises modifying payloads using a variety of state-based security mechanisms executed as data packets traverse the spatiotemporal network, including …

- Dynamic splitting and mixing,
- Dynamic scrambling and unscrambling,
- Dynamic encryption and decryption [362] [363]
- Dynamic junk data (or packet) insertion and deletion
- Time and zone dependent states

As example of state-based dynamic concealment is illustrated in **Figure 22** where security credentials and payload content change on a hop-by-hop basis. The states are further subdivided into zones, geographic regions (subnets) within the HyperSpheric cloud. Using the foregoing methods means that no two packets traversing the HyperSphere have the same construction. So even if in the unlikely event two packets could be identified as part of the same conversation or session, the packets won't have the same state-based security credentials (keys, seeds, tags, zip) and won't employ the same fragmentation, scrambling, encryption [364] [365], or junk data algorithms. In other words, identifying two related datagrams does not help improve a hacker's chance of reconstructing secure message content.

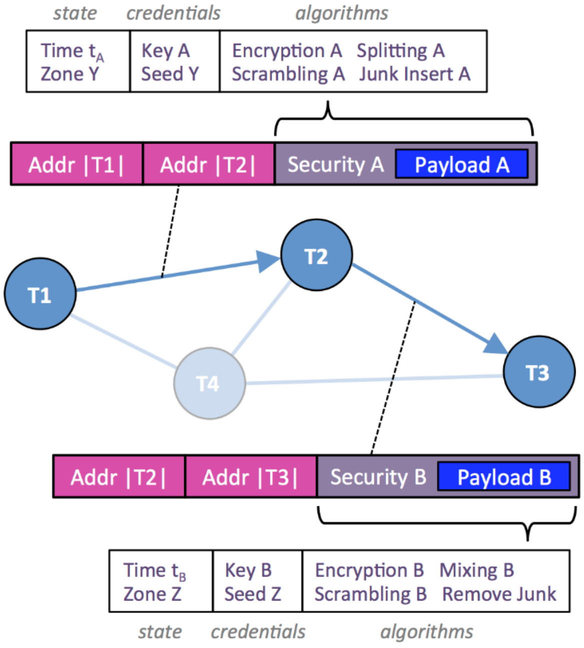


Fig.22: SDNP dynamic security changes payload concealment algorithms and credentials on a hop-by-hop basis

Another key feature of the SDNP cloud is its use of 'dynamic routing'. In the transport of any SDNP datagram, autonomous routing functions (as executed by authority nodes) direct successive packets across multiple changing routes of the HyperSphere' meshed network. As depicted in **Figure 23**, because no two successive packets traverse the same path, attacks on a specific server or router are meaningless because the successive packet will not use the same servers for transport. As illustrated, an exemplary data packet containing a digital sample of a single audio word is divided into three sub-segments |A|, |B|, and |C|. The related packets are then sent in succession across the HyperSphere's network of 'task' nodes using multiple paths, each different than its predecessor. The benefit of dynamic routing is multi-fold. First, because an attacker cannot identify which nodes will carry sequential packets, there is no means for them to gather the data or recover the original voice.

Secondly, because the packets are dynamically routed, the authority nodes can employ the most recently available propagation delay data from the network to choose the fastest routes, thereby minimizing the system's average propagation delay and improving audio QoS. Lastly, high value or critical messages can be sent redundantly in multiple instances (copies), each competing to arrive at the destination first. Aptly called 'race routing' the first packets to arrive are used and redundant latecomers are discarded. In the case of audio or live video, segments arriving out of order, i.e. too late to use, can be skipped and the sound or image reconstructed without their inclusion. Another unique feature of the HyperSphere is its ability to support identity and privacy as an integral part of SDNP operation. Referring again to **Figure 21**, security of the upper layers 5, 6 and 7 in the SDNP protocol stack relies on identity-trust-chains using the HyperSphere's network-native CA-certificates.

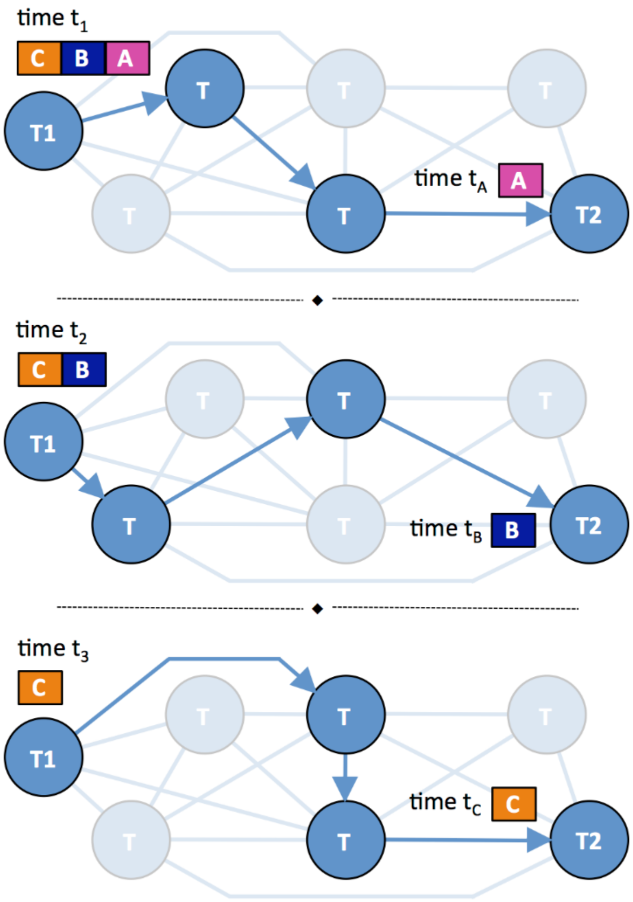


Fig.23: SDNP dynamic meshed routing of datagrams autonomously changes paths to minimize propagation delays and confound tracking

In SDNP Session Layer-5, communication sessions prevent fraud with AAA (authentication, authorization, administration) and validation of HyperNode identity. SDNP Presentation Layer-6 employs HyperNode CA-certificates to support end-to-end encryption. SDNP concealment methods, however, are state dependent and are agnostic to account and user identity. Application Layer-7 security is application specific using CA-certificates to establish DyDAG blockchain ownership, HypWallet ownership, and various software apps.

As a final point, because of its unique implementation of dynamic security methods and novel network-native identity trust chains, the installation of HyperNodes onto any device is symmetrically sandboxed, meaning the device cannot see inside the application to determine what tasks the HyperNode is performing, and the HyperNode cannot access any user data within the device. Attempts to install fraudulent HyperNodes will not match the user's HyperSpheric identity, preventing access to the device or the HyperSphere.

The concept of sandboxing extends to more than one device, where a group of HyperNodes can be clustered with common ownership. By installing HyperNodes onto a community of devices, e.g. on employee's personal devices in a BYOD friendly company, an *ad hoc* private network can be deployed on top of the HyperSphere to facilitate a public-private network. The many roles of HyperSphere's enterprise grade CA-certificates are further elaborated in the following section.

In summary, the combination of the foregoing features makes the SDNP packet communication unique in networking and telecommunication, especially considering its novel operating characteristics of:

- State-based security credentials and packet concealment operating over a stateless meshed network,
- Anonymous data packet transport of transactions linked to identity-trust-chain based CA certificates,
- The ability to realize sandboxed private networks within a public cloud.

In this manner security and privacy are maintained without sacrificing provable identity or verifiable asset ownership.

2) HyperSphere Identity & Certificate Authority

As described previously in this manuscript, the HyperSphere acts as its own network-native certificate authority in generating identity-trust-chains for its users and their devices [366] [367]. During account setup, the HyperSphere first establishes a parental "identity" certificate as either a verified 'true identity' owner or alternatively using a pseudonym. For the purpose of banking, asset management, legal and business transactions, a user's true identity [368] must be established through a know-your-client anti-money-laundering (KYC/AML) identity [369] [370] confirmation procedure.

The account creation process shown previously in **Figure 12**, establishes an irrevocable link between a person's identity and their personal identity-trust-chain of CA-certificates. Regardless of whether an account is established using verifiable true identity or pseudonymously, the account and its trust chain digitally signs (and therefore is connected to) all hardware on which HyperNodes reside [371] [372].

In true identity accounts, the topmost personal CA-certificate, the 'parent' CA-certificate is linked to identity documents, e.g. passport, driver's license, social security number, etc. as evidenced by image scans, biometrics, signatures, etc. When executed by a bank, qualified merchant, or by a trusted third-party agency during account setup, the independent confirmation procedure confirms and corroborates the legal identity of the person or corporation using multiple sources of ID validation. Once a trusted legal identity is established, the account owner is able to obtain a HyperSphere-issued 'root' certificate.

The approved root certificate enables its owner to make prodigy and subordinate certificates useful for signing specific transactions or authenticating specific devices. In this manner a person or their devices can engage in commerce without revealing their personal identity or risk identity theft. As shown in **Figure 24**, the account holder's identity certificate– their parental CA-certificate, is used to generate a personal root certificate. The identity certificate then signs the account holder's root certificate [373] [374], which in turn is used to sign and authorize one or more intermediate certificates (IM CA-certificates) [375] and ultimately leaf (end entity) certificates. Both the identity certificate and its root CA-certificate, once used to sign subordinate certificates, can be placed in cold storage (i.e. offline) as a backup in case its antecedent CA-certificates become corrupted.

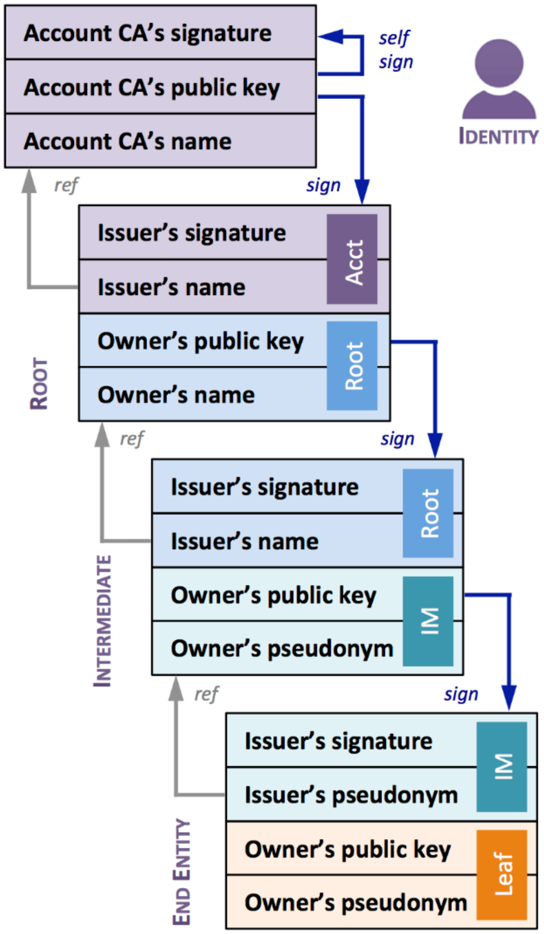


Fig.24: HyperSphere CA-certificate digitally signed trust-chain

A CA-certificate confirms ownership of a public key by the named subject of the certificate [376]. In the signing process, each certificate passes its public key to a subordinate, i.e. a would-be issuer, which in turn encrypts confidential info using the public key and returns it to the signing authority. Using its private key, the signing authority is able to decrypt the file, proving it alone is the owner of the public key.

The authority then signs the issuer's identity information with an encrypted version of its private key and passes it back to the issuer. The certificate issuer can in turn digitally sign subordinate certificates creating a chain-of-trust tracing back to the root and parent CA-certificates. In the HyperSphere, while the controlling certificates involve the identity of the account holder's identity, the IM and leaf certificates may use pseudonymous identities to further protect user privacy.

In addition to protecting personal privacy, CA-certificates also prevent fraud. All derivative CA-certificates sharing a common lineage from a parental certificate are useful only to the parent certificate owner's accounts and devices. Even if an account's login information is stolen, a thief will not be able to match the pedigree of the account holder's personal CA-certificate to their devices and accounts. In the case where the account owner and its signer cooperatively commit fraud, criminal investigation will invariably discover and expose the conspiratorial relationships through the irrevocable identity-trust-chain [377] [378].

As such, HyperSphere identity protects account security, transactional integrity, and personal privacy while thwarting criminality. In the HyperSphere, users are able to access identity-trust-chains to execute AAA verified [379] [380] transactions without added cost or delays. The term AAA refers to a process of 'Authentication, Authorization, and Administration' where (i) the certificate is first checked for a valid signature, (ii) the corresponding transaction process is approved for the confirmed user, and finally (iii) all relevant records are updated including, as applicable, appending new blocks onto a blockchain.

Together, the unique combination of network-generated CA-certificates, identity-validation, and digital signing using a hypersecure realization of public-key-infrastructure (PKI) cryptography [381] [382] [383] [384], establishes the HyperSphere as the pioneer of enterprise-grade CA-certificates deployed natively over a public cloud. In contrast, enterprise-level CA-certification over the Internet is both vulnerable and expensive, with costs of hundreds of dollars per certificate not uncommon. And because the Internet is unable to confirm the true origin of a CA-certificate, undetected Internet fraud is rampant with malware infections at epidemic levels. With its pioneering deployment as a hypersecure 'privacy' network, the HyperSphere protects personal identity and privacy by combining identity-trust-chains and verified CA-certificate lineage with digitally signed authentication of devices, HyperNodes, accounts, blockchains [385], transactions, and wallets. The privacy network's protection provisions operate in a myriad of ways, including:

- Pseudonymous identity of user HyperNodes based on a disaggregated HyperSphere name-server function, dynamically assigned to cryptographic identities via dynamic IP addresses and dynamic port numbers, to prevent account mapping,
- Personal network-generated CA-certificates for trusted dynamic signing of transactions for devices, HyperNodes, and HypWallets, thwarting imposter attacks, certificate fraud, and cryptocurrency theft,
- Session based certificate exchange using personal CA-certificate to secure session dialog and prevent eavesdropping,
- End-to-end encryption with identity-based private key exchange capability combined with decentralized session-based certificates [386] [387] to ensure personal privacy independent of SDNP cloud operations,
- Stateless HyperNodes not containing a record of calls, files, communiqués, or cryptocurrency transactions on the device or HyperNodes (cloud portals) to prevent forensic attacks and content reconstruction,
- A distributed network with fully decentralized control, where all transactions and data routing use private keys with no master key or system authority, preventing usurpation of the network electronically or through offline attacks of sysops or

other personnel,

- Individually owned multi-tree blockchains with limited access for cryptocurrency transactions and record keeping comprising dynamic directed acyclic graphs (DyDAGs) eliminating the risk of privacy leakage through observer backtracing a master blockchain,
- Transaction validation of replicant blockchain observer segments (RBOS), through a decentralized cloaked (unidentifiable) jury-of-peers with limited blockchain provenance access to prevent backtracing, fraud, blockchain attacks while insuring blockchain transactional integrity.
- Root recovery capability using a newly disclosed device, the sequential quantum key or (SQK) facilitating account restoration without exposing the identity-trust-chain to a malefactor's usurpation by online cyberattack.

To prevent illicit attempts to generate fraudulent certificates outside the HyperSphere, the network also facilitates system level certificate authority linking each user account to a group using digital signature credentials impossible to imitate, as they are network-native, generated and signed through system operations.

As depicted in **Figure 25**, for added privacy protections, intermediate CA-certificates can utilize multi-factor authentication using dual signatures, one from the owner's root certificate, and a second certificate from the system generated group certificate. In addition to preventing fraud, the second authentication facilitates added protection against conspiratorial malfeasance in business transactions.

In any event, the HyperSphere is not a good platform for criminals to practice their trade. Account information remains indefinitely discoverable by law enforcement vis-à-vis authorized jurisdictions under court order or by subpoena.

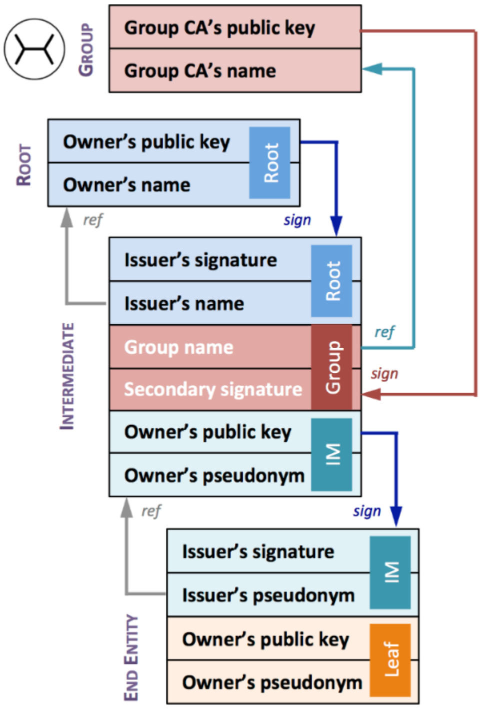


Fig.25: Multi-factor digitally signed HyperSphere CA-certificates

Likewise, while pseudonymous accounts are useful for engaging in legal confidential business, because of identity based ownership, in the HyperSphere they do not offer a conduit by which to subvert law or evade its agents.

In the HyperSphere all transfers from pseudonymous accounts to true identity accounts needed for banking are recorded on the blockchains [388] [389]. Another element of the HyperSphere is its novel use of topological trust networks. Although the foregoing methods rely on strong cryptographic defense using network-generated CA-certificates and identity-trust-chains not subject to fraud and theft, no system is immune to every attack. As such, the HyperSphere's architecture employs *topological trust networks*, or 'trust layering', to limit the potential damage of a successful intrusion into a person's accounts or devices– a security feature operating much the same way that fire doors prevent the rapid spread of fire to limit damage.

Figure 26 illustrates a hierarchical structure of the HyperSphere's topological trust network. The most secure portion, the security core, contains an account holder's identity based 'root certificate'. After it is used to generate 'intermediate' CA-certificates (not shown), the root certificate is stored offline in 'cold storage' such as a bank vault to prevent account usurpation. As a downside to its superior identity-based privacy protection, damaged or lost root CA-certificates may become permanently unrecoverable. To protect root CA-certificate privacy while insuring their recoverability, the HyperSphere employs a new cryptographic key, the sequential quantum key or (SQK), introduced herein for the first time.

SQK employs methods adapted from quantum physics, namely the quantum observer effect [390] [391], the process whereby observing a system changes its state. This effect includes quantum entanglement, the pairing of states where anything affecting one particle's state also impacts its entangled pair too. Although an SQK may eventually be realized using quantum electron devices, in the HyperSphere its quantum behavior can be emulated using multidimensional software realized across the HyperSphere's stratified virtual-network layers. For example, in one embodiment an SQK key's implementation comprises a number of key segments (cells), each of which contains an ASCII alphanumeric character. The SQK, comprising an encrypted version of a certificate access passcode includes both user-selected and system-generated components.

SQK decryption requires knowing an owner's passphrase and executing a read-write process in a precise order, i.e. reading, selecting and entering data into each segment in the proper sequence. Only when all the segments are viewed and modified in the proper read-write sequence will access to the root certificate recovery process be unlocked. Committing a single sequence misstep or entry error will result in a cascade of dead ends and meaningless challenge-response dialogs without revealing the entry has already failed. In this manner the misdirection consumes a hacker's CPU cycles wasting time, energy, and money. Without the proper read-write sequence, even knowing the passphrase is useless because the QSK is multidimensional, appearing at the HyperSphere user level as a cryptographic password having a different length than the passphrase.

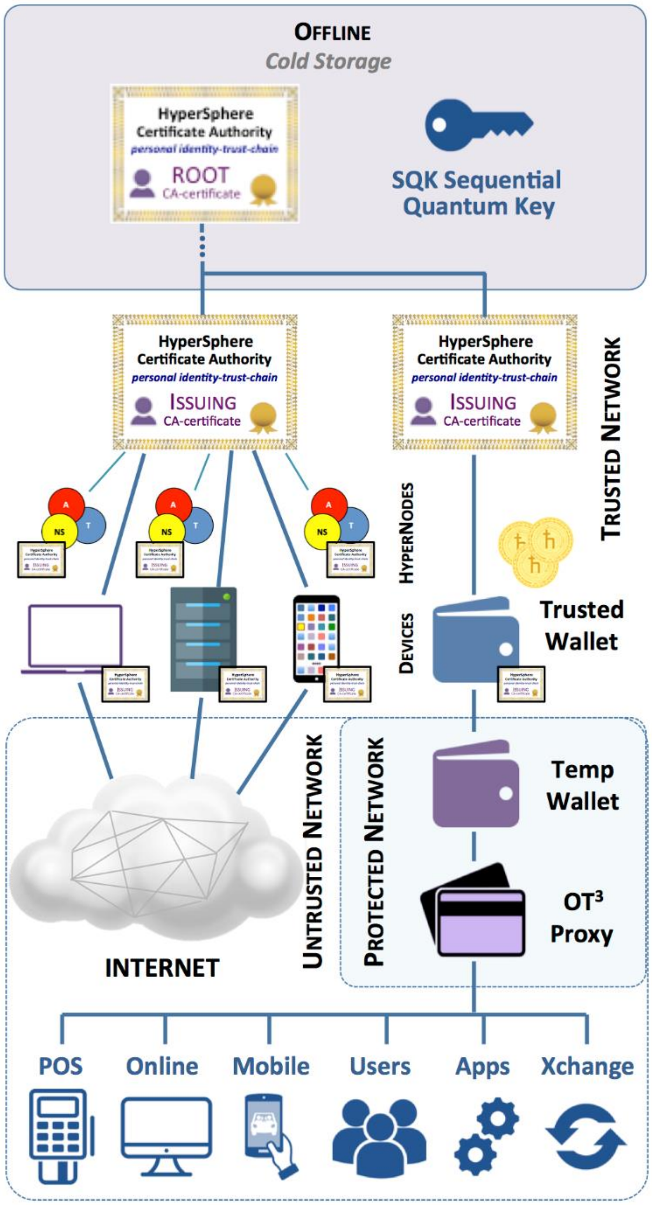


Fig.26: Topologically hierarchical trust networks in the HyperSphere

The missing pieces of the passphrase exist on at least three different virtual-network layers, appearing only if the proper sequence is entered. As such, the length of the SQK segment field length is variable, its appearance changing as entries are made or viewed. This variable key length feature makes it impossible for a cyber-attacker to guess how long of a passphrase they are looking for.

For example, if the entry field has a constant length of 16 segments and each segment may constitute one of 37 alphanumeric characters (26 letters, 10 ten numbers, 1 null entry), the odds against a successful single-dimension brute-force incursion skyrocket well beyond 10^{25}-to-one per virtual-network dimension used. If the passcode entry segment-length varies, however, the odds against discovering a successful passphrase using brute force attacks increase exponentially.

Operation of the SQK will be described in greater detail in a separate publication and in various patent applications pending and in preparation.

Returning to **Figure 26**, beyond offline storage (also known as air gap or DMZ security), the HyperSphere partitions its topological trust networks into three zones, namely trusted networks, protected networks, and untrusted networks. In trusted networks, the HyperSphere's network-native leaf CA-certificates are used to sign all network- connected devices and all installed HyperNodes. Even though the same devices may interact with untrusted networks such as company networks, university clouds, cybercafé subnets, or the Internet, the HyperSphere's symmetric sandboxing of HyperNodes prevents incursion or surveillance of the HyperContract execution.

A separate leaf certificate is also used to sign an account owner's trusted HypWallet holding cryptocurrency and other digital assets. This trusted asset does not, however, interact directly with the unprotected network of online and POS transactions, mobile and other applications, users or independent digital currency exchanges. Instead, all transactions are processed through a protected network comprising a temporary wallet separate from the user's personal trusted HypWallet. The temporary wallet in turn executes transactions with the one-time transaction token, the OT^3 proxy, preventing any access of vendors or users to a HyperSphere account holder's HypWallet or their blockchains. As such, the HyperSphere's built-in topological trust network protects both parties in a transaction from fraud and theft against third parties and also against one another.

3) Dynamic Directed Acyclic Graphs (DyDAGs)

Aside from the Internet's fundamental security flaws, cryptocurrency transactions over the Web are made vulnerable by reliance on a single communal blockchain accessible by everyone and anyone. In contrast, the HyperSphere eliminates the use of a common public blockchain altogether [392] [393], instead adapting multiple connected blockchains having personal identity-based ownership. To ensure transactional integrity through peer consensus, blockchain interconnectivity is facilitated using a multi-tree data structure best described as a directed acyclic graph or DAG, or 'digraph' [394].

The HyperSphere employs a novel variant of this DAG data structure used not only in its cryptocurrency generation, payments, and transfers, but also in its network operations, fragmented data transport, disaggregated data storage, and identity-trust-chains. To better understand how the DAG applies to HyperSpheric operations, we should first consider graph theory– the topological theory of the properties and applications of graphs. While in mathematics the term graph has several interpretations, in the broadest sense a graph is a collection of vertices and edges that join pairs of vertices. Applicable to a diverse range of disciplines including physics, biology, chemistry, electronics, computer science, topography, communications, commerce, and more, graphs provide topological insight into connectivity, relationship, hierarchy, and processes. One class of topologies, 'directed' graphs, is particularly well suited in describing processes, flows, and algorithms containing sequence information. Shown in various forms in **Figure 27**, directed graphs comprise graphs with vertices connected by edges employing vectors (arrows) signifying directionality [395] [396] [397] [398]. As depicted, a graph containing at least one graph cycle (a path of edges and vertices wherein a vertex is reachable from itself, i.e. a loop) is referred to a cyclic graph. In theoretical physics, an example of a cyclic process is a Carnot engine, a reversible isothermal gas expansion process (used to model the upper limit on the efficiency of thermodynamic engines converting heat into work). In each Carnot cycle temperature and entropy repeat the same loop, returning the system to its original state unchanged from the last cycle. In e-commerce, cyclic processes are problematic because they provide a means to change the past with no record of the change, affording the opportunity to commit undetected fraud and theft. For this reason, in accounting erroneous ledger entries cannot be changed, but instead must be amended as a new entry comprising a debit-credit pair recorded the date of the change.

Like traditional accounting ledgers, blockchains and DAGs comprise sequential records containing no 'cycles', meaning transactions proceed unidirectionally, never returning to the same vertex. Other examples of DAGs include ancestral family trees, epidemiological graphs of infectious disease spread from a single origin or index case, and computer malware diffusion, where each generation's antecedents are followed by their own progeny, and so on.

While it has been suggested on the Web that a blockchain and a DAG are distinct concepts– that a DAG is a new construct intrinsically superior to blockchains, a more accurate description is that a blockchain is a one-dimensional DAG comprising a single tree. In other words, a blockchain is the degenerate form of a DAG, a chain evolving in one dimension. DAGs can also exist in two dimensions: a blockchain with a single sidechain is the trivial case of a 2D DAG comprising a single common tree.

In graph vernacular, a tree comprises vertices connected to a common ancestor (indicated in the illustration by red colored vertices and edges). It follows that a 2D multi-tree DAG is simply a DAG containing multiple independent trees containing both common and distinct vertices. Conceptually, the advantage of multi-tree DAGs over a single-chain (1D DAG) blockchain is 'parallelism'– the ability to divide content and spread transactions across multiple 'interconnected' blockchains.

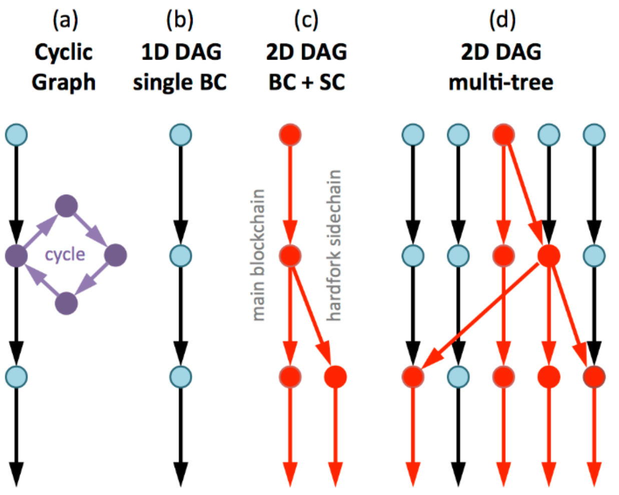


Fig.27: Various types of directed graphs (a) cyclic (b) 1D blockchain

(c) 2-D blockchain & sidechain (d) 2D multi-tree DAG

Compared to conventional blockchains, parallel processing offers the potential for improved transactional efficiency, shorter chain lengths, lower storage demands, and faster transaction processing. Converting a single communal blockchain into multiple interconnected blockchains, albeit a step in the right direction, does not alone fix today's cryptocurrency issues of blockchain technology.

Cryptocurrency's slavish reliance on nonce-hash puzzle solving remains fundamentally energy and time inefficient, irrespective of transactional processing efficiency improvements offered by DAGs. Furthermore, all cryptocurrency transactions over the Internet remain vulnerable to security and trust attacks including blockchain consensus exploits, privacy invasions, fraud, and cryptocurrency theft. Alone, converting cryptocurrency to DAGs cannot (and will not) prevent crypto-wallet theft and blockchain attacks. Only a holistic approach to security, privacy, and cryptoeconomic transactional integrity can possibly hope to overcome the Internet's ongoing epidemic of cyber-theft and fraud.

As described previously, the HyperSphere is based on state-based communication made in accordance with Secure Dynamic Network & Protocol technology, methods, and apparatus. In graph theory, this means that each time a HyperNode performs a task or executes a transaction the vertex's state at that moment is distinct in space and time. As such, the HyperSphere uniquely comprises a *spatiotemporal* network [399] [400] [401]. Accordingly, all transactions in the HyperSphere are dynamic and state-dependent, constantly changing in accordance with time and location.

In order to adapt the features of multi-tree DAGs to operate on a SDNP based dynamic spatiotemporal network, the HyperSphere employs a new graph topology, the *dynamic directed acyclic graph* or DyDAG, introduced here for the first time. In a DyDAG topology, vertices are defined by two characteristics– identity (vertex name or number), and state, symbolically as vertex v_x and state s_y. A state is the condition defining the rules by which the vertex operates and interacts with other vertices. In the HyperSphere, a vertex's state includes time, its resident security zone, and other location information. As such, revisiting the same vertex does not constitute a cyclic loop so long that the state is different.

For example, in the Carnot cycle each repeated loop is cyclic because whenever the system returns to a vertex, the state of the vertex is exactly the same as the prior cycle. In contrast, time travel in the sci-fi blockbuster "Back to the Future– Part II" is an example of acyclic spatiotemporal behavior. In the story, the characters Doc Brown and Marty McFly travel to the future in their DeLorean time machine [402] fully expecting nothing to change during their travels. Upon their return to their time and place of origin, to their chagrin they discover everything to be horrifically unfamiliar. Metaphorically, even though the vertex v_x was the same as before, the state s_y had changed unexpectedly. In this sense, the HyperSphere intentionally changes states constantly and in unexpected ways, confusing and confounding any cyber-hacker trying to discern a pattern.

As graphically represented in **Figure 28**, a DyDAG sequence comprising a transaction from (v_1, s_1) to (v_2, s_2) to (v_1, s_2) does not constitute a cyclic graph so long that the states $s_1 \neq s_2$. Although in a two-dimensional planar projection of a three-dimensional DyDAG the graph appears cyclic, in 3D the graph illustrated as a helix or spiral clearly shows the state-space is not cyclic or closed loop. In essence, the network autonomously exhibits a sequence of irrevocable changes with such rapidity it defies analysis. By including a state variable, a 2D multi-tree DAG becomes a 3D DyDAG blockchain of superior performance, integrity, and security. The HyperSphere applies this DyDAG principle is a number of ways in the HyperSphere including:

- Hypersecure SDNP communication using state-based security credential and algorithms.
- Data transport over a distributed network of active and redundant HyperNodes minimizing propagation delay while improving network resiliency (described below).
- Personal CA-certificate based identity-trust-chains used to chronicle the inclusion or revocation of HyperSphere connected devices and HyperNodes, thereby controlling access and privileges.
- Personal CA-certificate based identity-trust-chains used to sign and manage perpetual DyDAG blockchain transactions, RBOS observers, and OT^3 proxy payment processors.
- Personal CA-certificate based identity-trust-chains used to sign and manage perpetual DyDAG data in HypWallets.
- Transitory DyDAG blockchains ('tBC') used in HyperContract job execution of contract pledges, task execution, juror consensus, and token generation through minting or by melting and recycling (re-minting).

In regard to the use of a DyDAGs in network operation, the SDNP cloud intrinsically forms a dynamic DAG comprising four tiers of HyperNode resource providers. Nodes are added to the network based on the number of prospective minters wishing to earn cryptocurrency and by automatic node instantiation in the event of local network congestion or DoS attacks. In each instance, the more HyperNodes joining the network the more redundancy the cloud exhibits and the more efficient the network becomes in finding and using the shortest propagation delay paths for data routing.

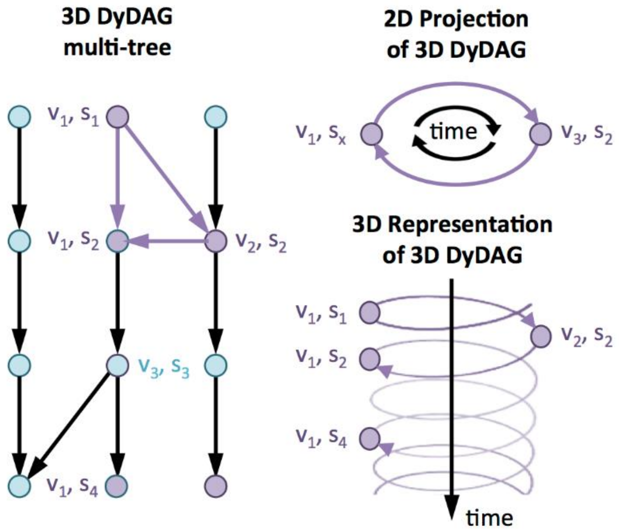


Fig.28: Dynamic directed acyclic graph (DyDAG) properties

In graph theory vernacular, SDNP network operation represents 'spatiotemporal destination-oriented dynamic directed acyclic graphs for meshed and multipath routing' [403] [404] [405] [406] [407]. Another benefit scaling with nodal density is resiliency, the ability of the network to maintain an acceptable level of QoS (quality of service) while surviving misconfigurations, faults, power failures, natural disasters, and attacks. The resilience of a network scales non-linearly with the number of participating nodes [408] [409] [410] [411] [412]. While theoretically the total number of combinational connections scales with the number of nodes n by the relation n•(n-1)/2 approaching n^2 for a large number of nodes, many of the connections are excluded as cyclic.

Although in a DyDAG reusing a node isn't truly cyclic (because the states differ), in realtime networks only short hop-counts are valuable in delivering low propagation delays [413] [414] [415] [416] [417] [418] and are also beneficial in achieving low routing power [419] [420] [421] [422] [423] [424] [425], especially important in mobile Last Mile connections. A representative model of a DAG describes the number of combinations "a" by a recurrence equation comprising k outflows (exiting edges) over 'n' nodes.

$$\mathrm{a_n} = \sum_{\mathrm{k}=1}^{n} n(-1)^{k-1} \binom{n}{\mathrm{k}} 2^{(n-k)} \mathrm{a_{n-k}}$$

In the binomial expression shown [396] [408], the number of available paths rises proportionally with the population of participating nodes in the network. Although the expression is more realistic than the idealized permutation population n•(n-1)/2, it does not embody certain features of dynamic DAGs. For example, cyclic loops excluded in a DAG may not be cyclic in a DyDAG because of state changes. Conversely, in nodes executing transactions at extremely high transaction rates, some nodes may (at least for brief intervals) behave as elements of a static DAG, whereby a number of possible loops (outflows) should be excluded from the tree population as cyclic. And although while *mathematically* speaking distant remote nodes comprise valid DyDAG trees, in realtime networks they must be excluded for their unacceptably long propagation delays (meaning they are so far away from the callers their participation in the network doesn't help transport at all). In other words, in a spatiotemporal DyDAG graph, the trees must be excluded.

4) Network-Native DyDAG Blockchains

To prevent the fraudulent generation and falsified validation of cryptocurrency, the HyperSphere does not employ mining to generate new coins. Instead of trusting an unknown miner and a potentially corruptible jury-of-peers to validate Proof-of-Work solutions of numerical and cryptographic puzzles, the HyperSphere synthesizes cryptocurrency through a reliable internal process executed by its network of HyperNodes. This generation method is not observable to outside observers or subject to packet sniffing and is unrelated to PoW nonce-hash puzzle solving. In its unique implementation, cryptocurrency generation occurs adjunctively as an intrinsic part of network operation during data transport in execution of HyperContracts without requiring additional energy or effort.

In operation, the HyperSphere utilizes multi-tree DyDAG blockchains to generate cryptocurrency and to record ownership. The DyDAGs may comprise 'perpetual' or 'transitory' blockchains depending on their purpose and application. *Perpetual blockchains* (BC) establish ownership by linking extant cryptocurrency to personal CA-certificates using an identity-trust-chain lineage derived from a corresponding parental certificate.

Transitory blockchains or 'tBC' are, in contrast, temporary distributed ledgers used to execute HyperContracts, synthesize cryptocurrency, and ratably apportion compensation to participating resource providers. Unlike the permanence of a perpetual blockchain, once the task of a transitory blockchain is completed its blockchain is destroyed. In this manner perpetual blockchains do not get burdened carrying unnecessary and irrelevant blocks of minutiae.

All cryptocurrency synthesis in the HyperSphere starts with a HyperContract, a business agreement between resource providers and their clients– service providers and merchants. Each HyperContract comprises a *job specification* and a *reward pledge* describing the compensation reserved for resource providers participating in the contract's successful execution.

The process of job execution contol is shown in **Figure 29**. As shown, vertical lines represent perpetual blockchain held by a HyperNode owner and signed by the owner's corresponding CA-certificate based identity-trust-chain. The roles of participating HyperNodes are represented by their metamorphic function performed, either as name server |NS|, authority |A|, or task |T| nodes for job execution, or authority |A| nodes participating as observers in jury-of-peer consensus.

Each participating node has DyDAG perpetual blockchain, shown as vertical lines to illustrate pledging and minting mechanisms. In the DyDAG matrix shown new blocks are appended onto these perpetual blockchain, in sequence ordered from top to bottom and time stamped accordingly. In the same illustration, horizontal arrows represent transitory blockchains tBC. Transitory blockchains are impermanent– executed sequentially, they modify perpetual blockchains and are subsequently discarded.

As depicted, the minting process of token generation occurs sequentially from top to bottom with tasks executed left to right. As listed in the order shown in the HyperContract, these processes involve the following milestones:

- HyperContract pledging at time t_{mp}
- HyperContract task execution over the duration Δt_t
- HyperContract consensus at time t_c
- Token minting at time t_g

In HyperContract pledging at time t_{mp}, the decentralized HyperSphere Marketplace successively concludes contract negotiation, at which time the merchant sponsor distributes the token pledges to the committed contract participants recording the pledge onto their blockchain as a pending transaction without actually transferring the tokens.

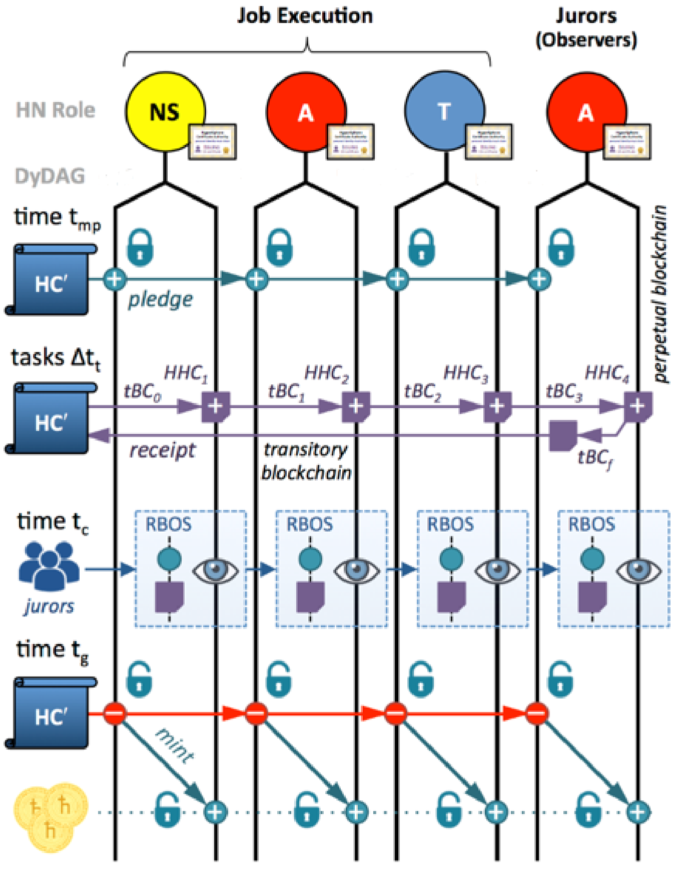


Fig.29: Job execution control

In this manner the pledge acts as a blockchain version of an escrow by locking the currency to prevent double spending [426]. HyperContract execution occurs over a period of time, i.e. during the interval Δt_t when the HyperNodes execute a series of tasks (or subtasks) in accordance with the HyperContract's job specification. During data transit and micro-task execution, each HyperNode is delivered a cryptographic receipt, a transitory blockchain containing a series of hashed blocks [427] [428] [429] [430] [431] [432] [433] [434] [435] containing *HyperNode hop codes* or HHCs of the HyperNodes before it.

As shown in **Figure 30**, HyperNodes autonomously generate these cryptographic codes as part of a data packet's SDNP based routing instructions. Upon completion of their work each HyperNode adds its own cryptographic block to the transitory blockchain. The HyperNode then forwards the new longer blockchain onward to the next node, which in turn repeats the process. In this manner, each HyperNode has irrefutable evidence of its participation. For example, task node |T| receives transitory blockchain tBC_2, the hash of HHC_2 then forwards the revised transitory blockchain tBC_3 onto the next HyperNode. As such each HyperNode knows the plaintext value of its HHC but only the hash of the incoming tBC. In this manner, a string of unfakable self-consistent blocks is generated excluding the possibility of imposters.

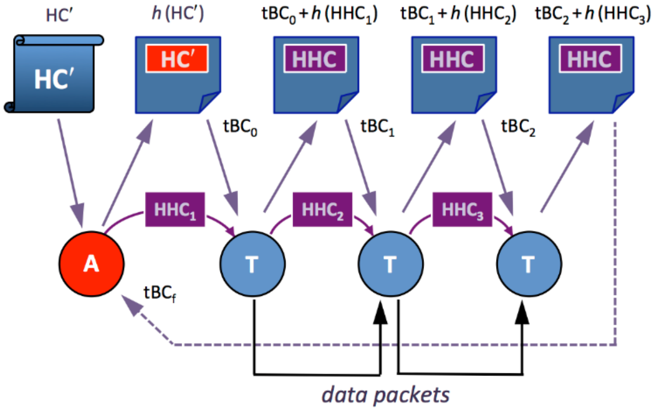


Fig.30: HyperContract transitory DyDAG blockchain and HyperNode hop code (HHC) generation

Expressed algebraically in terms of SDNP network generated HyperNode hop codes HHCj and cryptographic hash function *h* (HHCj) then:

$$\mathrm{tBC}_j = h(\mathrm{HHC}_j) + \mathrm{tBC}_{j-1}$$

In this process, the HyperContract itself forms the initial block of a transitory blockchain used in HyperContract execution, or $\mathrm{tBC}_0 = h$ (HC′). As data packets pass through HyperNodes in succession, a copy of the transient blockchain tBC_j is deposited, i.e. written onto the HyperNode's token blockchain with the transient blockchain growing in length as the job is executed. Upon reaching the terminus node, the final full-length transitory blockchain tBC_f is returned to the HyperContract initiator to confirm task completion. The full-length tBCf blockchain is concurrently forwarded to the jury-of peers specified in the HyperContract for checking.

At time t_c, consensus by a jury-of-peers confirms contract execution using a RBOS (replicant blockchain observer segment) to facilitate inspection without the possibility of backtracing. Upon confirmation of HyperContract completion, peer review, and consensus, every participating HyperNode owner is awarded compensation according to their contribution using a copy of the transitory blockchain establishing, i.e. 'proving' their performance. Once confirmed, the tokens are automatically converted, i.e. *minted*, and recorded into the HyperNode owner's perpetual blockchain.

Cryptocurrency synthesis where participating nodes prove their contribution in performing real tasks is referred to as *Proof-of-Performance* or PoP. Upon proving a HyperNode's performance at time t_g the tokes are unlocked and a new code is generated containing a hash of the tokens pledge and the transitory blockchain proving a valid peer-reviewed origination. Graphically the minting process is depicted as an unlocking and a debit from the left vertical line and a credit onto the right one. Tokens, once minted, may be converted to international fiat currency or used in the HyperSphere to solicit resources, a process equivalent to recycling.

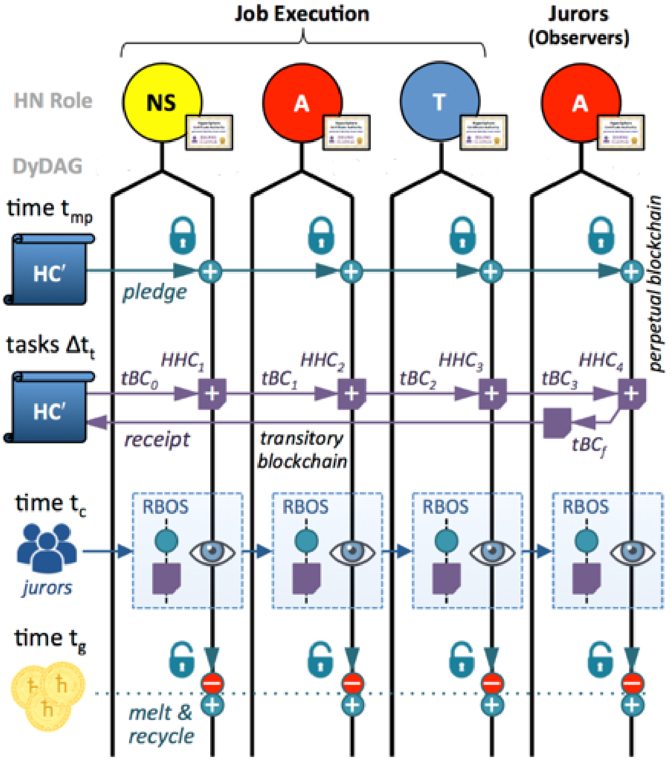


Fig.31: Token melting and recycling (re-minting)

In mechanics shown in **Figure 31**, a HyperContract makes melt and recycling simultaneously. The pledge is recorded on the HyperNode's perpetual blockchain as a pending transaction (without actually transferring the tokens). Locking the tokens into a digital escrow at the time of contract negotiation is important to prevent double spending, especially since the tokens are fungible and tradable as a liquid asset.

Task execution and juror consensus for recycling contract execution occurs in the same manner as a minting contract, except at the time of contract completion t_g when new tokens are generated. In the recycling process, the cryptographic identities of the original pledged tokens are destroyed, in HyperSphere taxonomy "melted" then re-minted as new tokens with new digital identities (depicted as a debit and concurrent credit on the perpetual blockchain).

Like newly minted cryptocurrency, recycled tokens employ a digital identity based on a cryptographic hash values *h* (x) derived from a transient tBC of HyperNode hop codes HHCj and the original HyperContract tokens. The HyperSphere's recycling process is entropic (lossy), not conservative, as the quantity of generated tokens re-minted by HyperNodes is less than the number of tokens pledged in the HyperContract, $\#\text{Tokens}_{\text{new}} < \#\text{Tokens}_{\text{pledge}}$, naturally reducing the number of tokens in circulation by reuse attrition.

5) Other HyperSphere Uniquities

Unlike in cryptocurrency mining, which only pays miners lucky enough to solve an arduous puzzle before others can, in Proof-of-Performance all HyperNodes participating in a successful HyperContract execution receive a contractually guaranteed return as minters. And because it occurs adjunctively with SDNP network operation, minting and recycling tokens essentially consumes no more electrical energy than performing communication or e-commerce itself. In essence, HyperSpheric cryptocurrency synthesis wastes virtually no energy at all. To fully appreciate cryptocurrency generation and transactional processing in the HyperSphere and how these processes differ from Bitcoin, Ethereum, and conventional blockchain applications, it is insightful to consider a device's system architecture.

As shown in **Figure 32**, a computer or communication device supports software applications using an 'operating system' (OS) such as Windows, MacOS, Linux, Android or iOS. The operating system is hosted on a platform comprising hardware and drivers typically including multiple CPUs, memory, and device connections [436] [437]. An operating 'kernel' provides resource scheduling and task management for the OS acting an interface [438], i.e. a liaison [439] between the hardware and an applications environment (referred to here as an 'application habitat' to avoid ambiguity). The application habitat hosts a variety of software including APIs, UI/UX, database, business, email, VoIP-messengers, remote access gateways, IoT, Web apps, and more. Most apps today are network enabled, facilitating Internet-of-Everything (IoE) connectivity [440] [441]. As depicted, the operating kernel interacts directly with both the application habitat and the underlying hardware platform. The kernel also interacts with the communication protocol stack, especially via Application Layer-7, and at layer 1.5 (the interfacial quasi-layer existing between PHY Layer-1 and Data Link Layer-2).

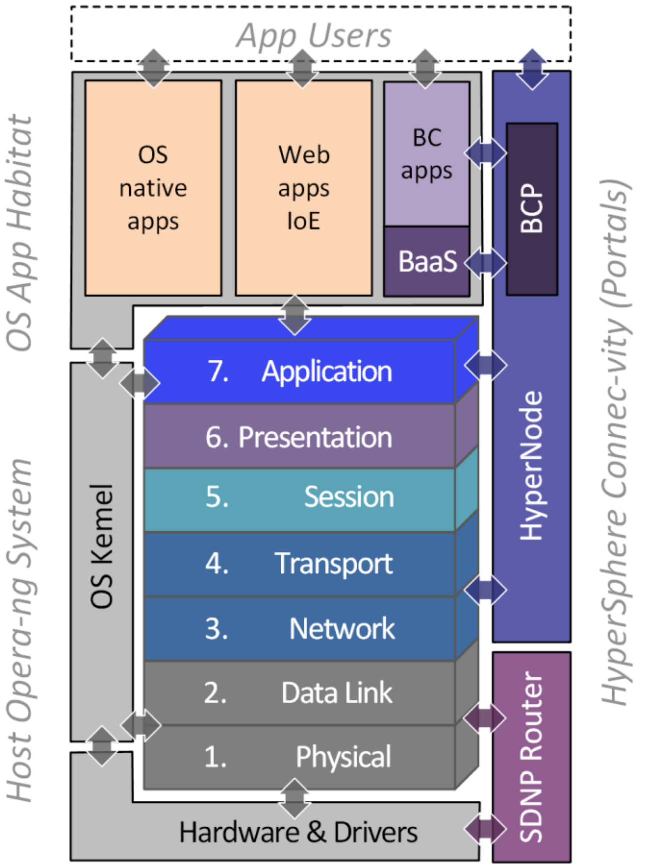


Fig.32: Device architecture illustrating interconnects among host operating system, apps, SDNP protocol stack, HyperNodes, and connectivity via a SDNP enabled router (optional)

In operation, signals received by PHY Layer-1 are passed up to Layer-2 and concurrently transferred to the OS kernel for job scheduling. In turn, the kernel schedules tasks through its interaction with Application Layer-7 to support software running atop the device OS (in the application habitat). In this mechanistic explanation, it is insightful to distinguish the primary communication role of Application Layer-7 (in the SDNP or TCP/IP protocol stack) from the functions of computer application programs (running within the OS's application environs). Specifically, Application Layer-7 data packets provide high-level network connectivity to specific applications but are incapable of operating independently from the OS-hosted applications.

In that sense the application habitat sits atop the OSI protocol stack immediately above Application Layer-7. In the parlance of layers of abstraction, Application Layer-7 supports software running in the application habitat above it and the software relies on Layer-7 supplied information for support. To function, the software and the data packet payloads must match in type, syntax, version, etc. For example, without database software installed on a device, SQL instructions received on Layer-7 will go unrecognized and unanswered.

Data packets carrying Hypertext Transfer Protocol (HTTP) content for distributed, collaborative, and hypermedia information over the Web is completely useless without a browser application able to interpret HTML or XML. Similarly, in conventional cryptocurrency blockchain transactions received as Layer-7 payloads cannot modify or append new blocks onto an existing blockchain without corresponding application support. All conventional blockchain and cryptocurrency transactions occur entirely within the app habitat of the host OS, not part of the protocol stack.

As a network portal to the HyperSphere, HyperNodes span the SDNP protocol stack and OS app habitat, communicating directly with the Network & Transport Layers-3 and -4, with SDNP Application Layer-7, and with its API and UI/UX in the OS apps habitat. In blockchain processing, the HyperSphere is wholly unique, generating HHC cryptographic HyperNode hop codes as part of Network Layer-3 and using this information in a blockchain processor or 'BCP', a network-connected software engine used in blockchain generation and transactional processes. The BCP then supports blockchain apps including BaaS (Blockchain as a Service) and various blockchain apps. Although BCP, BaaS, and BC apps are used to facilitate token transactions, the processing engines can also be employed as a service to HyperSphere users creating custom cryptocurrencies or tokenization of service provider businesses.

The HyperSphere's multi-layer cryptocurrency generation is entirely unique and easily distinguished by conventional blockchains processed entirely as an application running in the OS app-habitat above Layer-7 in the OSI protocol stack. For this (and innumerable other reasons), it is more accurate to refer to such conventional blockchain processors as "apps" rather than 'protocols' or 'networks' [442] [443] [444] [445]. The HyperSphere's BCP blockchain processor, in contrast, can truly be considered a protocol because it exists as part of the SDNP protocol stack, i.e. operating as a network-native operation both in minting new cryptocurrencies or when conducting e-commerce transactions.

Semantics aside, because BCP operation is HyperSphere network-native, blockchain processing is rapid– limited only by the speed of peer consensus rates for transactional validation. Despite its rapid process capabilities, the HyperSphere's cryptocurrencies are difficult to counterfeit because they employ cryptographic hop codes unique to SDNP network operation not observable from the OSI Session, Presentation, or Application Layers 5, 6 and 7. These codes include a combination of HyperContract information (including the hash of the pledge and a timestamp) and their own unique sequence of HyperNode hop codes.

Moreover, because of its purely internal coin generation and a cloaked (undisclosed) jury-of-peers, cryptocurrency counterfeiters are unable to match or predict network-generated blockchain content. Aside from its network-native blockchain processing and short-length DyDAG blockchains, another method to improve transactional speed involves the unique use of blockchain defragmentation. In a manner similar to defragging a hard disk drive (HDD), in the process of *blockchain defragmentation* available cryptocurrency is copied to the end of the blockchain at some regular schedule, e.g. at the end of every transaction or every day. By re-locating liquid currency near the bottom of the DyDAG blockchain, subsequent transactional verification requires only very short RBOS segments for confirmation, speeding validation and preventing backtracing altogether.

As depicted in **Figure 33**, during blockchain processing new blockchains are appended only to the end of the chain regardless as to whether they constitute a credit or a debit of assets. Blockchain assets are processed using a Last Iin First Out (LIFO) process, where the last acquired coins are used first to minimize transaction time. As shown, at time t2 currency added at time t1 is consumed. At time t3 an even earlier deposit must be found and confirmed to facilitate a current debit. At time t6, the asset needed to fund a current liability could involve identifying a deposit from far in the past, i.e. comprising a fragmented transaction resulting in a long RBOS and slow transaction resolution.

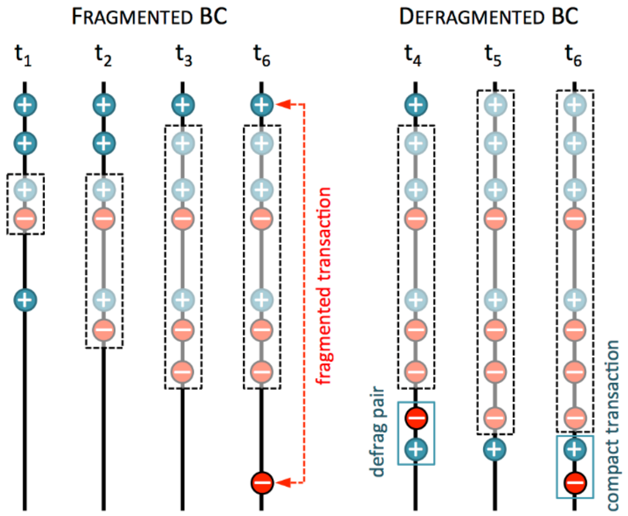


Fig.33: Defragmentation of blockchain speeds transaction rates by eliminating stranded assets via appending a credit-debit pair to BC end.

The solution to this conundrum is to clean up the blockchain "as you go" meaning to remove defragmented assets at a convenient time when other transactions are not occurring, and speed is not critical. The defrag process shown in the sequence from times t4 to t6 involves identifying stranded assets and relocating these assets to the end of the blockchain. Since added blocks are permanent, there is no means by which to change an earlier entry.

Instead, the BC defrag process involves adding "zero" to the blockchain, by recording a debit-credit pair as shown at time t_4. During validation the new debit will cancel the earlier deposit resulting a new asset relocated to the end of the chain as shown at time t_2. Then when a payment is made at time t6, the asset is already located at the end of the blockchain and a compact rapid transaction can occur. Another element of blockchain management is the use of auxiliary blockchains. While in communal blockchain arbitrary files are appended onto the main blockchain, with the HyperSphere's use of DyDAG blockchains as shown in **Figure 34**, content can be implemented as an auxiliary sidechain without disturbing the integrity of the main blockchain.

Without the ability to write arbitrary blocks onto the main blockchain, users are prevented from contaminating transactional blockchains with objectionable or illegal content. Instead the main blockchain records only a pointer linking it to an auxiliary blockchain, supporting entries other than cryptocurrency transactions useful for documentation purposes. If the documentation supports a transaction, such content can be included in an RBOS validation check by independent jurors.

Once the sidechain is complete, it terminates and records a second entry on the main blockchain establishing a firm chronology of events without recording the actual content. Because the second entry occurs at a different dynamic state, the DyDAG sidechain does not form a cyclic loop. The same auxiliary sidechain mechanism can be used for documentation unrelated to cryptographic transactions and can even be used to invoke subroutine calls of executable code via BC apps.

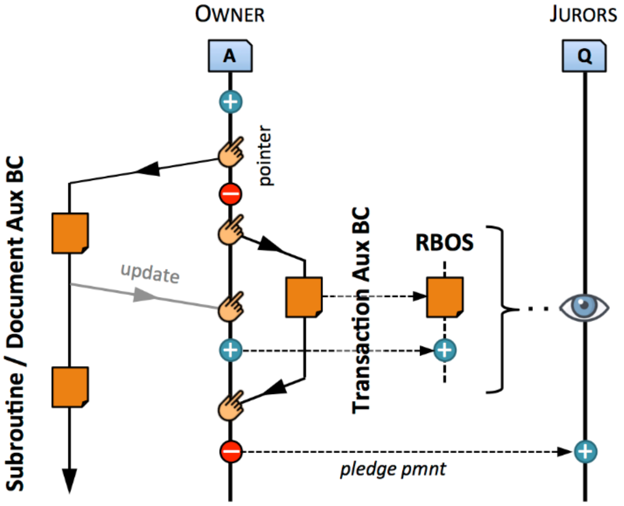


Fig.34: Auxiliary DyDAG blockchains for transactional documentation and sub-routine calls including RBOS juror validation

These processes may optionally record updates as to a subroutine's process status on the main blockchain while perpetually maintaining processes in parallel to the spatiotemporal state of the blockchain, thereby enabling the prospect of executing a *Turing complete* process (see Glossary). Another unique feature of the HyperSphere is its ability to establish *ad hoc* tunneling communication, i.e. dynamic single-hop VPNs, between a HyperNode source portal and a remote portal. The purpose of these private tunnels is to divert traffic away from subnets suffering QoS degradation from congestion and to avert cyberattacks on the network [446] [447] or on blockchain transactions such as DoS or Sybil attacks. The method can also be used to ensure hypersecure communication over uncontrolled Last Mile links.

As shown in **Figure 35**, once a HyperNode inter-portal tunnel is established data can flow using direct routing to the remote portal unprocessed by intermediate nodes, much like an express train passes through local train stops without stopping (or even slowing down). Application of HyperNode tunnel communication is especially valuable in repelling cyber-assaults. For example, in the event of a rapid rise in localized network congestion where a denial-of-service-attack is suspected, the node under attack can temporarily suspend incoming packet support (or optionally open a queue buffer), establish a tunnel beyond the reach of attacked device or subnet, then reestablish all ongoing sessions redirecting traffic to and from the remote portal.

While this response methodology won't prevent DoS from delaying the establishment of new incoming calls and sessions, it allows the surrounded node to establish open new links to safety on a priority basis, even when the source is surrounded by botnets. Because botnets lack the dynamic security credential to interpret the SDNP protocol, they cannot trace the location of a remote HyperNode portal. HyperNode tunneling is especially valuable in protecting cryptocurrency transactions to avoid blockchain attacks such as Sybil, 51%, and DoS methods.

By specifying cloaked jurors in a HyperContract, the transacting parties are unaware of which HyperNodes are performing asset and transaction consensus validation. Moreover, by connecting to cloaked jurors through a HyperNode tunnel, their inter-portal communication is privileged and not subject to metadata surveillance and hacking by other network nodes. HyperNode tunneling is automatically executed by any HyperNode seeking exceptional transactional security or upon detecting a DoS assault. Once an attack is detected, tunnel traffic is assigned priority over all local traffic. Ongoing sessions are reinitiated through the remote node without any knowledge of the botnet attackers

The HyperSphere also supports tunneling executed on an end-to-end basis. Unlike inter-portal tunneling, in end-to-end tunneling the communicating parties exchange cryptographic keys prior to and unrelated to the opening of a session or placing a call. Ideally, the keys can be exchanged between two devices in person without ever employing an intervening network. The application of end-to-end encryption facilitates personal privacy in the HyperSphere independently from the SDNP's security protocols.

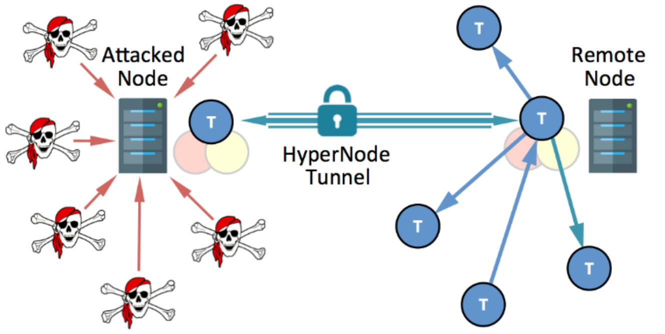


Fig.35: SDNP inter-portal HyperNode tunneling to avert network congestion and repel DoS and BC consensus attacks

6) *HyperSphere Development Support*

Users can address the HyperSphere in several ways, namely:

- Application Programming Interfaces (APIs) – APIs are developed by merchants and service providers in order to support their clients with products and services. APIs operate on SDNP protocol Application Layer-7 and in a host device's OS application domain.
- HyperNode portals – HyperNodes are preconfigured portals

used by resource providers to earn embedded tokens by delivering services to merchants and service providers. HyperNodes operate at multiple levels of the SDNP protocol stack raging from the Network Layer-3 to Application Layer-7 and in a host device's OS application domain.

- HyperSpots – HyperSpots are hardware platforms specifically designed as HyperSphere network hosts for HyperNodes, generally optimized for embedded tokens minting by providing resources for cloud-based communication nodes, cloud-based computing nodes, and disaggregated data storage nodes. HyperSpots operate primarily on PHY Layer-1 and Data Link Layer-2, but support HyperNodes operating from Network Layer-3 and up.

In order to support open source development of the foregoing, the HyperSphere offers SDKs (source development kits) and a variety of pre-coded software service routines and utilities. Such system software, certified by the HyperSphere Development Corporation and signed by system-native CA-certificates, perform a variety of services and functions. HyperSphere utility library programs may include the following functions:

- HyperNode installation and signing service
- API starter template
- Device registration and signing service
- Account creation utility with CA-certificate generation
- Wallet creation utility and signing service
- Consensus validation service
- RBOS transaction validation service
- OTP3 one-time transaction token proxy service
- HyperNode tunnel protocol service
- SQK sequential quantum key registration service
- Auxiliary sidechain editor utility
- Blockchain defrag utility

As detailed, HyperSpheric services are not simply software programs, but include network connectivity without which the functions will not be authorized or executed. In other words, stealing a device may give a criminal access to program code, but does not give them access to confidential security credentials needed to access records and activate programs. Cloning a device also will fail to penetrate the HyperSphere's network privacy provision.

7) HyperSphere Global Intellectual Property

The HyperSphere's technology contains a considerable portfolio of intellectual property including utility patent applications, use trademarks, copyrights, and trade secrets. Patents are divided into several sets of multi-invention application filings (including US, PCT, Taiwan, and foreign counterparts), comprising the following:

- Secure Dynamic Network and Protocol, *US patent app US14/803869*, filed 20 Jul 2015, priority date 26 Jan 2015, 377 pages as issued, *US patent number* 9,998,434 on 12 Jun 2018 [330]
- Secure Dynamic Network and Protocol, 584 pages as filed, *Taiwan application 105102426*, filed 23 May 2015, priority date 26 Jan 2015 [448]
- Secure Dynamic Network and Protocol, 584 pages, *PCT application PCT/US16/14643,* WPO foreign counterparts filed in Australia, Brazil, Canada, Europe, India, Indonesia, Israel, Japan, Korea, Russia, Singapore, South Africa, and Ukraine [449]
- Secure Dynamic Network and Protocol, *continuation patent 15/946863*, filed 6 Apr 2018, priority date 26 Jan 2015 [340]
- Methods and Apparatus for HyperSecure Last Mile Communication, 584 pages, *US patent app 15/943418*, filed 2 Apr 2018, priority date 3 Apr 2017 [342]
- System For Open Source Decentralized Electronic Communication and E-Commerce, *US provisional application 62625220*, filed 1 Feb 2018, patent application in preparation [343]
- The HyperSphere– a Real-time Cybersecure Privacy Network with Embedded DyDAG Dual Cryptocurrency for Global e-commerce, *US prov patent app 62/696160*, filed 10 Jul 2018, patent application in preparation [344]

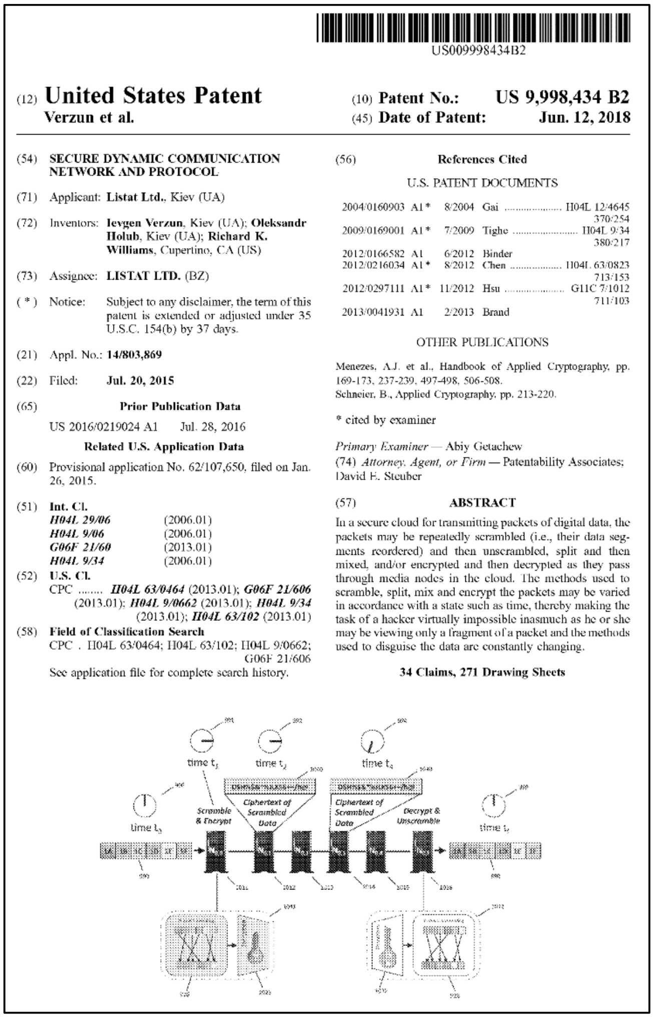
Figure 36 illustrates the HyperSphere's first issued patent, the Secure Dynamic Network and Protocol, US patent number 9,998,434, issued 12 Jun 2018 with 35 granted claims. Created under contractual IP engineering and development agreements, all relevant patents are irrevocably licensed to the HyperSphere IPBank for unrestricted use by HyperSphere service providers, merchants and resource providers exclusively within the HyperSphere ("HyperSphere IP").

Except by special license made available to professional communication private networks, unlicensed use of HyperSphere IP outside of the HyperSphere is strictly prohibited. No license shall be granted for deployment of HyperSphere IP as public networks or systems competing with the HyperSphere and its services.

8) Innovation's Impact on Network Vulnerability

Since the advent of modern physics, disruptive innovations [450] [451] have occurred at a rapid and ever-accelerating pace. In little more than a century, human technological innovation has witnessed the discovery and the development of radio communication [452], the transistor [453] [454], the integrated circuit [455], the microprocessor [456] and the personal computer [457], the Internet [458], the Web [459], and more recently the blockchain and cryptocurrency [460]. In the case of such disruptive innovations, the driver of technological innovation is not purely academic nor is it solely economic.

Instead, as characterized by repeated cycles of *invention*, *adoptio*n, *adaptation*, and *re-investment*, each discovery drives a cycle of engineering development and subsequent commercialization, resulting in economic expansion (commercial and market adaptation), and ultimately funding a new phase of research, discovery, and invention. During economic expansion of any burgeoning new tech industry, opportunity attracts participation across the entire socio-economic spectrum including those motivated by commercial, altruistic, as well as nefarious purposes. New technology invariably, however, creates opportunity for mischief, villainy, and malefaction.



US009998434B2

(12) **United States Patent**
Verzun et al.

(10) **Patent No.: US 9,998,434 B2**
(45) **Date of Patent: Jun. 12, 2018**

(54) **SECURE DYNAMIC COMMUNICATION NETWORK AND PROTOCOL**

(71) Applicant: **Listat Ltd.**, Kiev (UA)

(72) Inventors: **Ievgen Verzun**, Kiev (UA); **Oleksandr Holub**, Kiev (UA); **Richard K. Williams**, Cupertino, CA (US)

(73) Assignee: **LISTAT LTD.** (BZ)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 37 days.

(21) Appl. No.: **14/803,869**

(22) Filed: **Jul. 20, 2015**

(65) **Prior Publication Data**

US 2016/0219024 A1 Jul. 28, 2016

Related U.S. Application Data

(60) Provisional application No. 62/107,650, filed on Jan. 26, 2015.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 9/06	(2006.01)
G06F 21/60	(2013.01)
H04L 9/34	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0464*** (2013.01); ***G06F 21/606*** (2013.01); ***H04L 9/0662*** (2013.01); ***H04L 9/34*** (2013.01); ***H04L 63/102*** (2013.01)

(58) **Field of Classification Search**
CPC . H04L 63/0464; H04L 63/102; H04L 9/0662; G06F 21/606
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2004/0160903	A1*	8/2004	Gai	H04L 12/4645 370/254
2009/0169001	A1*	7/2009	Tighe	H04L 9/34 380/217
2012/0166582	A1	6/2012	Binder	
2012/0216034	A1*	8/2012	Chen	H04L 63/0823 713/153
2012/0297111	A1*	11/2012	Hsu	G11C 7/1012 711/103
2013/0041931	A1	2/2013	Brand	

OTHER PUBLICATIONS

Menezes, A.J. et al., Handbook of Applied Cryptography, pp. 169-173, 237-239, 497-498, 506-508.
Schneier, B., Applied Cryptography, pp. 213-220.

* cited by examiner

Primary Examiner — Abiy Getachew
(74) *Attorney, Agent, or Firm* — Patentability Associates; David E. Steuber

(57) **ABSTRACT**

In a secure cloud for transmitting packets of digital data, the packets may be repeatedly scrambled (i.e., their data segments reordered) and then unscrambled, split and then mixed, and/or encrypted and then decrypted as they pass through media nodes in the cloud. The methods used to scramble, split, mix and encrypt the packets may be varied in accordance with a state such as time, thereby making the task of a hacker virtually impossible inasmuch as he or she may be viewing only a fragment of a packet and the methods used to disguise the data are constantly changing.

34 Claims, 271 Drawing Sheets

Fig.36: Cover sheet of 12 Jun 2018 issued SDNP patent 9,998,434

Aside from banking, no industry has been subjected to criminality, fraud, and theft to the degree that the network communications and computing industry experiences. Almost as quickly as a new network technology goes live, hackers start finding ways to attack and subvert it [461] [462] [463] [464] [465] [466] [467]. In self-preservation, network operators necessarily turned to cryptography [468] [469] [470] [471] [472] in an attempt to secure transactions, and developed cybersecurity mechanics to recognize and detect threats, to mitigate attacks, and as a last resort, to at least contain or limit cyber-attack damages [473] [474] [475] [476] [477]. Recently, the cybersecurity industry has been further pressured to protect against both criminal and unethical 'commercial' personal privacy invasions [478] [479] [480] [481].

Unfortunately, an overreliance on cryptography has proven to be the Internet's proverbial Achilles heel, allowing hackers to pool resources to devise new attack stratagems. Moreover, privacy protection on the Internet has been especially problematic given the nearly total absence of identity and privacy provisions built into the TCP/IP protocol stack (aside from SSL/TLS). Given these pre-existing risks, the advent of new technologies and innovations can profoundly impact Internet security, privacy, and transactional integrity.

The potential impact of quantum communication and quantum computing on security and privacy is especially profound. For example, in cryptography (on which today's Internet's security wholly depends), the impact of quantum computing [482] [483] has uncertain implications– massive increases in compute-power should enable cryptographers to deploy more sophisticated cyphers (enhancing security) but likewise provide hackers with the computational prowess to launch equally sophisticated brute force attacks (degrading security).

The future of quantum communication is equally compelling [484] [485] [486] [487] [488] including the prospect of enhancing security by harnessing quantum-based deterministic properties [489] [490] [491]. But like quantum cryptography, new communications methods may engender new means by which to hack the PHY physical connection or its corresponding data link. In short, there is no way to project the impact of quantum technology on cryptography, computing, and communication.

And despite beliefs to the contrary [492] [493] [494], simply converting Internet-based blockchain transactions from a shared public communal blockchain to multiple parallel DAGs will not inoculate cryptocurrency transactions from attack. Although potentially beneficial in improving transaction performance rates [495] [496] from parallel processing, a multi-tree DAG implemented over the Internet is not (as purported) an entirely new topological concept in distributed ledgers [497] [498], but simply the interconnection of multiple, albeit shorter, blockchains in a parallel structure.

If static cryptography is unable to prevent exploits against a single blockchain, the same vulnerabilities will persist when paralleling multiple blockchains. In essence, a DAG processed over a static network is not sufficient to prevent blockchain attacks because the Internet's underlying communication technology used to process the transactions online is fundamentally vulnerable. In general, the development of any new technological innovation such as quantum computing [499] creates parallel opportunities both to enhance but also to disrupt cybersecurity reliant on the same technology.

In contrast, the HyperSphere employs multidimensional security offering greater resilience to vulnerabilities arising from technological innovation simply because it doesn't rely on a single technology or a predictable channel of communication for transactional and task execution. Multidimensional properties include the following:

- Using quantum computing for brute force code breaking of a data packet is rendered meaningless by the incomplete data contained within the packet lacking of metadata useful in identifying related datagrams in a sea of network traffic.
- Using quantum computing for brute force code breaking of a data packet doesn't help in decrypting other data packets since security credentials and concealment algorithms are dynamic, changing faster than they can be broken.
- The HyperSphere's metamorphic HyperNode's are stateless,

meaning they forget what they have done immediately after they execute any task leaving no record to inspect.

- Data transport occurs over a meshed network, secured on a hop-by-hop basis using dynamic concealment methods, meaning there are no master keys able to inspect data traffic, content, or even metadata.
- Since routing is dynamic, traveling through the network at near the speed of light, a hacker's intervention (also traveling at the same speed) can never catch the packet it is chasing. By the time the hacker's packet arrives at a HyperNode, the state of the DyDAG meshed routing has changed, metaphorically it's like reading yesterday's weather report.
- The application of DyDAG transitory blockchains (tBC) in HyperContract execution are stateless– destroyed after each task is completed, so supercomputing cannot be used to break a record that has already been destroyed.
- DyDAG perpetual blockchains (BC) are privacy protected by a multi-tree identity-trust-chain using pseudonymous identities, meaning no means exists to link the pseudonymous owner to their true identity CA-certificate.

In general, the HyperSphere employs time and state-based dynamic changes in its network operations, packet transport, and security credentials to greatly reduce the probability of a successful intrusion into the SDNP spatiotemporal meshed network or against HyperSpheric transactional processing. This does not mean that any given datagram might not be code-broken, but that the damage of the attack is limited because of the packet's limited content, short lifespan, and lack of contextual metadata.

IV. HyperSphere Markets & Applications

As a global network and cloud-based computing platform, the HyperSphere supports a wide range of services and functions creating economic value and enabling e-commerce. Markets, applications, and e-commerce supported by the HyperSphere include:

- Realtime communication,
- Distributed computing,
- Disaggregated data & cloud storage,
- Secure cloud-connected devices (IoT, V2X),
- e-Services, *and*
- Artificial intelligence (AI)

A) HyperSphere Realtime Cloud Communication

The dynamic routing capability of the Secure Dynamic Network & Protocol enables the HyperSphere to support the full range of electronic communication including telephony, VoIP, text messaging, live video, conference calls, audio and video content streaming, email, professional communication, Professional Mobile Radio connectivity, security networks, and control grids. Benefits include hypersecure communication, identity-trust-chain based privacy, low-propagation delay routing, low latency, redundant connectivity, and cost-performance optimization capability.

Unlike conventional networks, data traffic routing over the HyperSphere dynamically adapts for local network congestion and outages. Comprising a hybrid heterogeneous network of fixed backhaul (using 1st Tier resources), on-demand dark fiber, third-party ISPs, and dynamic peer-to-peer connectivity, network performance actually improves (rather than degrades) with the number of HyperSphere users– more HyperNodes improves the number of connections and DyDAG network resiliency.

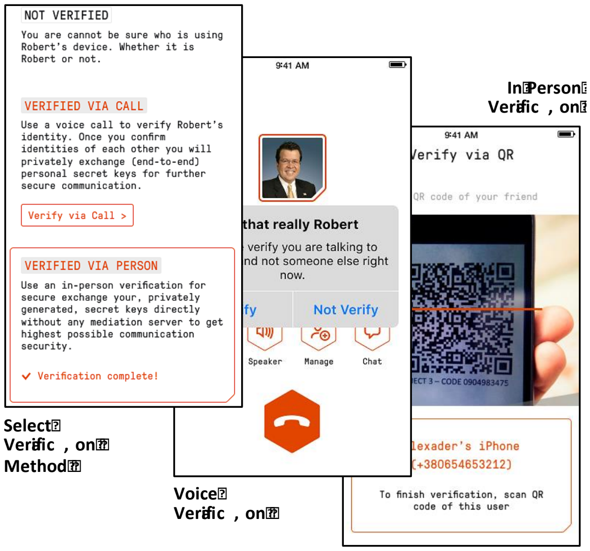
Another benefit of the HyperSphere in communication is its embedded cryptoeconomics. HyperNode owners earning tokens can use it to pay service providers for delivering communication services such as Internet access, telephony, private business networks, cable TV, audio streaming, video streaming, and other benefits, thereby reducing personal telecommunication expense in proportion to the HyperNode's activity in HyperSphere. To support HyperSphere e-commerce in its communication products and services, a range of service providers have already committed to develop and use HyperSphere communication services. Examples follow:

STEALTHTALK

StealthTalk is a cybersecure personal messenger developed exclusively for the HyperSphere featuring realtime hypersecure cloud communication including text, voice, group calls, live video, and large attachments (including videos, pictures, PDFs, files, etc.). StealthTalk differs from conventional Internet based messengers in a variety of ways to ensure privacy and security.

For one, StealthTalk operates as a private communication network over the HyperSphere public cloud. Upon installing the app onto any Android or iOS device, StealthTalk pairs itself to its host using a network authentication procedure unique to each device.

The application is sandboxed, not sharing its cryptographic keys or call history with the host, except through its UI/UX dialog during an active network connection. As such, cloning the device will not facilitate access to call logs, chats, attachments, or security credentials. Furthermore, no record of calls or callers appears on the phone's call log history thereby preventing metadata tracking or inspection.



NOT VERIFIED

You are cannot be sure who is using Robert's device. Whether it is Robert or not.

VERIFIED VIA CALL

Use a voice call to verify Robert's identity. Once you confirm identities of each other you will privately exchange (end-to-end) personal secret keys for further secure communication.

VERIFIED VIA PERSON

Use an in-person verification for secure exchange your, privately generated, secret keys directly without any mediation server to get highest possible communication security.

✓ Verification complete!

that really Robert

verify you are talking to nd not someone else right now.

Verify via QR

QR code of your friend

lexader's iPhone (+380654653212)

To finish verification, scan QR code of this user

Fig.37: StealthTalk identity validation for end-to-end personal privacy

Other features include self-destructing messages and a unique privacy mode limiting access of "private" communiqués or incoming calls to users only upon completing multi-factor identity authentication. In addition to its hypersecure communication data packet routing, StealthTalk offers users the opportunity to exchange private end-to-end encryption keys, separate from the network's security credentials.

As illustrated in **Figure 37**, in StealthTalk private end-to-end crypto-key exchange can be executed over the network based on personal confirmation by phone call, or preferably by exchanging keys in person, i.e. face-to-face, without using any network for the personal key exchange. StealthTalk may be used out of the box (i.e. as downloaded) or may be customized as a white-label communicator product for private corporations and BYOD friendly solution for secure enterprise communications. StealthTalk is a certified Microsoft co-sale partner. URL: *www.stealthtalk.com*

UPROTEL

UPROTEL (Unified Professional Communications) is a professional communication developer and network support provider offering system solutions for business and government including municipalities, armed services, emergency services (police, paramedics, fire), and port authority services [326]. UPROTEL is a pioneering adopter of early SDNP technology hosted over a private cloud for TETRA Professional Mobile Radio devices [327] supporting dispatcher-based professional communication.

Dating back to the 2000s, UPROTEL has supported a wide range of professional communication clients through Europe, Middle East, and USA, including the US Army. Product features include professional mobile radio (PMR) functions over IP networks (Wi-Fi, LTE); secure communication on unsecured lines; communication between different networks types (radio, GSM, VoIP, 3G/LTE); communication among incompatible devices (radios, smartphones, PCs); and mobile command centers. UPROTEL data and traffic management features include: advanced dispatching; monitoring and recording; indoor/outdoor positioning; regroup user by location; auto vehicle location (AVL); location-based tasks; object-oriented tasks; task sequences and queues. UPROTEL intends to expand its professional services onto the HyperSphere network. URL: *www.uprotel.com*

STEALTHMAIL

StealthMail is a Microsoft sponsored hypersecure email system especially developed for the HyperSphere to facilitate reliable, private and secure email communication not possible over the Internet. In addition to its SDNP-based fragmented data transport, StealthMail leverages the HyperSphere's identity-trust-chain and enterprise-grade CA-certificate authority to identify and quarantine imposters and to facilitate intelligent spam filtering. StealthMail offers a variety of features not available by Internet based emails. These features include:

- Stealth– email traffic is invisible to hackers, interlopers, and third parties, rending a company's emails secure and immune from surveillance or cyberattacks, obfuscating both content and packet metadata from sniffing, man-in-the-middle, and man-in-the-email attacks.
- Control– StealthMail gives exclusive control and ownership of end-to-end encryption keys and data to company client devices. User security features exist in addition to the network security features enabled by the SDNP protocol stack and the HyperSphere's dynamic routing over a meshed network.
- Email Encryption– StealthMail encrypts individually on the user's side and separately stores an email body and its attachments in a protected cloud via disaggregated data storage. The email itself contains only a secure crypto-link containing no user information whatsoever. All email content is instead transported using nested encryption comprising private key end-to-end user encryption and SDNP network hop-by-hop tunnel-protocol based encryption and state-based dynamic concealment.
- Email Revocation– StealthMail offers a company the ability to revoke historical email or data at any time including communiqués of both staff and third parties.
- Blockchain– StealthMail employs the HyperSphere's network native blockchain capability to identify and prohibit phishing attacks.
- Legal Compliance– StealthMail is flexible, adjustable to meet local legal regulations including its ability to comply with EU's GDPR (European Union's 'General Data Protection Regulation'), the United States Department Health and Human Service's 'Health Insurance Portability and Accountability Act' of 1996 (HIPAA) and others.

StealthMail employs a multidimensional approach to security using the most advanced encryption mechanisms currently available, easily upgradable as new methods arise.

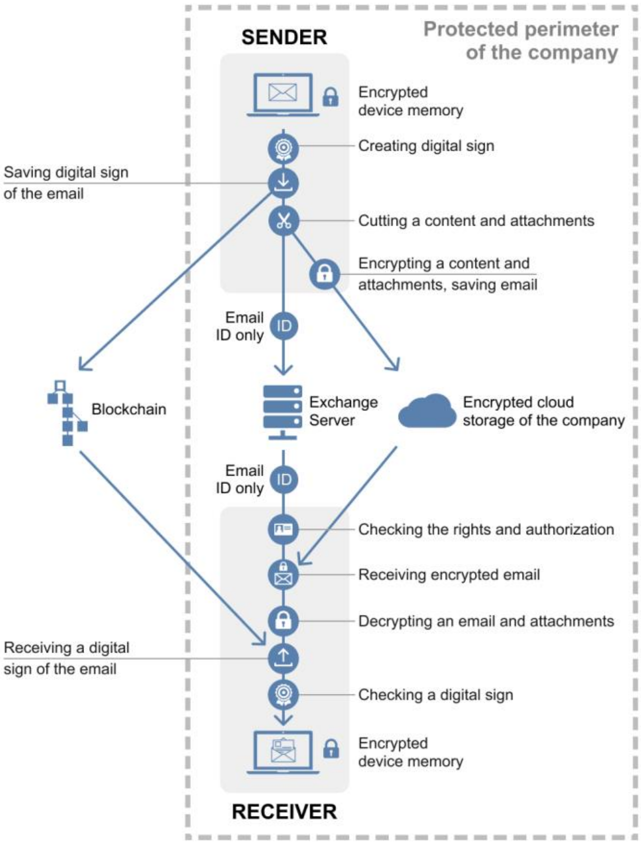

SENDER
Protected perimeter of the company
Encrypted device memory
Creating digital sign
Saving digital sign of the email
Cutting a content and attachments
Encrypting a content and attachments, saving email
Email ID only
ID
Blockchain
Exchange Server
Encrypted cloud storage of the company
Email ID only
ID
Checking the rights and authorization
Receiving encrypted email
Decrypting an email and attachments
Receiving a digital sign of the email
Checking a digital sign
Encrypted device memory
RECEIVER

Fig.38: Simplified StealthTalk email process flow chart

Methods include ECC 512+ bit elliptic curve encryption keys, 512-bit HMAC key for messaging, AES 256-bit encryption for data storage, TWOFISH 256-bit encryption for data transfer, RSA 812-bit encryption for signature and authority and SHA-3 512-bit hash for passwords. Algorithms as described are subject to change without notice. The aforementioned encryption characteristics exist atop the HyperSpheric cloud's dynamic security provisions and unique mail process (shown in **Figure 38**) facilitating nested security not corruptible by any party or network operator. Considering 91% of all intrusions are committed via email, Internet based email remains the weakest link in communication today, especially given its reliance on TLS/SSL transport security and session-based HTTPS, methods proven to be vulnerable to a variety of attack vectors. StealthMail, in contrast does not rely on these cryptographically weak protections to secure and privacy protect email communication, making it an ideal email platform for global email communication. StealthMail seamlessly integrates into Microsoft Outlook as an Add-In, thereby enhancing the familiar interface with advanced security features. StealthMail is a certified Microsoft co-sale partner. URL: *www.stealthmail.com*

Adventive Communications, a division of Adventive International, is a global developer of secure high-bandwidth microwave radios for industrial/enterprise applications and for communication network backhaul.

With numerous patents issued [500] [501], Adventive is pioneering a new generation of high-performance full-duplex radios for applications including transportation systems, security cameras and systems, corporate and university campus networks, factories, mining, refineries, power grids, and more.

Adventive Communications intends to enable its microwave radios with SDNP capability through pre-loaded HyperNodes. It also has plans to develop HyperSpot routers with Data Link Layer-2 SDNP protocols enabling superior Last Mile security. Such routers can be optimized for tokens minting with emphasis on communication, computing, or storage HyperNode functionality. A longer-term development involves a revolutionary new class of microwave radio capable of long distance high-bandwidth communication competing with optical fiber-based distribution.

As a pioneering developer of SDNP network technology, **Listat Software Development** Corporation offers contract development of cloud communication and computing software to enterprises wishing to expedite their adoption of the HyperSphere's capability and services. Listat provides high quality development of critical systems (be it dependable, security-critical, realtime, or performance-critical systems).

Listat develops realtime systems that manage tasks which are time critical, such as processing data in realtime (encoding, packing, transferring data) with control of accuracy up to 1 ms. Listat provides the most extensive range of solutions for professional communication market, supporting TETRA, PMR, DMR, VoIP, PABX, PSTN, ISDN, etc. and more. URL: Listat was also a major developer of SDNP technology for UPROTEL and the HyperSphere. URL: *www.listatsoftware.com*

B) HyperSphere Distributed Cloud Computing

Computing over the HyperSphere is executed in a distributed manner where HyperNode enabled servers, desktop PCs, and underutilized Bitcoin mining engines form a peer-to-peer network able to divide tasks and share workloads operating as a multi-node global computing environment. Subtasks may also be allocated to HyperNode connected notebooks, gaming consoles, mobile phones, tablets, and Internet appliances when on-line.

Universities and research institutes can also bridge computing networks using HyperNode clusters, thereby avoiding the need for deploying complex customized networking tools. Because HyperNodes operate across multiple protocol layers spanning the range from Network Layer-3 to Application Layer-7, HyperSphere interconnected computers are able to maintain perpetual session identity with user-defined encryption of content, facilitating a virtual meshed computer network with the potential to access billions of computers facilitating a shared virtual machine. Since HyperNode portals operate as symmetrically sandboxed applications, separating host content and device owner activities from HyperSpheric distributed computing tasks, complex projects can be executed without risk of data leakage.

When combined with the HyperSphere's disaggregated cloud storage capability, distributed computing is well suited to support big data projects. For perpetual computing needs such as weather analysis, monitoring of NEOs (near earth objects), and the Search for Extraterrestrial Intelligence (SETI), the HyperSphere facilitates the use of 3rd Tier and 4th Tier resources to lower costs and improve timely analysis of data. Another benefit of the HyperSphere in distributed computing is its ability to support tokenization of the computing environment. Tokens generated by the HyperSphere on behalf of the computing cloud may be used to control access, reward sharing, provide payment, or facilitate future discounts.

C) HyperSphere Disaggregated Data & Cloud Storage

With its network-native disaggregated data storage capability, the HyperSphere offers the perfect platform for supporting big data projects and for protecting the privacy of personal information in files containing credit history, financial information, medical records and more. Using its unique distributed storage methods, data breeches and cyber attacks on storage farms are neutralized by incomplete access to correlated files. Since drive mapping and security credentials are dynamic, the location and cryptographic identities of files and databases are available only to a file's owner signed by a valid CA-certificate at the time the data files are created. Subsequent network attacks are worthless as file content is distributed across the cloud using unique cryptographic keys not discoverable by conventional database attack stratagems. Benefits of the HyperSphere in disaggregated data cloud storage is its intrinsic ability to maintain globally distributed data backup files for disaster recovery circumventing regional risks of terrorism, power outages, fire, extreme weather, earthquakes, or acts of God.

Applications of the HyperSphere's disaggregated data files range from medical and insurance records to global corporate databases supporting CRM, ERP, RDB, and others. Disaggregated cloud storage may also be used in storing private blockchain record management useful in certification processes and in clinical trials.

AraLight

AraLight Life Sciences is an example of a startup directing their efforts toward creating a new generation platform for clinical trial management systems (CTMS) and Electronic Data Capture (EDC) including an extensive use of private blockchains for chronicling and preserving clinical trial test results using indelible time stamps, thereby preventing fraud in trial results. Unlike present day systems employing the transfer of data from one database to another throughout the trial and FDA product approval process, the AraLight solution employs a common database for all records, uniquely customizing record reporting for each target, e.g. content specifically for product developers, sponsors, hospitals, physicians, and the FDA.

D) HyperSphere Secure (IoT) Cloud-Connected Devices

The IoT application of the HyperSphere in cloud-connected devices (Internet-of-Things) offers several unique features not possible using the Internet. Firstly, hypersecure communication using the SDNP protocol over the cloud and in Last Mile communication facilitates a security shell containing the connected devices.

This quasi-unidirectional security shell enables control of IoT devices without providing access or network mapping attack vulnerabilities through low-level IoT devices. And although command and control instruction are unidirectional, sensor and feedback data can be transferred upstream to an IoT subnet controller without providing unfettered access to the cloud or risking network security.

Other benefits of the HyperSphere in cloud-connected device operation include the ability to capture and record sensor data onto a blockchain to ensure data integrity. Dynamic blockchains enable legally binding realtime reporting of the operating parameters of system critical applications like power grid management, nuclear power plant operation, chemical processing, transportation systems, airbag operation, or any other hardware device where an operator or manufacturer might be motivated to conceal fault conditions to avoid liability and culpability.

Still another benefit of the HyperSphere for cloud-connected device operation involves tokens payment for subscription based IoT devices. In this e-commerce model, consumers earning tokens by hosting HyperNodes can exchange their earned cryptocurrency to activate a device or to upgrade its performance level (see Applied BioPhotonics example).

APPLIED BIOPHOTONICS™

Applied BioPhotonics or ABP is the developer and global manufacturer of biophotonic apparatus including PBT therapeutic devices. PBT, an acronym for photobiomodulation therapy, is a revolutionary form of physical medicine employing red and near infrared light to stimulate tissue healing and maintain healthy cellular metabolism by energizing the intracellular organelle, mitochondria [502].

During treatment, photons absorbed by the mitochondria generate adenosine triphosphate or ATP, the primary source of energy powering living cells. Illuminated tissue or organs also beneficially release nitrous oxide, causing vasodilation, enhanced circulation, tissue oxygenation, pH normalization, reduction of pain and inflammation [503], and expedited healing of injuries. The professional version of the PBT device used by hospitals, physicians, and professional athletes has completed independent safety certifications in accordance with ISO, IEC, and the FCC. The device has FDA approval in the United States [504], Dubai, the UAE, and Taiwan. The company is now seeking FDA approval in Korea and China. Based on numerous issued and pending [505] [506], the next professional version of the device will employ network connectivity offering both Internet and HyperSphere cloud capability.

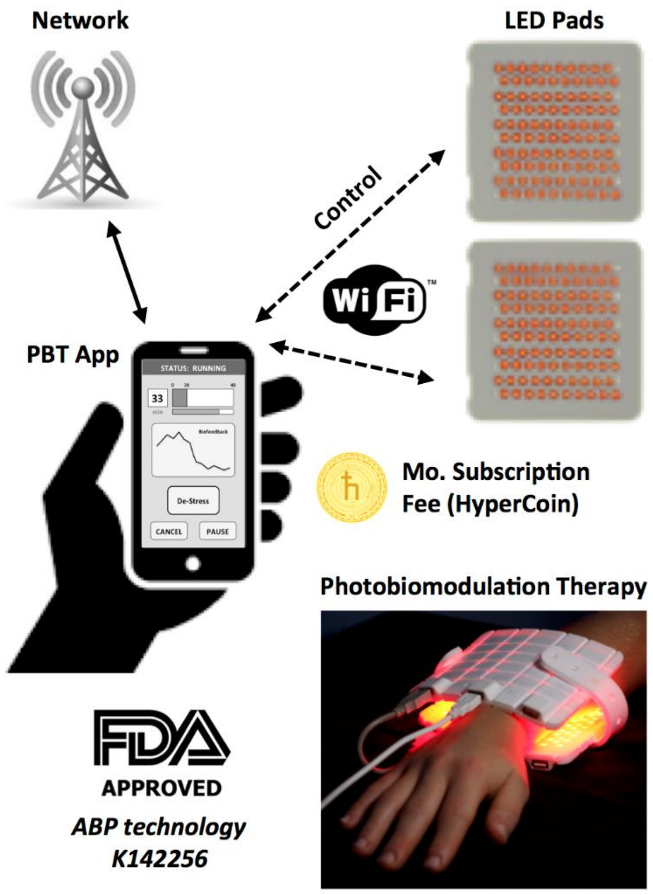


Fig.39: Subscription based photobiomodulation therapy app

In a consumer version of the PBT device shown in **Figure 39** (under development), the HyperSphere's cryptoeconomics is especially attractive for subscription-based use models where a smartphone app drives WiFi-enabled 3D-bendable LED pads dynamically controlling photobiomodulation of treated tissue. Conveniently, monthly subscription fees can be paid in tokens, possibly earned by a HyperNode hosted on the same smartphone. URL: *www.appliedbiophotonics.com*

E) HyperSpheric e-services

With its cybersecurity and privacy provisions, the HyperSphere is especially well suited to support a variety of e-services to its clients. The potential for HyperSpheric e-services is essentially limitless. A few examples include:

1. Online banking / Fintech
2. Wire transfer services
3. Point-of-sale (POS) purchases
4. ATM tellers
5. Online shopping
6. Estate & trust management
7. Insurance
8. Intellectual property
9. Business services
10. Transportation services
11. Online content distribution
12. Travel and tourism
13. Entertainment
14. Home and business security

For financially related products and services, the HyperSphere ensures transactional integrity through SDNP based hypersecure communication and network native CA-certificate based identity-trust-chains. By abandoning traditional communal blockchains vulnerable to fraud for private DyDAG blockchains, the proceeds of all financial transactions are indelibly recorded on private blockchains with defined identity-based ownership, protecting assets from theft while discouraging criminality through fund traceability.

Several provisions of the HyperSphere are especially valuable in offering financial services while protecting account privacy. These include the replicant blockchain observer segment (RBOS) based method for confirming blockchain transactions (that prevents transactional backtracing and privacy attacks) and blockchain defragmentation, a process that limits the RBOS length to very end portion of a DyDAG blockchain.

Another valuable financial transaction provision is the OT^3 proxy, the one-time-transactional token that supports POS and online payments from cryptocurrency without giving the payee access to the payor's blockchain records. That feature along with the CA-certificate signed HypWallet renders unauthorized withdrawals and fraudulent spending plaguing conventional credit cards ineffective in the HyperSphere.

The HyperSphere also enables banks, financial institutions, and businesses to execute international money transfers as an exchange medium vastly superior to SWIFT wires in security and efficiency. For example, a payment in United States dollars (USDs), transferred over the HyperSphere in the form of tokens, can be redeemed in Indian rupees without the need for currency exchange, improving financial efficiency, eliminating middle-men, and reducing transactional costs and service fees. In the field of asset management, e.g. trusts, estates, annuities, and insurance policies, the use of the HyperSphere auxiliary DyDAG blockchain supports the recording of legal documents, immutably chronicled as time-stamped blocks entered onto the auxiliary blockchain.

LifeSite™
Life's Information. All in One Place.

LifeSite was created to inspire and empower people by connecting their head and their heart - providing personal peace of mind today, and for family and loved ones tomorrow. LifeSite's ultra-secure, cloud-based, digital safe deposit box helps individuals and families, along with their advisors to organize, manage and share all of life's information and documents – for any stage of life. With security as a first priority, LifeSite combines secure file access and controlled, permission-based sharing with high-level document encryption and security, to provide safe and smart digital storage solutions. Features of LifeSite include:

- Pre-defined categories and fields – All privilege controlled, for entering and encrypting information in different categories such as personal, medical, people, pets, online accounts, career, finances, property, insurance and legal –

and provides convenient features to enter, attach and share information and documents. LifeSite is also PCI, GDPR, HIPAA and PIPEDA compliant.

- Secure file sharing – The LifeSite file vault eliminates the risk of emailing attachments through unsecure, unencrypted servers common in Internet communication and routing. Dynamic meshed transport over the HyperSphere's SDNP cloud facilitates an added degree of security by preventing packet tracking and metadata surveillance.
- LifeSite checklists – Checklists facilitate controlled collaboration with family members and advisors for a variety of life events and processes such as: preparing for a disaster or an accident, estate planning, saving for college or a home, planning for travel, having a child, preparing for death, caregiving, settling an estate, etc.
- Asset & transactional tracking (planned) – Transactional tracking using private blockchains immutably records assets, events, personal data, and account information using time-stamped secure blocks of hashed data– information critical to establishing proof-of-ownership and transactional chronology, especially as related to disputes over wills, estates, trusts, and other long-term and multi-generational assets.
- Encrypted Messaging– Secure, realtime message exchange with collaborators regarding additions, changes, or deletions for life information or documents.
- LifeSite also has companion apps available on iOS, Android and Amazon's Alexa.

In addition to network and data transport security offered by the HyperSphere, LifeSite employs its own end-to-end data protection, encryption, and security mechanisms (depicted in **Figure 40**) to ensure the ultimate in user privacy provisions. Features include:

- *Strong Passwords and multi-factor authentication* – Passwords alone aren't enough to protect accounts. While access to LifeSite requires a password that must meet stringent length and character strength requirements, two-factor authentication provides an extra degree of security. Additionally, the LifeSite mobile app uses biometric identification with fingerprint access.
- *Layered encryption* – LifeSite encrypts every single piece of information and all documents, during transmission and storage. SHA-256 and military-grade AES-256 encryptions are utilized and each user has a unique encryption key that's frequently rotated to guard against unauthorized access. Moreover, cryptographic key exchanges over the HyperSphere are fragmented preventing network attacks from detecting and reconstructing cryptographic credentials.
- *Zero-trust network* – LifeSite faithfully employs an architectural and operational philosophy of 'zero-trust'. This philosophy states "not to implicitly trust any network and to build security mechanisms in every layer to reduce the threat radius.
- *LifeSite is a zero-knowledge system* – Information is encrypted from end-to-end so that the LifeSite account holder is the only person who can read it; LifeSite (and the HyperSphere) never has access to it.

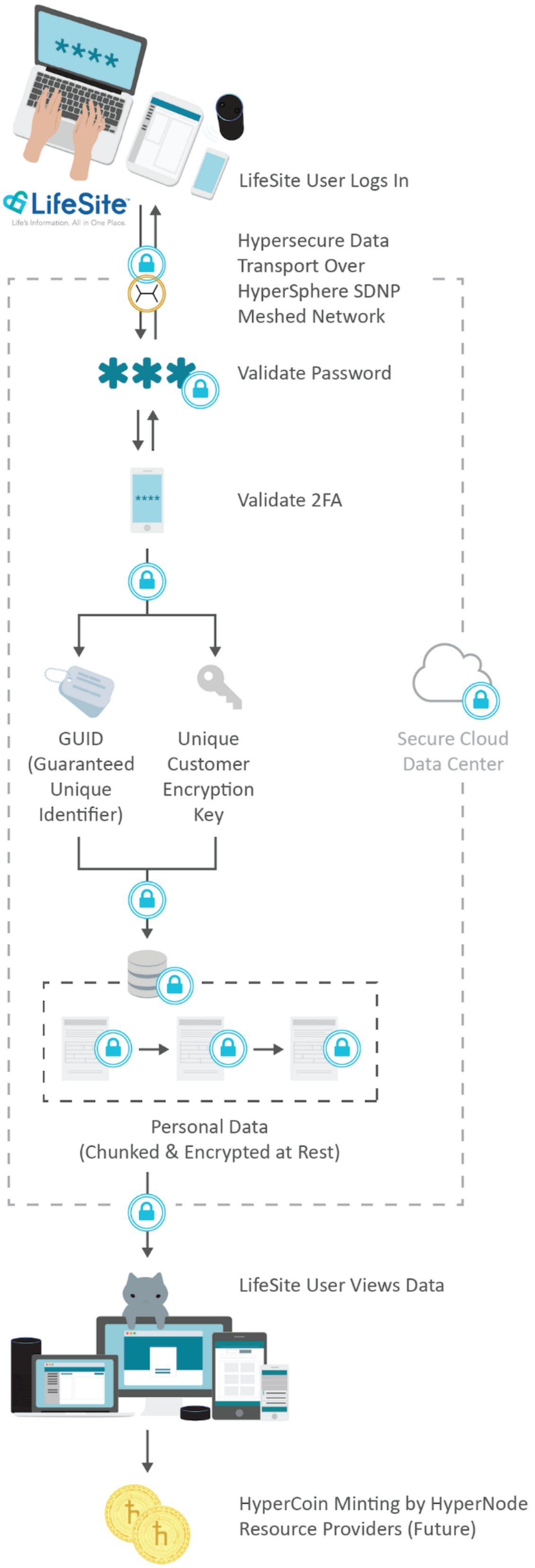

LifeSite User Logs In
LifeSite
Life's Information. All in One Place.
Hypersecure Data Transport Over HyperSphere SDNP Meshed Network
Validate Password
Validate 2FA
GUID (Guaranteed Unique Identifier)
Unique Customer Encryption Key
Secure Cloud Data Center
Personal Data (Chunked & Encrypted at Rest)
LifeSite User Views Data
HyperCoin Minting by HyperNode Resource Providers (Future)

Fig.40: LifeSite's hypersecure, encrypted end-to-end information flow

- *Fragmented data* – Additionally, passwords, user data and the unique user encryption key are split into pieces and stored separately, ensuring that they're unreadable while in storage. Finally, LifeSite never transmits or stores files, encryption keys and user passwords in unencrypted form, ensuring data is never compromised even if devices are lost or stolen.
- *Ransomware immunity* – The rise of ransomware has caused countless people to lose important information, with millions more still vulnerable and without a solution. LifeSite's hypersecure File Vault provides the answer to this problem. With data securely stored in a LifeSite File Vault, an infected user can refresh the lost files after a system restore on the device. Furthermore, optional file change history allows restoration of a file to a previously known-good state.
- *Realtime, secure document collaboration* – An essential component of LifeSite is to enable secure sharing and collaboration with family, friends, and trusted advisors. In a matter of seconds, users can provide, or revoke, access to any category of life information or files. It's also vital to track access and usage, hence a full audit trail is available in realtime at all times, even after collaboration has been revoked. The patented (US 9,369,445) [507] LifeSite object encryption ensures data is secure and controlled at all times.
- *Enhanced data transport atop HyperSphere (planned)* – Encrypted LifeSite information transport security is enhanced through the HyperSphere SDNP network; leveraging the hop-by-hop tunnel-protocol and dynamic routing and packet concealment.
- *Document signing (planned)* – LifeSite signing server generates a digital signature constructed from your device specific public key and a unique fingerprint of the file contents, which it then signs with your private key. The digital signature is published utilizing HyperSphere BaaS decentralized ledger, in the form of a dated transaction, leaving the original document untouched. Once a digital signature has been authenticated by the HyperSphere and appended onto the blockchain, it cannot be corrupted and will remain unaltered in perpetuity, allowing anyone in the future to verify the document's authenticity and integrity.
- *Offline Mode (planned)* – Ideal for disaster preparedness scenarios, offline mode for mobile devices provides fast and secure access to life information and files even when a data connection isn't available. Using state-of-the-art data storage and encryption techniques for mobile platforms, LifeSite is able to provide critical information when it matters most without impacting data security or privacy.

LifeSite was built to help families share information while still maintaining the highest level of security. With LifeSite users need not choose between convenience and security.
URL: *www.lifesite.co*

Adventive IPBank is a contract IP development company helping businesses, startups, and would-be inventors to define and develop an IP strategy, to expand its IP portfolio, to write and file patent application, and to manage IP prosecution to a successful fruition. Unlike a patent lawyer, Adventive IPBank comprises engineers and technical experts able to understand a client's intent and to make inventions on their behalf, either improving upon their invention disclosures or developing the new IP outright. Along with Listat Software Development services, Adventive IPBank was a major contributor and architect of the SDNP and HyperSecure Last Mile Communication patent applications, as well as a co-developer of HyperSphere specific inventive matter and work product.

In the future, Adventive IPBank intends to adapt the HyperSphere's DyDAG blockchain structure to record and track an idea's development and prosecution including content contributions, US and foreign filings for Taiwan, PCT and WPO, as well as filings for provisional, continuation, divisional, and continuation in part applications. The multi-tree structure is especially valuable in tracking IP development lineage and evolution.

Other e-services enabled by the HyperSphere include business services. Such services include web-based accounting, financial records, distributed CRM and contact management hosting, database management, medical and insurance records management, enterprise resource planning (ERP) distributed system hosting, and more. The HyperSphere is also able to support online cryptocurrency payment of monthly subscription-based services such as TV, movie, and audio streaming services, and as payment for on-demand services like ride sharing, hotels, dining, cruises, and tourism.

F) Artificial Intelligence & Machine Learning

With its distributed cloud computing capability and native cryptoeconomics, the HyperSphere provides unique opportunities in artificial intelligence and machine learning. For one, the decentralized HyperSphere Marketplace employs artificial intelligence in negotiating HyperContracts among resource providers and a merchant or service provider.

Secondly, with its enormous compute power, limitless disaggregated storage capacity, and data privacy protective provisions, personal information can be used to make personalized recommendations to users pseudonymously, using personal shopping or behavior-based data to predict interest or suitability of a product or service to individuals without needing to know their personal identity.

Once such AI-based recommendation service planning to go-live over the HyperSphere is a startup entitled **AVATARZ**. With nearly two decades of behavioral modeling experience, the company plans to deliver AI based product recommendations to consumers on behalf of its clients, and to tokenize their business to incentivize participation using BaaS support offered by the HyperSphere.

G) *HyperSphere BaaS and Tokenization Services*

With network-native DyDAG blockchain processing and adjunctive cryptocurrency generation through HyperNode Hop Codes (HHCs), the HyperSphere is capable of generating cryptocurrency, digital tokens, e-coupons, and other unfakable digital assets for HyperSphere users. It is able to facilitate Blockchain-as-a-Service (BaaS) functionality for merchants and service providers wishing to offer or employ custom digital wallets, transactions processes, record keeping, or customized functionality as part of their business model.

V. HYPERSPHERE FOUNDATION

Functioning as a non-profit foundation and decentralized trust, the HyperSphere Foundation has no employees, owners, shareholders, or executive officers. Structurally, activities are outsourced to independent contractors performing services for the HyperSphere in accordance with their respective roles and duties including governance and oversight, engineering development of applications and infrastructure, and invention and intellectual property prosecution. Operationally, the HyperSphere is fully decentralized comprising an autonomous dynamic meshed network of HyperNodes hosted by user devices– corporate, professional clouds, and individuals alike. In this sense, the HyperSphere can be referred to as the people's network, or metaphorically as the Internet of People, a decentralized global cloud everyone owns but no one controls. Use of proceeds derived from the sale of tokens in any future offering, public or private, shall be used to fund infrastructure development, IP creation, and to sponsor merchant and service provider adoption, and market development. As an open source platform for global cybersecure communication and cloud computing, the HyperSphere will seek to establish alliances with all industry consortiums, major corporations, industries, consortiums, professional societies, and universities to maximize the beneficial impact of the HyperSphere platform across the globe.

Acknowledgment

The authors would like to acknowledge the contributions of the HyperSphere's cofounder, Dmitri Bulkhukov, for his unwavering HyperSphere support and to Oleksandr Golub and 'the Team' for many years of invaluable technical contributions in developing SDNP technology and cybersecure networks. We would also like to thank Bill Pabst for his radio communication related expert advise, to the efforts of Chris Graham and Dave Steuber for their guidance the HyperSphere's successful patent prosecution and IP strategy, and to Laura E Williams for her assistance with the paper's intricate graphical illustrations.

VI. REFERENCES

[1] "Digital signatures," *Wikipedia* [online] https://en.wikipedia.org/wiki/Digital_signature

[2] "Distributed ledger," *Wikipedia* [online] https://en.wikipedia.org/wiki/Distributed_ledger

[3] "Blockchain," *Wikipedia* [online] https://en.wikipedia.org/wiki/Blockchain

[4] "Types of blockchains and distributed ledger technologies," *BlockchainHub*, pp. 1-12 [online] https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[5] "Cryptocurrency," *Wikipedia* [online] https://en.wikipedia.org/wiki/Cryptocurrency

[6] R. Beck et al, "Blockchain – the gateway to trust-free cryptographic transactions," *Proc. ECIS, 24th Euro Conf. Info Sys (ECIS Istanbul)*, 2016, pp. 2-14 [online] https://pdfs.semanticscholar.org/9a20/1289042464e21512119a27d2f6cfa8a67f5b.pdf

[7] "Banking is only the beginning– 36 big industries blockchain could transform" *CBInsights*, 1 Feb 2018 [online] https://www.cbinsights.com/research/industries-disrupted-blockchain/

[8] N. Ismael, "Blockchain will empower the people and break barriers to information," *Information Age*, 16 Nov 2017 [online] https://www.information-age.com/blockchain-will-empower-people-break-barriers-information-123469599/

[9] CrowdConscious (blogger), "Cryptocurrency driving change– corporate social responsibility, impact Investing, & now: the DAO," *Keepingstock.net* 18 Jul 2017 [online] https://keepingstock.net/cryptocurrency-driving-change-corporate-social-responsibility-impact-investing-now-the-dao-d70bd00140d5

[10] "Smart contract," *Wikipedia* [online] https://en.wikipedia.org/wiki/Smart_contract

[11] Sean, "Does notarization on the blockchain actually work?" *Decentralize Today*, 24 Jan 2017 [online] https://decentralize.today/does-notarization-on-the-blockchain-actually-work-d8006443c0b9

[12] J A Vorabutra, "Why blockchain is a game changer for supply chain management transparency," *SupplyChain 247*, 3 Oct 2016 [online] http://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain

[13] "How does blockchain money transfer work?" *Wirex*, 2018 [online] https://wirexapp.com/blockchain-money-transfers-work/

[14] R. Lifthrasir, "Permissionless real estate title transfers on the Bitcoin blockchain in the USA," *Medium*, 28 Jun 2017 [online] https://medium.com/@RagnarLifthrasir/permissionless-real-estate-title-transfers-on-the-bitcoin-blockchain-in-the-usa-5d9c39139292

[15] D. DeNicuolo, "The Future of electronics wills," *Bifocal (American Bar Assoc.)*, vol. 38, no 5; Jun 2017 [online] https://www.americanbar.org/publications/bifocal/vol_38/issue-5--june-2017-/the-future-of-electronic-wills.html

[16] C.L. Hennecken, "Death and Bitcoin- how digital currencies affect estate-planning," *Digital Currency Perspectives*, 30 Jul 2015 [online] https://www.digitalcurrencyperspectives.com/2015/07/30/death-and-bitcoin-how-digital-currencies-affect-estate-planning/

[17] T.M. Lockyer, "The blockchain trust disruption," *Medium*, 11 Dec 2017 [online] https://medium.com/@mattdlockyer/the-blockchain-trust-disruption-d70b52bc5f27

[18] R Botsman, "How the blockchain is redefining trust," *Wired*, 27 Dec 2017 [online] https://www.wired.com/story/how-the-blockchain-is-redefining-trust/

[19] J. Raczynski, "How might blockchain revolutionize the legal industry," *Thomas Reuters*, 9 Jun 2016 [online] https://blogs.thomsonreuters.com/answerson/might-blockchain-technology-revolutionize-legal-industry/

[20] J. Ito et al, "The blockchain will do to the financial system what the Internet did to media," *Harvard Bus. Rev.*, 8 Mar 2017 [online] https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

[21] C. Centeno, "Securing Internet payments," *Inst. Prospective. Tech. Studies*, No. 6, Jan 2002, pp. 1-48 [online] http://www.europarl.europa.eu/stoa/webdav/shared/3_activities/privacy/protection/ipts_securing_internet_payments_en.pdf

[22] F. Holotiuk et al, "The impact of blockchain technology on business models in the payments industry," *13th Intl. Conf. Wirtschaftsinformatik*, (St.

Gallen Switzerland,) 12 Feb 2017 [online] https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1100&context=wi2017

[23] J. Bertrand, "How blockchain is driving cloud adoption," *Digitalist Mag*. 14 Feb 2017 [online] http://www.digitalistmag.com/digital-economy/2017/02/14/blockchain-driving-cloud-adoption-04904064

[24] M.A. Aimunawar, "Securing electronic transactions to support e-commence," *Universiti Brunei Darussalam* [online] https://arxiv.org/pdf/1207.4292.pdf

[25] A.M.S. Rahma et al, "Hybrid model for securing e-commerce transaction," *Intl. J. Adv. Eng. Tech*, vol. 1, no. 5, Nov 2011, pp. 14-20 [online] http://www.archives-ijaet.org/media/2I5-IJAET0511524-hybrid-model-for-securing-copyright-IJAET.pdf

[26] G. Souter, "Blockchain could 'revolutionize' insurance," *Bus. Insurance*, 16 Mar 2018 [online] http://www.businessinsurance.com/article/20180316/news06/912319906/Blockchain-could-revolutionize-insurance

[27] D. Koch, "Blockchain: A new world of opportunity for small businesses?" *Digitalist Mag.*, 15 Mar 2017 [online] http://www.digitalistmag.com/digitaleconomy/2017/03/15/blockchain-new-world-of-opportunity-for-small-businesses-04965128

[28] "How blockchain will disrupt your business," *Techwire Asia*, 8 Jan 2018 [online] http://techwireasia.com/2018/01/blockchain-disrupt-business/

[29] M. Anthese, "Three Ways Blockchain Will Disrupt Traditional Business And Impact Marketing In 2018," *Forbes Community Voice*, 29 Jan 2018 [online] https://www.forbes.com/sites/forbesagencycouncil/2018/01/29/three-ways-blockchain-will-disrupt-traditional-business-and-impact-marketing-in-2018/2/#40c35e1a1bdb

[30] S. Grybniak, "5 ways to put blockchain to use as a small businesses owner," *Business.com*, 12 Sep 2017 [online] https://www.business.com/articles/5-ways-small-businesses-can-use-blockchain/

[31] N. Kuznetsov, "Why blockchain matters to small businesses," *Entrepreneur*, 9 Jan 2018 [online] https://www.entrepreneur.com/article/305853

[32] B. Carmody, "7 ways blockchain will enable entrepreneurs in 2018," *Inc.* [online] https://www.inc.com/bill-carmody/7-ways-blockchain-will-enable-entrepreneurs-in-2018.html

[33] O. Solon, "As tech companies get richer, is it 'game over' for startups?" *The Guardian*, 20 Oct 2017 [online] https://www.theguardian.com/technology/2017/oct/20/tech-startups-facebook-amazon-google-apple

[34] D. Glance, "Initial Coin Offerings are disrupting how startups are funded – but what are they?" *The Conversation*, Sep 2017 [online] https://theconversation.com/initial-coin-offerings-are-disrupting-how-startups-are-funded-but-what-are-they-84857

[35] L. Shen, "Telegram ICO Raises $1.7 Billion, Even As Bitcoin Price Falls," *Fortune*, 30 Mar 2018 [online] http://fortune.com/2018/03/30/bitcoin-price-telegram-ico-presale/

[36] Y. Lee, "Venture capital or ICO? Startups face cash-raising dilemma," *Bloomberg*, 21 Jan 2018 [online] https://www.bloomberg.com/news/articles/2018-01-21/to-ico-or-not-to-ico-that-is-the-question-for-today-s-startups

[37] "Society for worldwide interbank financial telecommunication (SWIFT)," *Wikipedia* [online] https://en.wikipedia.org/wiki/society_for_worldwide_interbank_financial_telecommunication

[38] K. N. Das et al, "Eyes wide shut - the $1.8 billion Indian bank fraud that went unnoticed" *Huffpost*, 26 Feb 2018 [online] https://www.huffingtonpost.in/2018/02/25/eyes-wide-shut-the-1-8-billion-indian-bank-fraud-that-went-unnoticed_a_23370779/

[39] "Deutsche Bank sends $35b to exchange by mistake," *pymnts.com*, 19 Apr 2018 [online] https://www.pymnts.com/news/banking/2018/deutsche-bank-derivative-trading/

[40] N. Arnand, "SWIFT: the messaging system at the heart of the $1.8 billion Punjab national bank fraud," *Quartz*, 20 Feb 2018 [online] https://qz.com/1210659/swift-the-messaging-system-at-the-heart-of-the-1-8-billion-punjab-national-bank-fraud/

[41] A. Kahate et al, "Security and threat models – secure electronic transaction (SET) protocol," *IndicThreads*, 3 Jan 2008 [online] http://www.indicthreads.com/1496/security-and-threat-models-secure-electronic-transaction-set-protocol/

[42] N. Kaliya et al, "Simple secure electronic transaction (SSET) protocol," *Intl. J. Adv. Eng Rsrch*, Sci (IJAERS) 22 Oct 2016 [online] https://www.researchgate.net/publication/312323825_simple_secure_electronic_transaction_SSET_protocol

[43] "3-D Secure," *Wikipedia* [online] https://en.wikipedia.org/wiki/3-D_Secure

[44] "What are 3D Secure, ACS and MPI?" *GPayments* [online] https://www.gpayments.com/about/3d-secure

[45] "New and Improved 3-D Secure," *Visa* [online] https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-3d-secure-2-program-infographic.pdf

[46] "What is SSL?" *Comodo* [online] https://www.instantssl.com/ssl.html

[47] "Why have SSL certificates with internal names been banned," *Digicert*, 2013 [online] https://whitepapers.em360tech.com/wp-content/files_mf/1406823775Internal_Names_Banned.pdf

[48] H. Graceful, "TLS/SSL Vulnerabilities," *GracefulSecurity*, 21 Jan 2017 [online] https://www.gracefulsecurity.com/tls-ssl-vulnerabilities/

[49] "POODLE," *Wikipedia* [online] https://en.wikipedia.org/wiki/POODLE

[50] W. Whitteker, "Point of sales (POS) systems and security," *SANS*, Oct 2014 [online] https://www.sans.org/readingroom/whitepapers/bestprac/point-sale-pos-systems-security-35357

[51] N. Lord, "What is POS Security? Protecting data in POS environments," *Digital Guardian*, 11 Oct 2016 [online] https://digitalguardian.com/blog/what-pos-security-protecting-data-pos-environments

[52] "Transport Layer Security," *Wikipedia* [online] https://en.wikipedia.org/wiki/Transport_Layer_Security

[53] "Heartbleed," *Wikipedia* [online] https://en.wikipedia.org/wiki/Heartbleed#cite_note-30

[54] J. Steinberg, "Massive Internet Security Vulnerability -- Here's What You Need To Do," *Forbes*, 10 Apr 2014 [online] https://www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do/#72bb84963fdf

[55] "ShellShock: all you need to know about the Bash Bug vulnerability," *Symantec Connect Community*, 25 Sep 2014 [online] https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability

[56] K. Sigler, "Heartbleed, Shellshock and POODLE: The sky is not falling," *SC Media*, 24 Oct 2014 [online] https://www.scmagazine.com/heartbleed-shellshock-and-poodle-the-sky-is-not-falling/article/537941/

[57] "SSL/TLS certificates beginner's tutorial," *Talpor Solutions Blog*, 19 Jul 2015 [online] https://blog.talpor.com/2015/07/ssltls-certificates-beginners-tutorial/

[58] "What is HTTPS?" *Comodo* [online] https://www.instantssl.com/ssl-certificate-products/https.html

[59] "X.509," [online] https://en.wikipedia.org/wiki/X.509

[60] T. Fisher, "Cryptographic Hash Function," *Lifewire*, 5 Jan 2018 [online] https://www.lifewire.com/cryptographic-hash-function-2625832

[61] "What is the SSL Certificate Chain?" *DNSimple* [online] https://support.dnsimple.com/articles/what-is-ssl-certificate-chain/

[62] “Chain of trust,” Wikipedia [online] https://en.wikipedia.org/wiki/Chain_of_trust

[63] "How certificate revocation (doesn’t) work in practice," *Netcraft*, 13 May 2013 [online] https://news.netcraft.com/archives/2013/05/13/how-certificate-revocation-doesnt-work-in-practice.html

[64] G. Keizer, "Hackers steal SSL certificates for CIA, MI6, Mossad," *Computerworld*, 4 Sep 2011 [online] https://www.computerworld.com/article/2510950/security0/hackers-steal-ssl-certificates-for-cia--mi6--mossad.html

[65] P. Lambert, "Compromised certificate authorities– How to protect yourself," *TechRepublic*, 13 Sep 2011 [online] https://www.techrepublic.com/blog/it-security/compromised-certificate-authorities-how-to-protect-yourself/

[66] P. Paganini, " 2011, CAs are under attack. Why steal a certificates?" *Security Affairs*, 15 Dec 2011 [online] http://securityaffairs.co/wordpress/647/cyber-crime/2011-cas-are-under-attack-why-steal-a-certificate.html

[67] P. Passeri, "Cyber attacks statistics," *Hackmageddon*, 19 Apr 2018 [online] https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

[68] P. Paganini. "How cybercrime exploits digital certificates," *Inforsec Institute*, 28 Jul 2014 [online] http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates/#gref

[69] K. Zetter, "Attackers stole certificate from Foxconn to hack Kaspersky With Duqu 2.0,” *Wired* [online] https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/

[70] H. Shinotsuka, "How attackers steal private keys from digital certificates," *Symantec Connect Community*, 22 Feb 2013 [online] http://securityaffairs.co/wordpress/647/cyber-crime/2011-cas-are-under-attack-why-steal-a-certificate.html

[71] C. Cimpanu, "The market of stolen code-signing certificates is too expensive for most hackers," *BleepingComputer*, 22 Feb 2018 [online] https://www.bleepingcomputer.com/news/security/the-market-of-stolen-code-signing-certificates-is-too-expensive-for-most-hackers/

[72] R.A. Grimes, "Digital certificates are helping deliver malware," *CSO Online*, 5 Apr 2016 [online] https://www.csoonline.com/article/3051755/data-protection/digital-certificates-are-helping-deliver-malware.html

[73] S. Yegulalp, "Fake antivirus software using stolen certificates, typosquatting," *InfoWorld*, 16 Dec 2013 [online] https://www.infoworld.com/article/2609529/antimalware/fake-antivirus-software-using-stolen-certificates--typosquatting.html

[74] "Timeline of computer viruses and worms," *Wikipedia* [online] https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

[75] V. Adiuru, "Protection against email borne attacks," *IBM Security*, 2017 [online] ftp://public.dhe.ibm.com/software/au/pdf/Protection_against_email_borne_attacksWP_AU.pdf

[76] N. Provos et al, "Ghost in the Browser," *Univ Maryland*, 2017 [online] http://www.cs.umd.edu/class/spring2017/cmsc818O/papers/ghost-in-browser.pdf

[77] "How to remove a web browser redirect virus," *Bleeping Computer*, 18 Jul 2017, pp. 1-25 [online] https://www.bleepingcomputer.com/virus-removal/remove-web-browser-redirect-virus

[78] L. Constatin, "Unusual file-infecting malware steals FTP credentials," *Computerworld*, 15 Jul 2013 [online] https://www.Computerworld.com/article/2483952/malware-vulnerabilities/unusual-file-infecting-malware-steals-ftp-credentials.html

[79] B. Casey, "Is FTP malware threatening network port security?" *SearchSecurity* [online] https://searchsecurity.techtarget.com/answer/Is-FTP-malware-threatening-network-port-security

[80] M. Kumar, "Over 20 million users installed malicious ad blockers from Chrome store," *The Hacker News*, 19 Apr 2018 [online] https://thehackernews.com/2018/04/adblocker-chrome-extention.html

[81] S. Khandelwal, "CCleaner attack timeline— here's how hackers infected 2.3 million PCs," *The Hacker News*, 17 Apr 2018 [online] https://thehackernews.com/2018/04/ccleaner-malware-attack.html

[82] A. Greenberg, "The Petya plague exposes the threat of evil software updates," *Wired*, 7 Jul 2017 [online] https://www.wired.com/story/petya-plague-automatic-software-updates/

[83] T. Katsuki, "Crisis– the advanced malware," *Symantec*, 2012, pp. 1-14 [online] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/crisis_the_advanced_malware.pdf

[84] D. Palmer, "Adobe patches security flaws in Acrobat and Reader," *ZDNet*, 9 Apr 2017 [online] https://www.zdnet.com/article/adobe-patches-security-flaws-in-adobe-acrobat-and-reader/

[85] L. Mathews, "New Mac malware found hiding in a fake Adobe flash update," *Forbes*, 9 Feb 2017 [online] https://www.forbes.com/sites/leemathews/2017/02/09/new-mac-malware-found-hiding-in-a-fake-adobe-flash-update/#171be46a1ba1

[86] B. Tedesco, "Adware variants discovered," *Carbon Black*, 23 Sep 2016 [online] https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/

[87] H. Dong et al, "Beyond the blacklists/ detecting malicious URLs through machine learning," *Blackhat Asia (Singapore)* 28-31 Mar 2017 [online] https://www.blackhat.com/docs/asia-17/materials/asia-17-dong-beyond-the-blacklists-detecting-malicious-url-through-machine-learning.pdf

[88] "Malicious URL Threat Encyclopedia," *Trend Micro* [online] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malicious-url

[89] P. Ducklin, "Typosquatting – what happens when you mistype a website name?" *Naked Security* [online] https://nakedsecurity.sophos.com/typosquatting/

[90] M. Rouse, "Ransomware?" *WhatIs.com* [online] https://searchsecurity.techtarget.com/definition/ransomware

[91] V. Mohan et al, "Frankenstein/ Stitching malware from benign binaries," *UT Dallas* [online] https://www.utdallas.edu/hamlen/mohan12woot.pdf

[92] S. Kandelwal, "New Android malware secretly records phone calls and steals private data," *The Hacker News*, 3 Apr 2018 [online] https://thehackernews.com/2018/04/android-spying-trojan.html

[93] C. Lueg, "8,400 new Android malware samples every day," *G Data Software*, 27 Apr 2017 [online] https://www.gdatasoftware.com/blog/2017/04/29712-8-400-new-android-malware-samples-every-day

[94] "Current Android malware," *Spreitzenbarth* [online] https://forensics.spreitzenbarth.de/android-malware/

[95] S. Gallagher, "Chinese company installed secret backdoor on hundreds of thousands of phones," *Ars Technica*, 15 Nov 2016 [online] https://arstechnica.com/information-technology/2016/11/chinese-company-installed-secret-backdoor-on-hundreds-of-thousands-of-phones/

[96] [D. Goodin, "Malware found preinstalled on 38 Android phones used by 2 companies," *Ars Technica*, 10 Mar 2017 [online] https://arstechnica.com/information-technology/2017/03/preinstalled-malware-targets-android-users-of-two-companies/

[97] "Malware for iOS, the iPhone," *Wiki* [online] https://www.theiphonewiki.com/wiki/Malware_for_iOS

[98] "Vault 7: CIA hacking tools revealed– iOS exploits," *WikiLeaks* [online] https://wikileaks.org/ciav7p1/cms/page_13205587.html

[99] "Design pattern recovery from malware binaries," *Carnegie-Melon* 2018 [online] https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=6473

[100] D. Kim et al, "certified malware– measuring breaches of trust in the Windows code-signing PKI," *CCS*, 17 Oct to 30 Nov 2017, pp. 1435-1448 [online] https://acmccs.github.io/papers/p1435-kimA.pdf

[101] K. Shaw, "The OSI model explained/ How to understand (and remember) the 7 layer network model," *Network* World, 4 Dec 2017 [online] https://www.networkworld.com/article/3239677/lan-wan/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

[102] "OSI model," *Wikipedia* [online] https://en.wikipedia.org/wiki/OSI_model

[103] A.L. Russell, "OSI– The Internet that wasn't," *IEEE Spectrum*, 30 Jul 2013, pp. 1-10 [online] https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt

[104] M. Rouse, "What is TCP/IP (Transmission Control Protocol/Internet Protocol)?" *WhatIs.com* [online] https://searchnetworking.techtarget.com/definition/TCP-IP

[105] B. Hughes, "The Internet of things– an overview," *Computer Weekly*, Feb 2017 [online] https://www.computerweekly.com/opinion/The-internet-of-things-an-overview

[106] B. Wasik "In the programmable world, all our objects will act as one," *Wired*, 14 May 2013 [online] https://www.wired.com/2013/05/internet-of-things-2/

[107] "Vehicle-to-everything," *Wikipedia* [online] https://en.wikipedia.org/wiki/Vehicle-to-everything

[108] M. Rouse, "What is Internet of Everything (IoE)?" *WhatIs.com* [online] https://internetofthingsagenda.techtarget.com/definition/Internet-of-Everything-IoE

[109] "Abstraction layer," *Wikipedia* [online] https://en.wikipedia.org/wiki/Abstraction_layer

[110] E. Hertzog, "Design Systems and Abstraction Layers/ A Model for Better Understanding and Implementation," *UXPin*, 2018 [online] https://www.uxpin.com/studio/blog/design-systems-abstraction-layers-model-better-understanding-implementation/

[111] "What is a Hardware Abstraction Layer (HAL)?" *Techopedia* [online] https://www.techopedia.com/definition/4288/hardware-abstraction-layer-hal

[112] B. Schwartz, "Four types of database abstraction layers," *Databases*, 13 Aug 2006 [online] https://www.xaprb.com/blog/2006/08/13/four-types-of-database-abstraction-layers/

[113] "Hardware abstraction layer [real-time robotics framework]' *EEROS*, 30 Nov 2017 [online] http://wiki.eeros.org/eeros_architecture/hal/start

[114] B. Dickson, "How to deal with IoT challenges through abstraction," *TechCrunch*, 6 Apr 2016 [online] https://techcrunch.com/2016/04/06/how-to-deal-with-iot-challenges-through-abstraction/

[115] T. Tzook, "Hardware abstraction layer (flash3388/flashlib Wiki)," *GitHub*, 15 Oct 2017 [online] https://github.com/Flash3388/FlashLib/wiki/Hardware-Abstraction-Layer

[116] O. Vogel, "Service abstraction layer," *PwC Consulting*, 2001 [online] http://hillside.net/europlop/HillsideEurope/Papers/EuroPLoP2001/2001_Vogel_ServiceAbstractionLayer.pdf

[117] D. Reed, "Applying the OSI seven layer network model to information security," *SANS Institute*, 21 Nov 2003 [online] https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309

[118] J. Howe, "How WiFi Hotspot hacks occur," *Private WiFi*, 1 Jul 2011 [online] http://blog.privatewifi.com/how-wifi-hotspot-hacks-occur/

[119] S. Khandelwal, "New 4G LTE network attacks let hackers spy, track, spoof and spam," *The Hacker News*, 5 Mar 2018 [online] https://thehackernews.com/2018/03/4g-lte-network-hacking.html

[120] S. Gibbs, "Your phone number is all a hacker needs to read texts, listen to calls and track you," *The Guardian*, 18 Apr 2016 [online] https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you

[121] I. Shatilin, "How hard is it to hack a cellular network?" *Kaspersky Lab*, 24 Nov 2018 [online] https://www.kaspersky.com/blog/hacking-cellular-networks/10633/

[122] A. Hannah, "Packet sniffing basics," Linux J., 14 Nov 2011 [online] https://www.linuxjournal.com/content/packet-sniffing-basics

[123] B. McGee, "WPA2 has been broken. What now?" *Fortinet*, 16 Oct 2017 [online] https://www.fortinet.com/blog/business-and-technology/wpa2-has-been-broken-what-now.html

[124] "DDoS Quick Guide," *Natl*. *Cybersecurity Comm*. *Int*. *Cntr*., 29 Jan 2014 [online] https://www.uscert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

[125] "IP address spoofing," *Wikipedia* [online] https://en.wikipedia.org/wiki/IP_address_spoofing

[126] "What is IP address spoofing, attack definition & anti-spoofing measures," *Imperva Incapsula*, 2018 [online] https://www.incapsula.com/ddos/ip-spoofing.html

[127] B. Gupta et al, "An efficient analytical solution to thwart attacks in public domain," *Intl*. *Conf*. *Adv*. *Comp*. *Comm*. *& Cntrl*. *(ICAC3'09, Mumbai)*, 22-24 Jan 2009 [online] https://arxiv.org/ftp/arxiv/papers/1204/1204.5590.pdf

[128] B. Mistry, "Automated DDoS mitigation is not artificial intelligence," *Corero*, 23 May 2016 [online] https://www.corero.com/blog/727-does-artificial-intelligence-apply-to-network-security-and-ddos-attacks.html

[129] A. Lemke, "Why has no company designed AI that can defend a network from DDoS attacks? " *Quora*, 26 Dec 2014 [online] https://www.quora.com/Why-has-no-company-designed-AI-that-can-defend-a-network-from-DDoS-attacks

[130] T. Claburn, "Hold the phone/ Mystery fake cell towers spotted slurping comms around Washington DC," *The Register*, 3 Apr 2018 [online] https://www.theregister.co.uk/2018/04/03/imsi_catcher_stingray_washington_dc/

[131] K. Iyer, "This is how hackers can hijack cell phone towers!," *TechWorm*, 24 Aug 2016 [online] https://www.techworm.net/2016/08/hackers-can-hijack-cell-phone-towers.html

[132] L. MacVittie, "Layer 4 vs layer 7 DoS attack," *DevCentral*, 8 Jul 2008 [online] https://devcentral.f5.com/articles/layer-4-vs-layer-7-dos-attack

[133] "ICANN," Wikipedia [online] https://en.wikipedia.org/wiki/ICANN

[134] D. Bowie, "IP hijacking," *MIT CISSP*, 2003 [online] http://web.mit.edu/net-security/Camp/2003/DBowie_IP_Hijacking.pdf

[135] K. Barker, "BGP Works on which layer- layer 4 or application layer?" *Cisco Learning Network*, 25 Apr 2011 [online] https://learningnetwork.cisco.com/thread/15656

[136] A. Prohorenko, "TCP hijacking," *TechRepublic*, 23 Mar 2000 [online] https://www.techrepublic.com/article/tcp-hijacking/

[137] R. Mathur, "What is the difference between stalking, spying and surveillance?" *Quora*, 14 May 2017 [online] https://www.quora.com/What-is-the-difference-between-stalking-spying-and-surveillance

[138] A. Robertson, "Phone spying and PRISM Internet surveillance– what's the difference?" *The Verge*, 7 Jun 2013 [online] https://www.theverge.com/2013/6/7/4407782/phone-spying-and-prism-internet-surveillance-whats-the-difference

[139] D.M. Piscitello et al, "The presentation and session layers," in *Open Systems Networking– TCP/IP and OSI*, Boston MA, USA– Addison-Wesley, Sep

1993, ch 11, pp. 247-286 [online] http://securityskeptic.typepad.com/the-security-skeptic/osn/Chapter11.pdf

[140] Ayan, "Layer 5 Attacks (Session Layer Attacks)" *Tech Geek*, 15 Sep 2013 [online] http://bladesecurity.blogspot.com/2013/09/layer-5-attacks-session-layer-attacks.html

[141] "Malware & hackers collect SSH keys to spread keys," *SSH.com*, updated 29 Aug 2017 [online] https://www.ssh.com/malware/

[142] M. Rouse, "What is cross-site scripting (XSS)?" *WhatIs.com*, Feb 2018 [online] https://searchsecurity.techtarget.com/definition/cross-site-scripting

[143] T. Spring, "Sanny malware updates delivery method," *Threat Post*, 26 Mar 2018 [online] https://threatpost.com/sanny-malware-updates-delivery-method/130803/

[144] R. Hayes, "New malware "Sligshot" infecting users for 6 years," *Secplicity*, 15 Mar 2018 [online] https://www.secplicity.org/2018/03/15/new-malware-slingshot-infecting-users-6-years/

[145] D. Piscitello, "the security skeptic," *The Security Skeptic*, 21 Feb 2018 [online] http://securityskeptic.typepad.com/

[146] M. Rouse, "What is zero-day (computer)?" *WhatIs.com*, Nov 2017 [online] https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

[147] A. Zaharia, "Understanding fileless malware infections – The full guide," *Heimdal Security*, 3 Feb 2016 [online] https://heimdalsecurity.com/blog/fileless-malware-infections-guide/

[148] "How to protect against malicious software," *UCLA* [online] http://www.seas.ucla.edu/security/malware.html

[149] "Standard application layer protocol," *ATT&CK* [online] https://attack.mitre.org/wiki/Technique/T1071

[150] Hasherezade, "Malware crypters - the deceptive first layer," *Malwarebytes Labs*, 11 Apr 2016 [online] https://blog.malwarebytes.com/threat-analysis/2015/12/malware-crypters-the-deceptive-first-layer/

[151] "How to Hack Phone Calls?" *Spyze*, 2018 [online] https://www.spyzie.com/call-log/how-to-hack-phone-calls.html

[152] D. Palmer, "This Android malware features a 'dangerous' new attack," *ZDNet*, 9 Jun 2017 [online] https://www.zdnet.com/article/this-android-malware-features-a-dangerous-new-attack/

[153] B. Amro et al, "Malware detection techniques for mobile services," *Intl. J. Mob. Ntwrk Comm & Telematics (ISMNCT)*, vol. 7, no. 4-6, Dec 2017 pp. 1-10 [online] https://arxiv.org/ftp/arxiv/papers/1801/1801.02837.pdf

[154] "What is root access? What can you do with it?" *KnownHost*, 4 Aug 2017 [online] https://www.knownhost.com/blog/root-access-can/

[155] V. Zhang, "GODLESS' mobile malware uses multiple exploits to root devices," *Trend Micro*, 21 Jun 2016 [online] https://blog.trendmicro.com/trendlabs-security-intelligence/godless-mobile-malware-uses-multiple-exploits-root-devices/

[156] "How the CopyCat malware infected Android devices around the world," *Check Point (blog)*, 6 Jul 2017 [online] https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

[157] M. Jansen, " How to root Android phones or tablets (and unroot them) in 2018," *Digital Trends*, 25 Apr 2018 [online] https://www.digitaltrends.com/mobile/how-to-root-android/4/

[158] "How malware can "live forever" through persistent root attacks on Android," *Protectoria* [online] https://www.protectoria.com/2017/10/20/how-malware-can-live-forever-through-persistent-root-attacks-on-android/

[159] D. Kostadinov "Layer seven DDOS attacks" *Infosec Inst.*, 24 Oct 2013 [online] http://resources.infosecinstitute.com/layer-seven-ddos-attacks/#gref

[160] M. Rouse, "What is denial-of-service attack?" *WhatIs.com*, Dec 2016 [online] https://searchsecurity.techtarget.com/definition/denial-of-service

[161] L. Zeitser, "9 reasons for Denial-Of-Service (DoS) attacks- Why do they happen?" *Lenny Zeister* (blog) [online] https://zeltser.com/reasons-for-denial-of-service-attacks/

[162] "2018 data breach investigations report," *Verizon*, 2018 [online] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

[163] "What motivates hackers? Money, secrets, and fun," *Caliypix*, 11 Jul 2017 [online] https://www.calyptix.com/top-threats/motivates-hackers-money-secrets-fun/

[164] "Data breach," *Wikipedia* [online] https://en.wikipedia.org/wiki/Data_breach

[165] L. Bednash, "The true cost of data storage attacks and data theft," *RackTop Systems*, 27 Feb 2018 [online] http://www.racktopsystems.com/true-cost-data-storage-attacks-data-theft/

[166] "What do hackers do with your stolen identity?" *Trend Micro USA*, 21 Jun 2017 [online] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity

[167] M. Rouse, "What is SQL injection?" *WhatIs.com*, Jan 2010 [online] https://searchsoftwarequality.techtarget.com/definition/SQL-injection

[168] P. Kasireddy, "ELI5: What do we mean by 'blockchains are trustless'?" *Medium.com*, 3 Feb 2017 [online] https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6

[169] J.J. Xu, "Are blockchains immune to all malicious attacks," *Xu. Fin. Innov.*, 25 Feb 2016, pp. 1-9 [online] https://jfin-swufe.springeropen.com/track/pdf/10.1186/s40854-016-0046-5

[170] "51% Attack," *Investopedia* [online] https://www.investopedia.com/terms/1/51-attack.asp

[171] "Proof-of-work system," *Wikipedia* [online] https://en.wikipedia.org/wiki/Proof-of-work_system

[172] A. Bulkin, "Explaining blockchain – how proof of work enables trustless consensus," *Keeping Stock*, 3 May 2016 [online] https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

[173] J. McKendrick, " 9 reasons to be cautious with blockchain," *SDNet*, 17 Mar 2018 [online] https://www.zdnet.com/article/9-reasons-to-be-cautious-with-blockchain/

[174] "Distributed ledger technology & cybersecurity," *European Union Agency for Ntwrk & Info Security (ENISA)*, Dec 2016

[175] "Weaknesses," Bitcoin Wiki, updated 4 Feb 2018 [online] https://en.bitcoin.it/wiki/Weaknesses

[176] A. Boveman, "Timejacking & Bitcoin," *Culubas*, 25 May 2011 [online] https://www.upwork.com/job/BitCoin-Timejacking-Attack-explanation_~017812198b85e63e3a/

[177] I. Eyal et al, "How a mining monopoly can attack Bitcoin," *Hacking-Distributed*, 16 Jun 2014 [online] http://hackingdistributed.com/2014/06/16/how-a-mining-monopoly-can-attack-bitcoin/

[178] C.E. Kelso, "Bitcoin not as decentralized as assumed," *Bitcoin.com*, 16 Jan 2018 [online] https://news.bitcoin.com/cornell-researchers-bitcoin-not-as-decentralized-as-assumed/

[179] D. Siegel, "Understanding The DAO Attack," *CoinDesk*, 25 Jun 2016 [online] https://www.coindesk.com/understanding-dao-hack-journalists/

[180] A. Feder et al, "The impact of DDoS and other security shocks on Bitcoin currency exchanges– evidence from Mt. Gox," *J. of Cybersecurity*, vol. 3, no. 2, 2017, pp. 137-144 [online] https://academic.oup.com/cybersecurity/article/3/2/137/4831474

[181] T.J. Rush, "Defeating the Etherium DDoS attacks," *Medium* [online] https://medium.com/@tjayrush/defeating-the-ethereum-ddos-attacks-d3d773a9a063

[182] C. Cimpanu, "74% of all Bitcoin-related sites suffered a DDoS attack," *Bleeping Computer*, 6 Dec 2017 [online] https://www.bleepingcomputer.com/news/security/74-percent-of-all-bitcoin-related-sites-suffered-a-ddos-attack/

[183] Daniel, "Here's how blockchain can make spam and DDoS attacks a thing of the past," *CHIPIN*, 6 Nov 2017 [online] https://www.chipin.com/blockchain-fight-spam-ddos-attacks/

[184] B. Peterson, "Thieves stole potentially millions of dollars in Bitcoin in a hacking attack on a cryptocurrency company," *Business Insider*, 6 Dec 2017 [online] http://www.businessinsider.com/nicehash-bitcoin-wallet-hacked-contents-stolen-in-security-breach-2017-12

[185] D. Storm, " Blockchain exploits and mining attacks on the rise as cryptocurrency prices skyrocket," *Security Intelligence*, 8 Jan 2018 [online] https://securityintelligence.com/blockchain-exploits-and-mining-attacks-on-the-rise-as-cryptocurrency-prices-skyrocket/

[186] N. Whigham, "Restaurant-goer has Bitcoins stolen over unsecured public wireless network," *News.com.au*, 23 Nov 2017 [online] http://www.news.com.au/technology/online/hacking/restaurantgoer-has-bitcoins-stolen-over-unsecured-public-wireless-network/news-story/a82d75eb85763ee3d38678b430df3bf0

[187] T.B. Lee, "A brief history of Bitcoin hacks and frauds," *Ars Technica*, 5 Dec 2017 [online] https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/

[188] J.J. Roberts, "How Bitcoin is stolen: 5 common threats," *Fortune– The Ledger*, 8 Dec 2017 [online] http://fortune.com/2017/12/08/bitcoin-theft/

[189] "Securing your wallet" Bitcoin.org [online] https://bitcoin.org/en/secure-your-wallet

[190] R.A. Grimes, "Hacking bitcoin and blockchain," *CSO*, 12 Dec 2017 [online] https://www.csoonline.com/article/3241121/cyber-attacks-espionage/hacking-bitcoin-and-blockchain.html

[191] "How Bitcoins can be stolen: botnets, viruses, phishing, and more" *Coinbrief*, 2 Jan 2018 [online] https://99bitcoins.com/ways-bitcoins-stolen/

[192] S. Meiklejohn et al, "A Fistful of Bitcoins/ Characterizing payments among men with no names," *IMC*, 2013 [online] https://cseweb.ucsd.edu/smeiklejohn/files/imc13.pdf

[193] A. Coyler, "A fistful of Bitcoins– Characterizing payments among men with no names," *The Morning Paper*, 20 Feb 2017 [online] https://blog.acolyer.org/2017/02/20/a-fistful-of-bitcoins-characterizing-payments-among-men-with-no-names/

[194] A. Coyler, "Survey on security and privacy issues of Bitcoin," *The Morning Paper*, 15 Feb 2018 [online] https://blog.acolyer.org/2018/02/15/a-survey-on-security-and-privacy-issues-of-bitcoin/

[195] J. Barcelo, " User Privacy in the public Bitcoin blockchain," *J. Latex Class Files*, vol.6, no. 1, Jan 2007, pp. 1-4 [online] https://pdfs.semanticscholar.org/549e/7f042fe0aa979d95348f0e04939b2b451f18.pdf

[196] S. Goldfeder et al, "When the cookie meets the blockchain– Privacy risks of web payments via cryptocurrencies," *arXiv.org*, 16 Aug 2017, pp. 1-19 [online] https://arxiv.org/pdf/1708.04748.pdf

[197] H. Halpin et al., "Introduction to Security and Privacy on the Blockchain," *IEEE Euro Symp Security Prvcy Wrksp (EuroS&PW, Paris)*, 21-24 Apr 2017, pp. 1-3 [online] https://hal.inria.fr/hal-01673293/file/intro_final.pdf

[198] M. Borge et al, "Proof-of-Personhood– Redemocritizing permissionless cryptocurrencies," *IEEE Euro Symp Security Prvcy Wrksp (EuroS&PW, Paris)*, 21-24 Apr 2017, pp. 1-5

[199] "Bitcoin's blockchain is full of content that can land you in jail," *The Next Web*, 21 Mar 2018 [online] https://thenextweb.com/hardfork/2018/03/21/bitcoins-blockchain-content-land-in-jail/

[200] R. Matzatt et al, "A quantitative analysis of the impact of arbitrary blockchain content on Bitcoin," *Intl. Conf. Financial Crypto, Data Security*, 2018 [online] https://fc18.ifca.ai/preproceedings/6.pdf

[201] "INTERPOL cyber research identifies malware threat to virtual currencies," *INTERPOL*, 26 Mar 2015 [online] https://fc18.ifca.ai/preproceedings/6.pdf

[202] Tania H. "A guide to smart contracts and their implementation," *rubygrage.org*, 2018 [online] https://rubygarage.org/blog/guide-to-smart-contracts

[203] A. Colyer, "Designing secure Ethereum smart contracts– a finite state machine approach," *The Morning Paper*, 20 Mar 2018 [online] https://blog.acolyer.org/2018/03/20/designing-secure-ethereum-smart-contracts-a-finite-state-machine-approach/

[204] N. Szabo "Smart Contracts: building blocks for digital markets," *N. Szabo* [online] http://www.fon.hum.uva.nl/rob/Courses /InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[205] "Ethereum Definition," *Investopedia* [online] https://www.investopedia.com/terms/e/ethereum.asp

[206] K. Cook, "Blockchain 101: If Bitcoin's a fraud, how is Ethereum different?" *Nasdaq.com*, 7 Nov. 2017 [online] https://www.nasdaq.com/article/blockchain-101-if-bitcoins-a-fraud-how-is-ethereum-different-cm873522

[207] Ethereum Vs Bitcoin- What's The Main Difference?" *Huffpost*," 20 Dec 2016 [online] https://www.huffingtonpost.com/ameer-rosic-/ethereum-vs-bitcoin-whats_b_13735404.html

[208] R. Marvin, "Blockchain in 2017/ the year of smart contracts," *PCMag.com*, 12 Dec 2016 [online] https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts

[209] J. Young, "Blockchain can help save companies billions of dollars with fraud protection: Research," *CoinTelegraph*, 7 Jul 2017 [online] https://cointelegraph.com/news/blockchain-can-help-save-companies-billions-of-dollars-with-fraud-protection-research

[210] A. Kakadiya, "India's largest bank will now use blockchain to fight fraud," *Bits*, 22 Nov 2017 [online] https://www.bitsonline.com/india-largest-bank-blockchain-fraud/

[211] "EthTrade Club Review/ Ethereum "smart contracts" Ponzi fraud," *MLM Reviews*, 30 Apr 2018 [online] http://behindmlm.com/mlm-reviews/ethtrade-club-review-ethereum-smart-contracts-ponzi-fraud/

[212] H. Subramanian, "Fraud in Blockchains and Smart Contracts," *Finextra*, 2 May 2018 [online] https://www.finextra.com/blogposting/12293/fraud-in-blockchains-and-smart-contracts

[213] G. Greenspan, "Why Many Smart Contract Use Cases Are Simply Impossible," *CoinDesk*, 17 Apr 2016 [online] https://www.coindesk.com/three-smart-contract-misconceptions/

[214] P. Sayer, "A blockchain 'smart contract' could cost investors millions," *PCWorld*, 20 Jun 2016 [online] https://www.pcworld.com/article/3086211/a-blockchain-smart-contract-could-cost-investors-millions.html

[215] H. Lovells, "Blockchain smart contracts need a new kind of due diligence," *Lexology*, 21 Mar 2018 [online] https://www.lexology.com/library/detail.aspx?g=bebe2353-69c3-425b-89ad-d22ffd7b469c

[216] B. Dickson, "How blockchain can help fight cyberattacks," *TechCrunch*, 3 Dec 2016 [online] https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/

[217] G. Pisco, "Bitcoin exchanges are targets of global DDoS attacks/ report," *Bitcoin Magazine*, 5 Dec 2017 [online] https://bitcoinmagazine.com/articles/bitcoin-exchanges-are-favorite-targets-global-ddos-attacks-report/

[218] "Bitcoin Energy Consumption Index," *Digiconomist*, 2018 [online] https://digiconomist.net/bitcoin-energy-consumption

[219] "Ethereum Energy Consumption," *Digiconomist*, 2018 [online] https://digiconomist.net/ethereum-energy-consumption

[220] "Bitcoin mining now consuming more electricity than 159 countries including Ireland & most countries In Africa," *Powercompare UK*, 2018 [online] https://powercompare.co.uk/bitcoin/

[221] "The energy consumption of the crypto world," *Hacker Noon*, 7 Dec 2017 [online] https://hackernoon.com/the-energy-consumption-of-the-crypto-world-b20e3628e0d2

[222] N. Kobie, "How much energy does bitcoin mining really use? It's complicated," *Wired UK*, 2 Dec 2017 [online] http://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use

[223] W.M. Peaster, "Bitcoin energy consumption– facing the environmental concerns," *Blockonomi*, 4 Apr 2018 [online] https://blockonomi.com/bitcoin-energy-consumption/

[224] B. Jones, "The hidden cost of Bitcoin? Our environment," *Futurism*, 18 Dec 2017 [online] https://futurism.com/hidden-cost-bitcoin-our-environment/

[225] T. Loh, "Bitcoin could end up using more power than electric cars," *Bloomberg*, 10 Jan 2018 [online] https://www.bloomberg.com/news/articles/2018-01-10/bitcoin-outshines-electric-cars-as-driver-of-global-power-use

[226] "Proof-of-work system," *Wikipedia* [online] https://en.wikipedia.org/wiki/Proof-of-work_system

[227] S. Nakamoto, "Bitcoin P2P e-cash paper", *Gmane*, 31 Oct 2008 [online] http://article.gmane.org/gmane.comp.encryption.general/12588/

[228] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" *bitcoin.org (whitepaper)*, 24 May 2009 [online] https://bitcoin.org/bitcoin.pdf

[229] "Blockchain Size," *Bitcoin.com*, 2 May 2018 [online] https://charts.bitcoin.com/chart/blockchain-size

[230] "Average Block Size" Blockchain," *Bitcoin.com* 2018 [online] https://charts.bitcoin.com/chart/blockchain-size

[231] D. Dinkins, "Satoshi's Best Kept Secret– Why is There a 1 MB Limit to Bitcoin Block Size," *CoinTelegraph*, 19 Sep 2017 [online] https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size

[232] "Block size limit controversy," *Bitcoin Wiki* [online] https://en.bitcoin.it/wiki/Block_size_limit_controversy

[233] S. Nadeem, "If we lived in a Bitcoin future, how big would the blockchain have to be? *Hacker Noon*, 5 Dec 2017 [online] https://hackernoon.com/if-we-lived-in-a-bitcoin-future-how-big-would-the-blockchain-have-to-be-bd07b282416f

[234] "Proof of Stake (PoS) Definition," *Investopedia* [online] https://www.investopedia.com/terms/p/proof-stake-pos.asp

[235] A. Hickey, "IoT-Based DDoS Threats Loom," *Network Computing*, 12 Jan 2018 [online] https://www.networkcomputing.com/network-security/iot-based-ddos-threats-loom/1614938156

[236] A. Dorri, "Blockchain for IoT security and privacy– The case study of a smart home," *IEEE Pericom Wrkshp on Security, Privacy and Trust in IoT*, May 2017 [online] https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_and_Privacy_The_Case_Study_of_a_Smart_Home

[237] L. Toms, "Beware! data and identity theft in the IoT," *GlobalSign*, 22 Mar 2016 [online] https://www.globalsign.com/en/blog/identity-theft-in-the-iot/

[238] M. Anderson, "experts call for global data sharing to defend against cyberattacks," *IEEE Spectrum*, 17 Apr 2018 [online] https://spectrum.ieee.org/tech-talk/telecom/security/report-nextlevel-cyberattacks-demand-data-clearinghouse?utm_source=techalert&utm_campaign=techalert-04-19-18&utm_medium=email

[239] S. Dilek et al, "Applications of artificial intelligence techniques to combatting cyber crimes– a review, *Intl. J. Art. Intel. & Apps (JAIA)*, vol.6, no. 1, Jan 2015, pp. 21-39 [online] https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf

[240] P. Hernandez, "AI's future role in cybersecurity," *eSecurity Planet*, 7 Feb 2018 [online] https://www.esecurityplanet.com/network-security/ais-future-in-cybersecurity.html

[241] G. Dvorsky, "Hackers have already started to weaponize artificial intelligence," *Gizmodo*, 11 Sep 2017 [online] https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425

[242] S. Salinas, "How artificial intelligence can stop the malware threats of the future," *Information Age*, 14 Nov 2017 [online] http://www.information-age.com/artificial-intelligence-can-stop-malware-threats-future-123469554/

[243] "Post-quantum cryptography," *Wikipedia* [online] https://en.wikipedia.org/wiki/Post-quantum_cryptography

[244] W. Hurd, "Quantum Computing Is the Next Big Security Risk," *Wired*, 7 Dec 2017 [online] https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/

[245] S. Manning, "The Architect transcript," *The Matrix Reloaded* (2003 movie), 30 May 2003 [online] https://scottmanning.com/content/the-architect-transcript/

[246] R. Benzmuller, "Malware numbers 2017" *GData*, 27 Mar 2018 [online] https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017

[247] "What are Web threats– Internet browser malware," *Kaspersky Lab USA*, 2018 [online] https://usa.kaspersky.com/resource-center/threats/web

[248] A. Ng, "Gang robs Russian banks with over 1M hacked Android phones," *CNET*, 22 May 2017 [online] https://www.cnet.com/uk/news/russian-gang-robs-banks-over-1-million-hacked-android-phones/

[249] "Facts + statistics– Identity theft and cybercrime," *Insurance Information Institute*, 2017 [online] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

[250] R.E. Smith, "Are Web transactions safe?" *NOVA Online*, Nov 2000 [online] http://www.pbs.org/wgbh/nova/decoding/web.html

[251] "Evasive code-signed malware flourished before Stuxnet (and still does)," *Ars Technica* [online] https://firenewsfeed.com/technology/689126

[252] C. Jeannot, "Trust issues surrounding data privacy– Blockchain is the new backbone to the Internet," *ITProPortal*, 2 May 2018 [online] https://www.itproportal.com/features/trust-issues-surrounding-data-privacy-blockchain-is-the-new-backbone-to-the-internet/

[253] V. Manganaro, "Steve Wozniak, 40 years later & the essence of innovation," *Tech. Concepts Grp. Intl. (Russia)*, 29 Jun 2017

[254] N. Spivak, "Web 3.0: the third generation web is coming," *Lifeboat Foundation*, 2007 [online] https://lifeboat.com/ex/web.3.0

[255] N.K. Gyamfi, "Security challenges in implementing semantic web unifying-logic," *Research Gate*, Dec 2014 [online] https://www.researchgate.net/publication/308400135_Security_Challenges_in_Implementing_Semantic_Web-Unifying_Logic

[256] M. Clifton, " Semantic database– concept, architecture, and implementation," *Code Project*, 25 Oct 2014 [online] https://www.codeproject.com/Articles/832959/Semantic-Database-Concept-Architecture-and-Impleme

[257] A. Tinworth, "NEXT16– Blockchain will build Web 3.0, says Jamie Burke," *NEXT Conference*, 23 Sep 2016 [online] https://nextconf.eu/2016/09/next16-blockchain-will-build-web-3-0-says-jamie-burke/

[258] "Defining Web 3.0 (aka making sense of blockchain)," *Blocksplain*, 9 May 2018 [online] https://blocksplain.com/2018/05 /09/web3-blockchain/

[259] V. Singh, "An Internet of blockchains," *Kryptos Studio (Medium)*, 14 Dec 2017 [online] https://medium.com/kryptosstudio/an-internet-of-blockchains-2dd4fcc2008f

[260] M.G. Zago, "Why the net giants are worried about the Web 3.0," *Medium*, 16 Mar 2018 [online] https://medium.com/@matteozago/why-the-net-giants-are-worried-about-the-web-3-0-44b2d3620da5

[261] A. Walner, "How many cryptocurrencies do we really need?" *Wolverine Blockchain*," 4 Dec 2017 [online] https://medium.com/wolverineblockchain/how-many-cryptocurrencies-do-we-really-need-eac23d8737a9

[262] P, Schmid, "Is blockchain the next Internet?" *IA Magazine*, 20 Sep 2017 [online] https://www.iamagazine.com/viewpoints/read/2017/09/20/is-blockchain-the-next-internet

[263] Cretin, "It's 2018 – Blockchain is on its way to becoming the new Internet," *Medium*, 4 Jan 2018 [online] https://medium.com/@andrewcretin/its-2018-blockchain-is-on-it-s-way-to-become-the-new-internet-7055ed6851ec

[264] A. Scott-Briggs, "Is blockchain the new Internet," *TechBullion*, 27 Dec 2017 [online] https://www.techbullion.com/blockchain-technology-new-internet/

[265] H-J Pokmann, "Blockchain is the Internet (Web 3.0)," *Pulse*, 2 Apr 2018 [online] https://www.linkedin.com/pulse/blockchain-internet-web-30-hans-j%C3%BCrgen-pokmann

[266] "Bitcoin network," *Wikipedia* [online] https://en.wikipedia.org/wiki/Bitcoin_network

[267] R. Marvin, "Blockchain– the invisible technology that's changing the world," *PCMag.com*, 29 Aug 2017 [online] https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor

[268] "Internet," *Wikipedia* [online] https://en.wikipedia.org/wiki/Internet

[269] "What is a peer to peer network (P2P)?" *Lisk*, 2018 [online] https://blockgeeks.com/guides/what-is-blockchain-technology/

[270] A. Gonsalves, "Cisco says blockchain ledger technology has networking role," *SearchSDN*, 1 Aug 2017 [online] https://searchsdn.techtarget.com/news/450423763/Cisco-says-blockchain-ledger-technology-has-networking-role

[271] Z. Cole, "How blockchain technology could affect the future of network engineering," *Network World*, 9 Nov 2017 [online] https://www.networkworld.com/article/3236479/asset-management/how-blockchain-technology-could-affect-the-future-of-network-engineering.html

[272] M. Iansiti at al, "The truth about Blockchain," *Harvard Business Review*, Feb 2017 [online] https://hbr.org/2017/01/the-truth-about-blockchain

[273] L. Mearlan, "What is blockchain? The most disruptive tech in decades," *Computerworld*, 18 May 2018 [online] https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html

[274] "What is a communication protocol?" *Techopedia* [online] https://www.techopedia.com/definition/25705/communication-protocol

[275] "Communication protocol," *Wikipedia*, https://en.wikipedia.org/wiki/Communication_protocol

[276] "Lists of network protocols," *Wikipedia* [online] https://en.wikipedia.org/wiki/Communication_protocol

[277] "Chapter 6– common protocols," *CDN TTGT Media*, pp. 61-75 [online] https://cdn.ttgtmedia.com/searchNetworking/downloads/commonprotocols_ppa_ch06.pdf

[278] J. Monegro, "Fat protocols," *Union Square Ventures*, 8 Aug 2016 [online] http://www.usv.com/blog/fat-protocols

[279] K. Grimm, "Explaining fat protocols with pancakes (Joel Monegro)," *The Daily Bit*, 20 Mar 2018 [online] https://medium.com/the-daily-bit/explaining-fat-protocols-with-pancakes-joel-monegro-2cb85c766e82

[280] T. Pearson, "Will cryptocurrency have fat protocols or thin?" *taylerpearson.com* [online] https://taylorpearson.me/fat-thin/

[281] T. Paivinen, "Thin protocols," *Zeppelin Blog*, 3 Oct 2017 [online] https://blog.zeppelin.solutions/thin-protocols-cc872258379f

[282] E. Van Ness, "There's no such thing as 'fat protocols'," *evanvanness.com*, 24 Oct 2017 [online] https://www.evanvanness.com/post/166666272011/theres-no-such-thing-as-fat-protocols

[283] J. Brukman, "Fat protocols are not an investment thesis," *The Blockchain Investments Blog*, 26 Oct 2017 [online] https://blog.coinfund.io/fat-protocols-are-not-an-investment-thesis-17c8837c2734

[284] A. Oberhauser, "Blockchain protocol series– Introduction," *The Blockchain (Medium)*, 24 May 2015 [online] https://medium.com/the-blockchain/blockchain-protocol-series-introduction-79d7d9ea899

[285] D. Xiao, "The four layers of the Blockchain," *Medium*, 21 Jun 2016 [online] https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f

[286] A. Rosic, "What is blockchain technology– a step-by-step guide for beginners," *Block Geeks* [online] https://blockgeeks.com/guides/what-is-blockchain-technology/

[287] F. Phillips, "The 4 types of blockchain networks explained," *JD Supra*, 16 Feb 2018 [online] https://www.jdsupra.com/legalnews/the-4-types-of-blockchain-networks-83225/

[288] A. Chakraverty, "Here's how I built a private blockchain network, and you can too," *Hacker Noon*, 4 Sep 2017 [online] https://hackernoon.com/heres-how-i-built-a-private-blockchain-network-and-you-can-too-62ca7db556c0

[289] L. Mearlan, "How blockchain could solve the Internet privacy problem," *Computerworld*, 9 Apr 2018 [online] https://www.computerworld.com/article/3267930/blockchain/how-blockchain-could-solve-the-internet-privacy-problem.html

[290] M.J. Casey, "Can blockchain save us from the Internet's original sin?" *CoinDesk*, 27 Oct 2017 [online] https://www.coindesk.com/can-blockchain-save-us-from-the-internets-original-sin/

[291] B. Collins, "Blockchain– an Internet we can trust?" *IT Pro*, 12 Jan 2018 [online] http://www.itpro.co.uk/blockchain/30264/blockchain-an-internet-we-can-trust

[292] "What are blockchain's issues and limitations?" *CoinDesk* [online] https://www.coindesk.com/information/blockchains-issues-limitations/

[293] "Adjunct," *Wiktionary* [online] https://en.wiktionary.org/wiki/adjunct

[294] "What is dynamic routing?" *Techopedia* [online] https://www.techopedia.com/definition/19047/dynamic-routing

[295] "Mesh networking" *Wikipedia* [online] https://en.wikipedia.org/wiki/Mesh_networking

[296] "Propagation delay," *Wikipedia* [online] https://en.wikipedia.org/wiki/Propagation_delay

[297] "What is the fixed-line network and how does it work?" *NFON* [online] https://www.nfon.com/en_de/cloud-telephone-system/resources/glossary/the-fixed-line-network/

[298] "Backbone network," *Wikipedia* [online] https://en.wikipedia.org/wiki/backbone_network

[299] "Dark fiber," *Wikipedia* [online] https://en.wikipedia.org/wiki/dark_fibre

[300] "Backhaul (telecommunications)," *Wikipedia* [online] https://en.wikipedia.org/wiki/Backhaul_(telecommunications)

[301] "What is wireless network?" *Techopedia* [online] https://www.techopedia.com/definition/26186/wireless-network

[302] "Peer-to-peer," *Wikipedia* [online] https://en.wikipedia.org/wiki/Peer-to-peer

[303] Tech explained– Hash-puzzle and proof of work," *3583 bytes free*, ready? 6 Sep 2016 [online] https://3583bytesready.net/2016/09/06/hash-puzzles-proofs-work-bitcoin/

[304] C. Dwan, "Proof of work and the nonce," *dwan.org*, 13 Jul 2017 [online] https://dwan.org/index.php/2017/06/13/proof-of-work-and-the-nonce/

[305] "Cryptographic nonce," Wikipedia, https://en.wikipedia.org/wiki/cryptographic_nonce

[306] J. Tirone, "A prime number could be the answer to Bitcoin's power problem," *Bloomberg*, 11 Jan 2018 [online] https://www.bloomberg.com/news/articles/2018-01-11/bitcoin-seen-addressing-power-hog-problem-with-prime-number-find

[307] "Primecoin: cryptocurrency with prime number Proof-of-Work," *primecoin.io*, 7 Jul 2013 [online] http://primecoin.io/bin/primecoin-paper.pdf

[308] "Native (computing)," Wikipedia [online] https://en.wikipedia.org/wiki/Native_(computing)

[309] "Cloud native networking," *Cloud Native Computing Foundation*, 12 Jan 2017 [online] https://www.cncf.io/wp-content/uploads/2017/11/CNCF-Networking-Webinar-final-1-1.pdf

[310] "Private network," *Wikipedia* [online] https://en.wikipedia.org/wiki/Private_network

[311] "What is OTT (Over-the-Top Communications)?" Ribbon Communications [online] https://ribboncommunications.com/company/get-help/glossary/ott-over-top-communications

[312] L. Nohling, "What Does OTT or "Over the Top communications" really mean?" *edgewaternetworks.com*, 2 Feb 2016 [online] https://www.edgewaternetworks.com/blog/2016/02/what-does-over-the-top-communications-really-mean/

[313] "Telco-OTT," *Wikipedia* [online] https://en.wikipedia.org/wiki/Telco-OTT

[314] "IEEE 802.11," *Wikipedia* [online] http://en.wikipedia.org/wiki/IEEE_802.11

[315] "Ethernet physical layer," *Wikipedia* [online] https://en.wikipedia.org/wiki/Ethernet_physical_layer

[316] "DOCSIS," *Wikipedia* [online] https://en.wikipedia.org/wiki/DOCSIS

[317] "Comparison of wireless data standards," *Wikipedia* [online] https://en.wikipedia.org/wiki/Comparison_of_wireless_data_standards

[318] L. Laurenson, "A more pseudonymous Internet," *The Atlantic*, 8 Aug 2014 [online] https://www.theatlantic.com/technology/archive /2014/08/a-more-pseudonymous-internet/375704/

[319] "Pseudonymity,'" *Wikipedia* [online] https://en.wikipedia.org/wiki/Pseudonymity

[320] M. Collins, "The ideology of anonymity and pseudonymity," *Huffpost*, 2 Oct 2013 [online] https://www.huffingtonpost.com/malcolm-collins/online-anonymity_b_3695851.html

[321] M. Suster, "Why pseudonymity is such an important concept," *Both Sides of the Table*, 21 Sep 2011 [online] https://bothsidesofthetable.com/why-pseudonymity-is-such-an-important-concept-945700c909fb

[322] M. Doyle, "What is Network Metadata?" *LoveMyTool.com*, 11 Jul 2016 [online] http://www.lovemytool.com/blog/2016/07/what-is-network-metadata-network-metadata-is-human-readable-data-that-describes-your-network-traffic-it-is-generated-and-c.html

[323] "The 5 worst examples of IoT hacking and vulnerabilities in recorded history," *IoT For All*, 10 May 2017 [online] https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

[324] "Quality of service networking," *Cisco* [online] http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

[325] "Quality of service," *Wikipedia*, [online] https://en.wikipedia.org/wiki/Quality_of_service

[326] "UPROTEL- Unified Professional Telecommunication," *uprotel.com* [online] https://www.uprotel.com/

[327] "TETRAFlash" *TETRAApplications.com*, April 2011 [online] http://manualzz.com/doc/28930760/tetraflash-april-2011-v2---tetra

[328] "Security Requirements for Cryptographic Modules" in *Federal Information Processing Standards Publication (FIPS pub 140-2)*, Natl. Inst. Standards & Tech (NIST), 25 May 2011, pp. 1-69 [online] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[329] "FIPS 140-2," *Wikipedia* [online] https://en.wikipedia.org/wiki/FIPS_140-2

[330] I. Verzun, O. Holub, R.K. Williams, "Secure dynamic network and protocol," *US patent no. 9,998,434*, priority 28 Jul 2015, issued 12 Jun 2018

[331] "What is the difference between public and permissioned blockchains?" *Coindesk* [online] https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/

[332] J. Bennet, "Public vs private blockchain protocols– what's the difference?" *Brave New Coin*, 19 Mar 2018 [online] https://bravenewcoin.com/news/public-vs-private-blockchain-protocols-whats-the-difference/

[333] S. Brunozzi, "Making sense of non-public blockchains," *The Startup (Medium)*, 2 Apr 2018 [online] https://medium.com/swlh/making-sense-of-non-public-blockchains-915d5d538ae6

[334] S. Set, "Public, private, permissioned blockchains compared," *Investopedia*, 10 Apr 2018 [online] https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

[335] H. Kuchler, "Cyber attacks raise questions about blockchain security," *Financial Times*, 12 Sep 2016 [online] https://www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a

[336] "Blockchain risk management," *Deloitte*, 2017 [online] https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-blockchain-risk-management-27092017.pdf

[337] P Kasireddy, "Fundamental challenges with public blockchains," *Medium*, 11 Dec 2017 [online] https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

[338] P. Kasireddy, "Blockchains don't scale. Not today, at least. But there's hope," *hackernoon.com*, 23 Aug 2017 [online] https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

[339] T. Simonte, " The decentralized Internet is here, with some glitches," *Wired*, 5 Mar 2018 [online] https://www.wired.com/story/the-decentralized-internet-is-here-with-some-glitches/

[340] I. Verzun, O. Holub, and R.K. Williams, "Secure dynamic network and protocol," *US patent app 15/946862*, filed 6 Apr 2018 (divisional)

[341] I. Verzun, O. Holub, and R.K. Williams, "Secure dynamic network and protocol," *PCT patent app PCT/US16/14643*, filed 23 Jan 2016

[342] I. Verzun, O. Holub, and R.K. Williams, "HyperSecure last mile communications," *US patent app 15/943418*, filed 2 Apr 2018, priority date 3 Apr 2017

[343] I. Verzun and R.K. Williams, "System for open source decentralized electronic communication and e-commerce," *US prov patent app 62/625220*, filed 1 Feb 2018

[344] I. Verzun and R.K. Williams, "The HyperSphere– a real-time cybersecure privacy network with embedded DyDAG dual cryptocurrency for global e-commerce, "*US prov patent app 62/696160*, filed 10 Jul 2018

[345] R.C. Merkle, "Secure communication over insecure channels," *Puzzles*, 7 Dec 1975 [online] http://www.merkle.com/1974 /Puzzles1975.12.07.pdf

[346] R.C. Merkle, "Secure communication over insecure channels," Comm *of ACM*, vol. 21, no. 4, Apr 1978, pp. 294-299 [online] http://hashcash.org/papers/merkle-puzzle.pdf

[347] R. Merkle, A. Weber, ed., "Secure communications over insecure channels," *ITAS*, 2002 [online] http://www.itas.kit.edu/pub/m/2002/mewe02a.html

[348] S. Pasini, "Secure communications over insecure channels using a authenticated channel," *École Polytech Fed de Lauusanne (masters thesis)*, 6 Sep 2005 [online] https://infoscience.epfl.ch/record/99514/files/Pas05.pdf

[349] Hromkovič et al, "Dissemination of Information in Interconnection Networks (Broadcasting & Gossiping)," in *Combinational Network Theory (Chapter 5)*, Berlin-Heidelberg Germany– Springer-Verlag © 1995, pp. 125-212 [online] https://link.springer.com/chapter/10.1007/978-1-4757-2491-2_5

[350] S. Skiena, *Implementing discrete mathematics- combinatorics and graph theory with Mathematica*, Addison-Wesley © 1990 [online] http://www.wolfram.com/books/profile.cgi?id=38

[351] C.E. Shannon, "A mathematical theory of communication," *Bell Sys Tech J.*, vol. 27, Jul-Oct 1948, pp. 379-423 and 623-656 [online] http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

[352] “Inter-process communication,” *Wikipedia* [online] https://en.wikipedia.org/wiki/Inter-process_communication

[353] G.V. Bochmann, “Finite state description of communication protocols,” *Computer Networks*, vol. 2, no. 4-5, Sep-Oct 1978, pp. 361-372 [online] https://www.sciencedirect.com/science/article/pii/0376507578900156

[354] S. Raman et al, "A model, analysis, and protocol framework for soft state-based communication," *ACM SIGCOMM Comp Comm Rev*, vol. 29, no. 4, Oct 1999, pp. 15-25 [online] https://dl.acm.org/citation.cfm?id=316202

[355] "Representational state transfer," *Wikipedia* [online] https://en.wikipedia.org/wiki/Representational_state_transfer

[356] "Stateless protocol," *Wikipedia* [online] https://en.wikipedia.org/wiki/Stateless_protocol

[357] Understanding VPN IPSec tunnel mode and IPSec transport mode– What's the difference?" *firewall*.cx, 20 Jun 2016 [online] http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

[358] K. Shaw, "The OSI model explained– How to understand (and remember) the 7-layer network model," *Network World*, 4 Dec 2017 [online] https://www.networkworld.com/article/3239677/lan-wan/the-osi-model-explained-how-to-understand-and-remember-the-7-layer-network-model.html

[359] "Edge Internet transport layer application communication protocol specifications,” *Australian Sec & Investment Commission*, v1.03, 27 Jan 2016 [online] https://asic.gov.au/media/4055465/internet_acpspec.pdf

[360] “SSL Certificate framework 101– How does the browser actually verify the validity of a given server certificate?” *Information Security* [online] https://security.stackexchange.com/questions/56389/ssl-certificate-framework-101-how-does-the-browser-actually-verify-the-validity

[361] L. Phifer, "Tunnel vision– choosing a VPN– SSL VPN vs. IPSec VPN," *Info Sec Mag*, Aug 2003 [online] https://searchsecurity.techtarget.com/feature/tunnel-vision-choosing-a-VPN-SSL-VPN-vs-IPSec-VPN

[362] R. Böhme, ed. “Advanced statistical steganalysis” in *Information Security and Cryptography*, Berlin-Heidelberg Germany– Springer-Verlag © 2010 [online] https://www.amazon.com/advanced-statistical-steganalysis-information-cryptography/dp/3642143121/

[363] C. Swenson, *Modern Cryptanalysis– Techniques for Advanced Code Breaking*, Indianapolis IN, USA– Wiley © 2008 [online] https://www.amazon.com/modern-cryptanalysis-techniques-advanced-breaking/dp/047013593X

[364] W. Diffie et al, "New directions in cryptography,” *IEEE trans info tech*, vol. 22, no. 6, Nov 1976, pp. 644-655 [online] https://www.researchgate.net/publication/3082825_new_directions_in_cryptography

[365] W. Stallings, *Cryptography and Network Security– Principles and Practice*, 7th ed., Essex, England: Pearson Educ. Ltd. © 2017 [online] https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/0134444280

[366] "Certificate authority," *Wikipedia* [online] https://en.wikipedia.org/wiki/Certificate_authority

[367] J.C. Villanueva, "An overview of how digital certificates work," *Scape*, 14 Apr 2015 [online] https://www.jscape.com/blog/an-overview-of-how-digital-certificates-work

[368] J. Wu at al, “A decentralized certification authority based on real world trust relationships,” *2008 Intl Conf. on Comp Sci & Software Eng*, Jan 2008, pp. 1123-1126 [online] https://www.researchgate.net/publication/221195734_A_Decentralized_certification_authority_based_on_real_world_trust_relationships

[369] K. Raina, *PKI security solutions for the enterprise*, Indianapolis– Wiley 2003 © 2003, pp. 5-17, 179-225 [online] https://www.amazon.com/PKI-Security-Solutions-Enterprise-Paper/dp/047131529X

[370] "Applying for an Identity Document," *Western Cape Gov* [online] https://www.westerncape.gov.za/service/applying-identity-document

[371] W.R. Simpson, *Enterprise Level Security– Securing Information Systems in an Uncertain World*, 1st ed., Boca Raton– CRC Press, © 2003 pp. 55-67, 77-84, 201-206, 241-258, 303-334 [online] https://www.amazon.com/enterprise-level-security-information-uncertain/dp/1498764452

[372] M. Obaidat, *Security of e-Systems and Computer Networks*, Cambridge– Cambridge Univ. Press © 2007 pp. 80-102 [online] https://www.cambridge.org/core/books/security-of-esystems-and-computer-networks /ff5acb7addc6c5ecc2d2bd0a92a09152

[373] D. Cooper et al, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," *Internet Engineering Task Force (IETF)*, May 2008 [online] https://tools.ietf.org/html/rfc5280

[374] P. Yee, "Updates to the Internet X.509 public key, infrastructure certificate and certificate revocation list (CRL) profile," *Internet Engineering Task Force (IETF)*, Jan 2013 [online] https://tools.ietf.org/pdf/rfc6818.pdf

[375] "What is the purpose of the intermediate CA certificate?" *Thawte* [online] https://knowledge.digicert.com/solution/SO4261.html

[376] "Public key certificate," *Wikipedia* [online] https://en.wikipedia.org/wiki/Public_key_certificate

[377] T. Norman, *Integrated Security Systems Design– A Complete Reference for Building Enterprise-Wide Digital Security Systems*, 2nd ed., Butterworth-Heinemann © 2005 pp.201-247 [online] https://www.elsevier.com/books/integrated-security-systems-design/norman/978-0-12-800022-9

[378] C. Guerrier, *Security and Privacy in the Digital Era (Innovation, Entrepreneurship, Management– Innovation and Technology)*, 1st ed., Hoboken NJ USA– Wiley © 2016, pp. 3-16, 29-32, 179-223 [online] https://www.amazon.com/security-privacy-innovation-entrepreneurship-management/dp/17863 00788

[379] M. Nakhjiri, *AAA and Network Security for Mobile Access– Radius, Diameter, EAP, PKI and IP Mobility*, 1st ed., West Sussex, England, UK– Wiley © 2005 pp. 8-69, 203-233 [online] https://www.amazon.com/AAA-network-security-mobile-access/dp/0470011947

[380] R.C. Merkle, "Secrecy, authentication, and public key systems," *Stanford Elec Labs (Tech report 1979-1)*, Jun 1979 [online] http://www.merkle.com/papers/thesis1979.pdf

[381] R. Morselli et al, “KeyChains– A decentralized public-key infrastructure,” *Univ of MD Tech Report CS-TR-4788*, Dec 2006 [online] https://drum.lib.umd.edu/bitstream/handle/1903/3332/0.pdf;sequence=1

[382] "A Microsoft PKI quick guide - part 2- design,” *Techgenix.com* [online] http://techgenix.com/microsoft-pki-quick-guide-part2-design/

[383] R. Sinn, "Understanding the public key infrastructure" *openloop.com* [online] http://www.openloop.com/article/pki/pkiintro.html

[384] J. Katz et al, *Introduction to modern cryptography– principles and protocols*, 1st ed., Boca Raton FL, USA– CRC Press © 2008 [online] https://www.amazon.com/Introduction-Modern- cryptography-principles-protocols/dp/1584885513

[385] A. Lewis, "A gentle introduction to blockchain technology," *Bits on Blocks*, 9 Sep 2015 [online] https://bitsonblocks.net/

[386] B. Jayaraman et al, “Decentralized certificate authorities,” *Cornell Univ Lib*, revised 27 Oct 2017[online] https://arxiv.org/abs/1706.03370

[387] B. Jayaraman, “Decentralized certificate authorities,” *Univ. of Virginia*, created Oct 2017 [online] https://oblivc.org/docs/dca.pdf

[388] A. Lewis, "A gentle introduction to blockchain technology" *Brave New Coin* [online] https://bravenewcoin.com/assets/reference-papers/a-gentle-introduction/a-gentle-introduction-to-blockchain-technology-web.pdf

[389] S. Raval, *Decentralized Applications– Harnessing Bitcoin's Blockchain Technology*, 1st ed., Sebastopol CA USA– O’Reilly Media © 2016 [online] https://www.amazon.com/dp/1491924543

[390] "Quantum observer effect," *Wikipedia* [online] https://en.wikipedia.org/wiki/Observer_effect_(physics)

[391] H.J. Bremermann, “Quantum noise and information,” *Univ of CA Berkeley Technical Report* [online] http://digitalassets.lib.berkeley.edu/math/ucb/text /math_s5_v4_article-03.pdf

[392] S. Khatwani, "Different types of blockchains in the market and why we need them," *coinsutra.com*, 2018 [online] https://coinsutra.com/different-types-blockchains/

[393] "What is a distributed Ledger?" *CoinDesk* [online] https://www.coindesk.com/information/what-is-a-distributed-ledger/

[394] T. Harju, "Graph theory,” *Univ Turku Lecture Notes*, Finland, updated 2011, pp. 1-99 [online] https://cs.bme.hu/fcs/graphtheory.pdf

[395] F. Harary, *Graph Theory*, Reading, MA– Addison-Wesley © Oct 1994, p. 200 [online] https://www.amazon.com/theory-demand-printing-advanced-Program/dp/0201410338

[396] F Harary et al, "§8.8 acyclic digraph" in *Graphical Enumeration*, New York– Academic Press © 1973, pp.191-194 [online] http://www.logique.jussieu.fr/malod/harary.pdf

[397] "Harary graph," *Wolfram Math World* [online] http://mathworld.wolfram.com/hararygraph.html

[398] B.D. McKay et al, "Acyclic digraphs and eigenvalues of (0,1)-matrices." *J. Integer Sequences*, vol. 7, no. 04.3.3, 4 Aug 2004, pp. 1-5 [online] https://cs.uwaterloo.ca/journals/JIS/vol7/sloane/sloane15.pdf

[399] M. Sherman, *Spatial Statistics and Spatiotemporal Data– Covariance Functions and Directional Properties*, New York– Wiley © Dec 2010 [online] https://www.wiley.com/enus/Spatial+Statistics+and+Spatio+Temporal+Data%3A+Covariance+Functions+and+Directional+Properties-p-9780470699584

[400] V.M.V. Gunturi, *Spatiotemporal Graph Data Analytics*, 1st ed., Chum Switzerland– Springer Intl Pub © 2017, pp. 25-40, 43-57 [online] https://www.amazon.com/Spatio-Temporal-Graph-Analytics-Venkata-Gunturi/dp/3319677705

[401] Z. Galic, *Spatio-Temporal Data Streams*, New York- Springer-Verlag © 2016, pp. 47-66, 72-93 [online] https://www.springer.com/gp/book/9781493965731

[402] “Back to the future Part II,” *Wikipedia* [online] https://en.wikipedia.org/wiki/Back_to_the_Future_Part_II

[403] K. Kalinowska-Görska et al, "Constructing fair destination-oriented directed acyclic graphs for multipath routing," *J. Appl. Math*, vol. 20, no. 948521, 28 Apr 2014 [online] https://www.hindawi.com/journals/jam/2014/948521/

[404] S. Vutukury and J. J. Garcia-Luna-Aceves, “MDVA– a distance-vector multipath routing protocol,” in *Proc. 20th Annual Joint Conf. on IEEE Computer and Communications Societies (IEEE INFOCOM '01, Anchorage, Alaska, USA)*, vol. 1, April 2001, pp. 557–564 [online] https://ieeexplore.ieee.org/document/916780/

[405] S. Vutukury and J. J. Garcia-Luna-Aceves, “An algorithm for multipath computation using distance-vectors with predecessor information,” in *Proc of 8th IEEE Intl Conf on Comp Comm and Networks (Boston, Mass, USA)*, 11 Oct 1999, pp. 534–539 [online] https://ieeexplore.ieee.org/document/805570/

[406] S. Vutukury and J. J. Garcia-Luna-Aceves, “A simple approximation to minimum- delay routing,” in *Proc ACM Conf on Apps, Tech, Arch, and Protocols for Comp Comm (SIGCOMM '99, Cambridge, Mass, USA)*, vol. 29, no. 4, Oct 1999, pp. 227–238 [online] https://dl.acm.org/citation.cfm?doid=316188.316227

[407] S. Cho et al, “Independent directed acyclic graphs for resilient multipath routing,” *IEEE/ACM Trans on Ntwrk*, vol. 20, no. 1, 30 Aug 2011, pp. 153–162 [online] https://ieeexplore.ieee.org/document/6003807/

[408] R.W. Robinson, "Counting labeled acyclic digraphs." in *New Directions in Graph Theory* (F. Harary, ed.), New York– Academic Press © 1973 [online] https://www.amazon.com/exec/obidos/ASIN/012324255X/ref=nosim/ericstreasuretro

[409] R.W. Robinson, "Counting unlabeled acyclic digraphs" in *Combinatorial Mathematics Proc. 5th Australian Conf (Melbourne, 24-26 Aug 1976, C.H.C. Little, ed.)*, Berlin-Heidelberg Germany: Springer-Verlag © 1976, pp. 28-43 [online] https://www.amazon.com/exec/obidos/ASIN/0387085246/ref=nosim/ericstreasuretro

[410] N.J.A. Sloane, “Sequence A003087/M1696” in *The On-line Encyclopedia of Integer Sequences* [online] http://oeis.org/A003087

[411] N. Alon et al, "The Shannon capacity of a graph and the independence numbers of its powers," *IEEE Trans Info Theory*, vol. 52, no. 5, Jun 2006, pp. 2172-2176 [online] https://www.researchgate.net/publication/3085852_The_Shannon_capacity_of_a_graph_and_the_independence_numbers_of_its_powers

[412] Y. Ohara et al, “MARA– maximum alternative routing algorithm,” in *Proc of the 28th Conf on Comp Comm (IEEE INFOCOM '09, Rio de Janeiro, Brazil)*, April 2009, pp. 298–306 [online] https://ieeexplore.ieee.org/document/5061933/

[413] R. Ellis, *Entropy, Large Deviations, and Statistical Mechanics*, Berlin-Heidelberg Germany: Springer-Verlag © 2006 [online] https://www.springer.com/gp/book/9783540290599

[414] A. Lasota et al, *Chaos, Fractals, and Noise- Stochastic Aspects of Dynamics (Applied Mathematical Sciences)*, 2nd ed., Berlin-Heidelberg Germany: Springer-Verlag © 1994 [online] https://www.amazon.com/Chaos-Fractals-Noise-Stochastic-Mathematical/dp/0387940499

[415] E. Ott, “§4.5 – entropies” in *Chaos in Dynamical Systems*, New York– Cambridge University Press, © 1993 pp. 138-144 [online] https://www.amazon.com/exec/obidos/ISBN%3D0521437997/ericstreasuretroa/

[416] M. S. Corson and A. Ephremides, “A distributed routing algorithm for mobile wireless networks,” *Wireless Networks*, vol. 1, no. 1, Mar 1995, pp. 61–81 [online] https://link.springer.com/article/10.1007%2FBF01196259

[417] V. D. Park and M. S. Corson, “A highly adaptive distributed routing algorithm for mobile wireless networks,” in *Proc 16th Annual Joint Conf IEEE Comp and Comm Soc. – Driving the Information Revolution (IEEE INFOCOM '97, Kobe, Japan)*, 9-11 April 1997, p. 1405 [online] https://ieeexplore.ieee.org/abstract/document/631180/

[418] M. Pióro and D. Medhi, “Ch 5 § 5.5, Gradient minimization and other approaches for convex programming problems,” in *Routing, Flow and Capacity Design in Communication and Computer Networks*, Boston, Mass, USA– Morgan Kaufmann, 2004 [online] https://www.amazon.com/Capacity-Communication-Computer-Networks-Networking/dp/0125571895

[419] K. Zhang and H Gao, “Finding multiple length-bounded disjoint paths in wireless sensor networks,” *Wireless Sensor Network*, vol. 3, no. 12, 2011, pp. 384–390 [online] http://file.scirp.org/pdf/WSN20111200001_57442028.pdf

[420] M. Richardson and I. Robles, “RPL – routing over low-power and lossy networks,” *Internet Engineering Task Force (IETF 94, Yokohama, Japan)* 1 Nov 2015 [online] https://datatracker.ietf.org/meeting/94/materials/slides-94-rtgarea-2/

[421] E. Mingozzi, “Routing over low-power and lossy networks,” *Internet Engineering Task Force (IETF Hunan Univ)* 25 Jun 2014 [online] http://technodocbox.com/Computer_Networking/73331769-Routing-over-low-power-and-lossy-networks.html

[422] C. Vallati and E. Mingozzi, "Trickle-F– Fair broadcast suppression to improve energy-efficient route formation with the RPL routing protocol," in *2013 Sustainable Internet and ICT for Sustain*, 2013 [online] https://www.researchgate.net/publication/261448548_Trickle-F_Fair_broadcast_suppression_to_improve_energy-efficient_route_formation_with_the_RPL_routing_protocol

[423] J.P. Vasseur et al, “RPL- the IP routing protocol designed for low power and lossy networks," *IPS Alliance* Apr 2011 [online] http://www.ipso-alliance.org/wp-content/media/rpl.pdf

[424] “Routing protocol for LLN (RPL) configuration guide,” *Cisco IOS Release 15M&T*, updated 18 Nov 2015 [online] https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/rpl/configuration/15-mt/rpl-15-mt-book.html

[425] Parasuram, “An analysis of the RPL routing standard for low power and lossy networks,” *UC Berkeley Tech Report*, 14 May 2016 [online] https://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-106.pdf

[426] A. Rosic, "The science behind cryptocurrencies– cryptography” *Blockgeeks* [online] https://blockgeeks.com/guides/cryptocurrencies-cryptography/

[427] "What is the difference between hashing and encrypting," *Security Innovation Europe*, 31 Oct 2016 [online] www.securityinnovationeurope.com/blog/page/whats-the-difference-between-hashing-and-encrypting

[428] "Cryptographic hash function," *Wikipedia* [online] https://en.wikipedia.org/wiki/cryptographic_hash_function

[429] "Difference between hashing and encryption," *SSL2buy.com*, updated 2017 [online] https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption

[430] “What is the difference between hashing and encryption?" *Quora* [online] https://www.quora.com/What-is-the-difference-between-hashing-and-encryption

[431] C. Joseph, "The difference between encryption, hashing, and salting," *Gooroo.io* [online] https://gooroo.io/gooroothink/article/13023/the-difference-between-encryption-hashing-and-salting/

[432] W. Jackson, "Why salted hash is as good for passwords as for breakfast, *GCN*, 2 Dec 2013 [online] https://gcn.com/articles/2013/12/02/hashing-vs-encryption.aspx

[433] A. Gholami, "Security and privacy of sensitive data in cloud computing," *KTH School of Comp Sci and Comm (doctorial thesis)*, Apr 2016 [online] https://kth.diva-portal.org/smash/get/diva2:925669/fulltext01.pdf

[434] G. Hatzivasilis, “Password-hashing status," *Cryptography*, vol. 2 no. 10, 2017 [online] www.mdpi.com/2410-387X/1/2/10/pdf

[435] M. Buvaneswari et al, "Integrity rule generation and tiger hashing technique for efficient and secure cloud data storage," *Euro J Sci Research*, vol. 147, no. 3, Nov 2017, pp. 275-286 [online] http://www.europeanjournalofscientificresearch.com/issues/pdf/ejsr_147_3_03.pdf

[436] “Operating system design/kernel architecture,” *Wikibooks* [online] https://en.wikibooks.org/wiki/operating_system_design/kernel_architecture

[437] Rathnaike, “What is– operating system, kernel and types of kernels?” *Linked In*, 16 Jan 2017 [online] https://www.linkedin.com/pulse/what-operating-system-kernel-types-kernels-aajitha-rathnayaka

[438] “Kernel,” *Wikipedia* [online] https://simple.wikipedia.org/wiki/kernel_(computer_science)

[439] “What does kernel mean” *Techopedia.com* [online] https://www.techopedia.com/definition/3277/kernel

[440] “What-is-the-main-function-of-the-kernel-in-operating-systems?” *Quora* [online] https://www.quora.com/What-is-the-main-function-of-the-kernel-in-operating-systems

[441] “User mode and kernel mode,” *Microsoft docs* [online] https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

[442] V. Jain, "Fat protocols in enterprise blockchain?" *Pulse*, 5 Mar 2018 [online] https://www.linkedin.com/pulse/fat-protocols-enterprise-blockchain-varun-jain

[443] J. Bruckman, "Fat protocols are not an investment thesis," *The Blockchain Investments Blog*, 26 Oct 2017 [online] https://blog.coinfund.io/fat-protocols-are-not-an-investment-thesis-17c8837c2734

[444] A. Mashinsky, "Fat protocols vs. DApps– Creating long term value on the public blockchain," *hackernoon.com*, 2 May 2018 [online] https://hackernoon.com/fat-protocols-vs-dapps-creating-long-term-value-on-the-public-blockchain-565637747557

[445] D. Xiao, "The four layers of the blockchain," *Medium*, 21 Jun 2016 [online] https://medium.com/@coriacetic/the-four-layers-of-the-blockchain-dc1376efa10f

[446] "A mathematical theory of communication," *Wikipedia* [online] https://en.wikipedia.org/wiki/a_mathematical_theory_of_communication

[447] “Stabilizing communication protocols - *IEEE J. & Mag.* [online] https://ieeexplore.ieee.org/document/88464/

[448] I. Verzun, O. Holub, and R.K. Williams, “Secure Dynamic Network and Protocol”, *Taiwan app 105102426*, filed 23 May 2015, priority date 26 Jan 2015

[449] I. Verzun, O. Holub, and R.K. Williams, “Secure Dynamic Network and Protocol,” *PCT application PCT/US16/14643*, WPO foreign counterparts filed in Australia (*2016266557, 22 Aug 2017*), Brazil (*112017-016047-1, 26 Jul 2017*), Canada (*2975105, 26 Jul 2017*), Europe (*EPO 16800413.3, 23 Aug 2017*), India (*201717030184, 25 Aug 2017*), Indonesia (*P00201705680, 25 Aug 2017*), Israel (*253679, 26 Jul 2017*), Japan, (*2017-540650, 26 Jul 2017*), Korea (*10-2017-7023539, 23 Aug 2017*), Russia (*2017130148, 25 Aug 2017*), Singapore (*11201706093T, 26 Jul 2017*), South Africa (*2017/05738, 26 Jul 2017*), and Ukraine (pending).

[450] C.M. Christensean et al, "What is disruptive innovation?" *Harvard Bus. Rev.*, Dec 2015 [online] https://hbr.org/2015/12/what-is-disruptive-innovation

[451] C. Christensen, "Disruptive Innovation," *Clayton Christensen*, 2018 [online] http://www.claytonchristensen.com/key-concepts/

[452] "Invention of radio," *Wikipedia* [online] https://en.wikipedia.org/wiki/invention_of_radio

[453] "History of the transistor," *Wikipedia* [online] https://en.wikipedia.org/wiki/history_of_the_transistor

[454] “Richard K Williams on Innovation (including his personal recollections of professor emeritus John Bardeen, 2-time Nobel laureate and inventor of the transistor),” *University of Illinois at Urbana-Champaign (UIUC)*, Oct 2013 [online] https://www.youtube.com/watch?v=cpVYhQANjR8

[455] “Invention of the integrated circuit,” *Wikipedia* [online] https://en.wikipedia.org/wiki/Invention_of_the_integrated_circuit

[456] Mackenzie, "The man who invented the microprocessor,” *BBC News*, 2 May 2011 [online] https://www.bbc.com/news/technology-13260039

[457] V. Manganaro, "Steve Wozniak, 40 Years later & the essence of innovation," *Technology Concepts Group Intl*, 29 Jun 2017 [online] https://www.technologyconcepts.com/steve-wozniak-40-years-later-essence-innovation/

[458] E. Andrews, "Who invented the Internet?" *History*, 18 Dec 2013 [online] https://www.history.com/news/who-invented-the-internet

[459] "History of the Web," *World Wide Web Foundation*, 2018 [online] https://webfoundation.org/about/vision/history-of-the-web/

[460] V. Gupta, "A Brief history of blockchain, *Harvard Bus. Rev.*, 28 Feb 2017 [online] https://hbr.org/2017/02/a-brief-history-of-blockchain

[461] A.K White, *Hacking– The Underground Guide To Computer Hacking, Including Wireless Networks, Security, Windows, Kali Linux And Penetration Testing*, Alan Kay White © 10 Nov 2017 [online] https://www.amazon.com/Hacking-underground- computer-including-penetration/dp/1979881103

[462] J. Forshaw, *Attacking Network Protocols– A Hacker's Guide To Capture, Analysis, And Exploitation*, 1st ed. J. Forshaw © 2018 [online] https://www.amazon.com/attacking-network-protocols-analysis-exploitation/dp/1593277504/

[463] G. Weidman, *Penetration Testing– A Hands-On Introduction To Hacking*, 1st ed. George Weidman © 2014 [online] https://www.amazon.com/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641

[464] K.D. Mitnick, forward by S. Wozniak, *The Art Of Deception– Controlling The Human Element Of Security*, © 17 Oct 2003 [online] https://www.amazon.com/Art-Deception-Controlling-Element-Security/dp/076454280X

[465] K.D. Mitnick et al, *The Art Of Intrusion– The Real Stories Behind The Exploits Of Hackers, Intruders And Deceivers*, New York– Wiley © 2002 [online] https://www.amazon.com/art-intrusion-exploits-intruders-deceivers/dp/0471782661/

[466] K.D. Mitnick et al, *The Art of Invisibility– The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*, New York– Little, Brown & Co. © 14 Feb 2017 [online] https://www.amazon.com/Art-Invisibility-Worlds-Teaches-Brother/dp/0316380504

[467] J. Erickson, *Hacking– The Art of Exploitation*, 2nd ed., Joe Erickson © 2008 [online] https://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441

[468] "Hash function," *Wikipedia* [online] https://en.wikipedia.org/wiki/hash_function

[469] K. Ahmad et al, "E-commerce security through elliptic curve cryptography," *Intl. Conf Info Sec Prvcy (CISP2015, Nagpur)* vol. 78, 11 Dec 2016, pp.867-873 [online] https://www.sciencedirect.com/science/article/pii/S1877050916310559

[470] M. Tiwari et al, "An efficient and secure micro-payment transaction using shell cryptography," *ABES Eng. LNICST*, vol. 115, 2013, pp. 461-469 [online] https://link.springer.com/chapter/10.1007/978-3-642-37949-9_40

[471] M. Rouse "What is DCOM (Distributed Component Object Model)?" *WhatIs.com*, 2018 [online] https://whatis.techtarget.com/definition/DCOM-distributed-component-object-model

[472] A.D.N.M. Fernando et al, "E-commerce security using cryptography techniques," *Intl. J Sci. Rsrch Pub*, vol. 6 no. 10 Oct 2016, pp. 86-93 [online] http://www.ijsrp.org/research-paper-1016/ijsrp-p5814.pdf

[473] M. Collins, *Network Security Through Data Analysis– Building Situational Awareness*, 1st ed. Michael Collins © 2014 [online] https://www.amazon.com/Network-Security-Through-Data-Analysis/dp/1449357903

[474] W. Allsopp, *Advanced Penetration Testing– Hacking The World's Most Secure Networks*, 1st ed., Indianapolis IN, USA– Wiley © 2017 [online] https://www.amazon.com/Advanced-Penetration-Testing-Hacking-Networks/dp/1119367689/

[475] N.A. Adams ed., *Data Analysis For Network Cyber-Security*, London– Imperial College Press © 2014 [online] https://www.amazon.com/Analysis-Network-Cyber-Security-Niall-Adams/dp/B011FPSIPC

[476] E. Gilman et al, *Zero Trust Networks– Building Secure Systems In Untrusted Networks*, 1st ed., Evan Gilman and Doug Barth © 15 Jun 2017 [online] https://www.amazon.com/zero-trust-networks-building-untrusted/dp/1491962194

[477] M.H. Ligh et al, *The Art Of Memory Forensics– Detecting Malware And Threats In Windows*, Linux, And Mac Memory, 1st ed. New York– Wiley © 22 Jul 2014 [online] https://www.amazon.com/Art-Memory- Forensics-Detecting-Malware/dp/1118825098

[478] M. Bazzell et al, *The Complete Privacy & Security Desk Reference*, Michael Bazzell & Justin Carroll © April 2016 [online] https://www.amazon.com/complete-privacy-security-desk-reference/dp/152277890X/

[479] W. Hartzog, *Privacy's Blueprint– The Battle To Control The Design Of New Technologies*, Harvard © Apr 2018 [online] https://www.amazon.com/privacys-blueprint-battle-control-technologies/dp/0674976002

[480] M. Bazzell, *Personal Digital Security– Protecting Yourself From Online Crime*, M. Bazzell © 31 Jul 2013 [online] https://www.amazon.com/personal-digital-security-protecting-yourself/dp/149108197X

[481] T. Payton, *Privacy in the Age of Big Data– Recognizing Threats, Defending your Rights, and Protecting your Family*, London– Roman & Littlefield © 16 Apr 2015 [online] https://www.amazon.com/Privacy-Age-Big-Data-Recognizing/dp/1442242574/

[482] D.J. Bernstein et al, ed. *Post-Quantum Cryptography*, Berlin-Heidelberg Germany: Springer-Verlag © 2009 [online] https://www.amazon.com/post-quantum-cryptography-daniel-j-bernstein/dp/3540887016/

[483] Z. Brakerski "Quantum FHE (almost) as secure as classical," *iacr.org*, 31 Oct - 3 Nov 2016 [online] https://eprint.iacr.org/2018 /338.pdf

[484] L.P. Luo et al, "Authenticated semi-quantum direct communication protocols using Bell states," *Quantum Info Proc*, vol. 15, no. 2, 1 Feb 2016 [online] https://researchoutput.ncku.edu.tw/en/publications/authenticated-semi-quantum-direct-communication-protocols-using-b

[485] Allevi et al, "Bracket states for communication protocols with coherent states," *Intl J. Quantum Info*," vol. 12, no. 02, Mar 2014 [online] https://www.worldscientific.com/doi/abs/10.1142 /S0219749914610188

[486] C. Shukla, "Design and analysis of quantum communication protocols," *Jaypee Inst Info Tech (JIIT PhD thesis)*, Nov 2014 [online] www.jiit.ac.in/download/file/fid/796

[487] C. Jones, " Design and analysis of communication protocols for quantum repeater networks," *New J. Phys.* vol. 18, no. 083015, 5 Aug 2016 [online] http://iopscience.iop.org/article/10.1088/1367-2630/18/8/083015/pdf

[488] M. Smarnia "Experimental quantum multiparty communication protocols," *Quantum Info (Nature)*, vol. 2 no. 16010, 21 Jun 2016 [online] https://www.nature.com/articles/npjqi201610

[489] Sharma et al, "A comparative study of protocols for secure quantum communication under noisy environment– single-qubit-based protocols versus entangled-state-based protocols," *Cornel Univ Lib.*, 1 Mar 2016 [online] https://arxiv.org/abs/1603.00178

[490] D. Joy et al, "Efficient deterministic secure quantum communication protocols using multipartite entangled states," *Cornel Univ Lib.*, 25 Mar 2017 [online] https://arxiv.org/abs/1703.08666

[491] Rothstein, J. "Information, Measurement, and Quantum Mechanics." *Science*, vol. 114, no. 2955, 17 Aug 1951, pp. 171-175 [online] http://science.sciencemag.org/content/114/2955/171/tab-pdf

[492] "DAG vs the blockchain," *BTCManager*, 19 Dec 2017 [online] https://btcmanager.com/dag-vs-blockchain/

[493] "Everything you need to know about directed acyclic graphs (DAGS)," *Coin Bureau*, 31 Mar 2018 [online] https://www.coinbureau.com/education/directed-acyclic-graphs-dags/

[494] Heiditravels, "More than blockchains– how Hashgraph & DAGs are different," *Steemit*, Nov 2017 [online] https://steemit.com/cryptocurrency/@heiditravels/more-than-blockchains-how-hashgraph-and-dags-are-different

[495] Galyna, "Blockchain vs Tangle (DAG), why does it solves blockchain's problems?" *Get Crypt*, 5 Dec 2017 [online] https://getacryp.com/blockchain-vs-tangle-dag/

[496] B. Wang, "Blockchain 3.0 with directed acyclic graphs (DAG) for ten of thousands of transactions per second," *NextBigFuture.com*, 17 Feb 2018 [online] https://www.nextbigfuture.com/2018/02/blockchain-3-0-with-directed-acyclic-graphs-dag-for-ten-of-thousands-of-transactions-per-second.html

[497] R. Demush, "Introduction to DAG and blockchain-less cryptocurrencies," *DZone Security*, 1 Mar 2018 [online] https://dzone.com/articles/introduction-to-dag-and-cryptocurrencies-that-work

[498] W. Murphy, "In 10 years we won't have blockchains," *CoinDesk*, 17 Feb 2018 [online] https://www.coindesk.com/10-years-wont-blockchains/

[499] S. Dolev, "The quantum meltdown of encryption," *TechCrunch*, 22 Jul 2018 [online] https://techcrunch.com/2018/07/22/the-quantum-meltdown-of encryption/

[500] W.G. Pabst, “Full duplex network radio bridge with low latency and high throughput,” *US patent no. 8,520,565*, filed 7 May 2010, issued 27 Aug 2013

[501] W.G. Pabst, “Full duplex network radio bridge with low latency and high throughput,” *US patent no. 8,670,358*, filed 26 Jun 2013, issued 11 Mar 2014

[502] M.R. Hamblin et al, “Mechanisms for Low Light Therapy” in *Proceedings of SPIE--the International Society for Optical Engineering, (SPIE conf.)*, 2017 [online] https://books.google.com/books/about/Mechanisms_for_Low_light_Therapy.html?id=SFRRAAAAMAAJ&hl=en

[503] R.K. Williams, “Advances in photobiomodulation therapy – a new paradigm in pain management,” *Pain Med. vol. 6, no. 6 (Proc of 4th Intl. Conf. on Pain Medicine, San Francisco), 19-20 Oct 2017* [online] https://painmedicine.conferenceseries.com/speaker/2017/richard-k-williams-lightmd-applied-biophotonics-usa

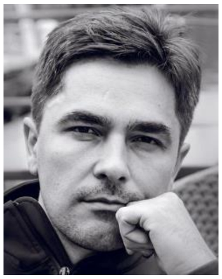
[504] “Applied BioPhotonics Phototherapy System ABPT1003,” *US FDA 510(k) no K142256*, 18 Dec 2014 [Online] https://www.accessdata.fda.gov/cdrh_docs/pdf14/k142256.pdf

[505] R.K. Williams et al, “Flexible LED light pad for phototherapy,” *US patent no 9,895,550*, filed 14 Apr 2014, issued 20 Feb 2018

[506] R.K. Williams, “Phototherapy system and process including dynamic LED driver with programmable waveform,” *US patent no 9,877,361*, filed 6 Nov 2013, issued 23 Jan 2018

[507] S. Mahajan et al, “Bin enabled data object encryption and storage apparatuses, methods and systems,” *US patent no 9,369,455*, filed 10 Nov 2014, issued 14 Jun 2016

Author Biographies



Evgen Verzun is a serial entrepreneur, veteran software developer and pioneer in secure communication, expert in real-time systems, networking, cybersecurity and interdisciplinary technology, and a prolific inventor. His software has been deployed across the globe in numerous professional and radio communications applications. Users include the US Army (during the Iraq war), emergency services in Germany and in the Middle East and by various port authorities. In 2000, Evgen received his Engineering Degree in R&D computer systems followed by a Master of Science degree from National Technical University of Ukraine 'Kyiv Polytechnic Institute’ in 2006. The same year, he also earned a Bachelor of Finance degree from the International University of Finance.

In 2003, as CEO and CTO, Evgen founded Listat Engineering, a global software development company with operations in Europe and the Middle East offering customized FIP140-2 compliant private networks including applications of TETRA professional mission-critical and time-critical communications. In 2009, he also founded UPROTEL, a global communications company providing operational support professional communications network users.

In 2011, Evgen embarked on a quest to bring professional communication quality services to consumer telephony, adapting dispatcher-based methods to minimize latency through dynamic routing, and preventing network usurpation by pioneering autonomous dynamic encryption and concealment techniques on a hop-by-hop basis.

The results of this development– the Secure Dynamic Network & Protocol (SDNP), represent the first fully distributed meshed network for realtime communications with military grade security, creating the first viable protocol alternative to TCP/IP and establishing a technological base on which to develop a global cybersecure privacy network,

In 2017, he expanded this vision in cybersecure networking and realtime communication to include network-native enterprise-grade certificate authority and embedded cryptocurrency employing energy-efficient Proof of Performance census validation in a fully decentralized system– the HyperSphere.

He also devised an innovative dual-cryptocurrency architecture to ameliorate the undesirable economic impact of cryptocurrency volatility preventing merchants from broadly adopting digital currency to engage in e-commerce. Together with Richard K Williams and Dmitri Bulkhukov, in 2017, Evgen co-launched the HyperSphere Foundation project. Evgen is a member of the *Institute of Electrical and Electronic Engineers* (IEEE).

Richard K Williams is a serial-parallel entrepreneur and veteran technologist, engineer, scientist, and philanthropist, as wells as a prolific inventor, writer, and speaker. Richard received a Bachelor of Science in electrical engineering (BSEE) from the University of Illinois in Urbana-Champaign (UIUC) in 1980 and a Master of Science from the University at Santa Clara in electrical engineering (MSEE) in 1987. His academic studies included semiconductor technology and device physics, digital and analog circuit design, quantum mechanics, power electronics, control theory, radio communication and electromagnetics, material science, and computer engineering. He also studied molecular biology and electrophoresis at the University of California Berkeley.

Richard pioneered power semiconductor electronics at Siliconix, Inc. from 1980 to 1998 where as Senior Director of Device Concept & Design, he developed the world's first trench power MOSFET, motor control power ICs for disk drives, high voltage ICs for displays and fluorescent lighting, and automotive ICs including an airbag controller for Mercedes Benz and ABS control systems for Honda. He also pioneered the first switching voltage regulators ever used in notebook computers and cell phones and developed battery management ICs for the Motorola Startac mobile phone, for Sony camcorders, for Apple's blackbird series of notebooks, and for lithium-ion battery protection in mobile phones. From 1998 to 2012, Richard was CEO, President, CTO and founder of Advanced Analogic Technologies Inc. (AATI) specializing in power management ICs including pioneering the LED camera flash, white LED backlight control for the world's first color smartphones, and dynamic LED drive for HDTVs. In 2005, Richard took AATI public on Nasdaq underwritten by five banks including Morgan Stanley and Merrill Lynch. The IPO was 32 times oversubscribed. In 2012, Skyworks made an unsolicited bid to acquire AATI.

Thereafter, as CEO and CTO, Richard founded Adventive Technology Ltd. specializing in interdisciplinary technology development incl. semiconductor packages, high bandwidth microwave radios, and more. He also founded Applied Biophotonics Ltd. pioneering the development of photobiomodulation therapy (PBT) devices and biotechnology.

In 2012 he also started Adventive IPBank joining with Listat Engineering to develop and prosecute intellectual property of the Secure Dynamic Network and Protocol (SDNP), a key inventive component of the HyperSphere. Together with Evgen Verzun and Dmitri Bulkhukov, in 2017, Richard co-launched the HyperSphere Foundation project.

Richard became a Member (M) of the *Institute of Electrical and Electronic Engineers* (IEEE) in 1976, a Senior Member (SM) in 1997. He is a founding member of the IEEE's *International Symposium on Power Semiconductor Devices* (ISPSD), and has also served as an IEEE Adcom committee chairman, on the technical program committee of the International Electron Device Meeting, and on the technical review board of the *Transactions on Electron Devices*.

In 2013, Richard received the Distinguished Alumni Award from the ECE Department of the University of Illinois (UIUC). In 2017 at the ISPSD conference, Richard was inducted into the IEEE Hall of Fame. He also serves as an honorary professor and guest lecturer in Southeastern University in Nanjing China (formerly Nanjing Institute of Technology). A prolific writer and frequent invited public speaker, Richard has published over 100 professional articles, co-authored several books, and holds over 300 US and international patents. Richard's hobbies include jogging, basketball, music, and drumming.

Appendix A

HyperSphere Countermeasures & Features

The following tables describe the HyperSphere's countermeasures and features designed to mitigate or ameliorate vulnerabilities and deficiencies of the Internet, third-party certificate authorities, unitary-communal blockchains, and conventional PoW cryptocurrencies. Although any one defensive mechanism may be subverted, the HyperSphere employs a multi-dimensional approach to deliver security, privacy, and transactional integrity, minimizing attack causalities by (i) limiting the scope or extent of the damage through access containment, (ii) limiting the duration by which an exploit remains effective using state-based dynamic security and credentials (iii) providing ownership traceability to recover assets and to trace perpetrators, (iv) using hop-by-hop autonomous security lacking any master key or control provision, i.e. fully decentralized operation, and (v) supporting user-owned security features (such as end-to-end encryption or client specific AAA) of which, HyperSpheric network operations has no knowledge or involvement. To maximize performance, transactional efficiency and network QoS, the HyperSphere executes operations using network-native processes including (i) adjunctive cryptocurrency synthesis using Layer-1.5 (Network & Transport Layers) generated HyperNode Hop Codes (HHCs); (ii) network generated CA-certificates for signing, devices, HyperNodes, HyperContracts, and various transactional processes; and (iii) DyDAG based routing of fragmented data packet network traffic for minimizing propagation delays and maximizing cloud throughput. An abridged list of HyperSphere features includes the following:

- *De-centralized (node, juror, AI mrkt)* – The HyperSphere operates as a fully decentralized network with no central control or authority using distributed HyperNodes for communication, disaggregated storage, and cloud computing; a decentralized jury-of-peers for consensus and HyperContract resolution, and an artificial intelligence (AI) based marketplace for HyperContract negotiation (matching merchant/service providers to HyperNode/resource providers).
- *Stateless HyperNodes, 4-tier res pvdr* – The HyperSphere employs stateless HyperNodes performing nodal functions as 'resource providers' without retaining any transactional data or record after the task is performed, i.e. HyperNodes operate as stateless DyDAG vertices. HyperNodes are classified into four tiers based on nodal capability (transaction rates, capacity, etc.) and QoS performance history in HyperContract execution. Compensation of resource providers depends on a HyperNode's tier level and on its ratable participation in successful HyperContract execution.
- *SDNP dyn frag, state-based, disag data* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs dynamic fragmentation to parse payloads using system 'state variables' and state-based algorithms to realize a spatiotemporal network and transport datagrams therein. Data storage in the HyperSphere, both cached and non-volatile content is realized using disaggregated data spread across the HyperSpheric cloud.
- *SDNP dyn meshed routing, min prop* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs dynamic meshed routing whereby fragmented data packets are routed over a collection of DyDAG trees in accordance with minimizing propagation delay of realtime packets and minimizing local congestion in the spatiotemporal network.
- *SDNP anonymous packets, single hop* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs anonymous data packets whereby each datagram uses dynamic IP and port addresses of incoming and outgoing packets with no knowledge as to the originating source (point of origin) or ultimate destination of the packet. Anonymous data transport prevents meaningful surveillance or meta-data analysis of HyperSpheric network traffic.
- *SDNP dyn conceal, state-based, keyless* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs state-based dynamic concealment methods of datagram payloads, i.e. Application Layer-7 data. Executed on a hop-by-hop basis, dynamic concealment includes varying combinations and sequences of scrambling, encryption, junk-data, junk-packets, and splitting, and the inverse processes thereof. The algorithms and security credentials (including numeric seeds, encryption keys, etc.) are state-specific, varying with time, location, cloud, subnets, etc. with no master keys and no central point of control.
- *SDNP tri-ch, metamorphic HNs, multi-D* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs tri-channel communication, where device identities; transactional scheduling (or packet routing); and task execution (or data transport) are executed respectively by metamorphic HyperNodes operating as name server nodes, authority nodes, or task nodes. During HyperContract negotiation, each metamorphic HyperNode is selected to perform only one-of-three dedicated functions for a given HyperContract. This multi-dimensional approach to security thereby avoids the concentration of information within any single HyperNode for a specific contract. Because the network is dynamic, DyDAG routing of datagrams carrying transactional data of unrelated HyperContracts involves new security credentials independent of other contracts, thereby enabling metamorphic HyperNodes to service more than one HyperContract at a time.
- *SDNP dyn transport security, VPN tunnels* – In accordance with the Secure Dynamic Network & Protocol (SDNP), the HyperSphere employs single-hop Transport Layer-4 security operating as node-to-node ad hoc VPN connections with no master keys, i.e. employing peer-to-peer dynamic tunnel protocols.
- *Network native CA-certs, multi-factor* – HyperSphere transactions, assets, and devices support network-native generated CA-certificates with the option of multi-factor authorization including identity (owner), group, or system authentication.

- *Identity trust chain, SQK, ownership* – HyperSphere transactions, assets, and devices employ CA-certificate based trust chains linked to true-identity based accounts to ensure ownership and recovery. Multi-tiered CA-certificates including, system, group, identity, root, intermediate, and leaf certificates deliver privacy protections while enabling account recovery mechanisms. A sequential quantum key (SQK), held offline in cold storage facilitates account recovery of corrupted trust chains and root certificates.
- *Digitally signed assets, trust zones* – HyperSphere assets including HyperNodes, devices, DyDAG blockchains, and HypWallets, employ CA-certificate based digital signatures to prevent imposter access, where privacy provisions and access rights are arranged into 'trust zone' security shells.
- *Accts, pseudonymous trans, AAA* – The HyperSphere combines identity-based accounts to ensure proof-of ownership with pseudonymous CA-certificates for transactions to prevent identity theft and profiling. The use of AAA (authentication, authorization, and administration) combined with multifactor authentication prevents imposter exploits, account usurpation, and profiling. Through CA-certificates and identity-trust-chains, account-based ownership of personal DyDAG blockchains protects token blockchains from backtracing and theft common in unitary communal blockchains.
- *Private & temp wallets, OT^3 proxy* – The HyperSphere's use of HypWallets as digitally-signed security vaults to safely protect cryptocurrency and other private assets combined with the use of temporary wallets and one-time-transaction-token (OT3) proxies facilitates online and point-of-sale (POS) transactions using fiat currency or cryptocurrency without risking unauthorized access of personal account information or blockchain backtracing.
- *Lightweight multi-tree DyDAGs, defrag* – In addition its privacy and security benefits, the HyperSphere's application of multi-tree dynamic DAGs limits the length and size of token, auxiliary, and BaaS blockchains, facilitating high transaction rates, rapid resolution, and minimal data storage requirements.
- *Adjunctive crypto synth, HHCs, eco* – The HyperSphere's use of embedded network-native blockchain generation and adjunctive cryptocurrency synthesis using HyperNode Hop Codes (HHCs) facilitates an energy efficient, ecologically responsible (sustainable) method of cryptocurrency generation based on performing useful work (rather than puzzle solving). Energy consumption is one-trillionth (10–12) that of conventional PoW cryptocurrencies. Rather than utilizing a separate application program, cryptocurrency synthesis and BaaS blockchain generation occur in the HyperSphere using a HyperNode embedded blockchain processor (BCP).
- *HyperContract, transitory tBC* – The HyperSphere's use of HyperContracts prescribes transactions between merchants/service-providers and HyperNodes/resource-provides articulating the contract's deliverables. HyperContracts also specify cryptocurrency compensation (as a secured pledge) for active participation in the HyperContracts. Contract execution is documented by network-native HyperNode Hop Codes (HHCs) chronicled in a transitory DyDAG blockchain (tBC) recording each HyperNode's Proof of Performance (PoP). Because the HHCs are generated adjunctively from data transport and indelibly recorded on the tBC, imposters are unable to fake participation, or fraudulently claim their ratable right to mint new tokens.
- *Cloaked jurors, RBOS, HN tunnels* – The HyperSphere ameliorates blockchain and network attacks by preventing backtracing, minimizing the impact of denial of service attacks, and subverting cyberbots by employing cloaked jurors, replicant blockchain observer segments (RBOS), and ad hoc HyperNode tunnels to remote nodes.
- *DyDAG aux sidechains* – The HyperSphere supports DyDAG auxiliary sidechains for documentation, able to document time-stamped records on multiple sidechains without contaminating a main blockchain. In this manner, status updates depicting non-cryptocurrency transactions can be enshrined onto a main blockchain without interrupting cryptocurrency transactions.
- *User implemented features, other* – The HyperSphere supports user APIs on Application Layer-7 using open source services such a digital signatures of executable code, HHC code generation, blockchain processing and more. Merchants and service providers may also implement proprietary functions and security features such as end-to-end encryption, private multi-factor authentication methods, and more.

The following tables list common vulnerabilities of the Internet, certificate authorities (trust chains), conventional blockchains, and cryptocurrency-based transactions, identifying HyperSpheric countermeasures to the described vulnerabilities and deficiencies. The defensive provisions are grouped into four (color coded) broad remedies, namely: decentralization (yellow), security (blue), identity and trust (red), transactional integrity (green). Exemplary user implementable features are also described. Tables are topically arranged into the same groups as section II of the technical whitepaper including §A – Identity Fraud and Trust Attacks, §B – Network Attacks, §C – Data Breaches, §D – Blockchain Attacks, and Other (including §E – New Technology, §F – IoE, and §G – Web 3.0, Internet of Blockchains).

Legend

Decentralized, no oper cntrl
HyperSecure, SDNP
Identity (CA-cert), privacy
Transactional integrity

Part II **§A** **Identity Fraud** **& Trust Attacks**		**De-centralized (node, juror, AI mrkt)**	**Stateless HyperNodes, 4-tier res pvdr**	**SDNP dyn frag, state-based, disag data**	**SDNP dyn meshed routing, min prop**	**SDNP anonymous packets, single hop**	**SDNP dyn conceal, state-based, keyless**	**SDNP tri-ch, metamorphic HNs, multi-D**	**SDNP dyn transport sec, VPN tunnels**	**Network native CA-certs, multi-factor**	**Identity trust chain, SQK, ownership**	**Digitally signed assets, trust zones**	**Accts, pseudonymous trans, AAA**	**Private & temp wallets, OT^3 proxy**	**Lightweight multi-tree DyDAGs, defrag**	**Adjunctive crypto synth, HHCs, eco**	**Embedded tokens, recycling**	**HyperContract, transitory tBC**	**Cloaked jurors, RBOS. HN tunnels**	**DyDAG aux sidechains**	**User implemented features, other**
Deficiency/Vulnerability	**Target/Vector**																				
Money wire reroute/hijack	SWIFT / Internet	•	•	•	•	•	•	•	•	•	•	•	•					•			1
Accidental wire routing	SWIFT / Internet									•	•	•	•	•				•			1
Money wire fraud	SWIFT / Internet	•	•	•	•	•	•	•	•	•	•	•	•	•				•			1
Unrecovered wire cancel	SWIFT / Internet									•	•	•	•	•				•			1
Account theft	Bank accounts						•	•			•	•	•	•				•			1
Account theft	Crypto wallets						•	•			•	•	•	•				•	•		1
Identity theft	All accounts & assets	•					•	•		•	•	•	•	•				•			2
Online transactional fraud	3-D Secure	•	•	•	•	•	•	•	•	•	•	•	•	•				•			
POS transactional fraud	PCU DSS skimming	•					•				•	•	•	•							3
POS transactional fraud	PCU DSS data intercept	•	•	•	•	•	•	•	•	•	•	•	•	•				•			
CA cert, SSL-3.0 fraud	POODLE, downgrades	•				•	•	•				•	•								4
CA-cert, TLS fraud	Heartbleed	•				•	•	•				•	•								4
CA-cert, UNIX TLS bugs	Shellshock, Bashbug	•				•	•	•				•	•								4
CA-cert fraud, malware	Spyware (login)						•	•	•	•	•	•	•								5
CA-cert fraud, malware	Spyware (rootkit)						•	•	•	•	•	•	•								5
CA-cert fraud, malware	Spyware (eavesdrop)					•	•	•	•	•	•	•	•								5
CA-cert fraud, malware	Spyware (datascraper)							•	•	•		•	•								5
CA-cert fraud, malware	Spyware (phishing)							•	•	•		•	•								5
CA-cert fraud, malware	Spyware (MIM exploit)	•	•	•	•	•	•	•	•	•	•	•	•					•			
CA-cert fraud, malware	Spyware (key logger)						•	•	•	•		•	•								5
CA-cert fraud, malware	Scareware						•	•	•	•	•	•	•								5
CA-cert fraud, malware	Zero-day expl, Stuxnet	•					•	•	•	•		•									5
CA-cert fraud, malware	Trojan (Zeus, etc.)						•	•	•	•		•									5
CA-cert fraud, malware	Duqu 2.0						•	•	•	•		•									5
CA-cert fraud, malware	Crypto key theft	•	•	•	•	•	•	•	•	•	•	•	•					•			5
CA-cert fraud, malware	DoS (L4/L7)	•	•	•	•	•	•	•	•	•	•		•								
CA-cert fraud, malware	Econ (imposter fraud)	•								•	•	•	•	•	•		•	•			
CA-cert fraud, malware	Cyber espionage	•	•	•	•	•	•	•	•	•	•	•	•	•				•			
CA-cert fraud, malware	Cyber warfare	•	•	•	•	•	•	•	•	•	•	•	•	•				•			
CA-cert fraud, malware	Fake code signing cert					•	•	•	•	•	•	•	•	•				•			
CA-cert fraud, malware	Fake antivirus					•	•	•	•	•	•	•	•	•				•			5
CA-cert fraud, malware	Worm	•					•	•	•	•	•	•									5
CA-cert fraud, malware	Backdoor						•	•	•	•	•	•									5
CA-cert fraud, malware	Email virus						•	•	•	•	•	•									5
CA-cert fraud, malware	Web, HTTP virus				•	•	•	•	•	•	•	•									5
CA-cert fraud, malware	FTP virus				•	•	•	•	•	•	•	•									5
CA-cert fraud, malware	Ad-blocker virus						•	•	•	•	•	•									5

CA-cert fraud, malware	Anti-virus						•	•	•	•	•	•								5
CA-cert fraud, malware	System cleanup virus						•	•	•	•	•	•								5
CA-cert fraud, malware	Software install/updat						•	•	•	•	•	•								5
CA-cert fraud, malware	Java script virus						•	•	•	•	•	•								5
CA-cert fraud, malware	PDF reader virus						•	•	•	•	•	•								5
CA-cert fraud, malware	Media player virus						•	•	•	•	•	•								5
CA-cert fraud, malware	Messenger malware		•	•	•	•	•	•	•	•	•	•	•	•				•			5
CA-cert fraud, malware	Malicious URL	•						•					•							•	6
CA-cert fraud, malware	Adware virus/exploits						•	•	•	•	•	•	•							•	5
CA-cert fraud, malware	Typosquatting						•	•	•	•	•	•	•								5
CA-cert fraud, malware	Fork bombs						•	•	•	•	•	•	•								5
CA-cert fraud, malware	Live (zero-day) bombs	•					•	•	•	•	•	•	•								6
CA-cert fraud, malware	Time bombs	•					•	•	•	•	•	•	•								5
CA-cert fraud, malware	Logic bombs	•					•	•	•	•	•	•	•								5
CA-cert fraud, malware	Frankenstein, binaries	•					•	•	•		•	•	•								6
CA-cert fraud, malware	Computer OS virus	•					•	•	•	•	•	•	•								5
CA-cert fraud, malware	Mobile virus (iOS)		•	•	•	•	•	•	•	•	•	•	•	•				•		•	5
CA-cert fraud, malware	Mobile virus (Android)		•	•	•	•	•	•	•	•	•	•	•	•				•		•	5
OEM malware	Preloaded virus								•	•	•	•								•	6

1. End-to-end encryption, custom authentication
2. Custom authentication
3. Smartcard chip
4. IPSec tunnel protocol replaces TLS/SSL
5. Malware detection/virus checker, optional 2nd device authentication
6. Online database/blockchain of reported malware, banned sites, and bogons

Part II **§B** **Network Attacks**		**De-centralized (node, juror, AI mrkt)**	**Stateless HyperNodes, 4-tier res pvdr**	**SDNP dyn frag, state-based, disag data**	**SDNP dyn meshed routing, min prop**	**SDNP anonymous packets, single hop**	**SDNP dyn conceal, state-based, keyless**	**SDNP tri-ch, metamorphic HNs, multi-D**	**SDNP dyn transport sec, VPN tunnels**	**Network native CA-certs, multi-factor**	**Identity trust chain, SQK, ownership**	**Digitally signed assets, trust zones**	**Accts, pseudonymous trans, AAA**	**Private & temp wallets, OT^3 proxy**	**Lightweight multi-tree DyDAGs, defrag**	**Adjunctive crypto synth, HHCs, eco**	**Embedded tokens, recycling**	**HyperContract, transitory tBC**	**Cloaked jurors, RBOS. HN tunnels**	**DyDAG aux sidechains**	**User implemented features, other**
Deficiency/Vulnerability	**Target/Vector, Desc**																				
Surveillance, Signal Intrcept	PBI– Bluetooth, Zigbee			•			•	•													1
Surveillance, Signal Intrcept	Bus– USB, PCI, HDMI			•			•	•													1
Surveillance, Signal Intrcept	L1 Ethernet cable (Cat)		•	•	•	•	•	•	•												1
Surveillance, Signal Intrcept	L1 cable (coax, fiber)		•	•	•	•	•	•	•												1
Surveillance, Signal Intrcept	L1 radio/microwave		•	•	•	•	•	•	•												1
Surveillance, Signal Intrcept	Wireless receivers		•	•	•	•	•	•	•												1
Denial of Service (DoS)	L1 PHY interface			•			•	•											•		1
Surveillance, Packet Intrcept	Bluetooth decrypt			•			•	•													1
Surveillance, Packet Intrcept	L2 Ethernet MAC addr		•	•	•	•	•	•	•												1
Surveillance, Packet Intrcept	L2 DOCSIS-3 MAC addr		•	•	•	•	•	•	•												1
Surveillance, Packet Intrcept	L2 WiFi sniffer, MAC		•	•	•	•	•	•	•												1
Surveillance, Packet Intrcept	L2 WEP/WPA KRACK		•	•	•	•	•	•	•												1
Surveillance, Packet Intrcept	L2 3GLTE/4G/5G sniff		•	•	•	•	•	•	•												1
Packet Hijacking	L2 MIM, data corrupt	•	•	•	•	•	•	•	•										•		1
Wireless Packet Hijacking	Faux cell towr, corrupt		•	•	•	•	•	•	•										•		1
Last Mile Spying	L2 MAC radio monitor		•	•	•	•	•	•	•										•		1

Packet Sequence Sniffing	Sidejacking (cookies)		●	●	●	●	●	●	●												2
Public WiFi Session Hijack	Firesheep (Facebook)		●	●	●	●	●	●	●												2
WiFi Packet Hijack, Fraud	L2 evil twin hotspot		●	●	●	●	●	●	●												1
LAN Fake MAC Msg	L2/L3 ARP spoof MIM	●	●	●	●	●	●	●	●												
Denial of Service, DoS/DDoS	L2 MAC flood attack		●	●	●	●	●	●	●										●		
Datagram hijacking	L3 IP spoofing		●	●	●	●	●	●	●												
Datagram hijacking	L3 MIM, data corruptn	●	●	●	●	●	●	●	●												
Wireless Datagrm Intercept	Authen relay attack	●	●	●	●	●	●	●	●												
Denial of Service DoS/DDoS	L3 cyberbot subnet	●	●	●	●	●	●	●	●										●		
Bogon Black Hole IP Routng	IP address ruse	●	●	●	●	●	●	●	●										●		
Port Interrogation	L4 port profiling		●	●	●	●	●	●	●				●						●		
Denial of Service DoS/DDoS	L4 port attack		●	●	●	●	●	●	●										●		
HTTP Daemon Port Attacks	L4/L7 port 80 attack		●	●	●	●	●	●	●										●		
BGP Peer-to-Peer State Var.	L4/L7 routing exploits	●	●	●	●	●	●	●	●												
RIR WHOIS Combo Attack	L4 TLS zombie blocks	●	●	●	●	●	●	●	●				●								
TCP Handshaking Exploit	L4 Telnet/FTP fraud		●	●	●	●	●	●	●				●						●		
Fraudulent Session Authen	L5 CA-cert theft/fraud							●		●	●	●	●								
Malicious Session, Malware	L5 fake CA-certs							●		●	●	●	●								
SSH Downgrade Exploit	L5 fraud or spyware									●	●	●	●								
OS System Function Calls	L5/L7 library Trojan									●	●	●	●								
Denial of Service DoS/DDoS	L5 authenticate fraud							●	●	●	●	●	●						●		
Doc/Media Player Malware	L6 fake CA-certs							●	●	●	●	●	●								
Crypto Key Exchange Theft	L3/L6 packet hijacking		●	●	●	●	●	●	●	●	●	●	●						●		
Crypto Key Exchange Theft	L6 fake CA-certs							●		●	●	●	●								
Denial of Service DoS/DDoS	L6 worm infestations							●	●	●	●	●	●								
Denial of Service DoS/DDoS	L7 comm app malware							●	●	●	●	●	●						●		3
Spyware	L7 comm app malware							●		●	●	●	●								3
Denial of Service DoS/DDoS	L7 sec app malware							●	●	●	●	●	●						●		3
Spyware	L7 sec app malware							●		●	●	●	●								3
Browser	L7 app malware							●		●	●	●	●								3
Crypto theft	L7 BC malware							●	●	●	●	●	●			●	●	●	●		3
Usurpation of System	L7 OS malware	●	●					●	●	●	●	●	●								3
Usurpation of System	Network operator	●	●					●	●	●	●	●	●								

1. HyperNode SDNP enabled router
2. Authenticated cookie (single, multifactor), AAA
3. Online database/blockchain of reported malware

Part II **§C** **Data Breaches**		**De-centralized (node, juror, AI mrkt)**	**Stateless HyperNodes, 4-tier res pvdr**	**SDNP dyn frag, state-based, disag data**	**SDNP dyn meshed routing, min prop**	**SDNP anonymous packets, single hop**	**SDNP dyn conceal, state-based, keyless**	**SDNP tri-ch, metamorphic HNs, multi-D**	**SDNP dyn transport sec, VPN tunnels**	**Network native CA-certs, multi-factor**	**Identity trust chain, SQK, ownership**	**Digitally signed assets, trust zones**	**Accts, pseudonymous trans, AAA**	**Private & temp wallets, OT^3 proxy**	**Lightweight multi-tree DyDAGs, defrag**	**Adjunctive crypto synth, HHCs, eco**	**Embedded tokens, recycling**	**HyperContract, transitory tBC**	**Cloaked jurors, RBOS. HN tunnels**	**DyDAG aux sidechains**	**User implemented features, other**
Deficiency/Vulnerability	**Target/Vector, Desc**																				
Data Breach	Financial records	●		●						●	●	●	●	●					●	●	1
Data Breach	Business transactions			●		●			●	●		●	●					●	●	●	1
Data Breach	Credit info			●		●				●		●	●							●	1
Data Breach	Trade secrets, IP theft			●			●			●		●	●							●	1
Data Breach	Client lists & accounts			●						●		●	●							●	1
Data Breach	Personal information			●						●		●	●							●	1

Data Breach	Gov records (tax, SS#)	•		•						•	•	•	•							•	1
Data Breach	Health records			•						•		•	•							•	1
Data Breach	Military recds, vet/act	•		•						•		•	•							•	1
Data Breach	Personal files, media			•						•		•	•							•	1
Data Breach	Identity theft	•		•		•				•	•	•	•							•	1
Data Breach	Intelligence agencies			•						•		•	•							•	1
Database ID Usurpation	DB login overwrites	•		•		•				•			•					•		•	2
Transactional Record Attack	DB process interfere	•		•		•				•		•	•					•			2
SQL Injection	Login exploit, passwrd			•		•				•	•	•	•					•			2
SQL Injection	Inject worms, malware			•		•				•	•		•								2
SQL Injection	Access data			•		•				•		•	•					•		•	1
SQL Injection	Steal passwords			•		•				•		•	•					•		•	2

1. Custom database access control, user authorization, access control
2. Multifactor authorization

Part II **§D** **Blockchain Attacks**		**De-centralized (node, juror, AI mrkt)**	**Stateless HyperNodes, 4-tier res pvdr**	**SDNP dyn frag, state-based, disag data**	**SDNP dyn meshed routing, min prop**	**SDNP anonymous packets, single hop**	**SDNP dyn conceal, state-based, keyless**	**SDNP tri-ch, metamorphic HNs, multi-D**	**SDNP dyn transport sec, VPN tunnels**	**Network native CA-certs, multi-factor**	**Identity trust chain, SQK, ownership**	**Digitally signed assets, trust zones**	**Accts, pseudonymous trans, AAA**	**Private & temp wallets, OT^3 proxy**	**Lightweight multi-tree DyDAGs, defrag**	**Adjunctive crypto synth, HHCs, eco**	**Embedded tokens, recycling**	**HyperContract, transitory tBC**	**Cloaked jurors, RBOS. HN tunnels**	**DyDAG aux sidechains**	**User implemented features, other**
Deficiency/Vulnerability	**Target/Vector, Desc**																				
BC Fraud, Consensus Attack	Fake cryptocurrency			•		•	•		•	•	•	•	•		•	•		•	•		1
BC Fraud, Consensus Attack	51% attack	•		•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Denial-of-Service attck	•		•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Race attack			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Sybil attack			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Finney attack			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Segmentation			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Security vulnerability			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Timejacking			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Record hacking			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Tragedy of commons			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Spam attack			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Double spending			•		•	•		•	•	•	•	•		•			•	•		
BC Fraud, Consensus Attack	Spyware			•		•	•		•	•	•	•	•		•			•	•		
Cryptocurrency Theft	Crypto wallet theft			•		•	•		•	•	•	•	•	•	•	•		•	•		
Cryptocurrency Theft	Password/CA theft			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Private key security			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Clock skew attack			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Weak cryptography			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Security vulnerability			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Ransomware			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Endpoint vulnerability			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	WiFi packet sniffing			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Address redirect			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	DoS repudiation attack	•		•		•	•		•	•	•	•	•		•			•	•		
Cryptocurrency Theft	Implementation bugs													•	•						2

Cryptocurrency Theft	Test transaction attack			•		•	•		•	•	•	•	•	•	•			•	•		
Cryptocurrency Theft	Spyware			•		•	•		•	•	•	•	•		•			•	•		
Malware Attacks	BC transfer Trojans			•		•	•		•	•	•	•	•		•			•	•		
Malware Attacks	BC viral infection			•		•	•		•	•	•	•	•		•			•	•		
Malware Attacks	Zero day exploits			•		•	•		•	•	•	•	•		•			•	•		
Malware Attacks	Miner attack			•		•	•		•	•	•	•	•		•	•		•	•		
Privacy Leakage	Identity extraction									•	•	•	•		•			•		•	
Privacy Leakage	BC backtracing									•	•	•	•		•			•		•	
Privacy Leakage	Deanonymisation									•	•	•	•		•			•		•	
Blockchain Illegality	Copyright violations									•	•	•	•		•			•		•	
Blockchain Illegality	Stolen IP									•	•	•	•		•			•		•	
Blockchain Illegality	Business material									•	•	•	•		•			•		•	
Blockchain Illegality	Banned material									•	•	•	•		•			•		•	
Blockchain Illegality	Illegal content									•	•	•	•		•			•		•	
Blockchain Illegality	Illicit transactions			•		•	•		•	•	•	•	•		•			•	•	•	
Blockchain Illegality	Cyberhygiene									•	•	•	•		•			•		•	
Blockchain Illegality	Infection alerts									•	•	•	•		•			•		•	
Smart Contract Fraud	Ponzi schemes									•	•	•	•		•			•		•	
Smart Contract Fraud	Security vulnerability			•		•	•		•	•	•	•	•		•			•	•	•	
Smart Contract Fraud	Privacy leakage									•	•	•	•		•			•		•	
Smart Contract Fraud	Implementation bugs													•	•						2

1. Adjunctive synthesis via HHCs
2. Code debug protocols

Part II **§E, F, G** **Other Deficiencies** **& Vulnerabilities**		**De-centralized (node, juror, AI mrkt)**	**Stateless HyperNodes, 4-tier res pvdr**	**SDNP dyn frag, state-based, disag data**	**SDNP dyn meshed routing, min prop**	**SDNP anonymous packets, single hop**	**SDNP dyn conceal, state-based, keyless**	**SDNP tri-ch, metamorphic HNs, multi-D**	**SDNP dyn transport sec, VPN tunnels**	**Network native CA-certs, multi-factor**	**Identity trust chain, SQK, ownership**	**Digitally signed assets, trust zones**	**Accts, pseudonymous trans, AAA**	**Private & temp wallets, OT^3 proxy**	**Lightweight multi-tree DyDAGs, defrag**	**Adjunctive crypto synth, HHCs, eco**	**Embedded tokens, recycling**	**HyperContract, transitory tBC**	**Cloaked jurors, RBOS. HN tunnels**	**DyDAG aux sidechains**	**User implemented features, other**
Deficiency/Vulnerability	**Limitation/Risk**																				
Network Sequestration	Data & net oligopolies	•	•					•													
Centralized Operation	Network ops control	•						•													
Administrator Intervention	Network ops control	•						•													
3rd Party Cert Authorities	Fraud, theft	•								•											
Centralized Operation	Financial transactions	•						•													
Blockchain Mining	Mining time	•										•			•	•		•			
Blockchain Mining	Mining energy	•										•			•	•		•			
Blockchain Mining	Mining cost	•													•	•	•	•			
Blockchain Mining	BC size/weight	•										•			•	•		•			
Blockchain Validation	Peer consensus	•															•	•	•		
Cryptocurrency transaction	Online payment speed	•										•	•	•	•		•	•	•		
Cryptocurrency transaction	Point-of-Sales speed	•										•	•	•	•		•	•	•		
Cryptocurrency transaction	Asset transfer speed	•										•	•	•	•		•	•	•		
Cryptocurrency transaction	Online pmnt integrity	•				•	•		•			•	•	•	•		•	•	•		
Cryptocurrency transaction	POS integrity	•				•	•		•			•	•	•	•		•	•	•		
Cryptocurrency transaction	Asset xfr integrity	•				•	•		•			•	•	•	•		•	•	•		
Device Security Risk	IoT, V2X			•	•	•	•					•									1

Device Privacy Risk	IoT, V2X			●	●	●	●					●									1
Quantum Security Risk	Code breaking			●	●	●	●	●	●									●			

1. HyperNode SDNP enabled router

Glossary

The following terms define terms of art used in the technical whitepaper (including lexicons specific to the HyperSphere, its technology, and its inventive matter). Terms in square brackets [-] identify the source of the definition.

7-layer Open Systems Interconnection (OSI) Model *[networking, communications]* – A multi-layer abstraction model used to describe communication and computer networks where each layer provides services to the layer above it and relies on resources delivered from its underlying layer. The Internet's TCP/IP protocol and the HyperSphere's SDNP protocol both conform to the 7-layer OSI model.

51% attack *[cryptography, economics]* – A peer consensus attack where the majority of a jury-of-peers used to validate or repudiate blockchain or cryptocurrency transactions are controlled by a single entity or an oligopoly;

AAA *[networking, communications]* – An acronym for 'Authentication, Authorization, and Administration', the process used to determine computer and network access and set privileges granted to users;

Ad hoc *[Latin]* – Formed, arranged, or executed for a particular purpose; In the HyperSphere, the heterogeneous network of HyperNode resource providers comprises a mix of cloud-as-a-service providers, fixed network and ad hoc peer-to-peer communication nodes; HyperNode participation in the network is stipulated in HyperContracts between resource providers and merchants/service providers.

Anonymous data transport *[HyperSphere]* – In accordance with the Secure Dynamic Network & Protocol, payload transport through the HyperSphere employs anonymous datagrams containing only source and destination IP addresses on a hop-by-hop basis without revealing the identity of the communicating devices, i.e. the end points;

Applications habitat *[computing]* – The operating environment, i.e. the app environs of a host OS used to execute application programs under control of system's operating kernel;

Authority |A| node *[HyperSphere]* – HyperNode operation involving the administration of tasks and the routing of datagrams through the SDNP dynamic meshed network;

Blockchain *[cryptography, economics, HyperSphere]* – A linear database of time-stamped plaintext and cryptographic blocks immutably recorded as a one-dimensional DAG; Conventional blockchains generally comprise unitary communal digital ledgers with sidechains (called forks) for new lineages. The HyperSphere utilizes multiple blockchains topologically arranged as a multi-tree dynamic DAG.

Blockchain-as-a-Service (BaaS) *[cryptography, economics]* – The application of blockchain synthesis and transactional processing for user applications, generally involving market specific solutions (e.g. medical, fin-tech, IoT, etc.);

Blockchain processor (BCP) *[HyperSphere]* – HyperNode functionality used to synthesize and process blockchains and their applications including transitory blockchains, perpetual blockchains, and HyperSphere embedded cryptocurrency. Blockchain synthesis in the HyperSphere is 'network native', generated adjunctively using HHCs (HyperNode Hop Codes) synthesized during data transport through the network;

Blockchain protocol *[cryptography, economics]* – A misnomer describing operation of 'application software' in blockchain processing (sometimes inaccurately described as a communication protocol competing with TCP/IP);

Bogon *[networks, communication, Technopedia]* – "A bogon is an bogus IP address from the bogon space, which is a set of IP addresses not yet officially assigned to any entity by the Internet Assigned Number Authority (IANA) or a regional Internet registration institute. Bogon IP addresses are legitimate addresses."

Botnet *[networks, cryptocurrency, HyperSphere, Wikipedia]* – "A network of private computers infected with malicious software and controlled as a group" with or without the owners' knowledge, e.g., to send spam messages, launch DDoS attacks, prevent blockchain transactions or repudiation, etc.

CA-certificate *[cryptography, economics, HyperSphere]* – A digital certificate certified by a 'certificate authority' used to insure authenticity of software, devices, processes, and blockchains. In the HyperSphere, CA-certificates are network native, comprising an indelible trust-chain of system and identity based certificates;

Certificate authority *[cryptography, economics]* – The issuer of CA-certificates used for digital signing of devices, processes, transactions, and assets. In Internet based transactions, certificate authorities comprise trusted third-party sources subject to fraud and theft; In HyperSpheric transactions, CA-certificates are network-native comprising verifiable system-generated credentials able to detect and rescind fraudulent certificates.

Cloaked juror *[HyperSphere]* – In decentralized processes for transaction validation and repudiation by peer consensus, cloaked jurors specified by HyperContracts are unknown to the transacting parties and thereby not subject to peer surround attacks (e.g. Sybil attacks, 51% attacks, cyberbot attacks, etc.);

Cold storage *[computing, cryptography, HyperSphere]* – In cryptography, the storage of digital memory in a secure offline location (such as a vault or safe deposit box) containing root CA-certificates and other security credentials; In the HyperSphere, a sequential quantum key (SQK), a digital key providing a uniquely beneficial cryptographic recovery mechanism for root certificate corruption, is also securely held offline in cold storage.

Consensus *[cryptography, economics, HyperSphere]* – In decentralized processes for cryptocurrency transaction validation and repudiation by peer consensus, a jury-of-peers ascertains the integrity of a blockchain transaction; Conventional consensus validation is known to be susceptible to a wide variety of attack stratagems such as consensus attacks, denial of service attacks, and other exploits. In contrast, the HyperSphere uniquely employs 'cloaked jurors' to deflect consensus attacks.

Consensus attack *[cryptography, economics]* – A consensus attack is an exploit designed to corrupt, impede, or prevent an accurate assessment of blockchain or cryptocurrency transactions by an independent jury-of-peers; Consensus attacks include 51% attacks, Sybil attacks, and cyberbot DOS attacks among others.

Cryptocurrency *[cryptography, economics, HyperSphere]* – A cryptographic token used in e-commerce to procure resources, execute purchases, compensate resource providers, or otherwise act as a fungible financial instrument for business, investment, or access privileges; Cryptocurrency may be tradable, i.e. able to be bought and sold on digital currency exchanges, or conversely may be limited in its use to a specific ecosphere or market. Tradable cryptocurrency is notorious for rapid and unpredictable fluctuations in price, discouraging its widespread adoption in e-commerce. Compared to fiat currency, the legal definition of cryptocurrency as a utility token, a security token, or a commodity is complex and evolving, varying by country and with each particular cryptocurrency's use.

Cryptocurrency Mining *[cryptography, economics, HyperSphere]* – A common method by which conventional cryptocurrency is created through an intentionally costly or difficult effort with no certainty of economic return (hence the mining metaphor). Most cryptocurrency is generated using energy-intensive Proof-of-Work puzzle solving to cause artificial scarcity. HyperSphere cryptocurrency, in contrast is not generated using an energy-wasting PoW mining processes, but through Proof-of-Performance (PoP) based cryptocurrency minting, executed adjunctively with data transport through the HyperSphere.

Cryptocurrency Minting *[HyperSphere]* – The HyperSphere's uniquely energy-efficient method of synthesizing cryptocurrency adjunctively during data transport of HyperSphere network traffic; HyperNodes mint tokens as compensation for participation in the successful completion of HyperContracts. The number of tokens minted depends on the market-negotiated cost of a HyperContract (the contract's pledge) and each HyperNode's ratable contribution in a HyperContract's successful execution, i.e. through its verifiable Proof-of-Performance. During token minting, a HyperContract's pledge is ratably distributed, either by melting or recycling tokens, permanently retiring the cryptocurrency pledge from circulation. Energy consumption in PoP-based cryptocurrency minting is approximately one trillionth (10-12) that of PoW mining methods.

Cryptoeconomics *[cryptography, economics]* – The economics of e-commerce involving the use of cryptocurrency;

Cybersecurity *[cryptography, networks, computing, communications, HyperSphere]* – The ability of an electronic device or interconnected group of devices to repel unauthorized access and prevent external interference affecting normal operation. Conventionally, cybersecurity is achieved using encryption of data messaging and in virtual machines (such as smartphones and computers) by password protection restricting access to the operating system (OS) kernel. In the HyperSphere, security is dynamic and multi-dimensional, i.e. hypersecure including its reliance on Secure Dynamic Network & Protocol (SDNP) network stack and on-network native CA-certificate, blockchain processing, and cryptocurrency synthesis and transactional validation.

Decentralization *[networks, communication, economics, HyperSphere]* – The realization of a system, network, or commercial ecosphere lacking any central point of control; Transactional validation by peer consensus or autonomous routing of SDNP datagrams over dynamic meshed network represent examples of decentralized systems;

Defragmentation *[computing, HyperSphere]* – In computing and data storage, defragmentation is the process of compressing digital data in sequential storage files (such as hard disk drives of flash memory) by removing unused addresses, i.e. eliminating wasted address space. In the HyperSphere, blockchain defrag processing is a method to eliminate stranded blocks of assets (cryptocurrency) on a blockchain by introducing a credit-debit pair thereby canceling the stranded asset and introducing a new asset at the end of the blockchain, shortening the 'live' portion of the blockchain and accelerating transaction speeds;

Denial-of-Service (DoS / DDoS) attack *[networking, computing]* – A large class of cyberattacks intended to temporarily disable a computer or network by creating artificial network congestion to prevent validate communiqués or transactions from being processed. DoS attacks can be performed on any of the seven OSI layers. A distributed DoS attack or ‘DDoS’ is a generally a cyberbot attack from a large number of infected servers controlled by the DDoS perpetrator.

Directed Acyclic Graph (DAG) *[communications, mathematics]* – A directed acyclic graph is a graph having vertices connected by edges with direction, i.e. arrows indicating flow vectors. A blockchain is an example of a one-dimensional DAG. A blockchain with a sidechain fork is an example of 2-D DAG. In conventional graph theory, DAG vertices are ‘stateless’ maintaining consistent properties over time.

Disaggregated data storage *[computing, HyperSphere]* – The method of storing data in a distributed manner across a network of storage devices where no usable data is concentrated in any one device or address field. The HyperSphere employs disaggregated data storage for both cache and non-volatile data.

Dynamic Directed Acyclic Graph (DyDAG) *[HyperSphere]* – A directed acyclic graph whose vertices are state dependent where time is one of the state variables. DyDAGs are used extensively throughout the HyperSphere to realize a spatiotemporal network including their application in SDNP datagram routing over a dynamic meshed network, in transitory and perpetual blockchains, and in HyperNode Hop Code generation.

Dynamic concealment *[HyperSphere]* – Made in accordance with the Secure Dynamic Network & Protocol, dynamic concealment comprises the use of state-dependent security algorithms and credentials involving the sequential combinational application of encryption/decryption, scrambling/unscrambling, splitting/mixing, junk data insertion/deletion, and junk data packets, along with the use of spatiotemporal cryptographic keys and numeric seeds.

Dynamic meshed network *[networking, communications, HyperSphere]* – Made in accordance with the Secure Dynamic Network & Protocol, a dynamic meshed network is a spatiotemporal communication network comprising DyDAG routing of datagrams over a perpetually changing mesh of HyperNodes in order to minimize propagation delay, provide fragmented transport security, and facilitate redundancy;

Dynamic routing *[communications]* – Made in accordance with the Secure Dynamic Network & Protocol, dynamic routing of datagrams over the HyperSphere’s spatiotemporal communication network involves DyDAG routing of datagrams to minimize propagation delay, provide fragmented transport security, and facilitate redundancy;

Dynamic security *[cryptography, communications]* – Dynamic security comprises methods whereby security mechanisms change over time. Made in accordance with the Secure Dynamic Network & Protocol, dynamic security in the HyperSphere includes dynamic concealment, dynamic routing, and spatiotemporal security credentials.

Encryption / decryption *[cryptography, networking, communications]* – Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. Decryption, the inverse function of encryption, is the process used to recover unencrypted content (referred to as ‘plaintext’) from encrypted ‘ciphertext’ files;

Fintech *[technology, HyperSphere]* – A portmanteau meaning ‘financial technology’, the application of technology supporting the services sector including banking, investment, business consulting, enterprise consulting, accounting, auditing, taxation, enterprise secretarial services, human resources, and corporate governance; In the HyperSphere, fintech is a use case for deploying custom services atop the HyperSpheric network and the enhanced security and privacy it offers.

Fragmentation *[communication]* – The process whereby a data file or media content is parsed and divided into sub-packet fragments or “snippets,” un-interpretable in the absence of their corresponding fragmented counterparts;

Fragmented data transport *[HyperSphere]* – In accordance with the Secure Dynamic Network & Protocol, data and content (including voice, pictures, files and live video) are fragmented into sub-packets then transported across the HyperSphere’s meshed network using multiple anonymous datagrams;

Hash function *[cryptography, communication]* – A unidirectional process whereby source data of arbitrary size is mapped into a fixed-size hash code (“hash”) using an irreversible process, generally employing cryptographic methods. Cryptographic hashing essentially comprises file encryption sans a corresponding decryption key. Given the high degree of non-linearity in the hashing process, beyond some minimal length hash string it is statistically highly improbable that two different source files can produce the same hash result. As such, the identical matching of two hash codes is considered as proof their source files are of identical content. Cryptographic hash functions are used extensively in blockchain and cryptocurrency transactional processing to confer ownership, providing a mechanism for establishing trust in a trustless system;

Heterogeneous peer network *[HyperSphere]* – A dynamic communication network comprising a heterogeneous mix of disparate peers; HyperSphere resource providers comprise global computing clouds, infrastructure (IaaS) and platform (PaaS) providers, local ISPs, fixed cellular networks, dark fiber, and HyperSphere users hosting HyperNodes including cryptocurrency miners and farms, personal computers, gamers, notebooks, tablets, and smartphones, i.e. "the people's network". The HyperSphere is not, however, a conventional TCP/IP based peer-to-peer (P2P) network utilizing either unstructured and structured overlay architectures. Instead, the SDNP protocol operates as a DyDAG spatiotemporal network employing dynamic routing algorithms minimizing propagation delays;

HypWallet *[HyperSphere]* – A digitally signed HyperSecure cryptocurrency wallet in the HyperSphere; In the HyperSphere, cryptocurrency transactions occur through temporary wallets preventing unauthorized access to user assets.

HyperContracts *[HyperSphere]* – A digital contract used to execute transactions in the HyperSphere, to acquire resources, to prescribe job tasks and deliverables, and to specify compensation pledges therefor. During operation, HyperContracts are used to generate transitory blockchains (tBC) to track contract execution progress and confirm contract completion.

HyperNode Hop Codes (HHCs) *[HyperSphere]* – Network native cryptographic codes used in HyperSpheric blockchain processing, executing hypersecure BaaS services, and network-native generation of cryptocurrency;

HyperNode tunnel *[HyperSphere]* – A single-hop ad hoc VPN tunnel temporarily created between two HyperNodes to thwart DoS and consensus attacks, or to protect user privacy;

HyperSphere accounts *[HyperSphere]* – A HyperSphere network-native digital CA-certificate created from user identity information and used to generate account root CA-certificates;

HyperSphere Application Programming Interface (API) *[HyperSphere]* – Application Programming Interface for merchants and service providers to create HyperContracts and to utilize the HyperSphere in e-commerce;

HyperSphere marketplace *[HyperSphere]* – An artificial intelligence (AI) induced marketplace for negotiating HyperContract terms and conditions between service provider/merchants and HyperNode/resource providers;

HyperSphere merchants & service providers *[HyperSphere]* – The users of the HyperSphere; Merchants and service providers offering products and services to their clients utilize the HyperSphere as a platform to identity, engage, and pay resource providers through the execution of HyperContracts. As an e-commerce platform and business ecosphere, the HyperSphere is not a party to HyperContracts or a beneficiary thereof.

HyperSphere resource providers / HyperNodes *[HyperSphere]* – The computing, communication, and storage nodes used to provide resources to and perform tasks for merchant and service providers in the HyperSphere; Device owners install HyperNodes and engage in HyperContract execution, providing resources to merchants and service providers in exchange for minting a prescribed quantity of tokens. Collectively, HyperNode owners (rather than network oligopolies) form the HyperSphere's cloud and meshed communication network.

HyperSphere services *[HyperSphere]* – HyperSphere network-based functions and utilities used to facilitate and execute common tasks in the HyperSphere, in HyperContracts, and in APIs, e.g. digitally signing a device, synthesizing a blockchain, soliciting jurors, etc.

Identity CA-certificate *[HyperSphere]* – A private CA-certificate based on a user's personal or corporate identity used to assign and confirm ownership of assets, transactions, wallets, and devices in order to protect user privacy and prevent fraud, theft, or misrepresentation. Identity CA-certificates containing hashed personal or corporate information are used to generate root certificate then held in cold storage for safekeeping.

Identity theft *[economics, security]* – An illicit act where a perpetrator steals personal (or corporate) information of a victim then uses the information as an imposter to steal assets, criminally engage in fraudulent transactions, or other misrepresent their identity for nefarious purposes.

Imposter *[economics, security]* – In communication, networking, and e-commerce, a person or device that hides or misrepresents their true identity to commit illicit acts; Imposter exploits include packet hijacking, Man-in-the-Middle attacks, Man-in-the-Email attacks, CA-certificate fraud, and others.

Internet-of-Everything (IoE) *[networking]* – The concept or belief that eventually every electronic device, vehicle, person, company, and business process will (at some time in the future) be connected or executed over the Internet or the Web, including IoT, B2B, B2C, V2X, etc.

Internet-of-Things (IoT) *[networking]* – Network connectivity of autonomous electronic devices such as machines, robots, vehicles, sensors and monitors, or any device where human intervention is not required to control or maintain device operation. Because of automatic joining of IoT devices to local area networks (LANs) using autonomous protocols such as Alljoyn (an open connectivity foundation protocol), security experts are concerned that cybercriminals will be able to invade networks and launch exploits by first hacking dumb IoT devices unable to detect or repel intrusion.

Juror, jury-of-peers [cryptography, economics] – In decentralized systems and in cryptocurrency based e-commerce, a group of independent devices or network nodes used to determine the authenticity, validity, and integrity of a transaction (including the transfer of assets or cryptocurrency) through the process of juror consensus. In Internet based e-commerce, consensus attacks involve surrounding a transacting device with insincere or corrupted devices. The HyperSphere employs numerous defensive mechanisms against consensus attacks including the use of cloaked jurors and digitally signed HyperContracts and HyperNodes.

Man-in-the-Email (MiE) attack *[computing, communications]* – A cyberattack where an undetected imposter, acting under the pretense of being a valid intermediary, monitors or modifies the content of an email communication exchange;

Man-in-the-Middle (MIM) attack *[networking, communications]* – A cyberattack where an undetected imposter, acting under the pretense of being a valid intermediary, monitors or modifies the content of datagram traffic between communicating devices during network transport;

Merchants and service providers – See HyperSphere merchants and service providers;

Meshed network *[networking, communications, HyperSphere]* – A computing or communication network comprising a mesh of communicating nodes, where data traffic does not follow a prescribed or preferred path; In the HyperSphere, meshed data routing is executed in accordance with the Secure Dynamic Network & Protocol as a multi-tree DyDAG dynamically seeking minimum propagation delay paths.

Melting *[HyperSphere]* – The process of retiring a tokens from circulation and disabling its use; Melting occurs during recycling when a token pledge is released at HyperContract completion, whereby the pledged tokens are melted and new tokens are minted by all participating HyperNodes. Because the number of newly generated tokens are less than those newly minted, the process of recycling and melting represent cryptoeconomic negative feedback, reducing the number of tokens in circulation and stabilizing the HyperSphere's economy and currency value (especially important during economic recessions)

Metamorphic HyperNode *[HyperSphere]* – The feature whereby a HyperNode morphs into one-of-three possible node types – an authority node, task node, or name server node, in order to perform jobs and provide resources for a particular HyperContract; Although a HyperNode may only perform one of the three functions for a particular HyperContract, a metamorphic HyperNode can concurrently perform other functions to concurrently support different HyperContracts.

Mining – See Cryptocurrency Mining

Minting – See Cryptocurrency Minting

Name Server |NS| node *[HyperSphere]* – HyperNode operation involving the conversion, i.e. dynamic mapping, of phone numbers, URLs, and IP addresses to dynamic IP addresses and dynamic port numbers required to execute DyDAG routing of datagrams through the SDNP dynamic meshed network;

Negative feedback *[electronics, control theory, economics, HyperSphere]* – A self-regulating mechanism in any economic, electronic, or control system where a portion of the system's output is subtracted from its input. Negative feedback tends to stabilize system response by suppressing rapid transients in its state variable and in the value (or quantity) of the system's output. In the HyperSphere, recycling and melting regulates the number of tokens in circulation, especially during recessionary cycles (financial contraction) when new fiat currency entering the HyperSphere declines, forcing merchants to consume existing cryptocurrency to support ongoing business.

Network native *[networking, communication, HyperSphere]* – An intrinsic part of the network, i.e. operating as an integral component of a network and not as a separate system; In the HyperSphere, CA-certificate, blockchains, and cryptocurrency are network native, embedded into the system's autonomous decentralized operation.

Network sequestration *[networks, economics]* – The domination of access or control of network operations, infrastructure, traffic content, or metadata by a monopoly or an oligopoly. Critics claim that Web 2.0 is dominated by a limited number of vendors monopolizing network operations and usurping personal information of clients for sale to advertisers.

One-Time Transaction Token (OT^3) proxies *[HyperSphere]* – A transactional mechanism in the HyperSphere preventing unauthorized access to a user's private blockchains and wallets through a single-use token valid for purchase payment or other transactions, loaded prior to transaction execution.

Operating kernel *[computing]* – The function of a computer or smartphone used to schedule and assign device resources to execute supervisory tasks, host applications, and to transmit or receive data packets through the OSI protocol stack; Metaphorically, an operating kernel functions as an orchestra's conductor.

Peer-to-Peer (P2P) network *[computing, communication]* – A distributed application architecture that partitions tasks or workloads among equally privileged peers as equipotent participants in an application; Although supporting some P2P network features, the HyperSphere is not a true peer-to-peer network as its authority nodes dispatch tasks and administer privileges preferentially in accordance with the required specifications of a HyperContract and a particular HyperNode's ability to service such task requests.

Perpetual blockchains (BC) *[HyperSphere]* – DyDAG blockchains indefinitely maintained to chronicle a sequence of transactions; Blockchains containing hashed content may be safely published on multiple websites to provide an immutable and irrefutable record so as to facilitate trust in a trustless environment. Transactionally, perpetual blockchains are used to record tokens credits and debits. The HyperSphere's perpetual blockchains are digitally signed by leaf CA-certificates to substantiate identity-based ownership of assets through a trust-chain, even when transactions are executed pseudonymously. Perpetual blockchain transactions are validated using replicant block chain observer segments (RBOS) to prevent blockchain attacks and backtracing.

Privacy *[ethics, networks, computing, communications, HyperSphere]* ¬– Privacy is the ability of an individual or group to selectively seclude themselves, or information about themselves from others without prior authorization. In communication and networking, privacy refers to a user's right to control access to data, devices, and assets. While the meaning of privacy overlaps that of security, in general security refers to freedom from or resilience against potential harm (or other unwanted coercive change) exerted from external forces or malevolent parties. In contrast, privacy is the controlled access to personal and confidential information. So while security is necessary to ensure privacy, security is logically insufficient to protect privacy. In the HyperSphere, privacy protection is achieved through the use of identity trust-chains and network-native enterprise grade CA-certificates to control access to personal information and assets. Privacy and identity protection, like cybersecurity, is a fundamental premise and intrinsically beneficial feature of the HyperSphere.

Protocol *[networks, computing, communications]* – A formalized description or specification of digital message formats and rules required for exchanging information or commands among electronic devices and computers; According to Wikipedia "In computing, a protocol or communication protocol is a set of rules in which computers communicate with each other. The protocol says what part of the conversation comes at which time. It also says how to end the communication." As defined, a protocol describes a sequence of actions. As such, a passive file, database, blockchain, or application source code does not constitute a protocol.

Proof-of-Performance (PoP) *[HyperSphere]* – A method of proof used by HyperNode resource providers to establish its contribution to the successful completion of a HyperContract; In token minting, proof-of-performance is 'network-native' as recorded through the distribution of HyperNode Hop Codes (HHCs) generated adjunctively as data traverses the network. Each HyperNode's HHCs are appended sequentially in hashed form onto a transitory blockchain (tBC) used to substantiate the HyperNode's contribution and determine its ratable share of a HyperContract's pledge.

Proof-of-Work (PoW) *[networking, cryptography, economics]* – An energy intensive method used to mine conventional cryptocurrency through the solving of puzzles or mathematical problems, such as a nonce-hash challenges, prime number sequences, irrational number calculations, etc. Because each new block appended onto a unitary communal blockchain changes the conditions of the puzzle, miners compete for each new block. Those who are late in discovering a solution do not earn any compensation, whereby all the energy consumed and money spent on calculating the last challenge is lost, i.e. wasted. As such, environmentalists consider PoW challenges as ecologically irresponsible endeavors.

Public Key Infrastructure (PKI) *[Wikipedia, HyperSphere]* – "Roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption; The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, Internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred." In the HyperSphere, PKIs are employed in the exchange of network-native CA-certificates and HyperSphere specific trust chains comprising true identity and pseudonymous certificates.

Recycling *[HyperSphere]* – Negative cryptoeconomic feedback in the HyperSphere whereby tokens in circulation are pledged and consumed (melted) in the process of HyperNodes minting new cryptocurrency at the fruition of successful HyperContract execution;

Replicant Blockchain Observer Segments (RBOS) *[HyperSphere]* – A transitory blockchain (tBC) comprising a limited length replicant (copy) of a perpetual blockchain of sufficient extent to execute a decentralized juror-based consensus validation of a transaction; Analogous in function to that of messenger RNA (mRNA) in cellular metabolism, an RBOS comprises a short copy or "snippet" of a perpetual blockchain of sufficient length to verify viable blockchain cryptocurrency assets required to execute a transaction or commit to a pledge, but of insufficient length for hackers to perform backtracing or blockchain attacks. When combined with blockchain defragmentation, RBOS validation minimizes the length of blockchains used in consensus validation, thereby expediting validation and increasing cryptocurrency transaction rates.

Quantum computing *[physics, electronics, HyperSphere]* – The engineering application of quantum mechanics to computing, data storage, and communication; Quantum mechanics, a branch of physics, statistically predicts the behavior of the atomic and subatomic particles and forces not governed by deterministic classical physics. Quantum physics, the foundation of semiconductor devices and solid-state physics, describes a number of unique (and non-intuitive) quantum-mechanical phenomena such as quantum entanglement, superposition, the quantum observer effect, quantum-mechanical tunneling, the Pauli exclusion principle, wave-particle duality, the Schrödinger wave equation, the Heisenberg uncertainty principle, the photoelectric effect, superconductivity, blackbody radiation, the ubiquity of Planck's constant, and more. Quantum computing is anticipated to revolutionize the field of cryptography and security but has equally profound implications in empowering brute-force attacks on PKIs, CA-certificates, encrypted files, and on communication. Unlike the Internet, the HyperSphere's hypersecurity does not rely solely on encryption, but utilizes data fragmentation, decentralization, dynamic concealment and routing to minimize any reliance on cryptography, thereby offering enhanced resilience to network attacks employing brute-force cryptographic attack strategies and methodologies.

Resource providers – See HyperSphere resource providers

Root CA-certificate *[computing, communication]* – A private CA-certificate based on a user's identity certificate employed to confer and validate ownership of assets, transactions, wallets, and devices, and thereby protect user privacy preventing fraud, theft, or misrepresentation. Root CA-certificates containing hashed personal or corporate information are used to generate intermediate and user or 'leaf' certificates. After use, root CA-certificates are generally held in cold storage for safekeeping.

Secure Dynamic Network & Protocol (SDNP) *[communication, HyperSphere]* – A patented realtime dispatcher-based multilevel communication protocol and cybersecure alternative to the Internet's insecure TCP/IP protocol suite; The SDNP protocol forms the communication platform on which the HyperSphere operates.

Security – See cybersecurity;

Sidechain *[cryptography, economics, HyperSphere]* – An alternative branch to a main blockchain. In the HyperSphere, sidechains may be used for auxiliary documentation chains or contain subroutines for DyDAG network routing or other functions.

State based security *[HyperSphere]* – In accordance with the Secure Dynamic Network and Protocol, a method for dynamic datagram construction whereby the methods of dynamic encryption, dynamic concealment, and dynamic security credentials are state dependent, relying on both network time and location to control hypersecure transport through the HyperSphere's meshed network.

Stateless network operation *[networks, communications, HyperSphere]* – A network of computing and communication nodes that retain no record or history of its activity; In the HyperSphere, metamorphic HyperNodes exhibit collective amnesia, forgetting all tasks and jobs they execute immediately after the task is completed. HyperNodes, however, collect (and temporarily hold) HHCs, appending the codes onto a tBC to confirm their contribution to the successful completion of a HyperContract and to earn their ratable share of the contract's pledge. After HyperContract resolution, payment is disbursed and the tBC is destroyed.

Smart contract *[cryptography, communications, HyperSphere]* – A digital contract specifying tasks and functions to be performed in order for a resource to receive compensation; In conventional smart contracts, numerous resources compete to execute the contract, thereby wasting energy by having multiple suppliers doing the same job. Because contract execution is not complete until all the participating resources complete the same task, the "slowest" participant determines a smart contract's transaction time. In contrast, HyperContract completion is verified the distribution of HHCs, not by redundant execution. The number of resource providers required to execute a job is stipulated by the HyperContract's job description, not as part of the job's validation procedure.

SQK, a sequential quantum key *[HyperSphere]* – A sequential cryptographic key having millions of combinations not susceptible to brute force attacks or quantum computing analysis; SQK backup is preferably stored offline in cold storage to be invoked only as a 'last resort' emergency asset recovery procedure;

Sybil attack *[security, networks, cryptocurrency, Wikipedia]* – A network and blockchain consensus attack wherein "a reputation system is subverted by forging identities in peer-to-peer networks" named after Sybil, a book and case study on a dissociative identity disorder;

Task |T| node *[HyperSphere]* – HyperNode operation involving the execution of tasks and datagram routing through the SDNP dynamic meshed network; Task nodes are unaware of the identity of callers or of the routing paths used in an ongoing session.

Token *[HyperSphere]* – A utility token and tradable cryptocurrency of the HyperSphere; Tokens are minted by HyperNodes as ratable compensation for participation in the successful completion of HyperContracts. Merchants and service providers may also use tokens as a pledge in HyperContracts. The commercial and fungible value of a token is determined by supply and demand market dynamics (including cryptocurrency trading).

Token blockchain *[HyperSphere]* – A privately owned DyDAG blockchain used to record transactions, pledges, and minting of tokens;

Tokenomics *[cryptography, economics]* – The economics of a private or public cryptocurrency offering including token pricing, funds raised, payments accepted, founder rewards, air drops; The tokenomics of an token offering should not be confused with cryptoeconomics, the economic considerations of cryptocurrency use and its application.

Topological Trust Network *[HyperSphere]* – The controlled access to assets, processes, transactions, and blockchains in the HyperSphere through multi-tiered security shells having privileges determined by a user's identity and CA certificate;

Transitory blockchains or tBC *[HyperSphere]* – Temporary, i.e. transitory DyDAG blockchains used to conduct or execute a sequence of transactions; Unlike perpetual DyDAG blockchains, transient blockchains are discarded after use with no record of the tBC except for entries made onto perpetual blockchains during tBC processing and execution. A tBC may be passive, containing only hashed and plaintext data blocks, or may include executable code thereby functioning like a subroutine call.

Transmission Control Protocol / Internet Protocol (TCP/IP) *[network, computing, communications]* – The Internet protocol suite including rules and procedures for data communication and packet construction; TCP/IP, often referred to as a protocol stack or network protocol, is generally represented as abstraction layers in a 7-layer OSI stack.

Trust *[ethics, computing, communication]* – Firm belief in the reliability, truth, ability, or strength of someone or something; In communication and networking, trust refers to the honesty and integrity of a device to represent their true identity and to perform tasks in accordance with the rules established for the system. Trust in networking and e-commerce is established digitally through identity trust chains and CA-certificates. Trusted computing refers to computer operation consistently behaving in expected ways as enforced by computer hardware and software. Trust in decentralized systems refers to a process of consensus, using an objective jury-of-peers to determine the validity and integrity of a transaction or of asset ownership.

Trust chain *[cryptography, networking]* – The lineage and pedigree of CA-certificates utilized in identity based trust chains for signing devices, assets, software, assets, etc.

Turing complete *[computing, Wikipedia]* – A computer able to emulate a 'Turing machine' or a "programming language that is theoretically capable of expressing all tasks accomplishable by computers; Nearly all programming languages are Turing complete if the limitations of finite memory are ignored." Because, however access to unlimited memory on-demand (i.e. sufficient memory to execute any arbitrary task and for an unspecifiable duration without warning), present day computers are not Turing Complete, especially given the unpredictability of new computing platforms such as quantum technology. In contrast, because the HyperSphere comprises a heterogeneous peer network (cloud), the extendibility of the network to access limitless data storage and cloud computing capacity combined with immutable transactional records (data certified by indestructible blockchain records), renders the future realization of a truly Turing complete system plausible.

User CA-certificate *[computing, communication]* – A public leaf CA-certificate generated from a user's identity, system information, and intermediate certificates used to digitally sign devices, assets, code,

Vehicle-to-Everything (V2X) *[networking]* – Network connectivity of ubiquitous electronic devices; Because of the diversity of autonomous protocols used in network connectivity, security experts are perpetually concerned with the Internet's ability to repel a wide range of cyberattacks.

Virtual-Private-Network (VPN) *[networking]* – A cryptographic tunnel used to securely communicate between devices or HyperNodes.