A Secure Shared Network and a Proof of Credit Consensus Network

2021.08.05

Version 3.0

Abstract

This white paper presents the use cases, technical framework, and implementation details of Deeper Network, a Polkadot project which consists of the Deeper Connect line of devices, and the Deeper Network ecosystem. Deeper Connect is a blockchain-powered all-in-one solution that provides true internet freedom with enhanced security and a frictionless user experience. Deeper Connect devices enable a secure and private peer-to-peer network connection. Users of Deeper Connect will constitute a truly decentralized consensus network based on Deeper's unique Proof of Credit (PoCr) consensus mechanism. Deeper Connect is the first of its kind, combining cybersecurity technology with blockchain technology driven by an online sharing economy. Deeper Connect seamlessly segues users into the Deeper Network ecosystem powered by the Deeper Chain, a truly decentralized smart contract platform running on the Proof of Credit (PoCr) consensus mechanism. The Deeper Chain is characterized by its high security, high efficiency, and low energy consumption. Deeper Connect nodes can automatically participate in Deeper Chain mining. The Deeper Chain enables many foundational web services to be developed on the Deeper Network e.g. dDNS, dCDN etc. paving the way for a Web 3.0 revolution. Developers can also develop and distribute their own applications on the Deeper chain. dApps on the Deeper Chain will be better suited to protect user privacy and data, ensuring personal data sovereignty.

Contents

1 Plight of the Web 2.0 Era

Information replication began when Bi Sheng invented the first movable type using materials of porcelain. 100 years later, Johannes Gutenberg created the movable-type printing press in Europe. Nowadays, 1,000 years since Bi Sheng's invention, the internet is the most evolved technology to share and store information as it represents an incredible acceleration in information flow, giving easily accessible information to billions of people. Just like the printing press did back then, the Internet has revolutionized the diffusion of knowledge, this not being any longer the exclusive property of elites. The rapid development of internet technology has led us to this critical inflection point in history: the world we live in is profoundly being changed by data. With the rise of the Web 2.0 era, data has become more personal, as entire digital identities are built on the internet. As a matter of fact, In 2013, IBM proclaimed the importance of data, being for the "21st century what steam power was for the 18th, electricity for the 19th and hydrocarbons for the 20th" [1]. Yet the importance of data, the population largely remains unaware of the dangers of having personal data controlled by a select few entities, and the power they now wield over us.

1.1 Cybercrime

The spread of network viruses is an endless threat and causes serious economic damage [52]. In 2017, 1.65 million computers were hijacked by network viruses and forced to engage in digital currency mining [37]. With the development of the Internet of Things (IoT), the scope of malicious interference increased by leaps and bounds. IoT viruses can hijack personal computers, cameras, smart appliances, smart door locks, routers, and other Internet reachable devices. Starting with the Mirai virus [33] in June 2018, more than 600,000 networked devices have been hacked [50]. Additionally,

phishing attacks launched by malicious websites are able to obtain sensitive personal information such as usernames, passwords, and credit card details by masquerading as trusted individuals and organizations [40]. In 2017, the Kaspersky Anti-Phishing system triggered more than 246 million times, and 15.9% of its users became targets for phishing sites [16]. In the wake of financial losses caused by phishing websites, from December 2013 to December 2016, the FBI investigated 22,000 phishing scams in the United States, totaling up to 1.6 billion US dollars [31]. It is estimated that 2020 left a record in losses of almost a trillion dollars, twice more than in 2018 [43]. This was due in part to the coronavirus pandemic, as hackers preyed on clients, businesses, and a huge population that switched to remote work. Hackers are no longer targeting specific machines, but whole organizations using human operators as weak links in order to get access to whole networks. Travelex, a foreign exchange company with operations in 70 countries, is an example of this situation. The company had to face demands for payment to decrypt critical computer files after being hit by Sodinokibi, one of the most sophisticated ransomware attacks to date, delivering a devastating attack [15].

These figures come as no surprise, as the number of Internet users are constantly increasing at a rate of 1 million per day. It is estimated that by 2030 there will be 7 billion users around the world [35], with 1 trillion networked sensors embedded in the world around us as soon as 2022, and a total of 45 trillion in the next 20 years [2]. Cybercrime is the unavoidable parasite following this human activity, as of now it costs more than all natural disasters, and is more profitable than drug trade [34]. Cybercrime will become one the greatest risk to business and individuals.

1.2 Information Suppression and Internet Censorship

Information suppression and Internet censorship refers to the act of negating a certain degree of freedom of speech by depriving the user of certain rights on the Internet so that the user's ID or IP is unable to browse the web or send messages [5]. Many countries around the world have blocked a large number of websites for various reasons [25], [26], [54] including that of the USA, a long proponent of freedom of speech. The recent banning of Donald Trump's social media accounts show that even in the land of the free, freedom of expression on the internet is not guaranteed.

The GME stock incident is a censorship perfect recent example, as trading platforms like Robinhood and E-market suspended all trading for the involved stocks. Even gamer-friendly platform Discord, shut down a chat group named after the WSB group in order to thwart any further coordination of this trading group.

According to Freedom on the Net Global internet freedom has declined for the 10th consecutive year, as 26 countries' scores declined during the 2019-2020 period coverage. The United States score dropped for the fourth consecutive year. Even though Facebook, Twitter and other social media platforms were used as tools for social activism, surveillance of social media by federal and local enforcement agencies negated these tools effectiveness, some individuals experienced targeted harassment or were imputed spurious criminal charges for their posts or retweets. [47]

Along with all of its conveniences, the possibilities for censorship and surveillance are also inherent on the Internet. These problems are so common and widespread that people have been forced to give up a measure of privacy in exchange for the convenience of the Internet [55], and to often unknowingly forfeit data privacy rights [19] – personal data is often controlled by service providers and even sold to third parties for profit [22], [24]. That old quote from the 70's has never been more true, "if you're not paying

for the product, you are the product".

Note: Due to different policies in different regions and countries, Deeper Network will adjust and restrict the feature of accessibility for versions sold in different regions, and will launch different versions for countries to ensure that Deeper products can adapt to their laws and regulations. That does not necessarily mean that we agree with such restrictions, as we envision a borderless and free Internet. While respecting local laws, we keep taking pioneering steps into the long and collective process of democratizing the net.

1.3 Internet Trust Crisis

Since Internet service providers and other big fish online are able to monitor, store and sell users data, it is a given that the Internet lacks data privacy. Not to mention the fact that they can of course also profile you and share that data with government agencies. The extent of this surveillance is deep and extremely intrusive. From January 2005 to May 2008, there were more than 200 million suspected cases of personal sensitive records being breached [10]. As a consequence, medical institutions lost $6.2 billion dollars in 2014 and 2015 [41]. In 2018, the Facebook and Cambridge data breaches [49] once again attracted global attention to the threat of data leakage. In fact, data breach cases are common all over the world [27]. These panic-inducing data breaches are caused by the highly centralized nature of the Internet and the side effects of information trading [51].

Given the above problems, it's not surprising that today's Internet is not fully trusted, lack of transparency and reliable infrastructure has generated a trust crisis. In fact, suppression, censorship, deception, and other sorts of malicious activity are not uncommon.

Bitcoin appeared in 2009 as a consequence of the 2008 financial crisis. An event

when numerous banks and other financial institutions failed across the world, and had to be bailed out by governments at the expense of their taxpayers. This situation led to a total loss of confidence and trust in the financial system. Bitcoin was intended to be a decentralized form of digital cash aiming to eliminate the need for traditional intermediaries like banks and governments to make financial transactions. It was Satoshi's original vision that each computer should contribute with one vote in the mining process. Unfortunately that vision soon deteriorated. By 2012 specialized mining hardware devices had appeared starting the transition towards industrialization. Soon, huge industrial farms moved average hobbyist miners out of the game. This issue that unfairly concentrates supply in a few hands is referred to as mining centralization. If a group of miners controls 51% of the total supply, the network becomes centralized at that moment.

Deeper Network believes Satoshi's vision is achievable and wants to leverage the ground among its users by introducing its Proof of Credit (PoCr) consensus algorithm, such that everyone one can participate. We believe our vision is possible by means of the technology developed and the experience accumulated by our team over the years in the areas of hardware design, operating systems, cybersecurity, and blockchain.

1.4 Deeper's Core Beliefs

Deeper's core beliefs are:

1. Freedom: Democratizing the Net

   Lifting the heavy restrictions imposed by politics and censorship on information flow to achieve frictionless data exchange among the entire human race.

2. Fairness: Blockchain for everyone

   Leveraging the true value of blockchain technology to empower ordinary people

rather than to constitute one of the many mechanisms through which a privileged minority profits. A truly decentralized consensus network must be a platform where everyone is allowed to participate and benefit. It should serve society as a whole rather than a centralized organization or a group of powerful individuals.

3. Trust: Information is power, and it belongs to the people.

   Similar to houses, land and savings, personal data is a form of private property, and as such it merits a level of protection befitting its importance. Deeper's ultimate mission is to combine security and blockchain technology to create a trusted Internet that guarantees the sovereignty of personal data.

2 Project Overview

2.1 Deeper Connect

2.1.1 Introduction and Design Philosophy

Deeper Connect is a blockchain-powered all-in-one solution that provides true internet freedom with enhanced security and a frictionless user experience. The design philosophy of Deeper Connect is plug-and-play with zero configuration. Users can enjoy the protection of network security without the need to jump through any hoops. Neither technical knowledge nor a complex user manual is needed. All one needs to do is plug the device in between the modem and the router, power on the device, and enjoy all its benefits: circumventing censorship, protection against cyberattacks, set parental controls, participate in network bandwidth sharing and blockchain mining.

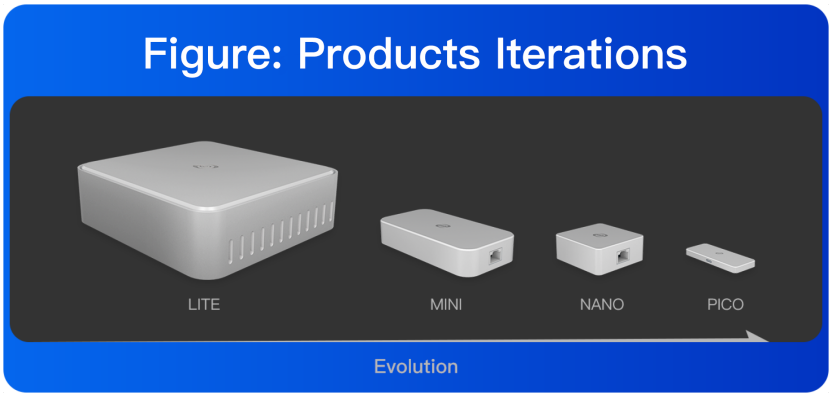

Figure 1: Products Iterations

Deeper Connect has seen generations of iterations ranging from 1) Deeper Connect Lite to 2) Deeper Connect Mini to 3) Deeper Connect Nano and now 4) Deeper Connect Pico, with each version more miniaturized. The vision of Deeper Connect has always been to make it as close to that of an ethernet cable as possible with the belief that

great technology blends into the background and gets out of users' way. The Deeper Connect Pico represents the latest embodiment of that ethos. The Deeper Connect range of devices has seen tremendous user adoption since its inception with thousands sold around the world; the Deeper Connect Mini is one of the top products on Indiegogo.

2.1.2 Solutions for a More Secure, Private, and Fair Internet

Deeper Connect has seen generations of iterations ranging from 1) Deeper Connect Lite to 2Deeper Connect serves as both a node in a decentralized private network and a next-gen firewall in the home network. Decentralized private networks are serverless and distributed; user data can never be logged, leaked, hacked, or subpoenaed. A layer 7 enterprise-grade firewall secures the user's entire home network. It blocks ads and trackers, monitors web traffic, and filters NSFW, NSFC on all internet devices.

2.1.3 Technical Tour de Force: AtomOS, Trident Protocol, IP Multiplexing

AtomOS

The core of Deeper Connects network security prowess lies with AtomOS, a network operating system designed and developed by Deeper. AtomOS is the world's first lock-free network operating system. The system properties of high availability, high performance, and high scalability all hinge upon its state-of-the-art lock-free design.

Trident Protocol

Deeper developed its own Trident protocol, a decentralized, shared communications protocol based on the blockchain with adaptive tunneling, and intelligent routing technologies to provide in-depth security protection as well as an improved user experience. It circumvents network censorship, secures data transmissions, maximizes the use of

network bandwidth, and reduces delays in the data packet transmission process. This is achieved thanks to the efficient integration of network technologies such as intranet penetration, data encryption, protocol camouflage, and tunnel layer congestion control. More details in section 5.1.

IP Multiplexing

Deeper's patented IP multiplexing technology enables zero IP address configuration and the intelligent adaptation of the router's IP address to automatically interface with the internet achieving the true plug and play experience for Deeper Connect devices.

2.2 Deeper Network

2.2.1 Laying the Foundation for Web 3.0

Deeper strives for true decentralization and internet democracy. True decentralization means that no single organization can dominate at all levels of the network, nor that any single point of failure will affect the overall network. Decentralized public chains, decentralized applications, and decentralized gateways are indispensable. For example, the current Ethereum Network is still centralized at the gateway level and is overly dependent on the API interface services provided by Infura for major dApps. Infura itself relies on AWS cloud services provided by Amazon. This means that the Ethereum ecosystem cannot be truly distinguished from a centralized network structure, and naturally, the disadvantages of the centralized network structure remain. The recent Infura downtime reaffirms this as it has led to the paralysis of most Ethereum dApps. Deeper Network is building decentralization at every level of the stack, from a decentralized public chain in the Deeper Chain to a decentralized gateway in the Deeper Connect, Deeper is laying the groundwork for the next generation of the internet.

2.2.2 Decentralized Private Network (DPN)

Decentralized Private Network is a P2P decentralized bandwidth sharing network for bypassing censorships and ensuring privacy. The network is server-less and distributed; user data can never be logged, leaked, hacked, or subpoenaed. Each node operator is empowered to be both a client and a server; node operators earn mining rewards for contributing bandwidth to the network. Mining incentivization ensures the robustness of the network compared to traditional P2P networking models.

2.2.3 Decentralized Web (DWEB)

Anyone can build their own website and register it on the Deeper Network. In Deeper Network, the IP address of the webserver is hidden, making websites resistant to censorship and DDoS attacks. Deeper Network also provides the foundational infrastructure services for Web 3.0 with Deeper's decentralized DNS (dDNS) and Deeper's decentralized CDN (dCDN). DNS is the architecture for resolving IP addresses and querying the Internet. Having a centralized DNS infrastructure makes the Internet extremely fragile, and prone to censorship and attacks. Decentralized DNS services help to make the Internet more democratic. CDN accelerates the web browsing experience by caching content in the cloud. Decentralized CDN allows faster edge access to cached content.

2.2.4 Decentralized Gateway (DGATE)

Deeper Connect is a decentralized gateway to web3.0. Not only can Deeper Connect users securely access various decentralized network services provided by Deeper Network, but they can also seamlessly access various third-party dApp applications, such as decentralized storage services in the Polkadot ecosystem or DeFi services. Decentralized gateways as nodes ensure that Deeper's ecosystem is resistant to issues like

the famous Infura downtime that rocked the Ethereum ecosystem as a result of having centralized gateway access to most of the services on the Ethereum network.

3 Hardware

The goal of Deeper Connect is to provide a plug-and-play hardware solution to security, sharing economy, and blockchain – an all-in-one solution. The highlights of Deeper Connect hardware are described below.

3.1 Cross-Platform

Deeper Connect is designed to be compatible with different hardware platforms. AtomOS has been successfully running on both Intel and ARM64 processors, allowing Deeper to take advantages of both platforms – Intel processors are powerful enough to handle all kinds of high network overload scenarios, which enables Deeper to not only cover the complex use cases of home networks, but also satisfy the enterprise-level requirements. On the other hand, the ARM platform is famous for low energy consumption and low cost, which is sufficient for routine home network needs and different kinds of mobile use cases. In the future, Deeper also has plans for ARM32 products, which would further reduce the hardware cost to under $10.

3.2 Low Energy Consumption

According to digiconomist's assessment [4], the accumulated total annual energy consumption of bitcoin mining worldwide reached 68.81 billion kWh; six times of the energy consumption for May 2017 (11.57 billion kWh). The energy consumption of all bitcoin miners around the world is equivalent to that of the Czech Republic, which is 0.31% of global energy consumption. The average energy consumption for each bitcoin transaction is 968 kWh, the same as the energy consumption of 32 U.S. families in one day. Currently, Bitcoin's annual carbon emissions amount to 33.85 million tons, or 1,300

kilograms of carbon per bitcoin [30].

The unique design of Deeper's PoCr consensus algorithm solves this issue by enabling mining rigs to participate in consensus networks with extremely low computing resources. Deeper Connect utilizes low consumption embedded processors to build a consensus network and network sharing. The maximum energy consumption of a Deeper Connect device is 15 watts. Deeper Connect Mini has a maximum energy consumption of 5W.

As seen in Table 1, Deeper Connect is the most energy efficient product on the market (roughly three orders of magnitude less energy consumption compared to common ASIC/GPU mining rigs) and has the potential to become the most profitable blockchain mining rig.

Hardware Type	**Energy Consumption**
Deeper Connect	5∼15W
ASIC mining rig	2,000∼3,000W
GPU mining rig	1,000∼2,000W

Table 1: Mining Rig Energy Consumption Comparison

3.3 Hardware Wallet

Deeper's security hardware also integrates a cryptocurrency wallet feature to provide users with the highest level of cryptocurrency security without needing any knowledge of blockchain or network security from the users.

Deeper Connect provides multiple security guarantees with AtomOS, which makes it impossible for crackers and malicious organizations to remotely obtain control of the hardware. As a result, the key information stored in the device is inaccessible to

crackers. Additionally, malicious attacks will be identified and recorded to help catch crackers.

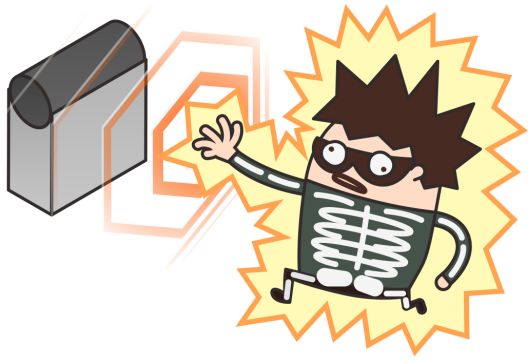

Figure 2: Malicious Access Will Be Blocked and Recorded

Deeper Connect employs triple encryption technology to guarantee the security of storage devices. Even if the hardware device is lost, nobody can crack into the data stored on the device. Triple encryption technology includes block device encryption, file system encryption, and file encryption.

3.3.1 Block Device Encryption

If the storage device is lost, crackers could read critical files by analyzing the data on the block device. To counter that, each block on Deeper Connect is encrypted with AES-CBC [14] (Figure 3), making it very difficult to crack the data because crackers can only access encrypted data.

3.3.2 File System Encryption

Simply employing block device encryption is not enough to ensure the security of the device. In order to further protect our storage media, Deeper Connect scrambled the

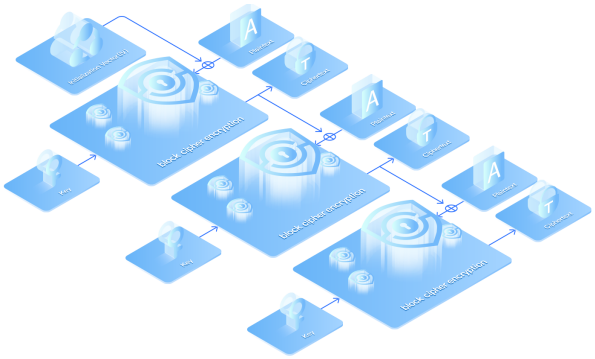

Figure 3: All Disk Data on Deeper Connect Is Encrypted with AES-CBC

key data structure of the general file system (Figure 4). This is how DeeperFS is implemented, a unique file system of Deeper's own design. Due to the strict confidentiality of the data structure of DeeperFS, crackers cannot retrieve any information from the block device related to the structure of the file system, and thus cannot access any critical file stored in the file system.

Figure 4: Encrypted File System Confounds Crackers

3.3.3 File Encryption

All critical files stored in the Deeper Connect file system have to be encrypted by AES-CBC. The decryption key for all files is only available within the compiled program

code, meaning only the Deeper program can access the plain text information if needed (Figure 5).

Figure 5: Triple Encryption Technology Guarantees Deeper Connect Data Security

3.4 Mining Rig with Network Security

On May 28, 2018, the "Packet of Death" was discovered in Ethereum (CVE-2018–12018) [39], where the attacker could freeze geth nodes by sending a death packet. Geth is the official client of Ethereum, extremely important for the Ethereum project: about 70% of nodes running geth contain key nodes for public exchanges and mining pools. With this bug, an attacker could torn down Ethereum and unleashed an earthquake on the Ethereum market.

After providing network sharing services, Deeper Connects will become Deeper chain mining rigs as well. Currently, the security issues of mining rigs has been overlooked. However, if a cracker targets mining software bugs or mining hardware weaknesses, such an attack would naturally have a significant impact on the value of the corresponding cryptocurrency. All of Deeper's products inherit network security genes and all of them are meticulously designed and fully tested. Deeper security devices running AtomOS

will be the the safest mining rigs in the world, maximally protecting the Deeper chain and the interests of all its miners.

Figure 6: Deeper Connect with Its Inherited Network Security Genes Provides Additional Protection for the Deeper Chain

4 Operating System

Deeper's software architecture consists of a data plane, a management plane, and a control plane. The data plane, implemented with Deeper's independently developed AtomOS, is responsible for handling user data packet transmission, reception, and deep inspection. The management plane is to provide a user-friendly interface for monitoring system operations or changing system configurations. The control plane handles communication between device and blockchain, communication between devices, and supports the blockchain consensus mechanism. The layered view of the software architecture is shown in Figure 7.

Figure 7: Software Layer View

The key to Deeper's software is AtomOS – a network operating system custom-built for deep security. It is also the world's first lock-free network operating system. The advanced design of AtomOS is the foundation of the reliability, efficiency and security

of the entire system. We will briefly introduce three aspects of AtomOS: packet I/O, packet scheduling, and deep packet inspection.

4.1 Packet I/O

Packet I/O falls into the I/O layer of AtomOS. It is one of the key technologies that determines user data flow latency and bandwidth throughput.

Traditional operating systems use a kernel network stack to transmit and receive data. The main disadvantages of this approach are high latency and low throughput. After traversing the network to a network device, the packet encounters a series of intermediate processing hurdles such as the network interface card, network device driver, kernel network stack, and socket before undergoing final processing (see Figure 8). In addition, this approach can incur frequent context switches and hardware interrupts, further increasing data latency, and reducing throughput.

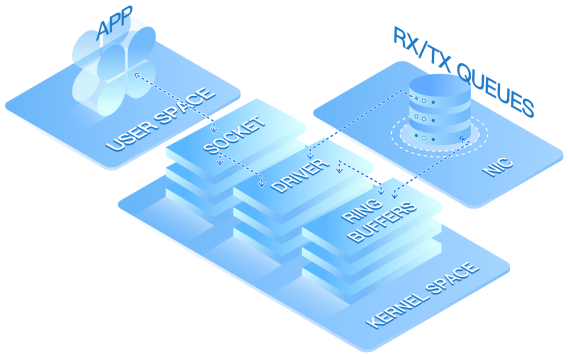

Figure 8: Traditional Operating System Data Transceiver

AtomOS employs zero-copy technology to access packets directly from network devices (see Figure 9). This technology not only bypasses the cumbersome Linux kernel network stack but also avoids frequent context switches and hardware interrupts. It

greatly reduces data packet latency and increases throughput. AtomOS implements zero-copy technology with DPDK [12], designed by Intel. The test data provided by Intel shows that DPDK increases throughput tenfold [13].

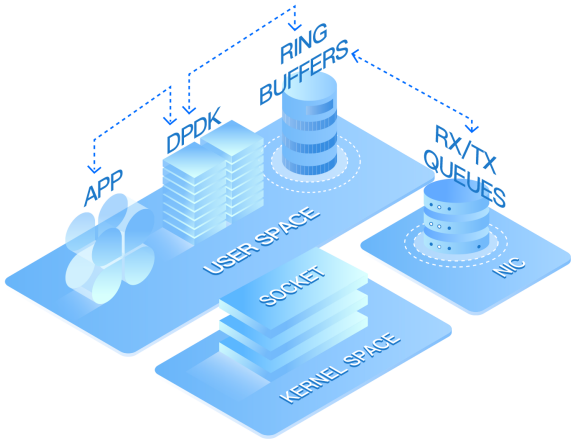

Figure 9: DPDK Data Transceiver

4.2 Packet Scheduling

AtomOS implements the world's first lock-free network operating system with Deeper's unique HIPE data structure. All network operating system issues can be solved on a HIPE-based structure; it embodies the components of our design philosophy: simple, efficient, and under control. Before illustrating the detailed implementation of HIPE, let's have a look at the general limits of current network operating systems.

1. High Performance and High Scalability

   As the size of CPU transistors decreases, Dennard's scaling law [11] gradually breaks down. Reduced transistor size increases static power consumption and detonates serious thermal energy conversion. In addition, the accumulated heat between transistors is considerable, making CPU cooling an urgent issue. Simply

increasing CPU frequency is no longer feasible due to the cooling issue. Therefore, major chip manufacturers have sensibly halted research on high-frequency chips. Instead, they have started to research low-frequency multi-core architecture. Cavium, a well-known processor manufacturer, launched a 48-core network processor back in 2012 [9]. AMD plans to release a 128-thread multi-core processor in 2019 [23].

The development of multi-core processors also brings challenges for the design of network operating systems. Traditional network operating systems are usually based on vxWorks, FreeBSD, Linux or other classic operating systems. VxWorks was designed as a single-core embedded real-time operating system and has been phased out by network device vendors in the last decade. Both Linux and FreeBSD are derived from UNIX, whereas UNIX was originally designed for control systems rather than data forwarding systems. The inherited design flaws of these classic operating systems make it difficult for them to enjoy the benefits of multi-core and even many-core processors.

2. High Availability

   Network operating systems are typically deployed at the boundaries of an assortment of network devices, meaning that if one network device is down, all connected devices in the network that rely on that device will also fail. Therefore, customers generally have extremely high demands for network device availability. In general, the availability of network equipment is required to reach 99.999%, that is, only five minutes of downtime per year is acceptable. Currently, network devices (especially network security devices) have to handle more traffic throughput and more features, making it increasingly challenging to maintain high availability.

3. Packet Order

   When a user accesses a website, dozens of network devices might be involved. If these devices do not maintain packet order, the sending user's data packets might be delivered to the receiving user in a completely random order. Packet disorder triggers the congestion control algorithm [21] of the TCP protocol to reduce the size of the TCP transmission window, thereby seriously reducing the throughput of the data stream and affecting user experience. As mentioned above, multi-core and even many-core processors are now mainstream. Although multi-core processors can process data packets in parallel, serious out-of-order issues might occur without proper consideration. Harnessing the potential of multi-core processors while maintaining packet order has become a hard nut for network operating systems to crack.

   Currently, all operating systems have to employ locks [29] to solve these issues. However, lock design has in turn become an issue in network operating systems. If the granularity of the lock is too big, these big locks will become the bottleneck of the entire system for processors with more and more cores. If the granularity of the lock is too small, it might lead to deadlocks and race condition problems, even though operating system performance may improve. If not handled properly, these problems will significantly impact system stability.

In order to satisfy the general needs of network systems and solve the issues of traditional operating systems, AtomOS employs the HIPE data structure to handle the global scheduling of shared resources in the network operating system. It ensures system correctness while taking full advantage of the benefits of multi-core performance. Next, the implementation of HIPE is briefly introduced.

1. Various shared resources of the operating system are categorized into N groups.

Large shared resources may span multiple groups, and small shared resources belong to a single group (see Figure 10 below).

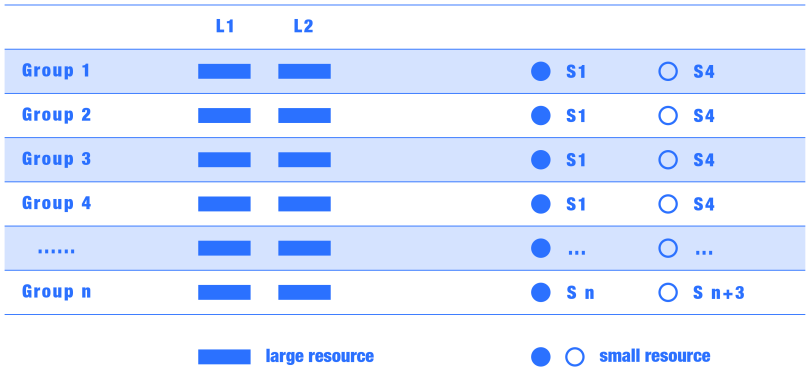

Figure 10: Shared Resources Categorized into N Groups

2. Access to each resource group is triggered by events. Each event that needs to access a shared resource is placed into the lock-free queue for the corresponding resource group. When an event in queue is popped, a CPU core is automatically assigned to process it. Since HIPE retains all events in the corresponding lock-free queue of each resource group, they must be processed sequentially and cannot be processed at the same time, thereby protecting shared resources.

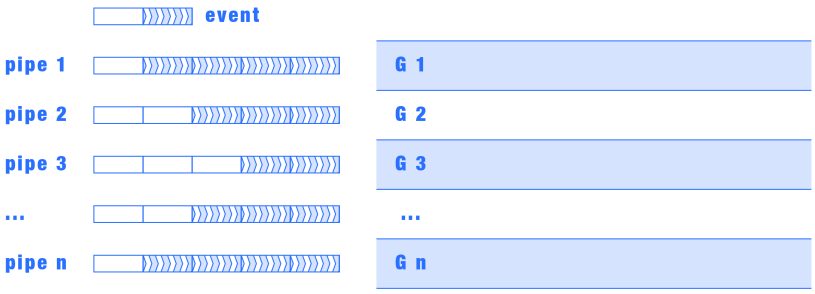

Figure 11: Access to Each Resource Group is Triggered by an Event in a Lock-free Queue

3. Since the number of resource groups in the system is much larger than the number of CPU cores, a continuous stream of data is available for each CPU to constantly process, making the performance of the entire system scalable with the number of CPU cores.

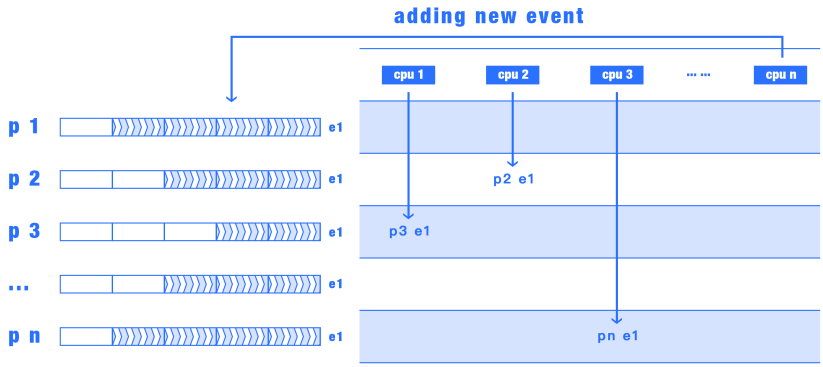

Figure 12: Resource Groups Processed in Parallel by CPUs

4. The lock-free design not only makes packet processing highly scalable, but also avoids the various race condition problems that spawn like flies when processes run in parallel. Moreover, since data packets sequentially traverse the HIPE pipeline, it guarantees that packet order in a particular data flow after the processing of AtomOS is consistent with its original order when receiving.

4.3 Deep Packet Inspection

Deep packet inspection is key for ensuring data flow under comprehensive protection.

AtomOS provides connection security for each layer in the OSI model (see Table 2), which provides Deeper Connect with a complete set of network security functions.

Nowadays the focus of network security has shifted from low layer to higher layer protocols. In addition to the various protections for network layers 1–3, AtomOS also implements the following advanced firewall functions for layers 4–7:

7. Application layer	Application Identification, Malicious Data Flow Detection
6. Presentation layer	Data encryption and decryption to prevent replay attacks
5. Session layer	Protocol session layer checking such as HTTP/SIP
4. Transport layer	Strict status check to prevent Flood attacks
3. Network layer	Fragmentation attack protection, IP spoofing protection
2. Data link layer	ARP spoofing protection
1. Physical layer	Retaining connection during power failure

Table 2: OSI 7-Layer Protection in Depth

- Strict TCP state check to prevent possible TCP masquerading and hijacking: for each TCP connection, AtomOS keeps track of its state in the session table, and only the packets that strictly satisfy the TCP state machine will be forwarded. At the same time, the authoritative NSS Labs firewall test cases in the industry were referenced during implementation to ensure containment of the various known TCP evasion methods.

- Application identification and flow control: AtomOS integrates an application identification engine that is reliable, efficient, and scalable. It identifies common network traffic and performs flow control or intelligent routing to optimize the user experience for key applications. Also, it guarantees a smooth tunnel service without consuming excessive local resources.

- URL filtering: AtomOS can automatically filter malicious websites (including malware downloads, phishing websites, etc.) to provide a secure Internet environment. Users can also enable parental controls to grade Internet content and assign proper access levels to each family member.

- Network Address and Port Translation (NAPT): By default, AtomOS avoids network address and port translation for internal flows, to make it cable-live zero-configuration internet access. However, in some situations, AtomOS can utilize the symmetric mode of NAPT to further hide internal network structure if necessary.

5 Networking

In addition to the feature of Deeper packet inspection described in Section 4.3, Deeper also independently designed Trident protocol, adaptive tunneling, intelligent routing, IP Multiplexing, and tunnel layer congestion control. These technologies provide the deepest packet inspection and the best user experience.

5.1 Trident Protocol

The goal of Deeper's tunneling technology (implemented by the Trident protocol) is to circumvent network censorship. For various reasons, certain governments worldwide are now more frequently conducting deep inspection and filtering of user network traffic [20]. Network censorship relies on firewalls or offline traffic analysis devices deployed at the boundary of the core networks. Therefore, in order to introduce the Trident protocol's bypassing feature, let us review the functionality of firewalls. Currently, firewall modes have been evolving from the basic port-based access control list to advanced content-based application identification. The advanced mode can be implemented in the following ways. The first four approaches belong to the passive identification method and the last one is proactive. Some firewalls can employ multiple approaches to identify applications of user data streams. Further, some artificial intelligence approaches such as Bayes' theorem [46] or decision tree [44] could be employed to perform application identification.

1. Basic Port Filtering

   Basic port filtering refers to the application identification approach that is based on the destination port. The Internet Assigned Numbers Authority (IANA) [18] is the organization that allocates network ports and their corresponding network

applications. As of now, almost all ports from 0 to 1024 have been allocated [28]. Firewalls are able to obtain a basic idea of user applications simply based on the network ports. For example, the destination port commonly used by the NFS protocol is 2049. Even without a clear content pattern, firewalls are still able to identify the application based on the specific destination port.

2. Content Identification

   Content identification refers to the application identification approach that is based on the content of data streams. Since network applications have to follow the predefined network protocol, data streams tend to have a distinct content pattern. For example, the commands commonly used by HTTP (GET/POST, etc.) always appear as the first packet after TCP handshake. Also, the first line of data always ends with HTTP/X.X (the HTTP version used). Firewalls are able to identify HTTP applications happening on a particular destination port based on this pattern. Similarly, all standard protocols have an identifiable content pattern. For some non-standard protocols, content patterns might be changed due to protocol version upgrades, so firewalls have to regularly upgrade their content pattern databases as well to accommodate these changes.

3. Packet Length Identification

   Packet length identification refers to the application identification approach based on packet length order or packet length distribution in data streams. This approach works very well especially when no clear content pattern is available for data streams. The packet length traversed between client and server generally follows some pattern in the negotiation phase of a network protocol. If a network protocol specifies during the negotiation phase that the client has to send a TCP packet with a payload length of 60 bytes as a request, the server has to send a

40-byte packet as a reply followed by another 20–30-byte packet. In this case, the network protocol has a clear pattern in terms of packet length, which can be easily identified by a firewall. In order to evade packet length identification, applications need to scramble or encrypt data packets to hide the pattern of packet length.

4. Packet Interval Identification

   Packet interval identification refers to the application identification approach based on periodic keepalive packets specified in a network protocol. In the tunneling protocol, the server and the client need to periodically send keepalive packets in order to monitor the availability of the tunnel. Keepalive packets generally are sent at a fixed interval and their size is fairly small. Non-standard tunneling protocols still maintain this pattern. As a result, firewalls used for network censorship can identify and block tunneling applications based on this pattern.

5. Active Detection Identification

   Active detection identification means that the firewall acts as a middleman to modify data packet content between client and server, and identify the application according to the data packet content returned from the server. For example, IRC control channels are typically utilized by malware [42]. Even though they conform to the standard IRC protocol (a network chat protocol specified by IETF), they do not support the simple mutation of commonly used IRC commands. Based on this pattern, firewalls can proactively send requests and analyze the server reply to distinguish whether the network application is normal chat software or malware. This approach enables firewalls to monitor the content from data flows but also proactively modify or send data packets for application identification.

Targeting all of the above identification approaches, Trident protocol combines two

tunnel modes to prevent any firewall identification attempts: protocol obfuscation mode and protocol camouflage mode. Since firewalls are unable to identify any traffic pattern in protocol obfuscation mode, internet censorship is not possible. However, for systems with whitelist, all unidentifiable applications are blocked as well. In this case, Trident protocol will automatically switch to protocol camouflage mode to circumvent internet censorship.

1. Protocol obfuscation mode.
    - Random port
        - Randomly negotiate the data session port.
    - Encrypted content
        - All packet contents are encrypted.
        - Ensure that content features cannot be expressed in regular expressions (regex).
    - Obfuscation of packet length
        - All packet lengths are randomized.
    - No periodic keepalive data packets
        - Data packet piggybacks keepalive packet.
        - No separate keepalive data packets exist.
    - Prevent active detection
        - Servers refuse to respond to any packets that do not follow protocol specifications.
2. Protocol camouflage mode. There are two camouflage modes available:

- HTTP protocol
  - The tunneling protocol is completely encapsulated in an "HTTP GET" and an "HTTP POST" message body. The "GET Response" command is used to receive downstream data, and the POST message body is used to send upstream data. Since the port is negotiated by client and server in advance, no specific string name pattern is available in HTTP fields.
- TLS protocol
  - In this mode, the session ticket function of TLS 1.2 is used. The tunnel traffic is like a standard HTTPS connection using the negotiated session ticket. Since there is no negotiation phase, the firewall cannot decrypt or encrypt as a middleman. AtomOS will also use encryption and anti-identification mechanisms similar to the protocol obfuscation mode described above.

Another common issue with P2P networks is NAT [36] traversal. NAT is a common function of network devices in an IPv4 network environment. Network devices are typically configured with private IP addresses in LAN. However, in order to transmit packets out to the Internet, the destination IP address and source IP address of the packet must be translated to public IP addresses. In order to resolve this contradiction, the network device serving as gateway can use NAT to convert the private IPv4 address into the public IP address of the gateway when the data packets are traveling from the LAN to the Internet. This approach not only solves the limitation issue of IPv4 addresses but also satisfies the requirement from organizations to hide internal network structure and isolate external networks. In practice, Deeper Connect might sit behind the NAT device of service providers and assign it a private IP address. However,

that would render Deeper Connect unable to receive connection requests from internet devices. We use the following techniques to solve this problem:

- If the receiver side of the connection has a private IP address and the sender has a public IP address, the receiver initiates connection requests in reverse.
- If both sides use private IP addresses, NAT type identification is further required to determine the proper way to initiate the connection request. AtomOS implements a protocol similar to the STUN protocol (RFC3489 [45]). The network device is able to identify the NAT type and publish it along with other information about the node during the initial stage of network registration. The eventuality of both network devices using Symmetric NAT or Port Restricted Cone NAT can be avoided when setting up the connection. For the other NAT types (Cone NAT or Restricted Cone NAT), the connection setup should provide a solution.

5.2 Adaptive Tunneling Technology

Deeper Connect uses an efficient, flexible, and adaptive proprietary tunneling protocol rather than a standard one such as IPSEC. In the process of designing and implementing adaptive tunneling technology, we have borrowed extensively from various industry-approved WAN acceleration technologies [53]. Given the high latency, high packet loss rate and out-of-order issues of multinational Internet, we improved these technologies in the data tunnel layer, which effectively maximizes bandwidth utilization and significantly improves the user's online experience.

1. Adaptive Data Compression and Merging

   With adaptive tunneling technology, Deeper Connect can determine if packets in the data stream are compressible and decide whether to perform compression. For

instance, the most common HTTP protocol is composed of mainly Latin characters, which can be compressed to save approximately 70% bandwidth and thereby greatly improve transmission efficiency. Meanwhile, given the fact that MP4 and other formats commonly used in video and audio traffic (or networks protocols such as HTTPS/SFTP which uses SSL and TLS encryption) have already approached the theoretical limit of information entropy [48], additional compression would only increase CPU consumption without saving bandwidth, resulting in compression processing and in turn transmission rate reduction. Therefore, adaptive tunneling needs to identify and process accordingly based on content for both CPU and bandwidth efficiency.

Through adaptive tunneling technology, Deeper Connect can also improve transmission efficiency by combining small data packets. Many network protocols have a large amount of control packets with little or no data in the payload. Taking a 30KB HTTP transport stream as an example, even if the client's protocol stack optimizes TCP ACK for every two packets, 40% of packets are still less than 100 bytes. Such a large proportion of packets containing a very small amount of data causes considerable transmission efficiency lag. For optimal transmission efficiency, adaptive tunneling technology can combine or compress and transmit data packets from multiple data streams without affecting the TCP connection latency (see Figure 13).

2. Application-Based Traffic Control

   Application-based traffic control functions according to the application type of the data stream, to ensure that latency-sensitive or volume-sensitive applications enjoy a higher QoS level. In a home network, bandwidth is often limited. When multiple applications are used simultaneously, the demand for bandwidth is often

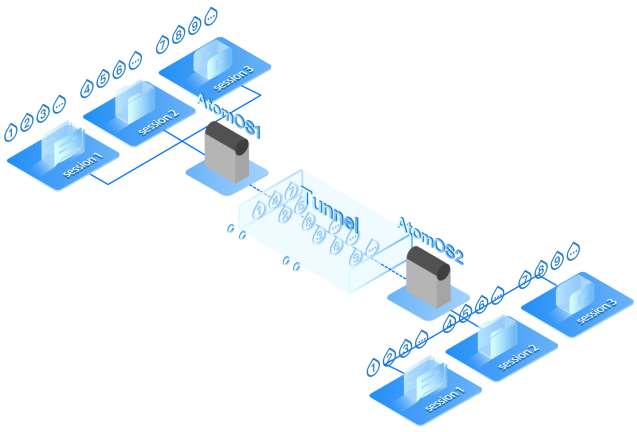

Figure 13: Automated Packet Consolidation, Compressed Transfer Schematic

much larger than what is available. To address this allocation issue, adaptive tunneling can automatically determine application type according to the user data stream and grant the corresponding QoS level. For example, web browsing or email downloads should be classified as latency-sensitive, whereas applications such as file downloads are not. Adaptive tunneling first automatically estimates the network tunnel's actual bandwidth and its bandwidth requirements. If demand exceeds supply, adaptive tunneling will control bandwidth usage based on the application's QoS level. Lower level applications will be temporarily buffered in a limited packet queue. If the packet queue is full, overflow packets will be discarded. Although general application use may be affected due to increased latency and packet loss, overall user experience is improved significantly.

5.3 Intelligent Routing Technology

Intelligent routing refers to automatic configuration of network routing based on data stream characteristics, and whether to transmit through a tunnel. We offer two modes, a

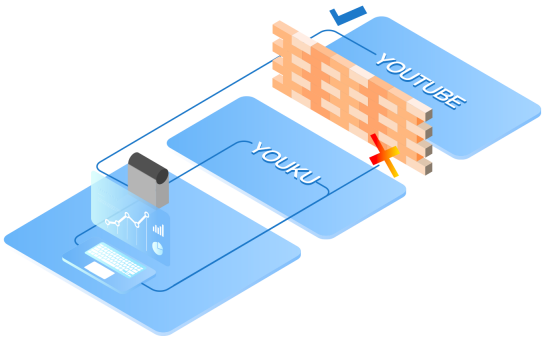

Figure 14: Intelligent Routing

privacy protection mode and a network circumvent mode. The default mode is network circumvent mode.

- Privacy protection mode: In this mode, all data flows related to tracing online browsing will be processed through the tunnel depending on the anonymity level set by the user.

- Network circumvent mode: In this mode, all online data flows will be processed over the tunnel depending on whether or not the website database shows if it is blocked in the local area.

Intelligent routing provides users with the following benefits:

1. Monetary Savings

   Network tunnels are established by two or more Deeper Connects. When one Deeper Connect tries to connect with another one to establish a tunnel, cryptocurrency payment (calculated according to bandwidth and traffic volume) is required through the secure shared network platform. Obviously, tunneling services cannot be offered free of charge. Intelligent routing automatically determines

whether to transmit through the tunnel according to the attributes of the data stream. This approach not only reduces the amount of tunnel usage but also avoids latency caused by tunneling, providing a better online experience without incurring additional expenses.

2. Anonymity Service

   Anonymity service refers to hiding the user's IP address to sidestep tracking. Since the network tunnel is end-to-end encrypted, the data stream transmitted through it will leave no trace. We will set levels according to user access object visibility, and based on user settings, decide whether to perform encapsulation on the corresponding data stream. Highly visible user data streams such as web page visits are at the highest level of anonymity service. For this level of the user data stream, encapsulation is mandatory. The less publicly available user data streams such as P2P downloads belong to the second-highest level of anonymous services. For this level, encapsulation is an optional setting to reduce user costs. Not only that, users can also choose a multi-hop routing mode for more rigorous anonymity services. In a multi-hop routing environment, the network tunnel will be established by several Deeper Connects instead of the usual two. The advantage of this is that Deeper Connect, as an intermediate node, cannot peek at the content because it cannot decrypt the user data stream. The last Deeper Connect node can decrypt the user data stream but cannot know the source. Therefore, the more Deeper Connects nodes in the route, the more difficult it is to track user activities.

5.4 IP Multiplexing Technology

AtomOS is the world's first zero-configuration OS that can implement intelligent routing and tunnel encapsulation in virtual wire mode. All network devices currently on the market that implement the tunnel function work in routing mode. That is, the user needs to have certain network technology as well as working knowledge of IP address planning and tunnel protocol configuration in order to correctly establish the tunnel. It also requires a certain amount of routing knowledge to forward the required traffic to the tunnel for proper encapsulation and decapsulation. AtomOS completely changes this, for no professional know-how is required of Deeper Connect users. After the user connects the AtomOS device to the home router uplink, AtomOS will enter the learning phase. It does not affect the forwarding of traffic, and automatically determines the direction of its connection according to the statistical rules of the IP addresses that appear on the two ports. There are hundreds of millions of nodes on the Internet, while the number of local IP addresses is relatively small and fixed. So after briefly analyzing traffic, we can tell which is the uplink port and which the downlink. AtomOS will proceed to learn the uplink IP/MAC address, DNS server, and other information for future tunnel negotiation and encapsulation.

We believe that the smart home gateway itself is a product with very low user operation frequency. There is no need for users to be aware of its existence most of the time, and little configuration is required to alter functions. Particularly in combination with our unique intelligent routing technology, user privacy and network transmission requirements are fulfilled at the lowest cost with no learning curve at all.

5.5 Tunnel Congestion Control

One of the key use cases of the Deeper Network is to provide users with network anonymity, which protects their privacy and enables them open access to Internet content without being censored or blocked. In the anonymity service (as shown in Figure 15), the user transmits data through the secure AtomOS tunnel between the Deeper nodes, so that the accessed Internet service cannot track the user's private data (e.g., IP address, location). At the same time, since data packets in the AtomOS tunnel are strictly encrypted, censorship firewalls are effectively blinded and unable to identify the Internet content being accessed by the user.

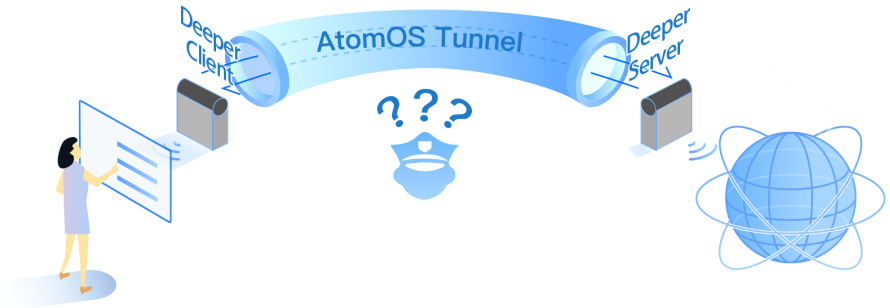

Figure 15: Secure Shared Service (SSS)

Through the combination of Deeper's unique network security and blockchain technologies, SSS effectively ensures the security and stability of the Deeper Network's anonymity services. However, the efficiency of data transmission in the AtomOS tunnel remains an open question. With SSS, there are two major challenges to data transmission:

1. SSS is primarily intended to access Internet content in other countries or regions. Long-distance data transmission, large transmission delay, and high packet loss/out-of-order rate are problems associated with such international Internet ac-

cess.

2. Although packets in the AtomOS tunnel are strictly encrypted and thus censorship firewalls cannot identify them, the firewalls may adopt a random packet drop policy (e.g., 1% random packet drop) for unrecognized data streams in order to downgrade their user experience.

To address the above challenges, Deeper is pioneering a connection-oriented, reliable transmission protocol at the tunnel layer. This is mainly to solve the problem of data transmission efficiency in SSS from the perspective of network congestion control. The complete set of congestion control solutions in the Deeper Network is called TBBR (Tunnel Bottleneck Bandwidth and Round-trip propagation time). It is composed of two core parts: 1) Deploying the new congestion control algorithm called BBR in the AtomOS tunnel so that in case of high packet loss rate, the AtomOS tunnel can still maintain a high transmission rate and low transmission latency; 2) Enabling fast packet loss detection and retransmission, so as to better adapt to high packet loss rate in SSS.

TBBR mainly focuses on improvements on the sender's side. The receiver side need not make any changes. The sender does not rely on any additional feedback from the receiver. This is one of the important design principles of TBBR. It enables easier deployment of TBBR as no changes are required from the receiver side. More importantly, in the high latency and high packet loss rate scenario of SSS, any additional feedback from the receiver side will undoubtedly increase network load, and in such an environment, no stable feedback can be guaranteed.

Traditional congestion control algorithms (such as CUBIC [17], TCP Vegas [7], TCP Reno [38]) are usually based on packet loss events. Packet loss is treated as a signal of network congestion. These kinds of algorithms control data sending rate via a sending window. The window size $W(t)$ at time t is controlled by the AIMD

(Additive-Increase/Multiplicative-Decrease) algorithm:

$$W(t+1) = \begin{cases} W(t) + \alpha & \text{if no packets loss is detected} \\ W(t) * \beta & \text{otherwise} \end{cases} \tag{1}$$

Clearly, the AIMD algorithm tends to keep increasing window size (i.e., transmission rate) until packet loss is detected. Once packet loss is detected, the window size will experience a sharp drop. This leads to two main problems:

1. It is counterproductive to treat all packet loss events as signals of network congestion. In fact, packet loss can also be caused by network errors. In addition, when using SSS, censorship firewalls may also deliberately drop packets. According to the AIMD algorithm, when packet loss occurs, transmission rate is drastically reduced. When packet loss rate reaches a certain level (e.g., 1% packet loss caused by censorship firewalls), the entire network transmission bogs down.

2. Since AIMD keeps increasing transmission rate until packet loss is detected, such a mechanism tends to fill up the entire network buffer (i.e., queue). The greater the number of packets waiting in the queue, the higher the queuing delay. Since memory prices are becoming cheaper and cheaper in recent years, network buffer space is increasing accordingly, which leads to tremendous queuing delays.

It can be seen that traditional congestion control algorithms achieve neither optimal transmission rate nor optimal network latency.

Deeper deploys a new type of congestion control algorithm called TBBR at the AtomOS tunnel. TBBR was developed based on the BBR algorithm [8] combined with tunneling technologies. BBR was first introduced by Google and has been widely de-

ployed in Google's WAN (Wide Area Network). Unlike traditional congestion control algorithms, TBBR/BBR no longer relies on packet loss events as signals of network congestion, but goes back to the essence of network congestion: The sender side is transmitting data faster than what network capacity can handle. In order to measure current network capability, TBBR/BBR continuously measures two key metrics, namely, BtlBw (Bottleneck Bandwidth) and RTprop (Round-trip propagation time). If the network path were a water pipe, the bottleneck bandwidth BtlBw would be the minimum diameter and the round-trip propagation time RTprop would be the length. The capacity of the entire network, i.e., BDP (Bandwidth Delay Product), is the product of the two:

$$BDP = BtlBW * RTprop \tag{2}$$

BDP can also be interpreted as the maximum amount of outstanding data that can be carried in the network without causing any queuing delay (i.e., without occupying any buffer space).

The main idea of TBBR/BBR is that when the data arrival rate at the network bottleneck equals BtlBw and the amount of inflight data in the network equals network capacity BDP, the network is operating at the optimal state of maximum throughput and minimum latency. TBBR/BBR controls the transmission rate by measuring BtlBw and RTprop. It is worth noting that the capacity of the entire network is dynamically changing. Thus, TBBR/BBR must continuously measure BtlBw and RTprop to update the transmission rate. In addition, BtlBw and RTprop cannot be measured at the same time. In order to measure BtlBw, one must fill-up the network buffer to obtain maximum throughput; in order to measure RTprop, the network buffer must be as empty as possible (i.e., no queuing delay) to obtain minimum latency. To address this problem, TBBR/BBR measures the two metrics alternatively and estimates them by

using the sampled values over a certain time window W_R at time T:

$$\hat{BtlBw} = \max(r_t), \forall t \in [T - W_R, T] \tag{3}$$

$$\hat{RTprop} = \min(RTT_t), \forall t \in [T - W_R, T] \tag{4}$$

Where r_t is the measured data transmission rate at time t, and RTT_t is the measured round-trip time at time t.

TBBR/BBR possesses the following two properties:

1. At a certain packet loss rate, TBBR/BBR still maintains a stable transmission rate that is close to the network bandwidth.

2. While maintaining the maximum throughput, TBBR/BBR tends to not occupy the network buffer, and thus reduces queuing delay.

Google has deployed BBR on their Google.com and YouTube servers. BBR has successfully reduced YouTube's median network transmission latency by 53%. In developing countries, this value is as high as 80% [8].

Deeper has transplanted the successful experience of BBR into the application of SSS, and deployed TBBR, the world's first tunnel congestion control, into the AtomOS tunnel. With TBBR, we find that Deeper Connect effectively reduces international Internet access delay while still maintaining a stable network transmission rate when firewalls deliberately cause packet drops.

Figure 16 compares the network throughput of the AtomOS tunnel with TBBR and that of the traditional tunnel IPSEC without congestion control under different packet loss rates. The experimental setup is 1 data stream, BtlBW = 100Mbps, and RTT = 100ms. The gray curve at the top represents ideal transmission rate, i.e., BtlBW * (1 -

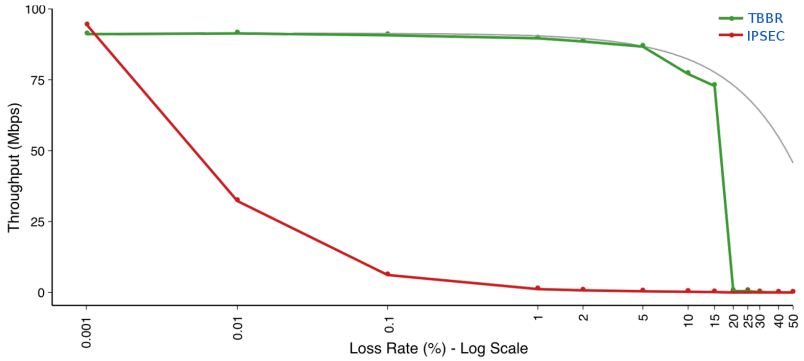

Figure 16: Network Throughput at Different Packet Loss Rates

p), where p is packet loss rate. As we can see from the figure, a very small packet loss rate (0.01%) can cause the throughput of IPSEC to drop to only 30% bandwidth. As packet loss rate increases, IPSEC has a throughput of only 5% of remaining bandwidth, where the transmission is almost paused. In sharp contrast, the throughput of the AtomOS tunnel stays close to ideal throughput even at an extreme 5% packet loss rate. At 15% packet loss, the AtomOS tunnel still maintains 75% bandwidth. In SSS, assuming censorship firewalls randomly drop 1% of unrecognized packets, the throughput of the AtomOS tunnel would be virtually unaffected and would stay close to ideal throughput; while IPSEC would have a throughput of only 5% of remaining bandwidth.

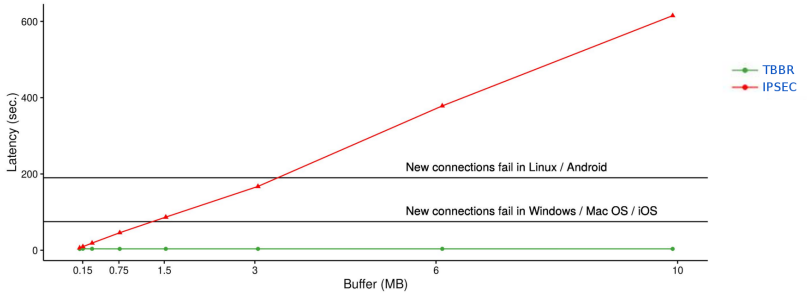

Figure 17: Network Latency for Different Buffer Sizes

Figure 17 compares the network latency of the AtomOS tunnel and IPSEC at different buffer sizes. The experimental setup is 8 data streams, BtlBW = 128kbps, and RTT = 40ms. The traditional tunnel IPSEC tends to occupy the entire network buffer space, which causes latency to increase linearly with buffer size. Even worse, if latency is larger than the network initial connection (SYN) timeout set by different operating systems, it will cause the connection to fail. In sharp contrast, the AtomOS tunnel always keeps latency to a minimum regardless of buffer size.

On top of BBR, the AtomOS tunnel implements further optimizations for fast packet loss detection and retransmission.

Traditional TCP mainly handles packet loss in two ways:

1. If the acknowledgment (ACK) of a packet is not received within a certain time period, i.e., retransmission timeout (RTO), the packet is considered lost and retransmission is triggered.

2. Instead of waiting for timeout, if three duplicate ACKs are received from the receiver, the sender also considers a packet as lost and triggers retransmission. This mechanism is called fast retransmission.

In TCP, when the receiver finds that some packets were skipped, it will send duplicate ACKs to remind the sender that some packets are still missing. There are two reasons a packet may be skipped: either it is lost or the packets arrived out of order, i.e., packets originally scheduled after a certain packet arrived at the receiver side first. When the sender receives a duplicate ACK, it cannot immediately determine which of the two scenarios occurred. Therefore, it is necessary to wait for further duplicate ACKs to determine that packet loss happened with a high probability. If packet loss is determined prematurely, it will lead to unnecessary retransmission that increases

network load; on the other hand, if packet loss is determined too late, it will cause a slow response to packet loss events.

Today, a commonly used fast retransmission mechanism is based on three duplicate ACKs. It requires at least 4 data packets to be sent (i.e., the sending window size is at least 4) to observe three duplicate ACKs; otherwise, the sender can only rely on RTO timeout for retransmission. Therefore, the current fast retransmission mechanism works poorly or not at all in the following cases:

1. Studies [3] have shown that from the perspective of the application layer, a TCP connection often needs to send a total of less than four data packets. In these cases, the current fast retransmission mechanism will never be triggered.

2. Network congestion may cause the sending window to shrink below 4, which also disables fast retransmission.

3. In cumulative ACK mode, the receiver may choose to delay sending ACKs to merge multiple ACKs into one in order to save bandwidth. In this case, even more data packets are needed to be able to trigger fast retransmission.

An effective fast retransmission mechanism should detect packet loss and trigger retransmission in time while reducing superfluous retransmissions. TBBR adopts a dynamic fast retransmission threshold algorithm. In a nutshell, if no more data packets can be sent (either due to sending window size limit or because the application layer has no more data to send), the threshold of fast retransmission is dynamically adjusted according to the number of packets that have not yet been acknowledged; otherwise, a threshold of 3 is used.

Regarding retransmission timeout RTO, traditional TCP adopts an algorithm called exponential backoff, i.e., if a packet times out under the current RTO, the packet is

Algorithm 1 Algorithm for fast retransmission threshold τ in TBBR

1: Assume that the number of currently unacknowledged packets is k
2: **if** there are no more packets to send **then**
3: $\quad \tau = \max(\min(k-1, 3), 0)$
4: **else**
5: $\quad \tau = 3$

retransmitted and the RTO is doubled. In extreme cases, if packet timeout happens n consecutive times, the RTO will explode to 2^n times the original RTO, which greatly stalls transmission rate. TBBR uses a smoother RTO growth curve that sets RTO to 1.5 times the previous value per timeout.

Although the overall design of TBBR is focused on the sender side, we can still improve network transmission efficiency from the receiver side. There are two main approaches:

1. Adopt selective acknowledgment (SACK [32]) at the receiver side. In contrast to the cumulative acknowledgment where the receiver only feeds back the minimum sequence number of the packets that have not been received yet, SACK allows the receiver to explicitly tell the sender which packets have been received and which have not. The sender can selectively retransmit only those packets that have not yet been received. In addition, if multiple data packets are lost in the current sending window, cumulative acknowledgment only informs the sender of one packet loss at a time, resulting in inefficiency. SACK can feed back all lost packets at once. Research shows that in high latency and high loss rate networks, SACK can greatly reduce the number of retransmitted packets and improve transmission efficiency.

2. Dynamically adjust the acknowledgment delay. As mentioned earlier, the receiver can choose to delay sending ACKs. While doing so makes better use of band-

width, it also delays packet acknowledgement and holds back fast retransmission. Especially in a high delay and high packet loss environment, it is crucial that the receiver acknowledges every packet in time. Therefore, at the receiver side, acknowledgement delay can be adjusted dynamically according to the delay and packet loss conditions of the current network.

6 Blockchain

There are two layers in the Deeper chain (Figure 18). The top layer consists of hundreds of validator nodes like any other blockchains. The bottom layer, also called the Deeper layer, consists of millions of Deeper devices. These devices earn credits by providing services in the Deeper network, e.g., sharing bandwidth.

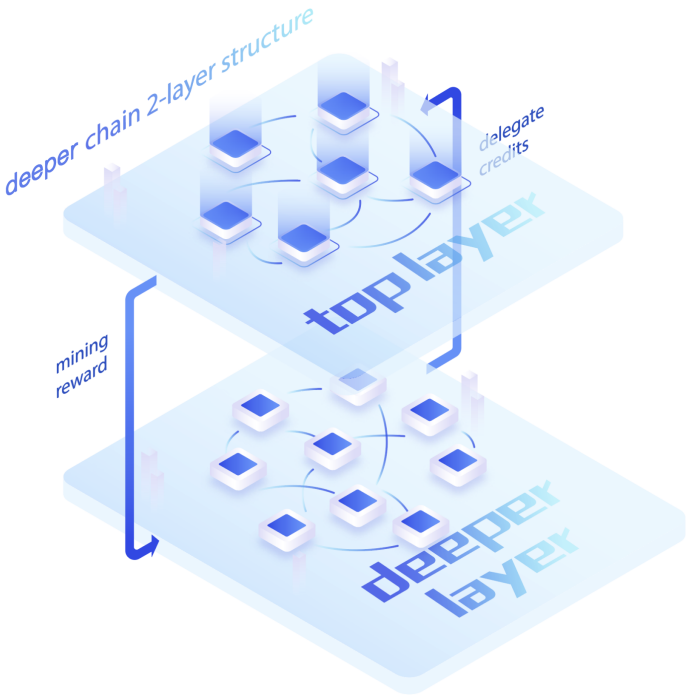

Figure 18: Deeper Chain 2-Layer Structure

Unlike the standard Nakamoto consensus protocols, our PoCr (Proof of Credit) does not rely on solving a significant computation puzzle to vote for consensus, and hence has low energy consumption. Our consensus mechanism is similar to proof of stake, but

a validator's voting power depends on both staked tokens and delegated credit scores. On one hand, the top layer is secured by credit scores of Deeper devices. The more people involved in Deeper services, the more secure the network will be. On the other hand, the mining reward distributed to Deeper devices will incentivize more people to participate in Deeper services. This closed loop will increase and secure the whole network.

6.1 Consensus Mechanism

6.1.1 Overview

Deeper Network uses an advanced PoCr consensus mechanism, which consists of three important mechanisms (modules): a credit system, a referral system, and a representative system. These three mechanisms form the core of the Deeper Network consensus mechanism. A brief description of each one of them is included next.

1. Credit System

PoCr, i.e. Proof of Credit. The credit system is the most important component among the three core PoCr mechanisms. As its name implies, it reflects the contribution of each participant based on each node's credit score, and distributes block rewards based on this.

There are two ways to increase credit score: (1) by staking DPR tokens in the early stage; (2) by participating in bandwidth sharing, and in network and consensus activities on the Deeper Chain. (1) Is backed by funds, (2) is supported by network contributions. This is the way Deeper Network builds its credit system.

Each node accumulates its own credit score by staking or participating in the Deeper chain applications, jointly collaborating to resist Sybil attacks. Since this is not done by use of computing power, financial resources or storage space, this design can reduce

energy consumption and hardware waste almost to zero. Likewise, it also can motivate each node to participate in numerous valuable applications on the chain, which can be considered a design that fits multiple purposes.

We can take the existing relatively perfect American credit system as a comparison to Deeper Network PoCr credit system. In the United States, everyone has a SSN (Social Security Number) related to almost all of his/her lifetime credit history. This simple number contains all information such as age, gender, educational background, work experience, taxation, insurance, bank information, criminal history, etc. The American Credit Management Association, the Credit Reporting Association, and the American Collections Association use this data to rate individuals' credit score in order to get a loan. This credit score ultimately impacts on all aspects of American life. The PoCr consensus mechanism credit score has some similarities, as it allows users to get different consensus incentives and grant them participation rights in on-chain governance. It ensures that all participants can contribute and that contributions are rewarded. As a result, Deeper Network is highly decentralized, more secure and fairer than other blockchain networks.

2. Referral System

Another important mechanism of PoCr is the referral system, which means that new nodes must be referred by the existing nodes in order to join the network. Moreover, after each referee joins the network, this particular node will automatically obtain a 100 credit score in order to reach the minimum threshold to start mining.

In order to quickly expand the network, Deeper Network has provided a key mechanism, a rewards system consisting of 1.8 billion DPR tokens to support the referral system. Any participant recommending a new user will get a portion of this rewards system.

A user must participate to be eligible for referrals either by investing or making

contributions to the project. Therefore, this participant certainly does not want his/her referee new user to do any form of sabotage, or simply not contribute to the network. The referral system encourages existing users to make efforts to select qualified and supportive new users to join the network. This is the referral system advantage and the way in which consensus and trust transmission is carried out.

The referral system is very often used in our daily lives and there are many examples that show this transmission of trust: internal recommendation when a well-known company is recruiting; a recommendation letter from a well-known and prestigious professor when an applicant wants to be accepted into a good school, etc. Therefore, the referral system can enable the entire network to expand rapidly, while ensuring that the new users participating in the network are relatively more credible, further strengthening the security of the entire Deeper Network.

3. Representative System

Before talking about the representative system of Deeper Network, let's review the structure of Deeper Network's entire network.

Deeper Network is composed of two layers: the validators at the upper layer and the Deeper Connect devices (also known as nodes) at the lower layer. The validators at the upper layer are mainly responsible for generating blocks, while the lower-layer Deeper Connect devices or nodes are mainly responsible for supervising and selecting the upper layer validators.

This design is inspired by the representative system adopted by some countries, that is, citizens form a parliament through elected representatives, and the parliament formally represents public opinion to exercise state power. In the Deeper Network chain, the validator is selected by the device nodes through their credit score offering, in turn, the selected validator represents the collective of nodes allowing them to participate in the consensus building of Deeper Network.

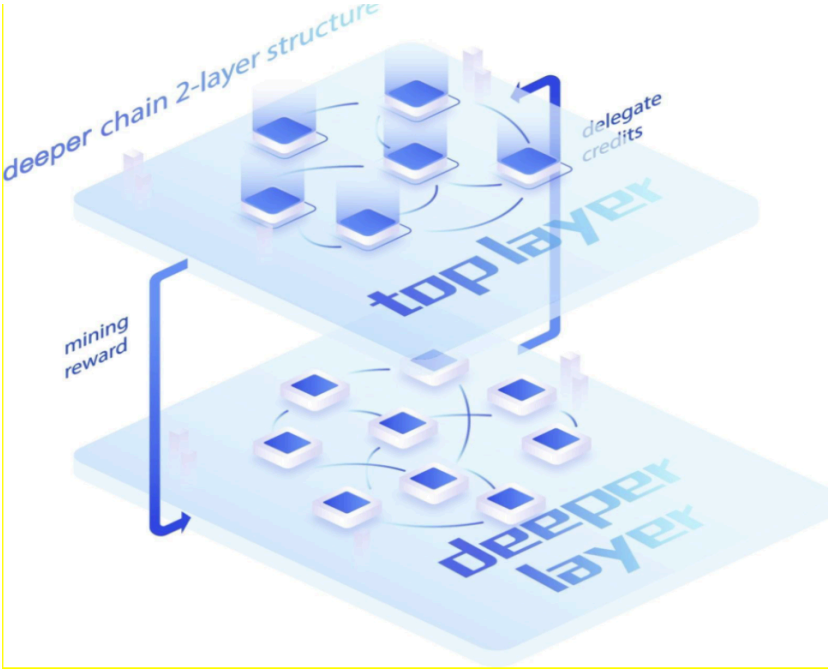

Figure 19: Deeper chain 2-layer structure

What it matters the most is that the validator node serves the lower layer node, and needs to allocate most of the block rewards to the lower layer node, which is fundamentally different from the super nodes in EOS and similar EOS ecosystems.

This architecture also brings two major features to Deeper Network:

The first major feature is the consensus scalability. Traditional blockchain projects, such as Bitcoin and Ethereum, have a little more than 10,000 nodes in their entire network. The problem they currently face is not the impossibility to increase their nodes number, but how much lower the consensus speed will be if such nodes are significantly increased. Therefore, from the perspective of consensus, it is difficult for the traditional blockchain projects to continue expanding the number of nodes, which will affect their operational efficiency.

However, Deeper Network's representative system is a two-layer architecture that

allows any number of participants to reach consensus, and each node can participate in the consensus to gain the corresponding incentive without affecting the efficiency, fully reflecting the network's fairness.

The second major feature is the TPS scalability (Transactions per Second). The Deeper Network two-layer architecture is a Layer1+Layer2 naturally scalable architecture. Every device has its own computing power, and is able to perform micropayment transfers. This computing power is integrated into the devices and added to the Deeper chain, greatly improving the operation efficiency of the entire system. It has built-in features to solve the scalability problem of TPS.

Deeper uses HotStuff [74] as its state machine replication (SMR) framework. HotSuff is the first Byzantine fault tolerant (BFT) protocol with both linear (i.e., $O(n)$) communication complexity and responsive network latency (i.e. the latency time depends on the actual network speed). HotStuff abstracts the chain paradigm from the BFT-style protocols and introduces pipelining architecture to greatly improve the network throughput.

In contrast to other BFT protocols, where there are different voting formats for each round (i.e., propose, pre-submit, submit, etc.), each round in Hotstuff is no longer treated differently. A vote on a block can also be considered the next stage vote on the parent block it references. That is, a vote on a block is considered a vote on the proposal of the block itself, as well as a pre-submission vote on its parent's block, a submission vote on its grandfather's block, and a decisive vote on its third-generation ancestor's block. A block is executed only if its third-generation block is voted successfully. Compared to other BFT consensus protocols, the introduction of pipelined architecture improves throughput by approximately three times.

Additionally, HotStuff uses a star communication pattern (i.e., everyone communicates through the leader) and threshold signatures to ensure linear communication per

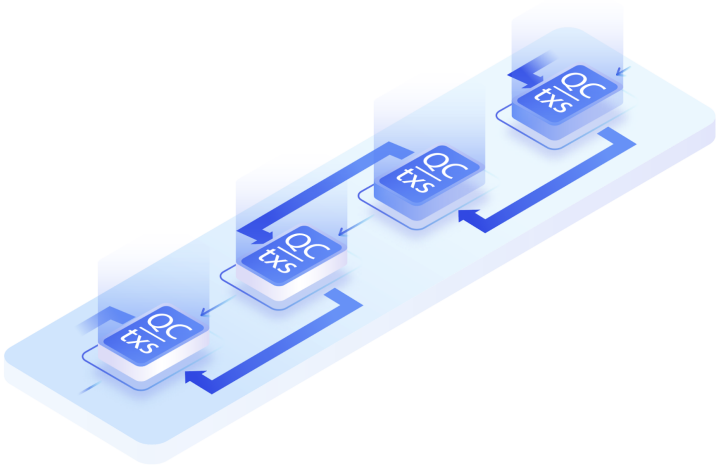

Figure 20: HotStuff Pipelining Architecture

block – the leader sends the block to validators, they produce partial signatures, and the leader simply reconstructs a threshold signature that serves as a proof of block validity. This allows it to scale consensus to a large number of validators simultaneously.

In Tendermint and PBFT, there are only 2 rounds to reach consensus. By adding 1(one) round of consensus with the help of a threshold signature, Hotsuff can update the complexity of the leader change to linear and ensures that the block production speed is the actual network delay. In contrast, the complexity of the PBFT's lead node change is $O(n^2)$, while Tendermint's block production speed is determined by system-defined parameters, and is not optimal based on network speed. Deeper chain provides user private protection functionality, so in addition to the need to protect against Sybil attacks on the public blockchain, nodes may also be subject to targeted bans by governments and service providers, which can result in lead nodes being blocked. With the linear complexity of HotStuff's initial leader change, this single point of failure will

not considerably slow down the network.

6.1.2 Liveness and Committee Selection

Hotstuff in the basic form abstracts the liveness and leader selection parts of consensus. These functions have to be implemented separately in each particular instantiation of Hotstuff, depending on the network topology and validator dynamics. Additionally, Hotstuff does not consider committee rotation, which has to also be implemented separately.

In Deeper, liveness is achieved through so-called timeout certificates. When the validator waits for a block proposal from a new round leader for the specified timeout period, and it does not arrive, they send a partially signed timeout message to the next leader, selected through a determined round-robin schedule. The new leader, upon receiving enough partial signatures, produces a timeout certificate, which they broadcast with a new-round message to all validators.

Committee rotation is performed in permissionless networks to leverage the benefits of BFT protocols while also ensuring robustness against the so-called adaptive adversary attacks. Adaptive adversary is a threat model whereas the adversary is able to dynamically corrupt correct replicas, as long as they do not control more than $(n-1)/3$ replicas (or, equivalently, 1/3 of the total weight of network validators) at a time. It is assumed that the time it takes to mount an adaptive attack is lower-bounded, which means that committee rotation must be performed frequently enough to prevent it.

For committee rotation, Deeper uses a randomness beacon based on a VDF [6]. VDFs are similar to VRFs – cryptographic functions with unpredictable output, which also generate a proof that can be used to verify the correctness of VRF's computation. VDFs, additionally, require a predetermined number of sequential steps to compute,

which puts a lower bound on the time it takes to produce an output. At the same time, verifying a VDF is significantly faster than computing it. Imposing a delay between acquiring the randomness input and output ensures that the first actor that is able to acquire the output will not be able to withhold it to reroll the randomness value.

The VDF is computed based on the threshold signature for a block proposal in round $k-2$, where k is the last block of the ePoCrh. The VDF is configured to be computed in approximately two rounds. That way, if a faulty leader tries to compute a VDF on their own and decide if they should withhold the input from everyone else, a timeout will be forced. When the VDF is computed, the committee members are selected by Algorithm 2.

Algorithm 2 Algorithm for committee members selection

R – the value of the randomness beacon in the current ePoCrh;
$H(x)$ – a hash function;
n – the total number of staking validators;
m – the total number of selected validators;
W_i – the weight of the i-th validator in consensus;
TW – the sum of all validator weights in consensus;

$C \leftarrow \{\}$
$S \leftarrow 0$
for $k \in \{0, \ldots, m-1\}$ **do**
    $V \leftarrow H(R||k)\%(TW - S)$
    $P \leftarrow 0$
    for $i \in \{0, \ldots, n-1\}/C$ **do**
        $P \leftarrow P + W_i$
        if $V < P$ **then**
            $C[k] \leftarrow i$
            $S \leftarrow S + W_i$
            break
return C

Note that this algorithm implies that each validator can only be selected once per

ePoCrh, and each validator participates in the fraction of ePoCrhs equal to their fraction of total weight.

After a committee is selected, the round leaders are chosen in a round-robin fashion by iterating through C. Each ePoCrh in Deeper lasts 17,300[1] blocks (slightly over 24 hours assuming 5 sec/block).

6.2 Proof of Credit

The Deeper network consists of two layers. The top layer contains hundreds of validators that generate new blocks constantly. The Deeper layer consists of millions of Deeper network devices. Proof of credit allows Deeper network devices to mine new tokens by sharing their bandwidth. Each device will be associated with an account, i.e., public address. The more bandwidth a device shares, the more credit score will be earned by the account. Each device will delegate its credit score to a validator. The consensus of the Deeper chain will be reached if more than 2/3 of the total voting power of validators agrees on a new block. After the new block is mined, the devices will be rewarded proportional to their credit scores. As in any credit score systems of modern society, each account's credit score, denoted as $\mathcal{C}$, is capped by some maximum value $\mathcal{C}_{max}$. To be more specific, we define $\mathcal{C}_{max} = 800$ and only when an account's credit score is equal or larger than 200, it can join the consensus and earn block reward.

6.2.1 Micropayment and Credit Score Update

There are two roles of Deeper network devices – a server device is a device that shares bandwidth to others; a client device is a device that is being served. For each MB of data that the server provides to the client, the client will pay the server a certain amount

[1]This value should be divisible by the committee size, so that each committee member can produce an equal number of blocks per ePoCrh, which is important for economics.

of tokens. This is called micropayments. If the client does not make the micropayment, the server can stop providing bandwidth anytime. We allow the server to choose the micropayment period, i.e., the server can stop the service after serving a threshold amount of data without receiving any micropayments. The micropayments happen in the Deeper layer which is off-chain. A device can accumulate multiple micropayments and submit the accumulated value to the validators. The credit score of the associated account will be updated after the submit transaction is verified.

6.2.2 Network Model and APIs

The topology of the Deeper layer is a big graph that contains millions of nodes (i.e., one node is one Deeper device). During each ePoCrh, we consider the graph is fixed. Between two ePoCrhs, the graph is randomly generated by some distributed random seed. We use the randomness generated at the end of each ePoCrh to construct the Deeper layer topology of next ePoCrh. More specifically, given a node, we will randomly assign 8 to 16 neighbor nodes to it. Thus, the degree of a node in the graph is between 8 to 16. This can be done by a smart contract. In the following, We define several APIs related to our network, payments, and credits:

- Fn randomize_graph() $\rightarrow$ Graph$\langle V, E\rangle$: return a randomized graph of current ePoCrh;
- Fn nbr$\langle V : Node\rangle(n : V) \rightarrow$ Vec$\langle V\rangle$: Given a node, return a list of neighbor peers that this node can connect to during current ePoCrh. Here, we assuming the list contains 8 to 16 peers;
- Fn submit(payments: Vec$\langle$MicroPayment$\rangle$, ledger: &mut Ledger): a server node submits accumulated micropayments to layer 1 ledger. The length of Vec is the

number of clients it serves during some period of time;

- Fn collect_fee(account: &Account, payments: Vec⟨MicroPayment⟩, ratio: f32): charge a fraction μ of the payments that a node collected, and deposit the rest $1 - \mu$ of payments into the node's account;

- Fn update_credit_score(account: &Account, payments: Vec⟨MicroPayment⟩): update credit score of an account based on the micropayments it received;

- Fn reward(ledger: &Ledger, n: &mut Node, credits:Vec⟨Credit⟩, amt: u32): distributes rewards to individual nodes after a new block is finalized. Here the reward depends on the credits of delegate devices.

6.2.3 PoCr Security

Sybil attack prevention is a key security consideration in public blockchains. There are many different approaches: proof of work, proof of stake, delegate proof of stake, etc. Bitcoin and Ethereum 1.0 use proof of work where a validator solves a difficult cryptographic puzzle in order to create a new block. After Ethereum 1.0, many blockchains adopt proof of stake where an elected validator will vote for a new block and the voting power is proportional to the total amount of tokens it staked. Deeper network uses a similar approach as Proof of Stake. The voting power depends not only on the staked tokens, but also on delegated credit scores. Thus, the Deeper chain is actually a mix of Proof of Stake and Proof of Credit. The security of Proof of Stake is well-studied. Hence, our major concern is the security of Proof of Credit.

The first step to make PoCr secure is to control the number of malicious nodes in Deeper Network. To achieve this goal, Deeper increases the difficulty and cost for a malicious party to control other nodes in two aspects: 1) Staking tokens. Deeper

requires all the devices to deposit some tokens before joining the network during the registration phase. Thus, if a malicious party wants to control a lot of nodes, it has to deposit a large amount of tokens which is essentially the proof of stake mechanism. This will significantly increase the cost of malicious parties; 2) Minimum credit requirement. A node has to reach a minimum threshold τ of credits before it can join the network and earn rewards. In this way, we encourage users to participate in bandwidth sharing to accumulate credits and also prevent newly created malicious nodes to join the network immediately.

Next, we discuss PoCr security from the perspective of how rewards are distributed and how credits are updated. Assume a server node collects payments $[p_1, p_2, \ldots, p_m]$ from m clients during one block time and it receives reward R after the block is finished. The transaction fee commission rate is μ. The net profit P is then given by:

$$P = R + (1 - \mu) * (p_1 + p_2 + \ldots + p_m) \tag{5}$$

Now we analyze the security of PoCr. Assume the malicious party can control a fraction θ (e.g., $\theta = 10\%$) of the total number of devices n. During each ePoCrh, assuming a malicious node randomly picks k neighbors among which the number of malicious ones is a random variable X. The probability that there are i malicious neighbors is:

$$P(X = i) = \frac{\binom{n\theta}{i}\binom{n(1-\theta)}{k-i}}{\binom{n}{k}} \tag{6}$$

Assuming k is small relative to n (i.e., $k \ll n$), the probability to have one malicious neighbor is close to θ (i.e., $P(X = 1) \approx \theta$) and the probability to have more than one malicious neighbor $P(X > 1)$ is much smaller than θ. Suppose this malicious server cannot provide service by refusing all other good peers but just collect fees from its

malicious neighbors, the net profit is given by $P = R + (1 - \mu) * p_1$, assuming it can only obtain one malicious neighbor.

design 1: Notice that the reward R is a function of credits core and which in turn is a function of $[p_1, p_2, \ldots, p_m]$. We define $R = 0$ if $m = 1$, i.e., no reward if a server only serves one neighbor. In this case, the net profit of a malicious node is negative $-\mu * p_1$ while the net profit of an honest node is positive $(1-\mu) * p_1$. This simple design is equivalent to removing the PoCr component from our system.

Our hypothesis is that in the long term, the micropayments will close to the operational cost of a server node. Thus, by removing PoCr, the users are not incentivized enough to share their bandwidth. Since the reward is proportional to the credit scores, the credit score update function should be designed in such a way that incentivizes the node to serve more clients. When the commission ratio μ is not set to 0, the commission fee will also be compensated when a node serves multiple nodes.

design 2: We can also remove the commission of micropayment by setting $\mu = 0$. In this case, we will not update the credit score of the server node if it only serves one client during one block. In this case, we rely on the fact that the probability to match two or more malicious nodes is very small. Therefore, in the block $T + 1$, the credit is calculated by updating its current credit at block T with an adjustable damping factor λ:

$$\mathcal{C}(T+1) = \begin{cases} \min(\mathcal{C}(T) + \lambda \sum_{i=1}^{m} p_i, \mathcal{C}_{max}) & \text{if } m > 1 \\ \mathcal{C}(T) & \text{otherwise} \end{cases} \tag{7}$$

design 3: Based on previous two designs, we will adopt design 2 and also add commission fee of 10%. The commission fee has two purposes. First, it will further enhance the security of the network comparing to design 2. Second, the collected commission fee will be put into a treasury pool. We will describe the use of treasury

pool in a later section.

In the above analysis, we assume the θ is small, which is the ratio of malicious devices over all devices. This is guaranteed by deposit initial tokens at registration and minimum credit requirement as we discussed before. In conclusion, a malicious party would rather follow the protocol and play honest to earn a better reward.

6.2.4 Incentivization Mechanisms

Deeper Network protocol includes several goals among which are: (1) encourage users to share idle bandwidth, (2) encourage Deeper Network devices to stay online, and (3) increase the size of the network in an organic manner. The first goal has been already discussed in the micropayment and PoCr sections. The remaining two points will be discussed in the next two subsections below.

Credit Decay

When a Deeper device stops joining the network, the system will gradually reduce its credit up to some predefined thresholds τ_0. Let τ to be the threshold that a user can delegate its credit score to earn reward, we set the predefined threshold $\tau_0 < \tau$. If the account's credit score is less than τ_0, there will be no credit score decrease. If the account's credit is larger than τ and it does not join the network sharing activities (either server side or client side), i.e. it's idle for a long time, its credit score will gradually drop to τ (e.g. a couple of months), and then its credit score will asymptocially drop to τ_0 but no further.

Initial Credit Byng

To encourage more users to participate in the Deeper network, we need a way to allow them to be able earning credits as fast as possible. This is where the initial credit buying comes into play. It only affects accounts that have credit scores less than

(which is the threshold that allows a user to earn reward). For a user whose current credit score C is less than t , the user can pay $\delta(\tau - \mathrm{C})$ tokens to buy its credit up to τ , where δ is an adjustable parameter that needs to be determined. The tokens used to buy credits will be distributed as block reward to miners including validators, stakers and credit score delegators.

7 Tokenomics

7.1 Overview

DPR, Deeper's native token, is used for financial incentives and payments for various services. It's the main value currency of the Deeper Network.

The total supply of DPR is 10 billion. Of this, 6 billion is allocated as block rewards. The initial block rewards consist of genesis staking and network bandwidth sharing reward. The number of DPR created per block decreases as the network grows.

The two main mechanisms involved in DPR tokens are micropayments (closely related to Proof of Credit) and staking (closely related to Proof of Equity).

7.2 Governance

There are two types of governance: off-chain governance and on-chain governance. The off-chain government requires a huge amount of coordination between the developers and communities. In the Deeper chain, we choose the latter one. In most of the on-chain governance models, people use their tokens to stake for a list of options. For example, the most common situation is the system can only be upgraded if the majority of stakeholders choose to upgrade it.

There is one caveat in the PoS world. The big stakeholders have more voting power compared to normal users. People make jokes on this saying that the blockchain is controlled by VCs because VCs are early investors which have a huge portion of tokens. There are different mechanisms designed to solve this issue. For example, quadratic voting is one of them. However, these designs are either too complicated and/or not solving the problem fundamentally.

In the Deeper chain, we use PoCr, the credit system, to solve this problem. For any

system upgrade or protocol change, the proposer will post a list of options and given a time window for voting. Instead of staking, any user account will vote according to its credit score. As long as its credit score is greater than the threshold value (e.g., the total credit score is 100 and the threshold value is 60), then it is a legit voter. This is very similar to a person who is "old enough" to vote. Big stakeholders cannot simply increase the credit scores easily. In PoS, a big stakeholder can gain a lot of voting power immediately. In PoCr, while a big stakeholder still can gain advantage by splitting into multiple accounts and accrue credits, it takes time and effort to increase and maintain the credit scores. Of course, if a big stakeholder creates and maintains a lot of high credits accounts, it means her contribution to the network is larger than others, and in return she will have more voting power. But in general this simple and effective design can greatly alleviate the imbalance issue between large stakeholders and normal users.

7.3 Treasury Pool

As we mentioned in PoCr Security section, we will charge 10% of commission fee for micropayments. It serves two purposes. One is to prevent Sibil attack of micropayment transactions between fake identities to gain credit scores. The other is to use the commission fee to establish a treasury fund. This treasury fund can be used in multiple ways.

We can dedicate a portion of this treasury pool to develop our ecosystem. For example, any developers can apply a grant to help enhancing the ecosystem, e.g. develop toolings or fix security issues of Deeper network.

We can reserve a portion of the pool to buy back users' DPR and burn it. i.e. This portion of DPR will be swapped into stable coins and any users who burned their DPR will be refunded by corresponding amount of stable coins. This mechanism allows our

system to control the total circulation of DPR in a decentralized way.

Eventually, the community will decide how to use the DPR in this pool.

8 Project Planning

8.1 Roadmap

See Table 3.

2018 Q3	Beta release of AtomOS, the world's first lock-free network security operating system high-performance seven-layer network security detection unique Trident protocol to provide users with a secure and private decentralized VPN
2018 Q4	Our first home hardware security gateway comes out equipped with AtomOS operating system, plug-and-play, zero-configuration
2019 Q1	Deeper Connect equipment public network test. At the moment 200+ paid nodes participate in the test.
2019 Q2	Partnerships with multiple Silicon Valley traditional venture capital firms and renowned blockchain institutions
2019 Q3	Third-generation Deeper Connect goes on sale
2020 Q1	Fourth-generation product, Deeper Connect Mini, is tested and goes into mass production
2020 Q2	Deeper Connect Mini goes live on the Indiegogo platform
2020 Q3	Deeper Connect Mini is launched on BestBuy, the world's largest 3C sales platform. Cooperated with China Mobile to develop cybersecurity products for smart homes
2021 Q1	Deeper Connect decentralized public chain goes live and the mining process starts.

Table 3: Roadmap

8.2 Token Economic Distribution Plan

Our token's abbreviation is DPR (Deeper Token).

Tokens are issued through statutory value in the form of Ethereum deposits.

Total tokens to be issued by the Deeper project: 10 billion (10,000,000,000).

Unsold DPR tokens will be reassigned to mining pool and bounty projects for community participants.

8.2.1 Token Matrix

We do appreciate our main contributors – we mean YOU! That's why we've decided to allocate 60% of the tokens to the community, our dear participants, and supporters of the Deeper Network (See Table 4). Via the concept of sharing is mining, you can effortlessly enjoy and profit from the mining journey.

Token allocation	Ratio
Mining	60%
Private Token Sale	20%
Team + Investors	10%
Market operation + cooperation + Token Treasure	5%
Core user IDO	5%

Table 4: Token Matrix

Appendix A Terminology

A. IDO

The IDO model does not finance from the user. It is not about the money, it is only for the people in the community. The identity of a person in the community is multiple. He is the product, the service and the project staff all in one. Remuneration: because token rewards are equivalent to the equity of the project and the identity of the shareholders.

B. SSS

Abbreviation for Secure Shared Service: a new species that combines network security, shared economy, and blockchain technology.

C. HIPE

HIPE is the original data structure of Deeper. AtomOS manages shared resources through HIPE for lock-free operation of the entire network operating system, thereby greatly improving the reliability, performance and scalability of the system.

D. Middleman changes

Or Man-in-the-middle attack (MITM): In the field of cryptography and computer security, this means that the attacker and the two ends of the communication establish two independent sessions and forward the received data from one session to the other session to make both ends of the communication think they are communicating with the other side directly through one single private session, but in fact the entire session is completely controlled by the attacker.

E. NAT traversal

NAT traversal refers to the problem of establishing a connection when the connected server is behind a NAT device. Since the device behind the NAT does not have a dedicated public IP address, a method to detect whether there is a mapping between the intranet and the public network IP and port is necessary: if there is, a direct connection may be possible; if not, an intermediate server performs two-way forwarding, see STUN protocol [45].

Appendix B Disclaim

This is a conceptual document ("White Paper") describing our proposed Deeper platform and Deeper tokens. It may be amended or replaced at any time. However, there is no obligation to update the White Paper or to provide the recipient with access to any additional information.

This whitepaper does not constitute an offer to buy securities or a solicitation for investment in securities in any jurisdiction, whether in the United States or elsewhere, nor does it constitute a contract of any kind. The information provided herein has not been reviewed by any regulatory authority. Publishing and distributing this whitepaper shall not be construed as this whitepaper having complied with the laws, regulatory requirements, rules and/or regulations in your jurisdiction.

No representations or warranties are made as to the accuracy or completeness of the information, statements, opinions or other matters described in this document or otherwise communicated in connection with the project. Without limitation, no representation or warranty is given as to the achievement or reasonableness of any forward-looking or conceptual statements. Nothing in this document is or should be relied upon as a promise or representation as to the future. To the fullest extent permitted under applicable law, all liability for any loss or damage whatsoever (whether foreseeable or not) arising from or in connection with any person acting on this White Paper, or any aspect of it, notwithstanding any negligence, default or lack of care, is disclaimed. To the extent liability may be restricted but not fully disclaimed, it is restricted to the maximum extent permitted by applicable law.

Although the company has taken reasonable steps to ensure that the information contained herein is accurately released and in the proper context, the company did not conduct any independent review of information extracted from external sources of the

third parties and did not confirm the accuracy or completeness of such information or the relied-upon assumptions. Therefore, the company shall not be obligated to provide any updates on the representations or guarantees regarding the accuracy or completeness of such information.

No information provided herein should be construed or perceived as business, legal, tax or financial advice regarding Deeper Network, the company, and/or tokens. If you are uncertain about financial and legal decisions, you should consult independent professional advisers, such as financial and legal advisers, regarding Deeper tokens, Deeper and/or the company and their respective operations and businesses, and the general state of cryptocurrency and other digital assets in your jurisdiction. You acknowledge that you might be required to carry the legal and financial risk of any purchase of Deeper tokens for an indefinite period of time or incur losses in case of unforeseen circumstances or interference of extraneous factors.

References

[1] "2013 IBM annual report," 2013. [Online]. Available: https://www.ibm.com/annualreport/2013/bin/assets/2013_ibm_annual.pdf.

[2] V. Afshar, "cisco enterprises are leading the internet of things," 2017. [Online]. Available: https://www.huffpost.com/entry/cisco-enterprises-are-leading-the-internet-of-things_b_59a41fcee4b0a62d0987b0c6.

[3] M. Allman, K. Avrachenkov, U. Ayesta, J. Blanton, and P. Hurtig, "RFC5827: Early retransmit for TCP and stream control transmission protocol (SCTP)," Tech. Rep., 2010.

[4] "Bitcoin Energy Consumption Index." [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[5] "Block Internet." [Online]. Available: https://en.wikipedia.org/wiki/Block_(Internet).

[6] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, "Verifiable delay functions," in *Proc. Annual international cryptology conference*. Springer, 2018, pp. 757–788.

[7] L. S. Brakmo and L. L. Peterson, "TCP Vegas: End to end congestion avoidance on a global Internet," *IEEE Journal on selected Areas in communications*, vol. 13, no. 8, pp. 1465–1480, 1995.

[8] N. Cardwell, Y. Cheng, C. S. Gunn, S. H. Yeganeh, and V. Jacobson, "BBR: Congestion-based congestion control," *Queue*, vol. 14, no. 5, p. 50, 2016.

[9] "Cavium™ Unveils 48-core, 2.5GHz OCTEON® III MIPS64 Processor Family: First SoC with Breakthrough Search Processing and Over 100Gbps Single-chip

Application Performance for Enterprise, Data-Center and Service Provider Infrastructure." [Online]. Available: https://www.cavium.com/newsevents-cavium-unveils-48-core-octeon-iii-mips64-processor.html.

[10] "Data Breach." [Online]. Available: https://www.privacyrights.org/data-breaches.

[11] R. H. Dennard, F. H. Gaensslen, V. L. Rideout, E. Bassous, and A. R. LeBlanc, "Design of ion-implanted MOSFET's with very small physical dimensions," *IEEE Journal of Solid-State Circuits*, vol. 9, no. 5, pp. 256–268, 1974.

[12] "DPDK." [Online]. Available: https://www.dpdk.org/.

[13] "DPDK Performance." [Online]. Available: https://www.intel.com/content/www/us/en/communications/data-plane-development-kit.html.

[14] S. Frankel, R. Glenn, and S. Kelly, "RFC 3602: The AES-CBC cipher algorithm and its use with IPsec," Tech. Rep., 2003.

[15] B. Goodwin, "Cyber gangsters demand payment from Travelex after Sodinokibi attack," 2020. [Online]. Available: https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack.

[16] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, "Spam and Phishing in 2017," 2018. [Online]. Available: https://securelist.com/spam-and-phishing-in-2017/83833/.

[17] S. Ha, I. Rhee, and L. Xu, "CUBIC: a new TCP-friendly high-speed TCP variant," *ACM SIGOPS operating systems review*, vol. 42, no. 5, pp. 64–74, 2008.

[18] "Internet Assigned Numbers Authority." [Online]. Available: https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority.

[19] C. India, "Privacy Awareness Week-Are We Responsible for Our Data Breach?" [Online]. Available: https://securingtomorrow.mcafee.com/consumer/privacy-awareness-week-are-we-responsible-for-our-data-breach/.

[20] "Internet Censorship." [Online]. Available: https://en.wikipedia.org/wiki/Internet_censorship.

[21] V. Jacobson, "Congestion avoidance and control," in *Proc. ACM SIGCOMM computer communication review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[22] A. Johnson, "Trump Signs Measure to Let ISPs Sell Your Data Without Consent," 2017. [Online]. Available: https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316.

[23] P. Kennedy, "AMD EPYC Rome Details Trickle Out 64 Cores 128 Threads Per Socket." [Online]. Available: https://www.servethehome.com/amd-epyc-rome-details-trickle-out-64-cores-128-threads-per-socket/.

[24] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," *Proceedings of the National Academy of Sciences*, p. 201218772, 2013.

[25] "List of Websites Blocked in India." [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_India.

[26] "List of Websites Blocked in Russia." [Online]. Available: https://en.wikipedia.org/wiki/List_of_websites_blocked_in_Russia.

[27] "List of Data Breaches." [Online]. Available: https://en.wikipedia.org/wiki/List_of_data_breaches.

[28] "List of TCP and UDP Port Numbers." [Online]. Available: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

[29] "Lock (computer science)." [Online]. Available: https://en.wikipedia.org/wiki/Lock_(computer_science).

[30] C. Malmo, "One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week." [Online]. Available: https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change.

[31] L. Mathews, "Phishing Scams Cost American Businesses Half A Billion Dollars A Year." [Online]. Available: https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year.

[32] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, "RFC 2018: TCP selective acknowledgment options," 1996.

[33] "Mirai Source Code." [Online]. Available: https://github.com/jgamblin/Mirai-Source-Code.

[34] S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," 2020. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[35] S. Morgan, "Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion," 2020. [Online]. Available: https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/.

[36] "Network address translation." [Online]. Available: https://en.wikipedia.org/wiki/Network_address_translation.

[37] M. Orcutt, "Hijacking Computers to Mine Cryptocurrency Is All the Rage," 2017. [Online]. Available: https://www.technologyreview.com/s/609031/hijacking-computers-to-mine-cryptocurrency-is-all-the-rage/.

[38] J. Padhye, V. Firoiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno performance: a simple model and its empirical validation," *IEEE/ACM Transactions on Networking (ToN)*, vol. 8, no. 2, pp. 133–145, 2000.

[39] PeckShield, "EPoD: Ethereum Packet of Death (CVE-2018–12018)." [Online]. Available: https://medium.com/@peckshield/epod-ethereum-packet-of-death-cve-2018-12018-fc9ee944843e.

[40] "Phishing." [Online]. Available: https://en.wikipedia.org/wiki/Phishing.

[41] M. Rechtoris, "Data breaches cost healthcare industry $6.2B." [Online]. Available: https://www.beckersasc.com/asc-turnarounds-ideas-to-improve-performance/data-breaches-cost-healthcare-industry-6-2b-4-points.html.

[42] D. Reed *et al.*, "RFC 1459: Internet Relay Chat Protocol," 1993.

[43] T. Riley, "The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report finds," 2020. [Online]. Available: https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/.

[44] L. Rokach and O. Z. Maimon, *Data mining with decision trees: theory and applications*. World scientific, 2008, vol. 69.

[45] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, "RFC3489: STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," 2003.

[46] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,, 2016.

[47] A. Shahbaz and A. Funk, "The pandemic's digital shadow," 2020. [Online]. Available: https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

[48] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[49] O. Solon, "Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data." [Online]. Available: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought.

[50] "Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K," 2018. [Online]. Available: https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/.

[51] B. Sullivan, "Online Privacy Fears Are Real." [Online]. Available: http://www.nbcnews.com/id/3078835/t/online-privacy-fears-are-real/.

[52] "Timeline of computer viruses and worms." [Online]. Available: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms.

[53] "WAN optimization." [Online]. Available: https://en.wikipedia.org/wiki/WAN_optimization.

[54] "Websites Blocked in Mainland China." [Online]. Available: https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China.

[55] M. Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?" [Online]. Available: http://time.com/4673602/terms-service-privacy-security/.