a

Blockchain Team Development

100% Security against DDoS and other Security Problems

DEFENSOR

WHITE PAPER | MAY 2018

BUILDING THE WORLD'S MOST SECURE NETWORK SECURITY SOLUTION, POWERED BY MILLIONS

CONTENTS

DEFENSOR IN 60 SECONDS

DEFENSOR™ is the world's first decentralized P2P (Peer-To-Peer) network security platform powered by crowdsourcing idle computing power and network bandwidth from millions of smart devices to deliver a state-of-the-art dynamic network security protection using blockchain technology.

DEFENSOR™ aims to disrupt the current traditional network security industry estimated to be worth US$173.57 billion by 2022[1] by building a multi-chain ecosystem powered by blockchain technology. This will enable network security businesses and developers to participate to provide cutting-edge network security solutions that caters to different needs & across diversified industry verticals.

QUICK FACTS:

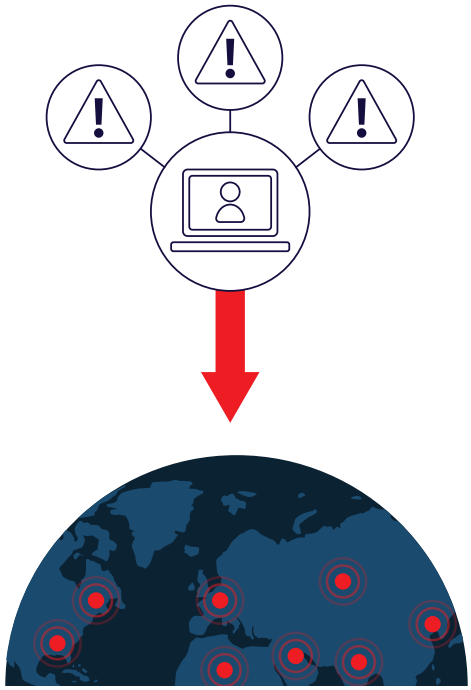
The multi-chain platform will be based on Ethereum, which will be extended through the Plasma Framework.

In comparison to existing network security solutions, the DEFENSOR™ platform will provide end-users with a highly secure, stable, and dynamic approach to network security needs that is cost effective.

The smart devices will form a vast resource pool of physical nodes to build a network security sidechain structure that interacts with the DEFENSOR™ mainchain.

Note: DEFENSOR™ is a work in progress. Active research is underway, and new versions of this White Paper will appear at https://defensor.io. For comments and suggestions, contact us at research@defensor.io

THE PROBLEM



The high level of dependency on technology and the internet today has resulted in opportunities for cyber attackers to exploit and significantly disrupt business operations through Distributed Denial of Service (DDoS) attacks.

The scale, sophistication and financial consequences of cyber attacks is growing in prominence every day, targeting and impacting millions of people, businesses, and institutions all around the world.

In October 2016, one of the biggest domain name service (DNS) providers Dyn experienced a major DDoS attack that disrupted the service of several high traffic websites such as Twitter, Netflix, and Spotify.

KEY FACTS ABOUT CYBER NETWORK SECURITY THREATS:

Almost
5 BILLION
personal data records is predicted to be stolen by cybercriminals by 2020[2]

Cybercrime damages is predicted to reach USD
$6 TRILLION
annually by 2021[3]

Average cost for cyber security was USD
$11.7 MILLION
for companies in 2017[4]

DDoS attacks are among the most high-risk threats that can compromise the stability of businesses. They are executed by hackers using botnets where they overload an online service such as a website with traffic to deny resources to legitimate users. Essentially creating a massive network of infected computers.

MAJOR CYBER NETWORK SECURITY ATTACKS IN RECENT YEARS:

Recently, cryptocurrency exchanges have become the most common targets of DDoS attacks. In Q3 2017, 75% of Bitcoin exchanges were hit with a DDoS attack due to the phenomenal rise of the price of Bitcoin with nearly 17% of botnets originating from China attacking mostly Taiwan, Hong Kong and the Philippines[5].

In Q4 of 2017, 84 countries were reported to have been subject to DDoS attacks[6]; half of the DDoS attacks targeted China (51.84%); China, the United States, and South Korea were both major sources of attack and the main targets of DDoS attacks; and the longest DDoS attack lasted 146 hours.

In Q4 2017, the Bitcoin exchange Bitfinex was temporarily taken offline after hackers attempted to execute a DDoS attack. This was one year after hackers stole US$72 million from Bitfinex.

In Q1 2018, the world-renowned technology exchange website GitHub suffered from a reflection-amplified DDoS attack “Memcached," the largest DDoS attack ever discovered.

In Q1 2018, Japan-based cryptocurrency exchange Coincheck suffered the largest recorded cryptocurrency cyber-attack with hackers stealing US$530 million.

To defend against DDoS attacks which have become more sophisticated and frequent with time, end-users and businesses including cryptocurrency exchanges need a breakthrough solution in network security protection.

THE SOLUTION

THE WORLD'S FIRST DECENTRALIZED P2P NETWORK SECURITY PLATFORM

that will facilitate faster threat detection and response than current market solutions by crowdsourcing idle network bandwidth at low cost and high efficiency with the ability to scale up with demand.

Faster Threat Detection & Response

Cost Effective Solution

Rapid Scalability Potential

FASTER THREAT DETECTION & RESPONSE

Unlike most of current network security solutions which are using a shield defense method of firewall structure, DEFENSOR™ will be using a grid defense method powered by millions of smart devices located across different locations around the world.

MOST MAINSTREAM SOLUTIONS | VS | THE DEFENSOR™ SOLUTION

SHIELD DEFENSE METHOD
Often ineffective, costly and required a long-term contractual commitments

GRID DEFENSE METHOD
Allows end-users to pay after a defended attack, providing significant cost-savings

This will allow DEFENSOR™ to intelligently detect any potential network security threats and dynamically defend the system from attacks at unparalleled speed. It's a faster & more effective solution towards making global networks a safer place that is rapidly changing everyday.

COST-EFFECTIVE SOLUTION

By crowdsourcing idle computing power and network bandwidth from millions of smart devices around the world, the DEFENSOR™ platform will ensure efficient and fast distribution of content and data across millions of physical nodes with minimal downtime.

Smart TVs

Set-top Boxes

Routers

This makes it suitable for building a low-cost, secure and scalable mainchain by leveraging off redundant power, bandwidth, and storage resources.

RAPID SCALABILITY POTENTIAL

The DEFENSOR™ platform will consist of a multi-chain architecture with an Ethereum-based mainchain and a number of sidechains. The mainchain will extend through the smart contract Plasma Framework to achieve coexistence with the sidechains which will all have separate functionalities. The mainchain will provide the core services whereas the sidechains will provide cutting edge network defense solutions. This will enable the potential for the platform through the multiple sidechains to scale quickly without overloading and compromising the mainchain functionality.

In comparison with the Ethereum single-chain technology, the DEFENSOR™ multi-chain platform will enable the customization and implementation of large-scale commercial applications while providing broad network security defense service. This has the potential to disrupt the current network security business model and improve the efficiency so that blockchain technology can be widely applied in network security. Businesses have the potential to use the platform to identify deficiencies in their network defense and to perform a stress test on their networks.

GAMECAST

Currently, DEFENSOR™ has an eco-partnership with GAMECAST, one of China's largest home broadband service provider for operations such as China Telecom, China Unicom, China Mobile, Huawei. The DEFENSOR™ technology is currently already embedded into GAMECAST's partner devices.

As of March 2018, this covers

200 MILLION
Smart TVs and Set-top boxes

46 MILLION
Registered users

3.2 MILLION
Daily users

This instantly offers DEFENSOR™ access to a significant number of physical nodes to power DEFENSOR™ cutting edge platform.

THE PARTICIPANTS

CONTRIBUTORS

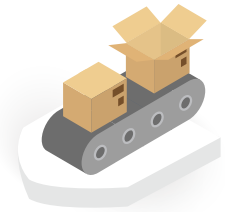
Users who sign up and connect their smart devices to the DEFENSOR™ resource pool.

END USERS

Enterprises and users who seek for robust network security solution would use DEFENSOR™ platform & willing to pay for the network security protection service.

NETWORK SECURITY THREAT VALIDATORS

Geographically diverse security experts and engineers who are detecting and categorizing attacks and non-attacks using different consensus mechanisms depending on the scenario from Delegated Proof of Stake (DPoS) to Proof of Stake (PoS) to Proof of Work (PoW).



SMART DEVICE MANUFACTURERS

Smart devices manufacturers who embed DEFENSOR™ system into all their smart devices in order to offer an innovative network security solution to their users.

DEVELOPERS

Developers may not participate in every transaction but rather participate in developing a more robust network defense system. Their role will mainly involve developing Decentralized Apps (DApps) on the sidechains to develop professional solutions for end users to purchase seeking network protection.

DEFENSOR™ VISION

Defensor's vision is to create a dynamic open source P2P network defense ecosystem for individuals, businesses, and developers around the world and mobilize and empower people to come together as a community to help protect global networks from increasingly sophisticated cyber attacks.

The DEFENSOR™ platform aims to be at the forefront application of blockchain technology in the field of network security and disrupting the traditional and/or centralized network security business model.

JOIN THE MOVEMENT

Network attacks affects millions of individuals, businesses and institutions everyday.

For individuals particularly, the implications and consequences can be dire ranging from identity theft and financial losses resulting from personal data and privacy breaches. And given the rampant adoption of technology and more internet connected devices being used in our everyday lives including routers, cameras and refrigerators, this creates opportunities for cyber criminals to use botnets to engage in wide-scale DDoS attacks to shutdown networks to potentially steal data in the process.

At DEFENSOR™, our mission is to empower a community of people to come together to learn how they can protect themselves and how they can help one another which was the basis for creating the “Let’s Defend Our World Together” movement.

Join us at **www.defendtogether.org** to help contribute to the movement by sharing your story, getting involved in the conversation or to make a donation to help us achieve our mission.

Together, let’s defend our world together.

THE TECHNOLOGY

INTRODUCTION

1

The DEFENSOR platform will be based on the new smart contract extension, the Plasma Framework.

The multi-chain platform (DEF) will contain one mainchain and multiple sidechains that will extend through the Plasma Framework to achieve co-existence. In addition, according to the different scenarios, the multi-chain will support multiple consensus mechanisms where the mainchain will support DPoS and the sidechain can support the appropriate consensus mechanisms according to requirements, such as PoW and PoS.

The mainchain is the core of the entire system, and the bottom layer will be built on a “molecular chain communication protocol” to efficiently integrate the node resources into an inter-connected resource pool. The upper layer will provide the DApp application platform externally through the DEF framework. Developers can then easily use JavaScript and large npm libraries to build DApps.

The sidechains will include network defense sidechains, data protection sidechains, user identity sidechains, and information sidechains where developers will be able to quickly build their own business sidechains. With enough users, developers and companies have the potential to create sustainable business models.

The two key technical elements in the DEF framework will be:

- AdSM (ARM Device Scheduling Mechanism), an optimized node scheduling mechanism depending on the characteristics of the DEF nodes

- Molecular chain communication protocol, a type of communication protocol between the physical nodes

2 ARM-BASED BACKBONE

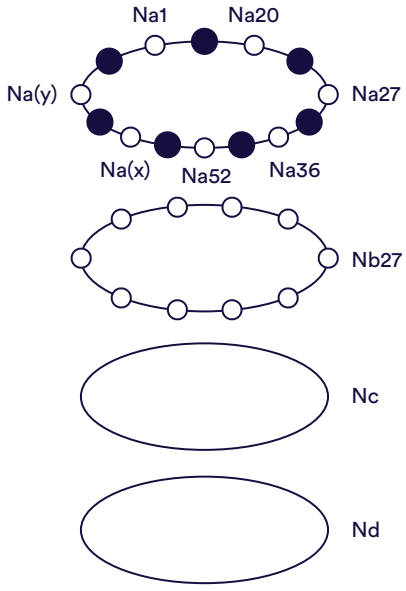
The current underlying blockchain nodes are based on the X86 architecture which are powerful but very energy-consuming. However the DEF nodes based on the home smart devices will be constructed as a new type of mainchain different to the existing mainstream mainchain.

DEF nodes will generally have the following characteristics:

ARM-based architecture, stable performance, low power consumption	Power always on (or standby)
Home broadband connection	Low usage rate, abundant idle time
Geographically scattered	Usage of SSD

Most of the Nodes formed by the DEF mainchain will be ARM-based smart home devices (such as smart TVs, smart set-top boxes and smart routers). Each device will have a corresponding resource identifier key. In the DEF mainchain architecture, the mainchain will be a multi-level ring structure, rather than a binary tree structure.

As shown in the figure:



In the mainchain, both the Node and Keymap will have a range of values. In order to ensure hash non-repeatability, the DEF backbone will select SHA-1 as a hash function which will generate a 2^{128} space, each of which will be a 128-bit Node ID. These Node IDs will be connected end to end to form a ring called a DEF ring. DEF rings of different pointer dimensions (such as geographic dimensions) will be interconnected to form a DEF pool.

Node ID will be arranged clockwise by size on a single DEF ring. Both the Node (machine's IP address and port) and the Key (resource ID) will be hashed onto the DEF ring, forming a structured chain that can be quickly retrieved. Any lookup can be found as long as the result of a circle along the DEF ring. This time complexity is O(N), where N is the number of network nodes.

But for tens of millions of DEF chain nodes, O(N) is intolerable. To solve this problem, the DEF reference chord algorithm adds a non-linear scheduling algorithm:

As noted previously, each DEF node generates a Node ID table, and will maintain a list of predecessors and successors. The length of the ID table is X (X is the number of bits, 128b in the DEF chain). The role of this list will be to quickly locate and periodically detect the health status of the successor node. For example, a node, call a M Node, and its Nth item holds the $(M+2^{n-1})$th successor node. That is, the successor stored is incremented by a multiple of 2.

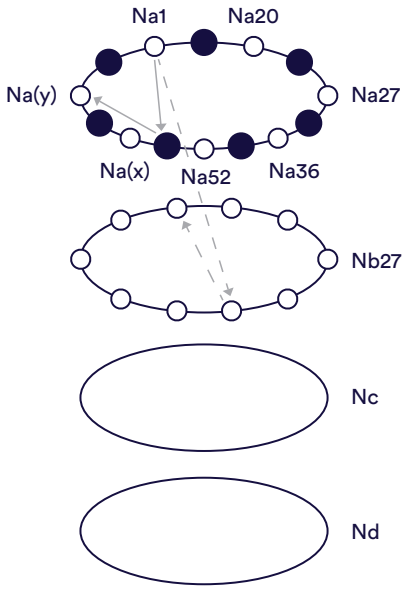
According to the Node ID corresponding to the node's Key, the node can find the node where the corresponding resource is located according to the above formula, that is, find the successor of the Key.

This will check whether the Key's hash falls between the M Node and its successor. If the result is "yes", the search will end.

In the Node ID table of M, the successor node of M that is closest to hash(Key) will be found and <hash(Key), which is also the successor node closest to Key in Node ID table will forward the lookup request to this node.

This optimized dichotomy search algorithm will have an extremely fast convergence rate.

As shown in the figure:



This scheduling mechanism will be based on the characteristics of the DEF chain nodes and specifically designed for the interconnection of the home smart devices. This is the AdSM which can complete fast connections among large ARM nodes and interconnection into chains.

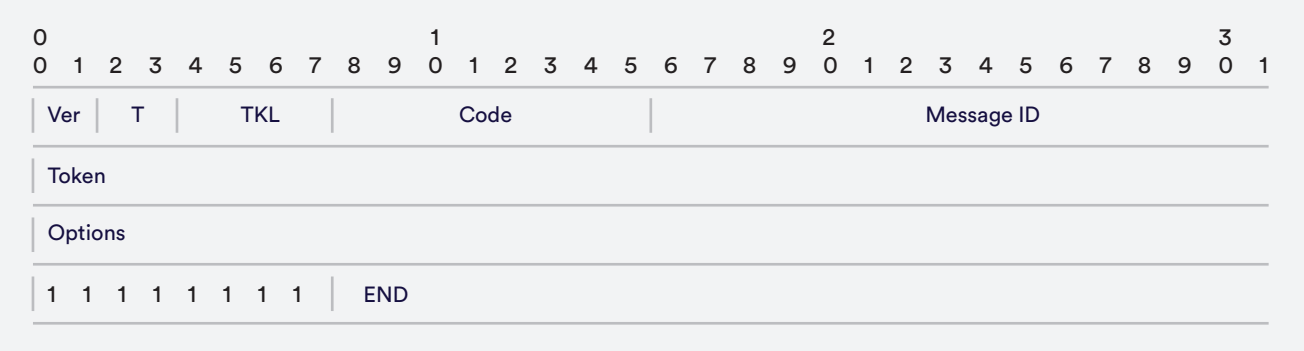
3 MOLECULAR CHAIN COMMUNICATION PROTOCOL (MCP PROTOCOL)

The DEF node will be mainly composed of home smart devices resulting in a low-power and stable multi-chain. As the nodes will need to communicate and broadcast vast amounts of information efficiently between each other, DEF will create a molecular chain communication protocol. The protocol will be optimized for the communication data structure of the smart devices.

The main advantages will be:

- Customized for communication between smart devices
- A Class UDP will be used instead of TCP which will help to establish a protocol stack which will be lightweight with the minimum length only 4B. All packet headers will use binary compression to reduce the amount of data where sending and receiving data will be performed asynchronously to improve the node response speed
- Support IP multicast, where it can send requests to multiple devices at the same time and a decentralized mesh topology can be formed

3.1 MOLECULAR CHAIN COMMUNICATION PROTOCOL SIGNALING FORMAT



Ver: 2bit version, the current version is 01. Messages with a non-1 version number are directly discarded.

T: Message Type: Confirmable(0), Non-confirmable(1), Acknowledgement(2), Reset(3)

TKL: Token Length, currently valid value 0-8. Others consider Message format error.

Code: 8 bit unsigned number, format: c(3bit class type).dd(5bit detail code)

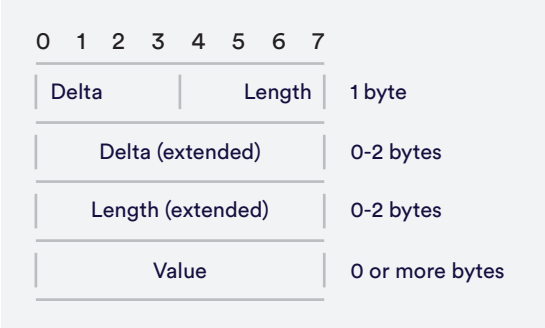
Message ID: It is used for repetitive detection of messages, and the match between Confirmable msg, non-Confirmable msg and ACK, reset msg.

Token: Used to match Request and Response

Option: Can be 0 or more. After each Option, it can be an Option, or Payload Maker and Payload or Message End.

End: If there is a End, it must be the End marker (0xFF) and the End up to the end of the packet. End marker and End must appear at the same time.

3.2 MCP OPTION FORMAT MESSAGE OF THE MOLECULAR CHAIN COMMUNICATION PROTOCOL:



DELTA:

The instance of Option in the message must be stored in the order of the number. The actual number of the option is determined by the Delta value of the Option + the value of the previous Option. The value of 0-12 indicates the Delta. If more than 12, need to occupy Delta extension.

LENGTH:

The Length of the option with value range 0-12. If more than 12, it needs to occupy the length extension.

VALUE FORMAT:

0 length character sequence
Opaque byte sequence
Unsigned integer

3.3 MOLECULAR CHAIN COMMUNICATION PROTOCOL (MCP) COMMUNICATION EFFICIENCY

Similar to HTTP, based on the REST model: servers present resources in the form of URIs, and clients can access them through methods such as GET, PUT, POST, and DELETE, but the relative HTTP simplification reduces the complexity (smaller code, smaller packets), and the smallest package which is only 4B. The information carried by the message is relatively simple and the data packet is 128 bits. Calculating with an effective bandwidth of only 1 Mbps using the molecular chain communication protocol, the delay between the underlying nodes of the blockchain can be as short as 5 milliseconds.

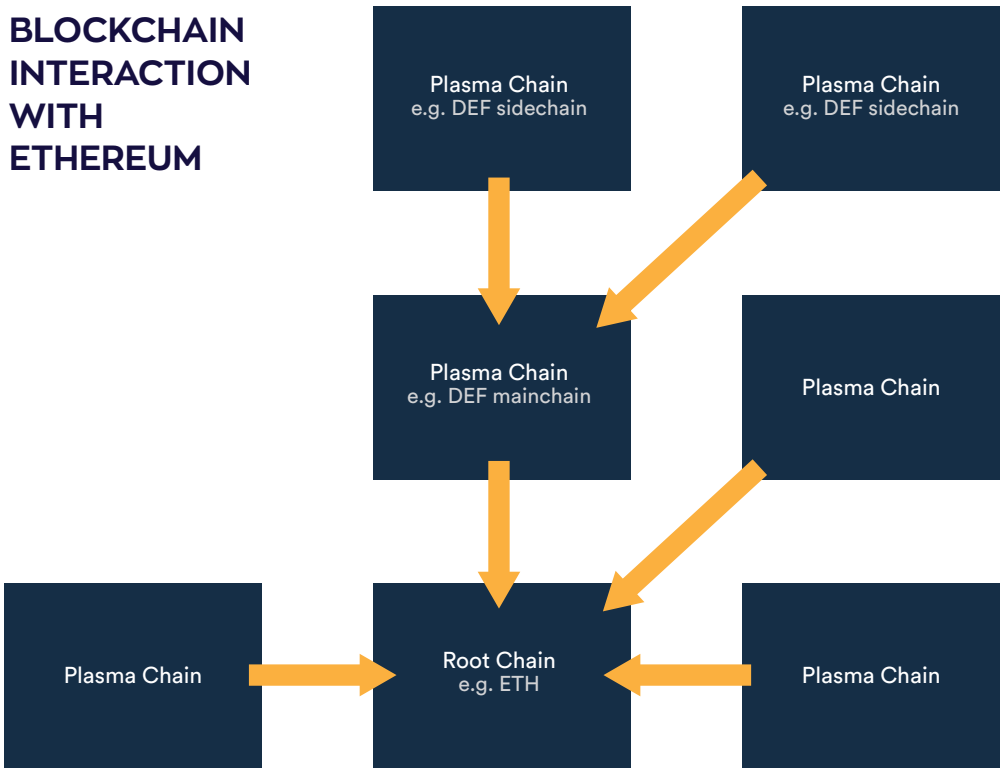
The 600-millisecond latency of the KAD (Kademlia) algorithm, which is now widely adopted, has increased efficiency by a factor of about 100. This also makes the DEF security chain nearly 100 times more efficient than other mainchains in communication efficiency.

BASED ON THE PLASMA FRAMEWORK

4

Given the stability of the current blockchain and its extensive use, the DEFENSOR™ team is very optimistic about the future of Ethereum. The DEF security chain is based on Ethereum, the mainchain extended through the Plasma Framework, also known as the Plasma blockchain. The Plasma Framework is a series of contracts running on the Ethereum blockchain. These contracts are responsible for customizing the run time rules of the Plasma blockchain, and the Plasma blockchain can extend through another Plasma blockchain, also known as the subchain or side chain. In this way, a blockchain with a tree structure interacting with Ethereum will be formed.

BLOCKCHAIN INTERACTION WITH ETHEREUM



In the Plasma blockchain, the node verifier is only responsible for notifying the mainchain of the related activities of the sidechain. In order to save storage space and provide verification efficiency, the verifier only needs to send the hash of the newly added block to the mainchain, and all other information is stored on the sidechain.

> One can view the root blockchain as the Supreme Court from which the power of all subordinate courts derive their power. It is the law of the root blockchain which allows for all lower courts to derive their judicial power. This allows for scalability in venues, it's only when the state of the lower courts is disputed or halted that one needs to move on to higher courts for a more represented venue.

Joseph Poon
Founder of Lightning Network

5 CONSENSUS MECHANISM

The biggest problem facing the current blockchain is throughput. While centralized network transactions can process tens of thousands of transactions per second, Bitcoin and Ethereum can only process a few transactions per second.

This throughput problem is related to the consensus mechanism. After many calculations, the DEF security chain enforces DPoS to ensure efficiency, and the sidechain chooses its own appropriate consensus mechanism according to the scenario requirements.

In order to improve the performance of the blockchain, 101 principals are selected via the DPoS mechanism from the public participation to create blocks. However, the performance of DPoS cannot be increased indefinitely. In a software system, its performance and throughput are physically constrained by the network bandwidth of communication between the nodes. In general, the bandwidth between two nodes in a public network environment can be maintained at 5 MB/s both in the uplink and the downlink, which is ideal. However, realistically, this value cannot be achieved. And if each transaction log requires 100 bytes, since the network requires broadcast transactions and broadcast logs, the network bandwidth consumption is doubled, so the maximum throughput in a single chain of two nodes does not exceed 25,000 per second (5MB/100 Byte/2=25000), assuming that the cluster contains more nodes, the maximum throughput needs to be scaled down based on the P2P synchronizer it uses.

Although the above-mentioned performance bottleneck exists in the DPoS consensus, efficiency of the DEF multi-chain will not be compromised with the inclusion of the molecular chain communication protocol and the Plasma Framework.

DATABASE

6

Most current blockchain systems choose to adopt simpler model non-relational databases to store data, such as Berkeley DB and LevelDB. These databases generally provide some simple data structures, such as B-tree, hashtable and Queue but does not support SQL to operate on data. Although these databases are sufficient for general electronic money systems, they are insufficient for application platforms, particularly for the finance, banking, e-commerce industries and current mainstream storage.

The system uses relational databases because of the following advantages of relational data:

- **Transaction processing**
- **Data update overhead is very small**
- **Complex queries can be performed such as Joins**

The DEF multi-chain platform will be run on SQLite, as it is a very lightweight embedded relational database (Android system also uses SQLite) with the maximum capacity to support 2T where data files can be freely shared between different endian machines with support for SQL, providing well-needed assistance for DApp developers.

SMART CONTRACTS

7

DEF chain smart contracts will be divided into standard and custom contract types during development and deployment.

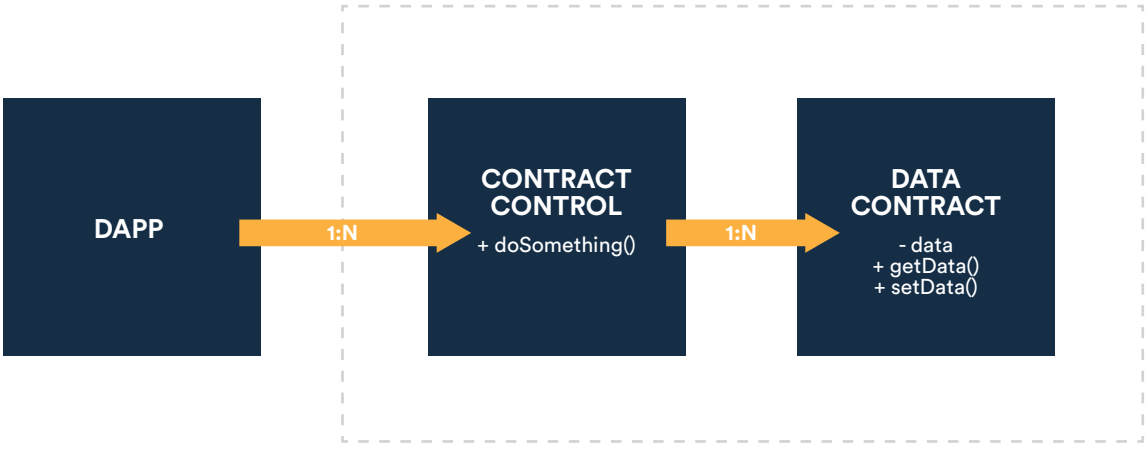
The standard contract will include relatively simple logic, such as asset consistency checks, automatic deal closure, multi-party confirmation transfer, and automatic settlement, which will generally meet the needs of developers.

Whereas, custom smart contracts will be able to support more complex user self-programming and can be used in large projects.

Smart contracts are divided into: controller contracts and data contracts

Controller contracts focus on the logical processing of data and external services. Data is accessed by accessing a data contract, and the data is processed logically, and then the data contract is written back. The controller contract does not need to store any data. It completely relies on external inputs to determine access to data contracts.

The data contracts focuses on the data structure definition and the read-write interface of the stored data. The data read/write interface is only exposed to the corresponding controller contract, and other methods of read/write access are prohibited to achieve the purpose of data unified access management and data access authority control.



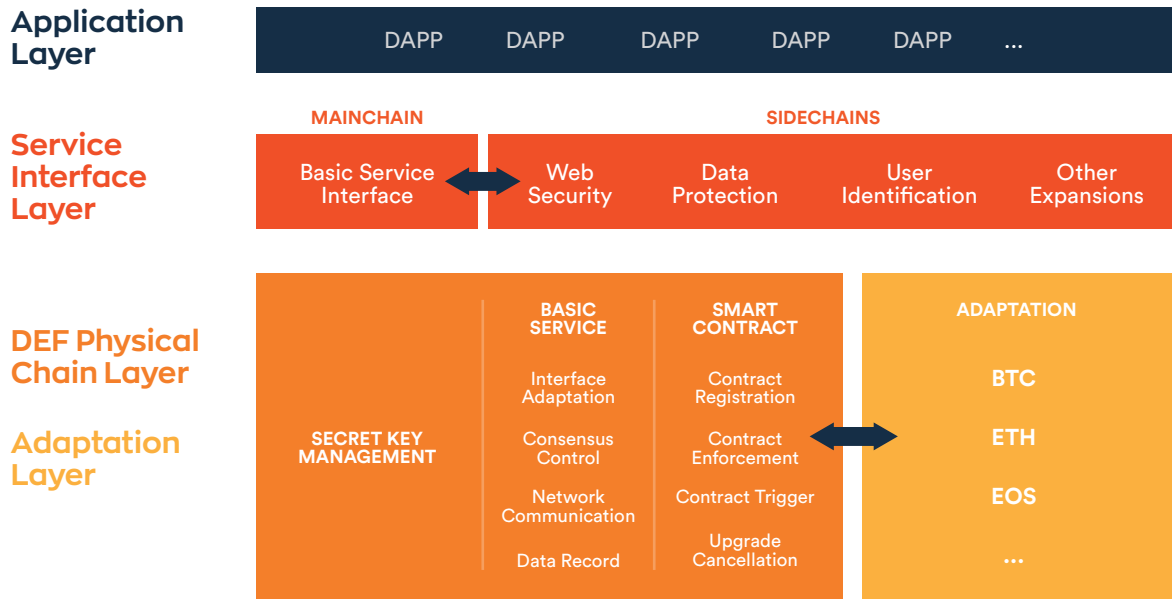
THE DEF FRAMEWORK

8

Developers will be able to use the DEF framework interface to implement DApps for various businesses while also providing an integrated testing environment using the same operating system without compromising the underlying components.

The DEF platform will also provide a command line tool to easily create a basic sidechain system. The core logic of the sidechain will be developed using NodeJS. The interface part will be developed using common front-end programming languages, such as HTML and Javascript. The back-end will communicate via the JSON-RPC protocol. Therefore, the DEF security chain will provide a highly efficient and customizable operating system setting a benchmark among decentralized solutions for network security.

The DEF framework will be mainly divided into a four-tier architecture: an application layer, a service interface layer, a DEF basic chain layer, and an adaptation layer.



APPLICATION LAYER

Applications that are responsible for direct interaction with development include, but are not limited to, web systems, apps, and other programs built with smart contracts and Internet records.

For example, a developer develops a DApp based on the DEF security chain for information harassment interception. Using the command-line tools provided by the DEF chain, the developer will only need to input several configuration items according to the prompts to quickly set up a sidechain to develop any type of application.

Secondly, the system also provides a series of APIs to help users build complex smart contract applications. These APIs cover consensus, strong random numbers, databases, cryptography, many more.

SERVICE INTERFACE LAYER

The service interface layer provides a series of API interfaces required for the development of DApps, enabling developers to perform rapid application development and reuse of components. Each of these service interfaces corresponds to various resource pools on the mainchain, including bandwidth, computing power, and storage. Developers can publish business applications directly after passing the "sandbox test" on the DEF chain with minimal cost.

ADAPTATION LAYER

The DEF security chain adds adaptations to other mainstream chains such as BTC, Ethereum, and EOS, and is therefore compatible with existing mainstream ecosystems. System users can manage other digital assets on the DEF chain, and other mainchains can also send data back to the DEF through triggers such as smart contracts.

BUSINESS MODEL

DEFENSOR™ will have two main revenue streams.

1 The first will be from monthly subscription fees to provide network security for end users who pay via DEF tokens. These end users will include individuals and businesses who seek for state-of-the-art network protection.

2 The second will be a % of associated expenses according to the contract if an attack occurred and was successfully addressed. If the platform is attacked, Defensor will invoke the highest efficient defense pool to disperse attacks and protect the end users to maintain continuous functionality.

TOKEN USAGE SYSTEM

The DEF token will be the main form of transactional currency in the DEFENSOR™ ecosystem for the participants to use and will be based on the Ethereum ERC-20.

Below are the various token use cases for the different participants of DEFENSOR™ platform.

Contributors

Contributors are the participants who sign up and connect their smart devices to provide idle network bandwidth and storage space to power the Defensor platform who in turn will be rewarded with DEF tokens. The amount of DEF token will be determined during the service period according to the contributor's service quality that is the length of single service length bandwidth contribution. After receiving the token, defenders can convert to Ethereum or Bitcoin or Fiat.

End Users

End users include individual or enterprise clients who as the service demanders can choose the corresponding defense and resource distribution capability on the Defensor platform by paying with DEF tokens. This has the potential to significantly reduce the network defense costs of small and medium-sized businesses. End users will also have the option to upgrade to a premium defense solution for households and enterprise environments by using DEF tokens. Services provided may include DDoS protection, cloud storage, cloud security and data integrity.

Network Security Threat Validators

Network Security Threat Validators will include geographically diverse security experts and engineers detecting and categorizing attacks and non-attacks using different consensus mechanisms depending on the scenario. Those that have detected any potential attacks will be rewarded with DEF tokens.

Smart Device Manufacturerers

By being part of the DEFENSOR™ ecosystem and embed the DEFENSOR™ technology in their respective smart devices, manufacturers will be rewarded with a portion of the revenue generated from their customers who have contributed.

Developers

Developers may not participate in every transaction but rather participate in developing a more robust security defense platform. By building DApps in the various sidechains of Defensor's multi-chain ecosystem, developers will be able to receive a share of the revenue generated from end users who purchase their professional security solutions.

GLOSSARY OF TERMS

ARM based architecture	Advanced RISC Machine (ARM) is a processor architecture based on a 32-bit reduced instruction set (RISC) computer.
Blockchain	A decentralized, digital ledger where transactions made in Bitcoin or other cryptocurrencies are recorded chronologically and publicly. The block contains information that, once it goes into the blockchain, it becomes part of the permanent and immutable database, connecting to other blocks in the blockchain like the links in a chain.
Consensus Mechanism	The method or protocol by which the participating nodes in a Blockchain Network arrive at a consensus for validating transactions or other commits onto the Blockchain. These nodes may also be referred to as miners. The most common consensus algorithms currently employed by most of current Blockchain networks are Proof of Work (POW), Proof of Stake (POS) or Delegated Proof of Stake (DPoS).
DAAPs	An application that is open source, operates autonomously, has its data stored on a blockchain, incentivised in the form of cryptographic tokens and operates on a protocol that shows proof of value.
DDOS	Distributed Denial of Service Attack; when a system is flooded with traffic from numerous sources.
DEF	Defensor token
DPOS	Delegated Proof of Stake leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates.
Decentralized	A state where there is no central control, power or function, or in reference to infrastructure, no central point of failure.
ERC-20	A type of token standard for Ethereum which ensures the tokens perform in a predictable way. This allows the tokens to be easily exchangeable and able to work immediately with decentralized applications that also use the ERC-20 standard. Most tokens released through ICOs are compliant with the ERC-20 standard.
Ethereum	An open source, decentralized platform based on blockchain technology created by Vitalik Buterin in 2013. It runs smart contracts on a custom built blockchain that allows developers to create markets, store registries of debts, and so on.

LEGAL DISCLAIMER

ABOUT DEFENSOR TOKENS AND P2P NETWORK SECURITY PLATFORM (“DEF”)

This White Paper summarises the principal ideas for the proposed Initial Token Offering (“ITS”) of DEF Tokens (the “Tokens”) by DEF Foundation Ltd. (a private company limited by shares) (“Issuer”). This White Paper in current form is circulated for general information for would-be token purchasers and to invite participant feedback only on the DEF Platform and the Tokens as presently conceived, and is subject to review and revision by the Issuer.

The DEFENSOR™ token sale will fund initial prototype development and testing of the economic instruments presented here. We expect, as would any prudent participant, that the details presented in this document may change during development and testing periods.

DEFENSOR™ and token purchasers’ interests are aligned to make DEFENSOR™ a viable network security platform.

Please do not replicate or distribute any part of this White Paper without this disclaimer in accompaniment. The information set forth below may not be exhaustive and no part of this White Paper is intended to create legal relations between a recipient of this White Paper and the Issuer, or to be legally binding or enforceable by such recipient against the Issuer. An updated version of this White Paper may be published at a later date and announced by the Issuer in due course.

REFERENCES

https://globenewswire.com/news-release/2017/10/26/1154373/0/en/Cyber-Security-Market-Is-Projected-To-Be-Around-173-57-Billion-By-2022.html

https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

https://www.accenture.com/t20171006T095146Z__w__/sg-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

https://cointelegraph.com/news/report-shows-cryptocurrency-exchanges-most-common-ddos-victims-worldwide

https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-ddos-intelligence-quarterly-report-reveals-accidental-attacks-and-cybercriminals-quest-for-cash