

8-2019

Blocks' Network: Redesign Architecture based on Blockchain Technology

Moataz Hanif

Follow this and additional works at: <https://commons.erau.edu/edt>



Part of the [Information Security Commons](#), [Social Media Commons](#), and the [Software Engineering Commons](#)

Scholarly Commons Citation

Hanif, Moataz, "Blocks' Network: Redesign Architecture based on Blockchain Technology" (2019).
Dissertations and Theses. 465.
<https://commons.erau.edu/edt/465>

This Thesis - Open Access is brought to you for free and open access by Scholarly Commons. It has been accepted for inclusion in Dissertations and Theses by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

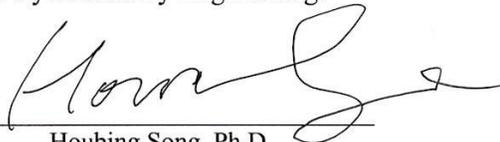
Blocks' Network: Redesign Architecture based on Blockchain Technology

Moataz Hanif

Blocks' Network: Redesign Architecture based on Blockchain Technology

by Moataz Aqeel Hanif

This thesis was prepared under the direction of the candidate's Thesis Committee Chair, Dr. Houbing Song, and has been approved by the members of the thesis committee. It was submitted to the Department of Electrical, Computer, Software, and Systems Engineering Department and was accepted in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity Engineering.



Houbing Song, Ph.D.
Committee Chair



Radu F. Babiceanu, Ph.D.
Committee Member



Jiawei Yuan, Ph.D.
Committee Member



Timothy A. Wilson, Sc.D.
Chair, Electrical, Computer, Software, and Systems Engineering



Maj Mirmirani, Ph.D.
Dean, College of Engineering



Lon Moeller, J.D.
Senior Vice President for Academic Affairs and Provost

9/16/19

Date

Blocks' Network: Redesign Architecture based on Blockchain Technology

Moataz Hanif

A Thesis in the Field of Cyber Security & Computer Science for the Degree of Master of Science in Cybersecurity Engineering Embry-Riddle Aeronautical University August 2019

Acknowledgements

I would like to express my sincere gratitude to Dr. Houbing Song, Assistant Professor of Electrical Engineering and Computer Science for allowing me to undertake this work. I would also like to thank Embry–Riddle Aeronautical University for facilitating a positive and forward-looking environment for research.

I would like to acknowledge my parents, who supported me with love and understanding. I would also like to acknowledge everyone who played a role in my academic accomplishments. Thank you all for your unwavering support.

Table of Contents

Table of Contents	v
Abstract	viii
List of Tables	ix
List of Figures	x
List of Abbreviations	xi
Chapter 1 Literature Review	1
1.0 Background of Study:	1
1.2.0 Issues Related to Blockchain Technology	5
1.2.1 51% Attack:	5
1.2.2 Anonymity:	6
1.2.3 Scalability and Latency:	6
1.2.4 Lightning Network:	7
1.3 Proof of Work:	8
1.4.0 Peep-to-Peer:	9
1.4.1 Peer-to-peer web hosting:	10
1.5 Hash Function:	11
1.6 Digital Signature:	12
1.7 Distributed Hash Table:	13
1.8 Zero-knowledge proof:	13
1.9.0 Blockchain types:	14
1.9.1 Public Blockchain:	14
1.9.2 Permissioned Blockchain:	14
1.10 Blockstack:	14
Chapter 2 The Platform of Blocks' Network	16
2.0 Introduction to platform:	16
2.1 The operation software:	19
2.2 The platform mechanism:	20
2.3.0 Using Zero-knowledge proof:	22
2.3.1 Threat model:	23
2.4 Distribution Standards:	23
2.5 Approach methods:	24
2.6 The Lowest-Level (Call Block):	26

2.7	The Middle-Level (Administration):	28
2.8	The Highest-Level (Operations Level)	29
2.9	Clauses of concession:	31
Chapter 3	Blocks' Network	33
3.0	Introduction to Blocks' Network:	33
3.1	Memory Pool:	35
3.2	Stagnation Mode:	35
3.3	Operations Waiting List Management:	36
3.4	Block size:.....	36
3.5	Difficulty scale:.....	37
3.6	Blocks' Network Architecture:	37
3.7	Consensus protocol:	39
3.8	Proof-of- Generation:	40
3.9	Coping protocol:	41
3.10	Category method for generation	42
3.11	Target Mechanism:	43
3.12	Implementation:	44
3.13	Categories Table:	46
3.14	The properties of Categories:	47
	3.14.1 Class A	47
	3.14.2 B, C, D, and E Classes	48
3.15	Interconnectedness:.....	52
Chapter 4	Process Optimization and Additional Chains	54
4.0	Pure Peer-to-Peer (Ordinary Nodes):.....	54
	4.1.0 <i>Ethereum Whisper</i>	54
	4.1.1 <i>VoIP and file sharing</i>	55
	4.1.2 <i>Skype Protocol</i> :	55
	4.1.3 <i>Tox (protocol)</i>	56
	4.1.4 <i>BitTorrent</i>	56
4.2	Redirection chain and DApp chain “Additional Chains”	57
4.2.1	Redirection chain “Additional Chain”	57
4.2.2	DApp chain “Additional Chain”	58
4.3	Cryptocurrency “Additional Chain”	59

4.4 Escalating Difficulty “Invalidation Category”	60
Chapter 5 Storage Mechanism for Distributed System	62
5.0 Storage mechanism (DHT bases).....	62
5.0.1 <i>Preference System Mechanism</i>	62
5.0.2 <i>The replication ratio</i>	64
Chapter 6 Conclusions and Future Research	65
6.0 Conclusion	65
6.1 Future research:.....	65
6.1.0 <i>AI algorithms:</i>	65
References.....	67
Additional Bibliography	72

Abstract

The Internet is a global network that uses communication protocols. It is considered the most important system reached by humanity, which no one can abandon. However, this technology has become a weapon that threatens the privacy of users, especially in the client-server model, where data is stored and managed privately. Additionally, users have no power over their data that store in a private server, which means users' data may interrupt by government or might be sold via service provider for-profit purposes. Furthermore, blockchain is a technology that we can rely on to solve issues related to client-server model if appropriately used. However, blockchain technology uses consensus protocol, which is used for creating an incontrovertible system of agreement between members across a distributed network. Thus, the consensus protocol is used to slow all member down from generating too fast in order to control the network creation pattern, which leads to scalability and latency problems.

The proposed system will present a platform that leverages modernize blockchain called Blocks' Network. The system is taking into consideration the issues related to privacy and confidentiality from the client-side model, and scalability and latency issues from the blockchain technology side. Blocks' network is a public and a permissioned network that use a multi-dimensional hash to generate multiple chains for the purpose of a systematic approach.

The proposed platform is an assembly point for users to create a decentralized network using P2P protocols. The system has high data flow due to frequent use by participants (for example, the use of the Internet). Besides, the system will store all traffic of the network overtly via Blocks' Network.

List of Tables

Table 1 Categories Table.....	47
-------------------------------	----

List of Figures

Figure 1 Centralized, Decentralized, and Distributed (from medium.com).....	2
Figure 2 Private key signing (from wikimedia.org)	12
Figure 3 DHT (from bitcoinwiki.org)	13
Figure 4 Blockstack architecture (from blockstack.org/whitepaper)	15
Figure 5 The platform of Blocks’ Network “Node structure”	17
Figure 6 Modular Code (from hackernoon.com)	19
Figure 7 Get the hash of card’s content for storage purposes	23
Figure 8 Send inputs from lowest-level to the highest-level/network’s storage	25
Figure 9 biometric pair of keys	27
Figure 10 Hashing Biometric input (from accesscontrolconsult.in)	27
Figure 11 Store key pair to Foundation Chain in the Blocks’ network.....	28
Figure 12 Highest-level’s Process (Generation)	30
Figure 13 Blocks' Network.....	34
Figure 14 Multilevel Inheritance	38
Figure 15 Target Procedure	44
Figure 16 Blocks’ Network Architecture	46
Figure 17 Blocks’ Network chains (control-lines)	52
Figure 18 Skype Node structure (from slideshare.net).....	56
Figure 19 Pure P2P Nodes alongside the Blocks’ Network Nodes.....	59
Figure 20 Distributed ledgers – Preference system Distributed ledgers	64
Figure 21 predictive modeling	65

List of Abbreviations

PoW – Proof of work

OIN – Operation identification number

PoG – Proof of Generation

P2P – Peer-to-Peer

BGP – Border Gateway Protocol

EGP – External Gateway Protocol

DHT – Distributed Distribution Table

NAT – Network Address Translation

ASIC – Application-Specific Integrated Circuit

AI – Artificial Intelligence

ML – Machine Learning

RAID – Redundant Array of Inexpensive Disks

Chapter 1 Literature Review

1.0 Background of Study:

Bitcoin is the first decentralized app that was introduced by Satoshi Nakamoto, [1]. It is the first cryptocurrency that launched under users' power which allows a group of people to store and share digital data (e.g. database) across multiple nodes (e.g. users) without a control from a particular central authority [2]. Bitcoin uses peer-2-peer network in order of ledgers distribution to share and store those ledgers among members inside the network without the need to go to an assembly point such as a server.

Blockchain technology has been modified since then, hoping this technology to be the replacement of Web 2.0. There are some developers who have used this technology for different purposes. One example is the "Follow My Vote" in which they adopt blockchain to run voting systems that cannot be intercepted by hackers [3]. There are many examples on how blockchain can be used; there are endless ideas that could be implemented with that technology.

The network has three common types, Centralized, Decentralized, and Distributed (Figure 1). The centralized system is Web 2.0 which so far is being used, when all traffic between two parties is stored in a server that is managed and stored privately. The distributed system is a subset of decentralized system [4] and it allows nodes to store and share data that was published from a certain entity (i.e. centralized) without having an impact on the stored data, which makes the nodes in the network act as public storage. The same with decentralized; it is using a distributed ledger system to share the data. However, each node can have its own decision and could have an impact on its data.

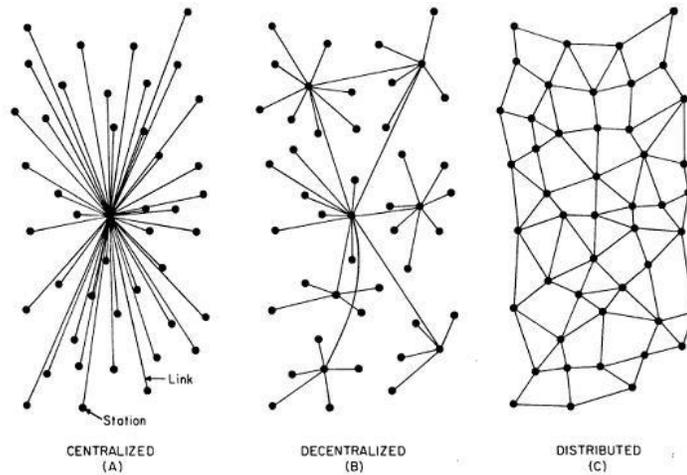


Figure 1 Centralized, Decentralized, and Distributed (from medium.com)

Data distribution is a technology that people claim to use to make the internet decentralized. However, in decentralization, each participant should obtain a copy from that distributed ledger (e.g., network’s database) to be an active node with the ability of updating that ledger frequently. Members inside a decentralized network do not have to trust others; thus, each one can verify the integrity of the obtained ledger since members could get a full copy of ledgers once they access the network. Nodes can verify the obtained ledger and compare it with the majority’s ledger. Moreover, transparency and integrity give public verifiability to the blockchain. Transparency is the verifiability of the data as it has been updated. This can be done by any person in the chain as they update. Integrity insures that the data has not been corrupted by checking the copies of the ledgers independently.

Centralization systems are entities where there is full control on a central system (e.g., database) providing online services, resulting in storing users’ data and transactions in a database that is controlled and managed privately. However, companies such as Google, Facebook, or Microsoft have the most users’ information inside the network; they are the controllers of the internet. Nevertheless, by downloading an app or registering on a website

that is controlled via a private entity, users will forfeit their privacy. This occurs when users accept the usage agreement by surrendering to that entity the permission to exploit users' data for analysis' purposes, or even worse for trading purposes.

WhatsApp was sold to Facebook for \$19 Billion [5], knowing that WhatsApp is a free app and non-profit (i.e., no-ads). So, why was its value so high? The short answer is users' data. In reality, when a customer goes to any store, there is no way for the seller to force him/her to sign-up in order to access the store or buy something. However, some stores ask customers if they want to sign-up by filling out a form with their personal information in order to get a chance to get a good offer in the future. Since the providers are dealing directly with people, they cannot force them to fill out forms, instead they are using a thoughtful strategy to make the customer want to do so and this can be by offering a discount, a free product, etc. In the end it is up to the customer.

In the reality of the digital world, there is an enormous difference. Almost all websites require signing-up to access their service. Besides collecting personal data, they try to collect information users are interested in, such as email addresses, users' hobbies, or even users' behavior patterns. All these are pieces of information crucial to a multitude of companies. The reasons behind collecting and studying users' behavior is to find a way of selling ads that relate to their interests.

In these cases, web servers gain the power over users and there is no way to sue them for exploiting users' data because the user wasn't allowed in the first place to use that service without accepting the usage agreement in one way or another. They are introducing the usage agreement with expansive content in a boring way to make the user give up reading, so users will accept it anyway.

Additionally, centralization databases' issues are not limited to confidentiality; there is also the defect of availability to consider. Taking a hosting server as an example, any failure in hosting servers will lead to inaccessibility, which means users cannot reach their information. Another type of availability failure is when the stored information is erased for an unknown reason to the user. That does not mean the servicer doesn't know the reason. For example, there are some users who have reported a missing file, and it seemed to happen because there was an error in the code of the server [6].

With all that, it does not mean that all centralization systems cannot be relied upon if there could be a guarantee of no possibility of abuse of power on their side. Moreover, we do not doubt that servers should know who is using their services, but not in the current way that is done in Web 2.0. Currently, providers are collecting more than what they should be allowed to have. However, they can verify users by their ID under zero knowledge proof without any more additional information regarding user's confidentiality. Moreover, the equalization of centralization systems (e.g. webservers) are very important which means when a new webserver appears into a network, in somehow the new entity will have a fair confrontation to compete with big webservers such as Google or Facebook. Therefore, by implementing a decentralize system appropriately it will increase the chances for this achievement. Furthermore, blockchain might help to solve some aspect that related to centralization, but still there are some flaws that relate to the scalability, latency, and trust in the decentralization systems.

1.2.0 Issues Related to Blockchain Technology

1.2.1 *51% Attack:*

The 51% attack happens when a specific member inside the network gain more than 50% of computing hash power against the rivals. However, there is no a particular purpose of obtaining 50% of the computing hash power of the network other than increasing the chance of winning the block reward that offers by the network among the average users, the reward is equal to 12.5 BTC per block [7]. Unfortunately, the case will be different if an adversary could achieve more than 50% of the computing power which he/she could use that power to make a massive difference inside the network since an adversary has better chance to generate blocks faster than other members, which lead to makes the network devoid of credibility. For instance, an adversary wants to send to another member 1 BTC, this transaction will be included in a block that is generated in a sub-chain which will be in a hold, waiting to be added to the public blockchain permanently. However, an adversary with 50% of computing power could apply double-spending attack and try to reverse that transaction by generating a new sub-chain that longest comparing it to the previous one to invalidate that transaction which is considered as a tampering method. BTC Guild has solved six blocks in a row with much less than 50% of the computing power of the network [8]. With all that, having more than 50% of hash-rate power of the network is something hard to achieve since there are millions of candidates inside the network unless the members of the mining community are united. The mining pool is something common in the blockchain network where candidates can work together and share their mining equipment to achieve more power than others to increase their chance of winning.

1.2.2 Anonymity:

The anonymity happened when users hide their identity to mislead other parties from knowing their true identity for various reasons such as hacking, illegal activities, et cetera. The anonymity is a part of web 2.0 and unfortunately is also a part of web 3.0. Taking bitcoin network as an example, there are a huge number of illegal activities happened behind that network under anonymous accounts [9]. Bitcoin cryptocurrency's value derives from supply and demand [10]. Furthermore, the inflation in the bitcoin cryptocurrency to reach thousands of dollars is that there are people who wish to exchange suspicious money through money laundering within the network and this is due to the anonymity that provided by the system.

1.2.3 Scalability and Latency:

The scalability is the capability of the system in order to measure the highest speed rate in writing transactions into a block that could be handled by the system. On the other hand, the latency, which is the measurement time form the point of submitting a transaction until it written to the block. However, the issue of latency results to the double-spending attack, that when a completed block goes back to the memory pool because it was generated in a short chain and there was a longer chain has been chosen. Moreover, there is a transaction fee that clients have to pay to the miners each time they made a transaction and to get a better chance that the transaction will be selected and speed-up the process of writing the transaction to the chain, client should offer high fee, that's mean when the fee amount increases, the chance of that transaction to be chosen via miner will increase as well. However, from various sources, there are some transactions that never been confirmed [11].

1.2.4 *Lighting Network:*

Lighting Network is a level “Layer 2” that added on the top of blockchain architecture which allows micropayment to go through bidirectional channels that occur off the chain in order to speed up the process of transaction completion [12]. Lighting network (in the Bitcoin network) has been introduced to solve the problem of scalability. However, there are many problems underlying the lighting network, making it highly undesirable. For example, the client must be online to receive funds [13] which is considered a serious flaw, especially for merchandisers. Furthermore, the way of sending funds from a destination to another should be done by users, using routing protocol.; however, in general, the routing is always considered as an unsolved problem. Therefore, the legal liability for all nodes at that level must be considered as a critical point.

Border Gateway Protocol (or BGP) is the internet standard External Gateway Protocol (EGP). It uses via Internet Service Providers (ISP) level; thus, ISPs can consolidate their networks together, in order to establish a communication network between clients at a worldwide range [15]. Mesh routing is an example of how the internet works, and it uses with the purpose of sending data package through nodes from point to another; however, mesh routing is a problem that never solves on the internet [16]. Thus, the BGP is used by providers under agreements so as to avoid controversy. That agreement based on how packages should send though the network without disputes. According to (news.fintech.io) and other sources, in May 2017, a Russian-controlled telecom hijacks financial services’ Internet traffic [17]. This proves that the routing is an issue that could not be solved if there are adversaries at that level.

The lightning network is utilizing nodes to carry-out transactions, in the case of bitcoin these transactions are considered as money which makes those nodes become custodian's funds. Further, the funds in the lightning network go through channels to nodes that their owners are unidentified by other nodes. Therefore, this results in fracturing the KYC/AML requirements [18]. Additionally, there a lot of funds that have been lost in the network in order of experimentation improvement. Finally, the completion time of the project of the lightning network is has been extended many times thus it is hard to tell the precise time of completion for this project which proves that lightning network is imperfect project.

1.3 Proof of Work:

Notably, the concept of proof of work was developed and published in 1993 by Cynthia Dwork. However, its application did not occur until its application in Bitcoin cryptocurrency by Nakamoto. Essentially, Proof of Work (PoW) is a concept whereby the mathematical problem is solved and verified through various points on the network. Usually, this will involve solving a target has by trial and error means until an acceptable solution is arrived at. The process of solving this mathematical problem is referred to as mining and is conducted randomly at various points of the network. Ideally, the first acceptable solution wins a reward for the work put in. In any case, the amount of time and processing power required to solve such a problem is amazingly high hence the need to keep the miners motivated (Lisk Academy 2019). Importantly, the winner of the mining process is rewarded in form of the cryptocurrency involved through facilitation fees for the transaction this concept ensures that the transactions remain valid and make it difficult and expensive to counterfeit any transaction data.

Perhaps the major benefits of using this concept are the degree of flexibility that is handed to the users. It allows the transactions to and rewards to go to the miner who worked more for it. In reality, it hands the value back to the miner rather than middlemen such as online payment services. In addition, the anonymity present in such a transaction guarantees the privacy of individual data while still availing proof of transaction. Moreover, it guarantees financial saving per transaction thanks to the trustless capability of the technology. [19]

1.4.0 Peep-to-Peer:

According to Lisk Academy (2019), the peer-to-peer network is the foundation of the functionality of any blockchain. The term peer particularly refers to the individual computing systems within a blockchain. Each of the peers within the network performs a specific task to facilitate the functions of the blockchain. The setup of this system of peers ensures that there is no need for the blockchain to have a central server to coordinate the execution of the task. Importantly, the peers form a decentralized functionality of the blockchain which essentially means that information and resources in a blockchain are stored in different points in the network. This ensures the security of the data within a particular blockchain since it is not stored in a single computing system but rather across all points within the network. The duplicity of data stored ensures recovery of data is possible even if only one computing system remains within a particular blockchain. Furthermore, a peer-to-peer network becomes stronger and faster as more computing systems join the network which is not possible in a client-server network.

In terms of administration within a peer-to-peer network, no single entity within the network can control the network or use the network in a privatized manner. The architecture

of a peer-to-peer network is such that all members of the network share both resources and data to the other users. Intricately, this means that each user assists in adding to the processing, storage and transfer capabilities of the network, which implies that the more users are in the network, the more the network can perform and process larger volumes of data. For this reason, a peer-to-peer network has become the building block of sophisticated blockchains and facilitates.

1.4.1 Peer-to-peer web hosting:

The hosting of the P2P website has not been put into application yet since the cohort machinery that enables the topmost rates of upstream for personal consumers is not yet utilized broadly. For this, Wireless Mesh Networking that enables the normal user to make good use of the total speed of upstream that their router is up to is necessary. This should be utilized instead of what other ISP taking advantage of them as they pass on information between the other routers for it to achieve its aim.

For a P2P website to be hosted there is a need for some kind of technology mixture between the numerous-redundancy RAID storerooms, communication of wire mesh, sharing of torrent and several types of encryption key hierarchy enabling a variety of varying capacities of clients to get the transmitted information shifted. This enables something energetic like a to-be-hosted forum. For the latter to be incorporated, it would be necessary for the system to be keeping itself updated, maybe through time-stamping every data packet being circulated.

Potential catalysts likely to source general P2P hosting utilization might be in existence. However, I believe that something that revisits the corporal hardware architecture

essentially connecting the internet back to its new web communication theory happens to be an excellent candidate.

Certainly, as usual, the major reason as to why the implementation of this has not yet taken place is for the reason that there is no adequate money in it. The absorption of the idea would be a bit quicker if either:

1. An individual obtains a way of distorting it greatly towards consumerism.
2. It dawns on the manufacturers of the router that there exists a huge Wireless-Mesh-ready routers demand.
3. There exists an international pattern moving away from the profit intention and headed for coming up with things just to ensure that all humanity is assisted. This is through establishing profusion and determined to obtain the best possible efficiency. [20]

1.5 Hash Function:

Hash function is an algorithm cryptographic that maps random size data to a string of fixed size. Two requirements of security called collision-resistance and one-wayness are normally needed by hash functions. Hash functions algorithms one main practical use is ensuring data integrity is received from sources online. A fairly manual and simple instance of hashes application is numerous scenarios of downloading files where in print hashes permit downloaders to confirm hashes integrity of received files. In blockchains, hash functions are used in generation of address (Addr) proof-of-work (PoW), bridge mechanism, generation of number (PNG), generation of block, message digest in signatures (MDS). Some applications are rather popular and typical even prior to blockchain birth, whereas others became famous recently because of blockchain and cryptocurrencies development.

The most famous used hash function in blockchains is SHA256, which is an algorithm from cryptographic hash functions family called SHA (Secure Hash Algorithm).

1.6 Digital Signature:

Apart from hash function, another blockchain cryptographic that cannot be avoided is the digital signature. The digital signature concept was discovered in 1976 by Hellman and Diffie when the public key cryptography's gate was opened by them. As a primary primitive of cryptography, the application of digital signature is for authentication of source, integrity, and non-repudiation of the source. Digital signature standard safety is unforgeability existential amid adaptively selected attacks of the message (EUF-CMA), which ensures that the latest message legitimate signature cannot be forged, even though the oracle of signing can be accessed that could offer services of signing.

Furthermore, digital signature does not encrypt the messages (Figure 2), it sends a message as plaintext with a signature that verify that message was sent from a certain person. Therefore, message encryption can be achieved by recipient public key "Asymmetric key encryption".

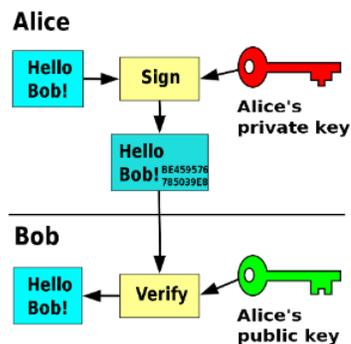


Figure 2 Private key signing (from wikimedia.org)

1.7 Distributed Hash Table:

Distributed Distribution Table (DHT) is a distributed data structure that is used to store entries associated with a key. Moreover, DHT has two main components, key, and value, for illustration, the key could be an address, and the value can be the content of the file that linked to that key. Therefore, users are allowed to search for a key via an entry, as with phone contacts when a user searches for a phone number (e.g., key) through names (e.g., address). DHTs is widely used in order to build and manage complex services. For example, BitTorrent is using DHTs for the distributed tracker. Gayle McDowell said about DHTs, “For any problem, have hash tables at the top of your mind as a possible technique to solve the problem.” (Figure 3)

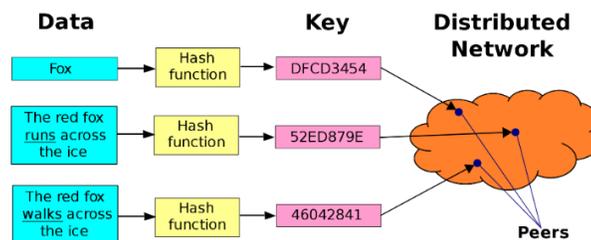


Figure 3 DHT (from bitcoinwiki.org)

1.8 Zero-knowledge proof:

A standard concept to guard the confidentiality and transaction anonymity is to cause transactions to be unlikable. Nevertheless, the system of e-cash requires to authenticate if the payer possesses the classified similar to the address where cash is coming from.

Auspiciously, the zero-knowledge proof was created to handle this suspense.

1.9.0 Blockchain types:

1.9.1 *Public Blockchain:*

It is a network open to the public where anyone can join the network to use network services or maintain network security. Examples of public blockchain networks are the Bitcoin network and the Ethereum platform.

1.9.2 *Permissioned Blockchain:*

It is a network that requires permission to access, read, or validate blocks within the network. Usually, permission blockchain networks do not require proof-protocols such as PoW; thus, validators are assigned in advance to generate blocks. Example of a permissioned blockchain is RippleNet where Microsoft, MIT, and CGI are working as transaction validators.

1.10 Blockstack:

Blockstack is a decentralized network that puts users in control of their identity and data. It stores encrypted data in private databases such as Amazon S3 or Google Cloud Storage. It stores data hashes in the blockchain to use as a pointer to these data at the private storage (Figure 4).

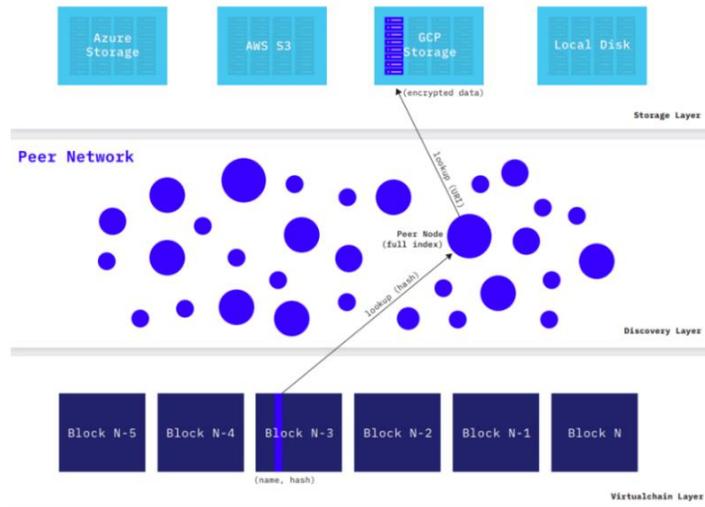


Figure 4 Blockstack architecture (from blockstack.org/whitepaper)

Chapter 2 The Platform of Blocks' Network

2.0 Introduction to platform:

The platform envisions to make all transactions of the internet distributed; thus, it intends to turn private storages (e.g., database) to public storage that could be viewed publicly under a specific condition. Further, the contents of webservers can be managed by their providers, and all actions that occurred inside that webserver are stored and managed publicly via distributed ledger technology. Therefore, data become available to everyone without the need of reaching the node of the backend provider unless necessary. Thus, the webserver becomes a secondary preference to download/view content that was previously viewed.

The importance of the system is to provide the same efficacy as the usage of the internet and transmit its storage into a decentralized network, and hence, there is no individual that has master control over the data. Consequently, the system contemplates conveying the appearance of web 2.0 that currently circulated with the preservation of its characteristics to web 3.0 semblance to get a distributed communication network. Therefore, the platform intends to transmit the client-server model to peer-to-peer web hosting that use Blocks' Network technology for the primary storage.

The platform leverages the Blocks' Network technology, and hence DHT will be assigning to be responsible for the data storage management that on an extensive range of nodes and accessing them with high efficiency. Therefore, it presents a project of a decentralized internet network, where nodes will have different positions relying on their level in the system. The network is using a peer-to-peer network, which is an overlay

network on the top of the IPs infrastructure where it will provide the network with high potential in the order of scalability [21].

The architecture of the platform introduces a multi-level model where each node at each particular level in the platform will be running under a unique functionality (Figure 5). Therefore, nodes' placement had been considered to obtain boundary layers where nodes are going to handle the participants' encounter for the purpose of interaction and hence achieving completed processes via communication tools, and storing outputs for that interaction in a distributed ledger.

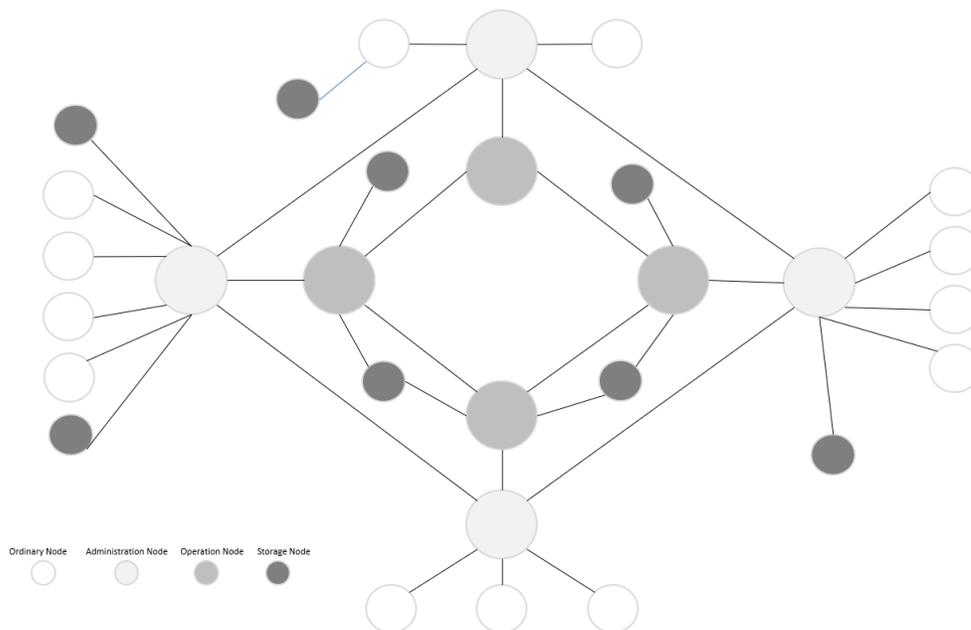


Figure 5 The platform of Blocks' Network "Node structure"

In the architecture of the network, the entry of participants is through the lowest level where members have to cope with an operation software called "Call Block", that is in the front-end (e.g., user side). Call Block loads essential functions that use for various options to enable communication between members. Also, it can obtain identification to grant

authorization; in addition to stores users IDs in the Foundation Chain (we shall be discussing this term in depth in chapter 3) and hence the functioning of communications' transmission inside the network started. All nodes at this level are defined as ordinary nodes.

Additionally, the administration level, it is the middle level in the architecture of the network where nodes at this level are liable on routing packages, and host-nodes indexing. Since the vital role that has been given to this level, nodes must run under a smart contract to illustrate the position that node has been obtained who are custodians on packages. All nodes at this level are defined as administration nodes.

In addition to that, the storage of network is a sub-level in the architecture where nodes at this position are responsible for storing/distribute data among nodes. Nodes must run under smart-contracts to clarify the size of space that is allocated to the system with build-in extendable contract clause.

Lastly, the highest-level (or Operation Level) is the backend node from the lowest level's perspective view. It retains web hosting nodes where these nodes are services, and resources, that other nodes in the network can take advantage of. Therefore, the highest level is accountable for embedding hosts via operation software to the network, where it conveys webserver's backend code onto Operation Chain (more details in a subsequent section); it ensures that a server's backend code is placed in a block that is immutable while it is updatable. Nevertheless, nodes at the highest level carry some crucial functions in its operation software, one of which is the ability of generation (i.e., mining); thus, operation software is controlled and managed directly by the provider. All nodes at this level are defined as operation nodes.

2.1 The operation software:

The implementation of the software is enabling the network communication's management where each level has its application. However, all applications are meeting in an assembly point that is the core code, which is immutable. Therefore, the operations software should be written under extensible functional code protocols (i.e., modular code). Additionally, the modular code is a code that can be modified, and interacted with, without modifying the core codebase. The core code also has flexibility, production stability, and scalability [22]. Moreover, there is no particular level could make any modification to operation unless the ability of adjustment clause built-in. (Figure 6)

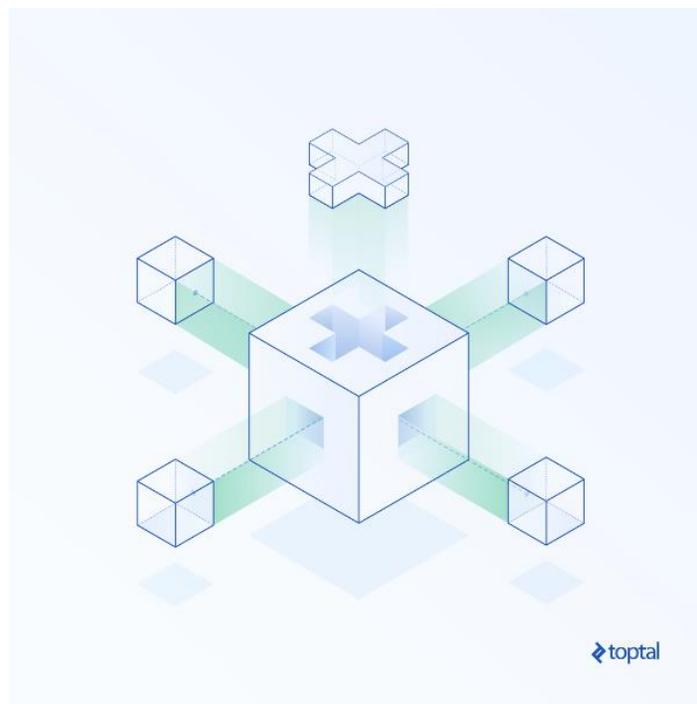


Figure 6 Modular Code (from hackernoon.com)

2.2 The platform mechanism:

In theory and practice, if an object that you owned becomes available to everyone, trading that object for profit will be useless — take the example of WhatsApp that was mentioned earlier. If WhatsApp's database was open to everyone, and each can obtain a copy of that database, trading that application for benefits is impossible.

Blocks' network is a public and a permissioned network that allows average users to join the network on its all levels. However, to gain a particular privilege in the network, the permission is needed. The permission could be accomplished via a smart contract that state the user's position at a precise timeline and hence the permission is hereby granted. Any users can gain a position as long as they become verified users.

The platform is introducing a way to transmit data from a centralized system to a decentralized system in order to limit the power of information analysis that is store privately. Therefore, users' data became available in their hands extensively, and new entities could access information stored in the distributed ledgers upon user's approval. So, everyone has the same object (e.g. users' data) in a way that information does not lead to the true identity of the user unless the disclosure statement was made. Therefore, using users' data in order to track and trade users' behavior will be useless. This could be achieved by inserting standards of conduct for each node's cluster separately in order to make it compatible with the distribution system.

The platform itself does not allow anonymous users to enter the platform, where the lowest level loaded with an identifier function. Thus, the authentication in the platform can be accomplished with participants' biometrics (e.g., fingerprint) since it is tough to modify.

However, users' identities remain confidential under their control, which they will have their owned storage in blocks' network (e.g., Foundation Chain). Upon successful verification, users can access the main page of the platform as a regular web search engine. Nevertheless, all actions from lowest to highest levels will be made under a public key, which is referred to as the identity of the user.

The public key is the ID that provider should obtain from a client upon a signing-up process to a host server; however, verifying a user's identity in order to access a server that contains a sensitive content (i.e., governments or banks webservers) could be achieved under the concept of zero-knowledge proof. Therefore, the user could obtain a valid token to grant access permission to that particular webserver. Furthermore, storing a public key or user token in a reason of examining the user's history inside the network is considering as a challenging task. Since the mechanism of the platform is to generate a new public key for each webserver automatically with the ability to create unlimited public keys manually and all public keys will be referred to one private key (e.g., fingerprint). Moreover, the client's traffic should run through PeerVPN, which is open-source, peer-to-peer VPN that is compatible with mesh network topology, and it does not require NAT configuration [23].

The platform intends to use web servers as a primary source for distribution, especially, at the outset (i.e., the start-up of the platform). The platform tries to collect as much as resources from elements that users are looking for or interesting-in, in their daily life to store these resources publicly. The first reason is that when a new entity joins the platform, that entity will have the same power of information that any other entities have; since all actions are distributed. One example of the benefit in making the power evenly between entities is that, say a new bank join the platform, if a user wants to request a loan online, user can

reference all blocks that contain financial history to that bank to get approval. Therefore, the new entity will make sure all referenced blocks are accurate since it was generated by a valid provider and can follow the client's financial history via one or more public keys. The second reason is that utilizing the distributed blocks as the primary method of looking-up (e.g., inquiries) instead of going back to a webserver and lookup for a file that was previously viewed. This will reduce replication of information inside the network that results in having inflation in data inside the system that contain the same files in different nodes. Therefore, the files that store in nodes should be viewed first to avoid generating that file again via generator inside the network; thus, this will increase the productivity of webserver to update their content continuously.

2.3.0 Using Zero-knowledge proof:

A zero-knowledge proof is a technique that used to prove a specific value known by a person to another party without revealing the actual content of that value. Therefore, the zero-knowledge protocol is adopted to be the main approach method of proofing user identity based on ID's in order to grant access authorization for a particular web hosting node. This could be accomplished by combining a hash function with a secure, real-time optical ID reader that runs on the client-side. Therefore, optical ID reader is going to take the information that on the client ID and convert it into a hash and hence match uses input with the generated hash at a real-time. Using the optical ID reader will not store the ID as a picture, it stores the hash of the content of the card and compares it with the input field that required by the web host in order to authenticate users (Figure 7). This method can prove the user's official name and birthday, without revealing more information than required; thus, it issues token-based authentication. The token is linked to the user's public key that

unique to that server which means a new token is needed for other webservers. The web host could issue a token to allow the user to access the webserver frequently with the option of limiting the number of accessing per token (e.g., one-time-use token).



Figure 7 Get the hash of card's content for storage purposes

2.3.1 Threat model:

Using IDs under zero-knowledge proof could be a dynamic solution; however, there is a possibility that fake-IDs will be used. Despite that fact, the ID will be linked to a private key that is a fingerprint which scientifically cannot be matched with another fingerprint. Therefore, linking a fake ID to a permanent private key could be risky; but that is not adequate to ensure identity accuracy. Moreover, a multiple-authentication-factor could take into consideration regarding this matter.

2.4 Distribution Standards:

The distribution standards have been addressed to reduce the issues related to information gathering that on web 2.0, where it is applied for web hosting nodes by making the interaction between client and provider based on the principle of sufficient communication. Additionally, when a candidate registers to the platform and hold a place in the operation block and become active host node, the highest-level applied a control criterion which

should be followed in order to route packages to that host server via administration node. However, ownerships still have full control over their web servers' content. Moreover, the standards are allowing adjustment to the current web servers to be compatible with web 3.0.

- All webpages should be introduced to users without authentication protocols, since each user will be authenticated by the platform automatically.
- Allow virtual credit cards to be as the primary payment method for the top level.
- Allow a real-time optical ID reader to be the main method for any additional authentication that under zero-knowledge proof to generate a valid token “Token based Authentication” (if-applicable).

2.5 Approach methods:

Starting from the lowest level, GUI provides the ability to run inquiries operation and execution operation. Firstly, the inquiries operation is using to find an input result from the network's storage. Secondly, execution operation is transmitting users' inputs to the highest level, and hence, it will lead to generating a transaction after the completion of that interaction, which will be added to a block (Figure 8).

All requests (i.e., inputs) will be routed through the administration node at the middle level in order to forward packages to the highest level (e.g., host) or to the sub-level (e.g., storage). Therefore, inputs will be pass through the network to the closest administration node determined by the bandwidth. Administration node is accountable to carry-out packages for transmission at a particular frequency range. Furthermore, from the routing table, the administration node will remain conscious of the appropriate route plan for

packages, and hence, the observed of that action will be updated to the routing table consistently.

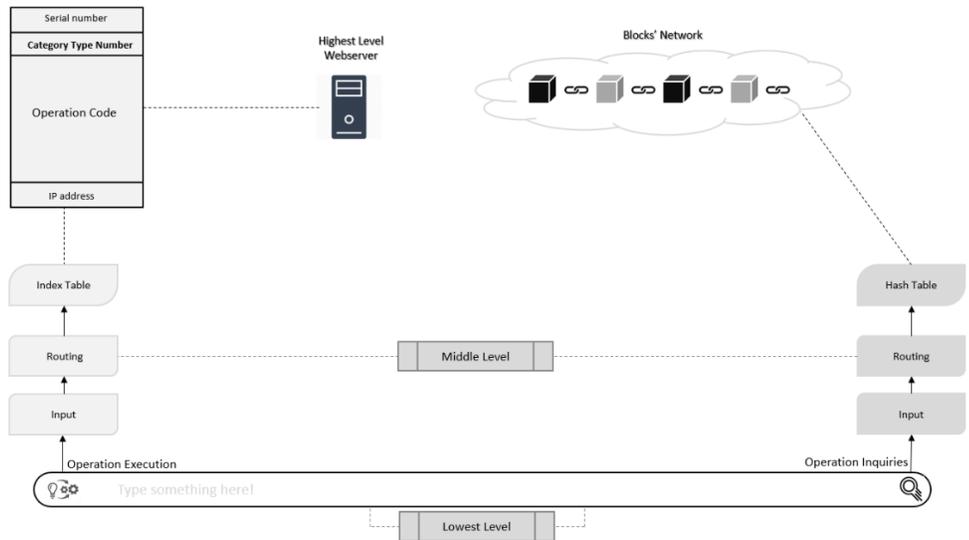


Figure 8 Send inputs from lowest-level to the highest-level/network's storage

Operation nodes at the highest-level must occupy a block in the Operation Chain in order to obtain Operation Identification Number (OIN) that is a unique number which is generated via the operation block (e.g. Operation Chain) that is using to activate the operation software which is resulting to activate participant server as well and hence allowing the accessibility from the lowest level nodes.

Upon successful access to a host, all completed actions that made upon interaction will be store at a memory pool that controls by operation node in order to include them to a block for generation. The generation method will made when a group of unconfirmed actions contained inside a block in order to find that block target to pass it to the blocks' network. Furthermore, upon generation completion, all conformed blocks will be distributed to storage nodes.

Blocks' network has in its architecture 16 categories ranges. These categories are used to arrange the blocks storage where each operation node will refer to a completed block through a target number that matches with the type of blocks (e.g., the type of service that provided by the host) to include that block into its appropriate chain.

The scaling difficulty of the generation has a probability ration of 50% in order to find a target. Therefore, the difficulty of finding a target is very low, which means generating blocks could be handled via an average hashing power in order to create high numbers of blocks very easily. Furthermore, there are some main categories considered as the networks' hub chains, which means they are not related to public storage (we shall be discussing this term in depth in chapter 3).

2.6 The Lowest-Level (Call Block):

The lowest level is the entry level of the network, where it holds all ordinary nodes who are authentic; under this ratification, certain privileges from this level could be given upon client demand, or in other words, providing the ability to users to be at the administration level, operation level, or storage level based on their desire.

The lowest level run under a software called Call Block that operate certain properties. The Call Block is the primary operation that run on the first level which it is providing an interactive page to users. It utilizes an access control protocol for identification and authentication in order to give the permission to access the platform.

The registration stage is executed through the Call Block software where it generates a block for each individual member that is an automated procedure. The registry class by the software is preconfigured and selected to a specific target range at the blocks' network.

The Call Block uses Biometric Access Control to generate a private key, by allowing users to sign-up in a real-time using biometric authentication (e.g. fingerprint); it will generate from user's biometric a key pair (Figure 9) where the public key is used as an ID which is a reference to client's identity.

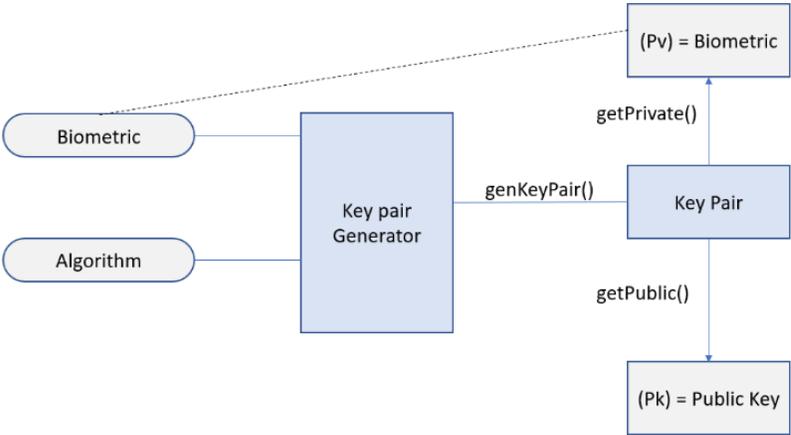


Figure 9 biometric pair of keys

Modern biometric technologies do not take a picture of the biometric (e.g. fingerprint) instead, transferring that biometric into dimensions and points that can be read as digit (Figure 10).



Figure 10 Hashing Biometric input (from accesscontrolconsult.in)

It sends the key pairs through cryptographic hash function in order to obtain a hash from that private key then store in blocks' network (Figure 11). Therefore, it compares that stored hash each time user accesses the platform with a real-time fingerprint which it is the main

method for authentication. The Call Block is taking a partial place in the storage of the network, called Foundation's Chain.

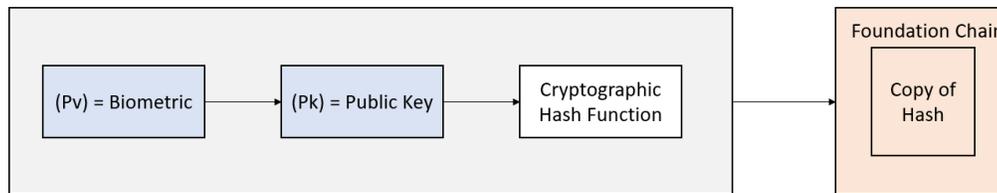


Figure 11 Store key pair to Foundation Chain in the Blocks' network

2.7 The Middle-Level (Administration):

The middle level is the primary routing process of network. Nodes at this level are accountable on transmit packages from destination to another, in addition to web-hosting indexing. Moreover, administration nodes accountability to scan constantly web hosting nodes that on the Operation Chain in advance via spider software technique then store the result of the scan to the index chain frequently.

The architecture of a web crawler is used via administration node for validation, next to the search process speed and hence stores observation to the index chain. Administrators use indexing process for regulatory affairs, which means that they will constantly update the status of the highest-level members in the index chain, thereby updating the index of the distributed table. Moreover, even if a block acquired by web host from the highest level within the Operation Chain, this does not mean that permanent access is granted because administrators have the ability to update the table index and remove some of the highest-level violators (e.g. violate guidelines).

Administrator nodes are highly reliable nodes that have a higher bandwidth comparing it with other nodes in the network. Members at this level are running administration software ordinarily that is not behind firewalls. The node must run their administration software permanently to be consider as an administrator. Moreover, administrators must execute a smart contract in order to be qualify. Therefore, any violation of the meddle-level's conduct leads to the termination of the contract which is a build-in clause.

Jidian Yang, Linweiya Chen and others, introduce a trusted routing scheme using blockchain technology in order to achieve the routing information of the routing node on a blockchain. Therefore, it will increase the ability of tracking that information of the routing node that also is unchangeable. Jidian Yang, Linweiya Chen and others, introduce the reinforcement learning model that used to help routing nodes dynamically select more trusted and efficient routing links. [24]

2.8 The Highest-Level (Operations Level)

The highest level (or Operation Level) is the workspace of the platform; it managed by the operation software that considers being the control panel of the highest level. This level can be accessed via stakeholders, which means anyone who willing to offer a service via a web-hosting server. The authentication in the highest level is required and it has a similar method of an authentication process that described previously. The main difference in the highest level is that the operating software requires more details about the host to be identified to grants generator's privilege. The provider can define the server's ownership, the server's IP, the server's category, and the server's description, etc. Therefore, web hosting information will be stored in a block of the Operation Chain where each host node could be defined by administration level through this chain.

Furthermore, all completed action that happened between a client and a web server (i.e., media files) will send to the unconfirmed pool (e.g., memory pool) that is a transient memory, until it releases by the generator to the blocks' network. Operation software gives the provider the ability of generation, "e.g., mining" to include transaction to the chain.

(Figure 12)

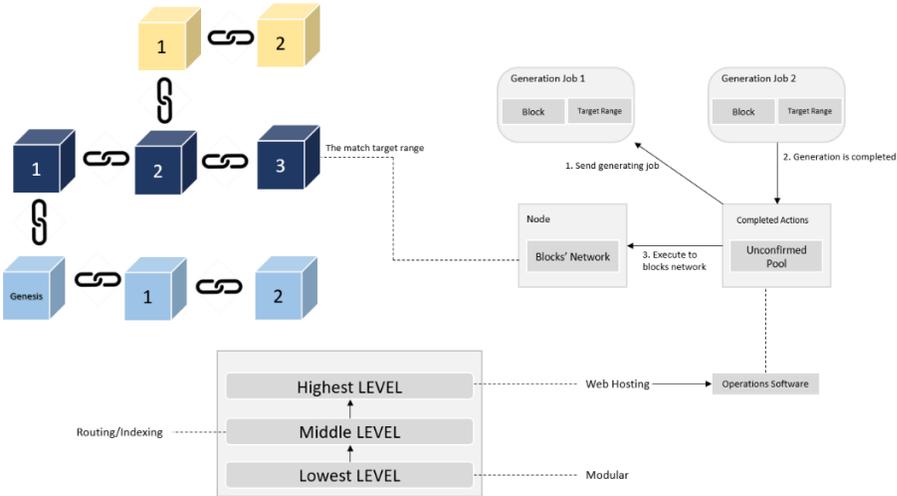


Figure 12 Highest-level's Process (Generation)

Webservers could require a pre-access authentication by obtaining a real-time authentication hash from clients, where the client will send a hash from the original document that proving his/her identity via a real-time optical ID reader to the host. Thus, the host node uses this hash compare it with the required input fields that entered by the user. This option is available to webservers that the real identity of user is their first priority such as banks.

Furthermore, if an operation was activated and took a place in the Operation Chain via generator, a unique number will be given in order to distinguish the generated blocks in the blocks network from others. Also, it used as reference for participants identity inside the

blocks' network. Operation Identification Number (OIN) will be refers to that unique number. However, the operation contains a modified condition to manage certain variables, such as the LHost "IPs" that are used for the web server, and the category target that the generator must select appropriately to find an appropriate type of array in the blocks' network that matches the type of transaction which is used for network storage order.

Over and above, after a provider included a block into the network, a client could verify that block integrity in the network at any time, since it will be immutable conformation block that has a reference to user public key. Additionally, ordinary nodes who were responsible of generating that block into the chain is also responsible to verify the integrity of that block if accurate or not after completion. Therefore, user can send back Invalidation request to the provider, which in this case will generate a new block inside the Invalidation Chain to indicates to that block as invalid. [These terms are discussed in more detail in chapter 3]

2.9 Clauses of concession:

It applies to the influencers' nodes in the network only where it enables only known members to occupy these types of nodes (operation, administration, or storage nodes) via smart contract. Furthermore, the chain division that provided via the structure of blocks' network allows difference characteristic for each class (We will explain this later in Chapter 3); thus, the ability to establish a smart contract for each level could be attainable. Therefore, the clauses of concession could be applying to each level extraordinarily.

The following are some obligations that every influencer node must follow regarding the position level of that node; first of all, members cannot occupy more than an influencer node

under one private key which means from the ordinary node a member should determine to turn into administrator or generator and however two cannot be considered together. Secondly, the range of frequencies within a given band for transmitting packages is a consider with the stable availability for administration nodes. [25] Therefore, all ordinary nodes can upgrade to generator nodes once the standers of distribution of web hosting are obeyed. Apart from that, not all ordinary nodes can become administrators. Additionally, each level is authorized to generate in its target range only without interference. For example, the software of the middle level cannot create blocks that out of its range “Class D” and vice versa for the highest level. Finally, all evidence that use to verify identity in a smart contract will execute under zero-knowledge proof that made between the platform and the users.

Chapter 3 Blocks' Network

3.0 Introduction to Blocks' Network:

Secure Hash Algorithm 512 (SHA512) is the main hash function algorithm that uses by blocks' network, due to its numerous ranges of hashes that it can produce. Therefore, the network will benefit from that massive range of the possibilities in the way of organizing the distributed ledgers of the network.

Blocks' network technology (blockchain-based) uses a multi-dimensional hash in a certain sense of block generation in order to obtain division in the network blocks. Consequently, the multi-dimensional hash is generating blocks in a shape that seems to have a network appearance (Figure 13), compare it with the blockchain that appears to have a sequential form (i.e., chain). Therefore, the structure of blocks' network has 16 categories, each category has its blocks of chain and all chains bind together as a network. Based on that, the ability of sorting block in the network will become more systematic. Also, achieving the ability to control the behavior for each chain separately. Blocks' network uses a Proof-of-Generation (PoG) protocol in order to include a block to the network.

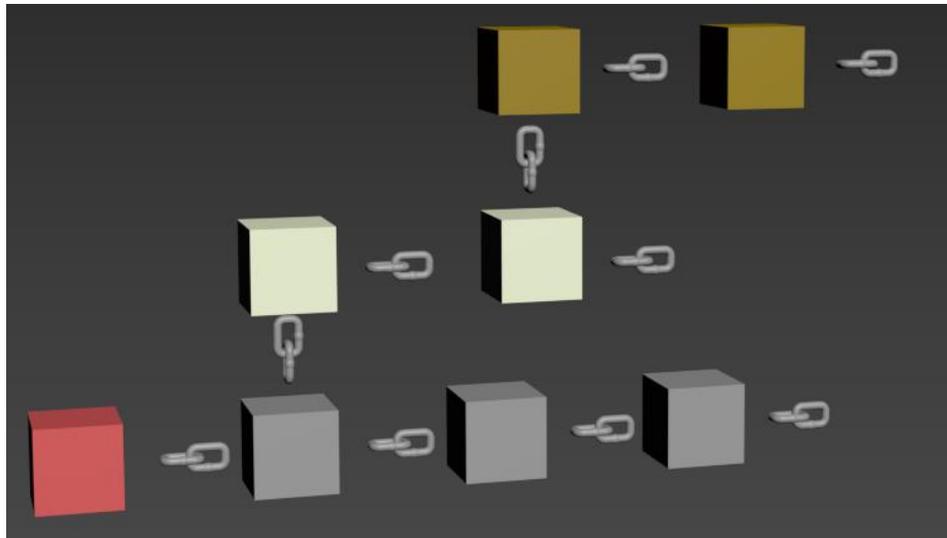


Figure 13 Blocks' Network

The procedure of using PoG is to include each block to its concerned chain via trusted generators, where chains are linked to classes of the purpose of discrimination. Class A is the primary storage of the network where all transactions that implemented through the highest and lowest levels mutually are store at this class. Therefore, clients and generators who have an influence on extending this class, which derives from supply and demand; this class has a high rate of movement. Other classes are defined as the hub chains which means they are holding the primary chains types of the network that play the most essential rule in a way that controls the network's behavior; those classes have a moderate rate of movement.

Moreover, the network running on peer-to-peer network and hence each node will become active node once it occupies a block in appointed level inside the network; a certain functionality will be given to each node under precise conduct depending on its possession inside the system. Further, PoG intends to take the generation process to the minimum levels of difficulty to find the target of a block readily. Moreover, blocks' network uses a post-

generation procedure that is an alternative to the consensus protocol that uses in blockchain technology.

3.1 Memory Pool:

Memory pool retains transactions that completed via generators to include them into a block and transmit that block to the network; each completed block will be assigned to an Operation Identification Number (OIN) independently. Therefore, each group of transactions in the memory pool is identified by their generator individually for the purpose of generation; thus, generators are in charge of generating transactions that under their OIN only. Furthermore, the memory pool observes timelines for all unconfirmed transactions in its perimeter. The timeline is used for detaching unconfirmed transactions that not been executed from its original generator under different purposes at a specific time; thus, allow other generators to have control over blocks that outside of that given timeframe. Moreover, there is a subsection of memory pool that is using to hold blocks, which means all unconfirmed transactions that grouped to a block will be in a hold, waiting to be transmitted to the network.

3.2 Stagnation Mode:

The stagnation mode is a restraint control process that utilizes to dominance the conduct of generation; however, to generate a block to an appointed category, the hash of the last block on the chain is needed as the previous hash input for the current block that wanted to be added. Therefore, when the hash of the last block in the network is selected via a generator to try to find a solution for that unconfirmed block, the operation identification number OIN that assign to that generator will hold the last block hash and prevent other operations from generating on it. Therefore, the last block on the chain will decline multiple

OINs to use its hash simultaneously. If so, this is deemed to be an overlap error in the network. Once the hash of the last block from the network is occupied by a certain OIN that will apply stagnation mode to all other operations until the current operation finds a solution and include the block entirely to the network. Knowing that the blocks' network is sort by categories, that means the process of generation is allowing 16 different operations to generate independently at the same time, at different chains. For all that, the process of manage the generation is implementing under Waiting List Management protocol.

3.3 Operations Waiting List Management:

It is the procedure for arranging the generation process throughout operations blocks sequentially to give generating preferences for each operation. The method of implementing the waiting list management protocol is to help in implanting the flexibility as well as achieving high generation productivity. The protocol takes into account some aspects such as the maximum waiting time, backlog of operations, operation entry time, operation throughput-rate, and operation memory pool size. In addition to that, the protocol's analysis arrangement could be identified and analyzed via OIN by perusing the quantity status inside the memory pool for each operation node. The circle measures the protocol of waiting list management process of generation. Therefore, the interval between each circle depends on the size of operations within the waiting list with the ability to update the status per second.

3.4 Block size:

According to (sociamedia.com), each person in the world will create 1.7 MB per second by 2020, and this is showing how much the size of the digital world is growing. According to (statista.com), the number of e-commerce transactions reached 38.5 billion in 2015.

These facts should be taken to consideration in the size of the block. Therefore, if the size of

the block is considered to be around 1-15 MB this will result in excessive consumption in hash; however, there is no concern in the hashes that will be occupied since the colossal variety that SHA512 could produce, but since the blocks will be used as storage for a daily internet usage, the consumption of hashes have to be taken into consideration particularly for small size blocks. Moreover, since each operation node will work individually, making the size of block small will increase the busyness of generation, especially by those generators who have activities that higher than their counterparts. Furthermore, 100 MB will consider as the address size of a block with the willing of extending the value up to 500MB per block. However, there is a chance some participants will not achieve 100 MB in a short time compared to the other competitors which result to keep the unconfirmed transaction under hold status for a while; this will lead to latency issue. Therefore, the network address suggestion solution that will be addressed in the category section.

3.5 Difficulty scale:

In blockchain technology, the measurement of difficulty scales is based on the numbers of active mining machines inside the network to find a specific given target [26]. However, in blocks' network, the speed factor is taken as a primary element; therefore, the difficulty of generation will drop into the lowest level of complexity in order to find a target facilely where the chance to find a target is 50%. Therefore, the generation of the block will measure in millisecond per block, and not more than $\frac{1}{100}$ second will be given for interlude.

3.6 Blocks' Network Architecture:

By defining clauses of the blocks with its content of each cluster of a chain as they appear in the blocks' network; this will result in establishing multiple classes where each class will

have its constructor. Moreover, from object-oriented programming aspect, the constructor is responsible for initializing the blocks' network, by creating attribute for each chain for each class, where each class will have its own array that assigned to a category. In addition to using multiple-level inheritance feature, which allows class to inherit characteristics and features from more than one parent class [27]. (Figure 14) Furthermore, the first block in the network will be the genesis block as the case with blockchain technology. Accordingly, the construction of blocks' network will start from here, and each block will be added to its category, and the block will forward another block to a different array if it does not match with the current chain array.

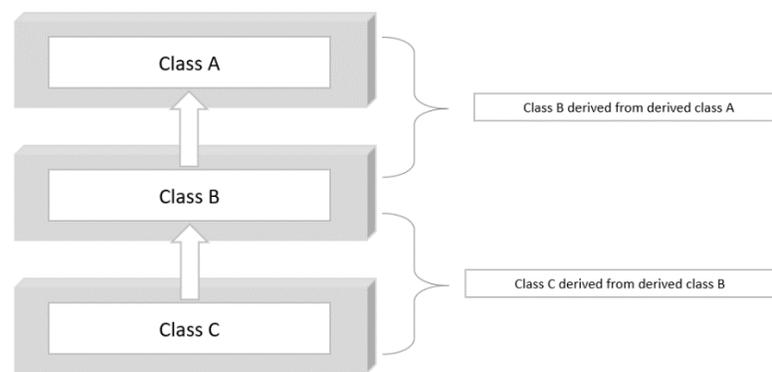


Figure 14 Multilevel Inheritance

The block will contain the following: first, the magic number that is arbitrary to distinguish the blocks from a network to another. Second, the block size which is addressed to be 100 MB. Third, the transactions that attach to the blocks. Lastly the header, which contains the OIN for distinction, version of the block, the Markle-Tree root hash, timestamp, hash of the previous block, a random number (e.g., Nonce), and finally the target type. [28]

3.7 Consensus protocol:

In the blockchain, the consensus protocol is an essential factor that is used upon consensus agreement in a way to make the network as accurate as it should be in order to give the network reliability. However, Proof-of-Work is used in some DLTs to obtain the network's precision for distribution system; thus, Proof-of-Work is used to slow all member down from generating too fast in order to control the network creation pattern. This is because Proof-of-Work takes members and makes them work collectively to find a specific target to include a block into the network. As a result of that, there is a chance two or more of members find a block's target at the same time which results in a fork in the network. The fork happened out-side the main chain, in the miner's side, when miners find a solution to a block, they add it to a grouped of the completed block that they have completed (if it exists). Then, one of those chains from the miners' side has to be considered by the community members as the continuance part of the main network chain. So, the deceleration factor that creates by the PoW is an essential factor for members to enhance their decision of making the network stability. The choice is made by considering the longest chain from all miners' side as well as accuracy for each block in each chain. However, the process of achieving this will take a while, resulting in the issues of scalability and latency. In addition, the difficulty of finding a target is requiring an enormous amount of computing power that could be obtained from a supercomputer ASIC (e.g., mining machine) which is consuming a lot of electricity that is very expensive to keep the network safe.

Proof of work is used in some platforms; however, these networks have limited functionality, which means they have a specific service to offer in their network for their members. For example, the Bitcoin network is offering only financial operations (e.g.,

network for digital currency); thus, this network is limited to a group of people who interesting in investing in that cryptocurrency or exchanging cryptocurrency for various purpose. The number of transactions per day in the blockchain network is 373,209 transaction [29]. Comparing that number of transactions with the internet's transactions number, which could be estimated in billions. Therefore, there is a weak probability that using the consensus protocol procedure will succeed to keep a high data flow network (e.g., internet network) cooperative, due to the massive amount of data that the internet generates per second.

3.8 Proof-of- Generation:

Proof of generation is utilizing via the network to increase the productivity of generation. Therefore, the crucial factors of proof of generation are each block most have OIN that refer to generator identity on the platform, and the digital signature. Consequently, the PoG mechanism is conferring the trust of its generators in the network. However, generators cannot reach this stage if they unauthenticated; thus, the trust is granted in advance until proven otherwise.

Moreover, the mechanism of the PoG is not about competitiveness between network's members to get a reward (which is the first case for generating in PoW), is about how to create more blocks to keep the internet distributed while maintaining accuracy. PoG introduce a concept "everyone's a winner." It helps network's members to avoid competition and focusing on working together. Since the difficulty of generation has a chance of %50 for each time generator searching for a target, which means the target should at a range of 15^{128} .

Finally, the generation procedure has two types; firstly, the standard generation type where it controls by the influencer's nodes depending on their position in the network — secondly, automated generators type, where it controls by platform's software. The automated generator is using to generate block for users to assign members' position in the network upon their request where these options are pre-configured options, and each option has been set to its target by the software.

3.9 Coping protocol:

The coping protocol is an action that use to put generated blocks under surveillance by its requestor to verify if that block is accurate or not. In logic theory, almost everywhere, a client is responsible for checking and verifying the integrity of an object after completion. Whenever a mistake has been found, the client will re-request correction. For example, if a school hired a student to be a grader, it is implied that the student has the capacity to verify other's works, there is no need for the grader to return to the professor in order of checking the grades, this will increase productivity. However, if the grader makes any mistakes, the student may voice complaints on the grader's mistake. One the mistake is identified then the grader can go back and change the grade and this the case with blocks' network. The platform trusts the generators to do their job. However, the platform has a post-generated option, which is a step that will consider if the block that included in the chain was inaccurate. The person who requested action from a server is responsible for that generation in the network, which the one is responsible for verifying the integrity of the block. In a case that block does not match the authentic demand, the client has to send an Invalid request to the generator. Therefore, the generator will link that request as an input for the inaccurate block, and then transmit it to the Invalidation Chain.

Moreover, accumulation in the number of invalid requests at provider-side for whatever the reason may be such as execution rejection via generator or unavailability, that will result on displaying a permanent notification to any users that access that generator webserver until invalid requests are release to the network. Additionally, the accumulation of invalid requests will cause the packets to not be forwarded to it via administrator-nodes , which will result in inaccessibility to that webserver for the lowest level.

3.10 Category method for generation

The engineering development of the category's phase has been addressed in order to increase the efficiency and ability to control the behavior of generating blocks; by sorting blocks into various scales that will make each category has a unique behavior. The behavior of the core code of generation should create distinctive functionally to each hash category; thus, it will be going to bits of help to distinguish blocks from others. Differently, blockchain technology has one chain in its appearance, and each block takes the previous block hash to generate the next block. However, changing a specific group of blocks in blockchain to give them a diffident characteristics behavior than other blocks that is something could not be accomplished; therefore, the changes should be applying to the whole blocks in the network.

In Blocks' network, each block obtains its uniqueness via Multi-Dimensional Hash Production that is using to confer the block with the ability of recognizing each hash input that it received; Furthermore, each block will take the previous block hash and persist generating new blocks that will be at the same category range, once a block it receives a new category hash type that different to its current streamline type, it will generate that

hash's block to a distinct dimension. This could be achieved by referencing an input entry to an output that has a different array [30].

3.11 Target Mechanism:

SHA512 can generate 16^{128} or (2^{512}) hashes; thus, it generates from the SHA-512, 16 independent categories in serials numbers that sequential which it starts from the first digit in hexadecimal order. For example, 0000 - 0FFF is one range of a category, and 1000 – 1FFF is the second category range and so on. $((16^{128}) \div 16)$ is the number of hashes possibilities we can obtain if 16 different categories are placed in the network, where each category will have a range of 15^{128} . So, by taking all users' daily actions and turn them into categories, the network will get organize and effective, and most importantly is give each range a unique behavior. By way of illustration, an average CPUs with 2.0 GHz could carry around two thousand million cycles per second [31] we can use this power at one category to increase the speed instead of using the power to check the whole network. This helps increase the rate of looking-up via content 16 times faster.

Additionally, the generation becomes also faster since the wide variety of number to find for each target. Accordingly, our chance to find a solution is very high. From an experiment, it will not take more than one millisecond to find a target. Hence, the addressed CPU will generate approximately 1000 block per seconds in this theory. The efficiency of generation could increase to more than 1000 blocks per second if the generators use a high-performance CPU.

3.11.1 Find a target:

The generator has to set the target block with its match from the table; (if the $T \geq 0 \mid \leq F$) (Figure 15).

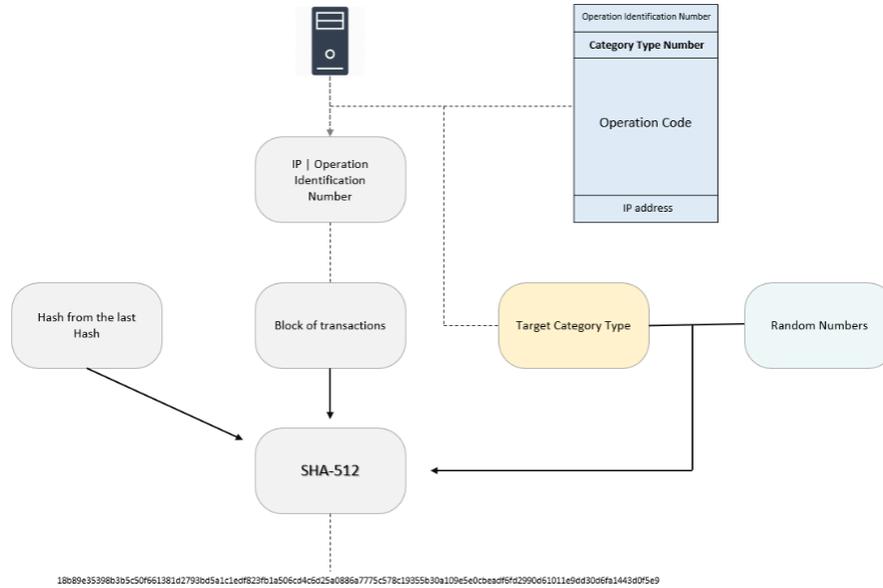


Figure 15 Target Procedure

3.12 Implementation:

In the start-up of the network, the genesis block will take any input that it receives from the generator in order to generate a new block in the chain. For instance, the genesis block has no previous hash which is equal to zeros, and there is a new block that wanted to be added to the network that has B Type Category, the method of generation will take the previous hash (in this case genesis block) and try to find a target that produce a hash of the concerned category (in this case is B Type). Upon completion, the network generates a hash that start with B (e.g. B12AF9.....). Furthermore, if the next process of generation of a block has the same range of category (e.g. B00012....) it will be included in the same range by taking the hash of “B12AF9.....” as the previous hash block of “B00012....”; therefore, it will continue in generating within the same range.

However, if a new block has been set to a different target category “4 Type Category” that unlike the current category range; the process of generation will take the last block in the chain “B00012....” as a previous hash and then start guessing randomly till it achieves the new concerned category, then forward the new hash to a different direction that reference to a new array.

The block itself has functionality to generate multi-dimensional hash which means that hashes with same category will run sequentially, while any disruption to that consecutive chain will be routed to a new array. Therefore, the new directed chain will have the same function of the previous chain in the method of generation with new behavior (as required) until a new hash category interrupts that chain and so forth.

However, moving to a new array does not mean the end point to the previous chain. Therefore, the network will have 16 different categories that are independent from each other but actually they all have a link point. Moreover, the core factor of Multi-Dimensional Hash Production is given the ability to have control over generated blocks inside the network without manipulation; however, going back in the chain to change a block that something could not be accomplished which is similar to the blockchain technology. Therefore, if any block has been tampered with that will affect the whole chain (Figure 16).

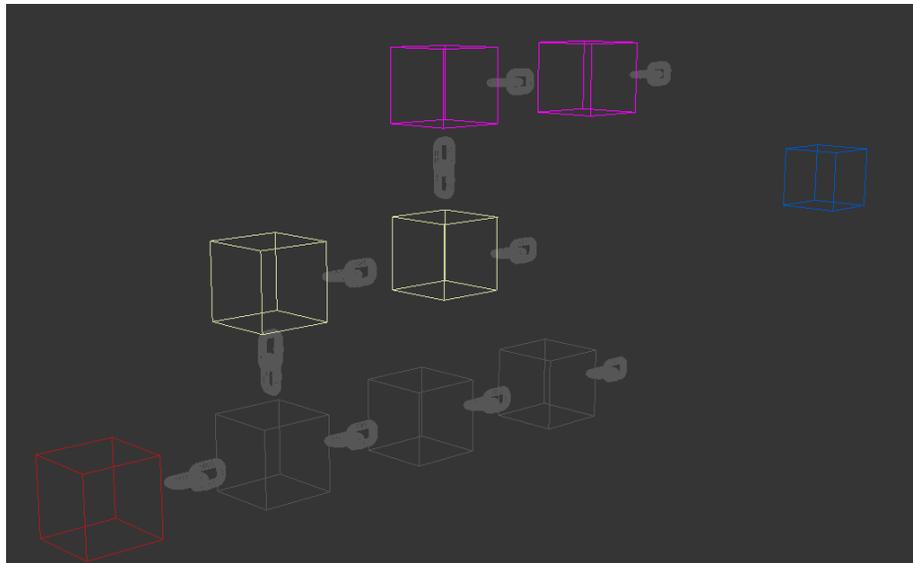


Figure 16 Blocks' Network Architecture

Blocks' network has 16 independent categories, 15 of them are running as consecutive blocks of chains, and one category is running differently "Invalidation Category." That means an Invalidation block does not need to run serially as a chain since it generated upon demand. Therefore, each Invalidation block will require the previous hash block as input to the desired block in order to mark it as invalid, then upon completion, the Invalidation block cannot be taken as the previous hash.

3.13 Categories Table:

The following table is about how categories are divided.

Table 1 Categories Table

Class Type	Category Name	Category Number	Target Range
A	Type – Finance	0	0 16 ¹²⁷
	Type – Medicine	1	1 16 ¹²⁷
	Type – Manufacturing	2	2 16 ¹²⁷
	Type – Governance	3	3 16 ¹²⁷
	Type – Education	4	4 16 ¹²⁷
	Type – Other	5	5 16 ¹²⁷
	Type – not set yet	6	6 16 ¹²⁷
	Type – not set yet	7	7 16 ¹²⁷
	Type – not set yet	8	8 16 ¹²⁷
	Type – not set yet	9	9 16 ¹²⁷
B	Type – Foundation	A	A 16 ¹²⁷
C	Type – Storage	B	B 16 ¹²⁷
	Type – Administration	C	C 16 ¹²⁷
	Type – Operation	D	D 16 ¹²⁷
D	Type – Index	E	E 16 ¹²⁷
E	Type – Invalidation	F	F 16 ¹²⁷

3.14 The properties of Categories:

The classes are delineating the type of each category. There are various types of classification that clarify the implementation to each type of category.

3.14.1 Class A

Class A contains the storage categories of the network. The categories in this class are manage by the webhost's (i.e. generator); thus, all actions that occur between ordinary nodes (i.e. client) and operation node (i.e. host node) will be forward to these ranges' categories in this class under generator privilege. The type of each category reflects the type of the service that provided via the host.

3.14.2 *B, C, D, and E Classes*

All categories at these classes are defined as the hub chains of the network where the blocks that generated under each category will represent a specific status. Class B is holding the management chains where these chains play important roles for the purpose of security and distribution.

i. Foundation category

Foundation category is responsible on the registration phase of all members at all levels in the network, where each member will have its own block store at this chain. The Foundation category is a chain of blocks that run in a link of sequential blocks where all members' information such as the private keys and all public keys that associate to a private key are store there.

Furthermore, the Foundation Chain is the basis block for each user, that because it is the first block that require via platform in order to access the network; blocks at this category could be accomplish when participates join the network via lowest level software where it allocates a block to each member individually.

Moreover, this chain is uses for the purpose of authentication that by obtaining an input then compare it with its match from this chain in order to grant access. This chain is confidential which means all data within a block will be store under hash function for comparison in addition to encrypt the hash result.

Foundation chain is does not store any plaintext instead storing hashes of the password. Despite that fact, encrypt the hashes of Foundation Chain will increase the security to the maximum extent. However, the speed factor should be taken into consideration because

some cryptographic algorithms take some time to complete encryption and decryption. Therefore, AES encryption is reliable in terms of speed. For example, an average CPU can encrypt 1 GB within 0.634 seconds, where a size of private key will be equal to 12.7KB [32].

ii. Administration category

Administration category is accountable on registering members under a default smart contract that build-in via administration software in order to give these nodes admin's privileges within the network's perimeter. This chain is responsible to store smart contracts of members to make them officially custodians on particular tasks. Administration nodes are responsible on routing process in additional to indexing management. For instance, the crawler protocol is applying by these nodes where administrators do not have the knowledge about the input final destination. Therefore, crawler architecture is used to scan all hosts webs through the Operation Chain in order to decide to who the input should be forward. Hence, based on this knowledge the index table will be updated for all administration node where it stores in the index chain.

iii. Operation category

The Operation category is using to register all host nodes in the highest level of the platform (e.g. service provider). Thus, beside the core code of the host server, the actual stakeholder's identity is essential to complete all the aspect of the smart contract that related to the operation level where the smart contract will state that a particular ordinarily node has become officially a web hosting node. Therefore, this will store into Operation Chain in order to issue Operation Identification Number (OIN) that generate via the block that later will used for block generation.

iv. Storage category

Notably, operation and administration nodes have the capacity of storing operational content of the system which means that the ability of storing the primary composition of the system that is used for the management of the network such as protocols or algorithms depending on their possession. However, storage category is dedicated to storage all ledgers only; in addition to share and update the distributed hash table among the influences' nodes. The storage phase is obtainable without restrictions to all members via smart contract. The smart contract is using to clarify that a particular candidate become a custodian on a certain information inside the network. The procedure of achieving that when a user declares his/her desire in becoming a custodian on the information from the lowest-level's operation software; where it executes a smart contract that contains a timeline (i.e. period of contract), storage space, and a root hash of all downloading files that candidate will obtain. The availability of storage node is taking into consideration in addition to the file's integrities. Any violation to the previous, will end the obligation between the platform and the candidate. Further, candidates must verify the storage space that they willing to offer to the platform; thus, the platform could estimate the offering space in order to be rewarded. Moreover, be an extra space should be assigned on the actual offered space which is going to be use for the purpose of load balancing.

v. Index Category

Index category stores the contents and IPs that related to the hosts' nodes of the highest level for the purpose of routing redistribution configuration in addition to looking-up. It is used various methods for web indexing and routing indexing (e.g. routing information base). This category uses and mangers by administrators' nodes where it used as reference which

nodes are looking for keywords and metadata that match with the provided inputs from lowest level (e.g. client side). Any failure in the routing process will feed this chain continuously with updates to perform better in the next time.

vi. Invalidation Category

The blocks in the network are immutable and any manipulation to a certain information in a block will effect the whole chain, this is will provide the network with the accuracy and precision. Further, blocks' network is assigning highly reliable members at the level of generation and hence the platform grants the trust to generators in advance; imprecision in generation always leads to a reputation risk. Moreover, it is challenging task to keep all blocks in the network fully accurate. Therefore, giving certain levels of the network the permission of generation is not adequate. The consensus protocol is could be handy factor to increase the accuracy; however, blocks' network takes the speed matter into high consideration, and yet there is always a chance for human mistakes to be occurred.

Invalidation category is introduced to carry the above issue, and therefore, it is playing an important rule among all chains to maintain a high precision public storage. It is a post-generation step, that responsible for invalidating generated blocks. It works by taking a hash of a certain block that is required to become invalid as the previous hash for an F-Type block. Once a target has been found, it will generate the new block in a different array without any effect on the chain in which it exists.

Furthermore, the Invalidation block has a different characteristic than other block; it does not need to run sequentially as chain that because it executed upon client demand. Therefore, each block can be executed individually and the previous hash that required by the Invalidation block is the block that wanted to be invalidated.

Additionally, a digital signature is an essential requirement to claim an Invalidation request that can be accomplish upon client demand. Thus, a digital signature must be included in the block as an input in order to avoid the misuse of Invalidation block, then the rectification statement in addition to the OIN with the client's ID (e.g. public key).

3.15 Interconnectedness:

Heretofore, nodes were described based on their possessions and their effectiveness over the network. The following table illustration the control lines (Figure 17).

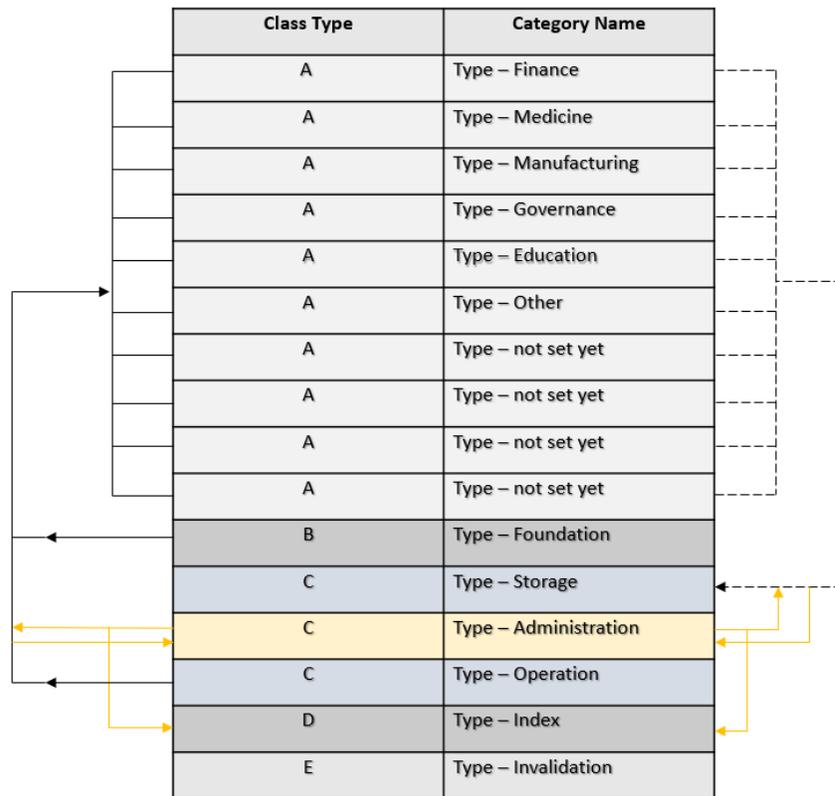


Figure 17 Blocks' Network chains (control-lines)

The interaction between ordinary nodes (e.g., members from the Foundation Chain) and generators nodes (e.g., members from the Operation Chain) will send to storage categories

(e.g., Class A). While administration nodes (e.g., members from administration chain) will have control over data flow between ordinary and generators and hence store improvement at index chain. Lastly, the invalidation category is control by Operation and Administration members.

Chapter 4 Process Optimization and Additional Chains

4.0 Pure Peer-to-Peer (Ordinary Nodes):

Heretofore, the above nodes were described as identified/reliable nodes, with each node at a given level being able to control the network partially. In addition, the distributed routing and hashing tables are an auxiliary factor in the schema.

Since the network run on P2P, that's mean all peers can communicate with each other off-chain; for instance, via VoIP, file sharing, or decentralized application (e.g., DApp). An example on DApp is a peer-to-peer chat protocol that used by Ethereum called Whisper.

However, the ordinary nodes (e.g., lowest level members) run on a pure P2P network which means without administration nodes or login server; ordinary nodes will not have adequate details to communicate with another peer.

4.1.0 Ethereum Whisper

Ethereum Platform runs two stacks beside the decentralized chatting protocol "Whisper". Consensus Stack, which is used as a consensus layer where it uses a computational power. Swarm, which is the storage layer and it used IPFS (Interplanetary File System). Lastly, Whisper stack that provides a messaging layer [33].

Whisper is the message layer which is an application that allows communication between member at the same layer. It uses Pitch-Black Darkness, according to (github.com) there is a difference between encryption and darkness, where the darkness describes as a method to increase the difficulty to provably the author of the message. Therefore, it means the difficulty of tracing individual is impossible since the message will continuously route to all neighbor nodes where or not that node is the recipient. Therefore, it uses PoW in order to

eliminate spammer and it used data distribution to prevent DDoS attack on effecting the status of the data.

4.1.1 VoIP and file sharing

In P2P network nodes cannot determine other nodes in order of file sharing as the case with client-server where the user has the knowledge about a practical destination via URL. Therefore, there some challenges related to peer-to-peer discovery. NAT Traversal is an issue since there are two NAT that needs to be traversed in two firewalls. Asymmetrical bandwidth is also an issue where content is going to flow from node to others, which means the upstream bandwidth of the node will be taxed. Optimization of P2P network is essential, where there can be either structured and unstructured, many of P2P are unstructured which means ad-hoc that is the network is not planned or designed or hierarchical it simply evolved as a function of who registers and where and the server the registrar may understand where those hosts are, therefore when we try to do file transfer, for example, it may not be obvious which are the logical nodes to actively sources for the files we're trying to transfer.

4.1.2 Skype Protocol:

Skype is a peer-to-peer VoIP client that was released in August 2003. “Skype claims that it can work almost seamlessly across NAT, firewalls, and better sound quality than other VoIP clients. It encrypts party-to-party calls, and stores user information in a decentralized manner. Skype also supports instant messaging and conferences. [34]”

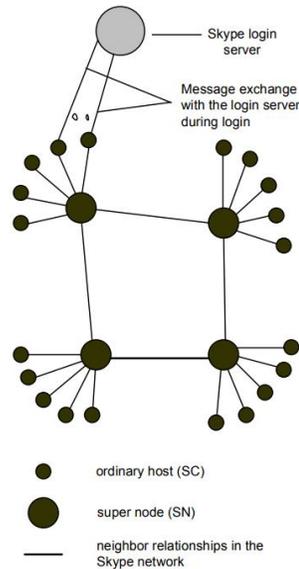


Figure 18 Skype Node structure (from slideshare.net)

Furthermore, each node has to register to the Skype login server, which is a centralized node (Figure 18). However, this is the only stage in which a client is treated with a centralized system. After that all communication between nodes is done via super node. Super nodes are ordinary nodes who upgraded via skype in order to make these nodes handle routing positions between the nodes.

4.1.3 *Tox (protocol)*

Tox is a peer-to-peer instant-messaging and video-calling protocol that offers end-to-end encryption. A reference implementation of the protocol is published as free and open-source software. More on that [35].

4.1.4 *BitTorrent*

BitTorrent is a peer-to-peer network that used for sharing file over the internet where members' devices are the files sources. Therefore, when a peer wants to download a file

through the network, the content of the data will be searched among peer. It uses a server called tracker to track which peers have which files available [36].

4.2 Redirection chain and DApp chain “Additional Chains”

Many methods have been discovered above in different ways of using P2P for communication. However, the blocks’ network intends to implement a suitable protocol that can be used to obtain a secure and efficient connection while maintaining decentralization.

The Call Block software in the lowest level (i.e., Client-side) intends to use Universal Plug and Play (UPnP) which is a set of networking protocols that use for ports’ configuration to make all peers who run the software to communicate regularly [37]. Moreover, Call Block is an extensible functional code protocol, which means it always can be updateable to merge a new P2P communication protocol to it. Therefore, with the ability of extensibility that provided via Call Block application together with the characteristics of Block’s network, we can reach the following:

4.2.1 Redirection chain “Additional Chain”

Redirection chain has been considered for the purpose of peers’ discovery, which it is acting as a decentralized address book that is distributed. Moreover, it managed by ordinary nodes in order of storing addresses. Accordingly, it will result to create a unique number that generated via the block for each node. The uniqueness of the number is given from the index number of the block which users can exchange which easy to memorize. Additionally, users can register new addresses that associate with their private key as the case with other P2P networks, where addresses are using for file-sharing or voice over IP when users

register to a server. Consequently, this chain is acting as a login server (i.e., registration) where the ledgers are distributed publicly.

4.2.2 DApp chain “Additional Chain”

Decentralized Application chain (or DApp chain) has been considered to store developers’ smart contracts to activate his/her node to run the communication protocol under an absolute privilege. Moreover, these nodes are highly reliable comparable with nodes in the Middle and the Highest levels that described previously. Let us assume that there was a smart contract has just occupied a place at the chain (i.e., DApp chain) which means this smart contract contained a strict communication protocol that provided via collaborator. All communication through this protocol should be off the chain. Moreover, any node who communicate with communication protocol is independent of the network in some way, which means when an ordinary node (i.e., client) wants to connect to that protocol; it will stand in the middle between the DApp node and the network as a whole (Figure 19).

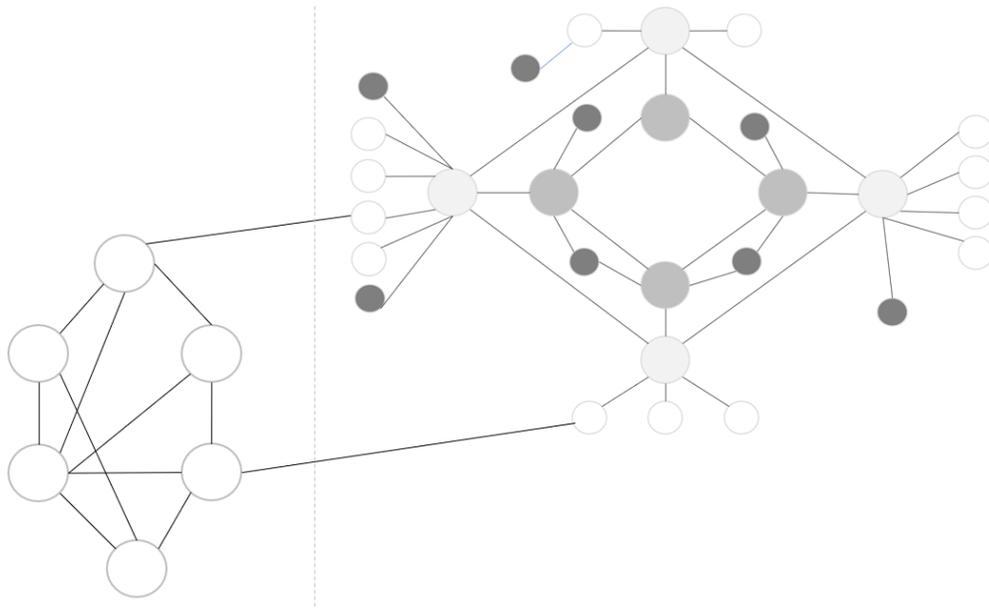


Figure 19 Pure P2P Nodes alongside the Blocks' Network Nodes

For example, when a developer/s launch a communication protocol (e.g., TOX protocol); the provider's node can upgrade other nodes under their control to a supernode. Therefore, establishing a pure P2P from the ordinary nodes that could be run parallelly beside the blocks' network architecture.

4.3 Cryptocurrency “Additional Chain”

The generators' work was described far from any cryptocurrency, which generators' work was described as a voluntary joint effort to make the Internet decentralized. However, a payment system should be introduced that allows for the imposition of bonuses for the volunteers who made the Internet decentralized through the cryptocurrency that the platform will adopt based on the current cryptocurrency standards association.

Moreover, “cryptocurrency is a type of decentralized digital currency. Cryptocurrencies utilize blockchain ledgers to record and validate transactions. [39]” A cryptocurrency is a number that generated via cryptography for security, which is linked to an address where

blockchain is responsible for storing these digital coins that associated with each address. Moreover, many of blockchain's platform relies on the mechanism of consensus, which maintains the legitimacy, accuracy in addition to the value of the cryptocurrency from forks' issues aspects. Further, those platforms create cryptocurrency by mining where the Bitcoin software (in the case of Bitcoin Network) is used to produce a digital currency every time a block was mined.

Blocks' network intends to include a cryptocurrency chain that works under cryptographic algorithms to increase the security of digital assets. The production of this chain will be controlled via all influencers' nodes in the network where they will work together for mining a block at a definite time, and then the generated cryptocurrency will be shared as a due reward.

4.4 Escalating Difficulty “Invalidation Category”

The system craves to interpolate additional rigid property which gives the uniqueness to this category. Therefore, the system envisions to append Escalating Difficulty to the Invalidation Category to have a different return statement which means whenever this category is executed, the operation software for an OIN that responsible on executing Invalidation block will return to a distinct statement that can be accomplished under “if condition” where the difficulty of execution next time will be increase for that operation-node software. Categorically, by granting a behavior to the software, which interprets as “if the F value has been reached, then execute the difficulty statement that was pre-set for that operation ID.”

Moreover, Invalidation execution occurs when an inaccurate block was added to the network, and if the generator issued a block into an inappropriate chain. Ultimately, administration nodes are responsible for monitoring Invalidation blocks.

Chapter 5 Storage Mechanism for Distributed System

5.0 Storage mechanism (DHT bases)

The storage is peer-to-peer network where members pool together their disk space to create a shared global memory. The storage of blocks' network is based on DHT algorithm. Furthermore, the operation nodes (members from the highest level) are responsible for dataset distribution to the closest storage node (members from the storage chain) that is available at that range. The network uses storage nodes for an array structure to arrange the data evenly among storage nodes. However, storage node does not have to store a full copy of the whole data inside the network. Otherwise, the entire data in the network could be share among storage nodes' members separately under certain properties.

Thus, creating a hash table for all appointed files between operation and storage nodes where this table is distributed among its concerned nodes. The hash table use to determinate the contents that available in each node. The internet has a massive amount of data which is something cannot be storable via all nodes in the network. Therefore, DHT is using to enhances the ability of storing a huge amount of data in nodes.

5.0.1 *Preference System Mechanism*

The mechanism of preference is used to balance the massive amount of data among nodes. Therefore, the usage of consistent hashing is playing an important rule to help to solve the problem of load balancing among nodes [38]. Moreover, DHT is using to manage the mechanism of updating data in all nodes within the network; thus, the files that entered to the network do not need to be share and update via all nodes' members instated, a portion

of the network should obtain and download a certain grouped of dataset bases on preset preference.

Preference system is requiring from each storage's node to store data under a particular range, which means the closest storage' node from where that file was issued. That could be achieved via IPs configuration of the generators' operations, where it can determinate each storage node location from the issuer distance. Operations' IPs gives us better chances for an arrangement where it sets blocks bases on their locations in order to determinate the city, region, and country of each block that exists on the network in sequence to find a node at the same range. Otherwise, it takes in its consideration the closest point possible to that block range and trudges ascending until it reaches a worldwide point.

The mechanism does not rely on random distribution; it defines each node based in its own smart contract as well as to give preference, where each node is responsible for a specific predetermined type.

However, this process keeps repeating for each time nodes go through updating until nodes achieve stable status. Furthermore, the preference system provides high-organized public storage based on storage chains' types as well as where these data should be stored, thereby enhancing data transfer between the nodes and the enhanced bandwidth-based routing process (Figure 20).

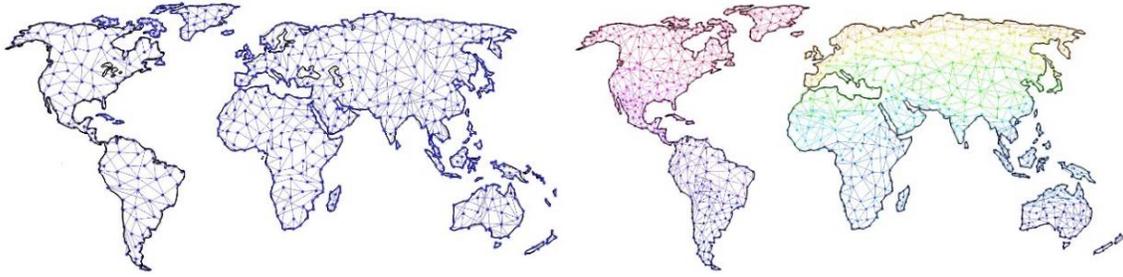


Figure 20 Distributed ledgers

Preference system Distributed ledgers

5.0.2 *The replication ratio*

The ratio of replication is a supporting factor that controls the distribution of data that sent through the operation nodes to storage nodes. The ratio of replication leverages IPs for the purpose of locating nodes locus; therefore, there should be no more than a ratio of 2 to 10 of duplicate files to each node at the same bond. The ratio is gradually increased depending on the coefficient of proportionality in the axial scalability, where the bonds that holding nodes has unstable connection. Furthermore, at the network perimeter level, there is should be a rational percentage of nodes that have a full copy of the ledger; therefore, the smart contract that inscribed in the storage-chain's blocks will refer to these nodes as the backup nodes.

Chapter 6 Conclusions and Future Research

6.0 Conclusion

Blocks' network is a systematic approach to a decentralized internet development plan and if implemented in an appropriate manner, will enhance the experience of using the internet, shifting attention away from concerns about privacy and the protocols of consensus.

6.1 Future research:

6.1.0 AI algorithms:

The AI's layer will take into account where it will be placed at the middle level in the architecture of the platform. Therefore, artificial intelligence will be created to handle all traffic between users and hosts without human intervention; which in turn will be using the steps of predictive modeling (Figure 21) to increase the statistics of the predict outcomes.

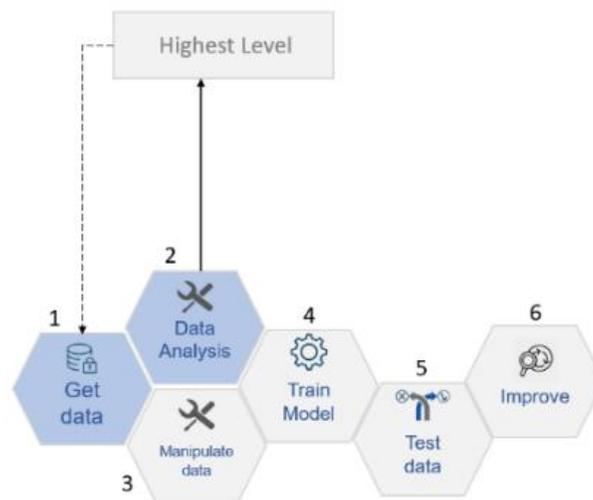


Figure 21 predictive modeling

It gets and stores all its resources in/from a decentralized system (i.e., Distributed Autonomous Organizations “DAO”) by giving it the support to obtain the ability to solve complex equations by feeding it from different trends. The middle level is an intelligence brain in the middle between users and service providers. Popular ML algorithms: Neural Networks, Deep Learning, Support vector machines, and random forest [40].

References

- [1] Kaushal, R. (2016). Bitcoin: First Decentralized Payment System. *International Journal Of Engineering And Computer Science*.
- [2] Nabilou, H. (2019). How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency. SSRN Electronic Journal.
- [3] The Balance. (2019). Blockchain Technology Can Change How We Vote. [online] Available at: <https://www.thebalance.com/how-the-blockchain-will-change-how-we-vote-4012008>
- [4] Medium. (2019). What is the difference between decentralized and distributed systems? [online] Available at: <https://medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems>
- [5] Cbsnews.com. (2019). WhatsApp co-founder: "I sold my users' privacy" to Facebook. [online] Available at: <https://www.cbsnews.com/news/brian-acton-whatsapp-on-facebook-forbes-interview-today-2018-09-26/>
- [6] dropboxforum.com. (2019). Lost files. [online] Available at: <https://www.dropboxforum.com/t5/Dropbox/Lost-files/idip/104075>.
- [7] Clock, B. (2019). Bitcoin Clock: 2020 Bitcoin Halving Countdown. [online] Bitcoinclock.com. Available at: <https://www.bitcoinclock.com/#current-bitcoin-block-reward>

- [8] Medium. (2019). End to end Bitcoin Blockchain with examples - Onur Deler - Medium. [online] Available at: <https://medium.com/@onurdeler/end-to-end-bitcoin-blockchain-with-examples>
- [9] Forbes.com. (2019). Tracing Illegal Activity Through The Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes. [online] Available at: <https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes>
- [10] Investopedia. (2019). What Determines the Price of 1 Bitcoin? [online] Available at: <https://www.investopedia.com/tech/what-determines-value-1-bitcoin/> [Accessed 22 Jul. 2019].
- [11] Bitcointalk.org. (2019). Is this possible that a transaction my never get confirmed ?. [online] Available at: <https://bitcointalk.org/index.php?topic=1879862.0>
- [12] Lightning.network.paper. (2019). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. [online] Available at: <https://lightning.network/lightning-network-paper.pdf>
- [13] Reddit.com. (2019). Lightning network usability - Being always online ? : Bitcoin. [online] Available at: <https://www.reddit.com/r/Bitcoin/comments/877ho4/>
- [14] claffy, k. (2012). Border gateway protocol (BGP) and traceroute data workshop report. ACM SIGCOMM Computer Communication Review, 42(3), p.28.
- [15] SearchNetworking. (2019). What is BGP (Border Gateway Protocol)? - Definition from WhatIs.com. [online] Available at: <https://searchnetworking.techtarget.com/definition/BGP-Border-Gateway-Protocol>

- [16] We Are All Satoshi. "Rick Reacts to the Lightning Network" Online video clip. YouTube. YouTube, Feb 18, 2019
- [17] Goodin, Dan, and Utc. "Russian-Controlled Telecom Hijacks Financial Services' Internet Traffic." Ars Technica, 27 Apr. 2017
- [18] Raval, Tony. "KYC And AML: What All Banks Need To Know." Forbes, Forbes Magazine, 11 Oct. 2018
- [19] Dwork, Cynthia; Naor, Moni (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". CRYPTO'92: Lecture Notes in Computer Science No. 740. Springer: 139–147.
- [20] [ndy](#) (2010, March 10). Why is p2p web hosting not widely used? [Blog post]. Retrieved from <https://stackoverflow.com/questions/737560/why-is-p2p-web-hosting-not-widely-used>
- [21] SDxCentral. (2019). What is the Definition of Overlay Networking (SDN Overlay)?. [online] Available at: <https://www.sdxcentral.com/networking/sdn/definitions/what-is-overlay-networking/> [Accessed 22 Jul. 2019].
- [22] freecodecamp.org. (2019). Write safer and cleaner code by leveraging the power of "Immutability". [online] Available at: <https://www.freecodecamp.org/news/write-safer-and-cleaner-code-by-leveraging-the-power-of-immutability-7862df04b7b6>.
- [23] Peervpn.net. (2019). PeerVPN - the open source peer-to-peer VPN. [online] Available at: <https://peervpn.net/> [Accessed 22 Jul. 2019].

[24] Yang, Jidian, et al. "A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks." *Sensors* (Basel, Switzerland), MDPI, 25 Feb. 2019, www.ncbi.nlm.nih.gov/pmc/articles/PMC6412336/.

[25] "Supernode in Peer -to-Peer Networks-A Tale of Multipurpose Solution." Medium, MoonX, 11 May 2019, medium.com/@moonxfamily/supernode-in-peer-to-peer-networks-a-tale-of-multipurpose-solution-78b960eba44e.

[26] En.bitcoin.it. (2019). Proof of work - Bitcoin. [online] Available at: https://en.bitcoin.it/wiki/Proof_of_work

[27] UCF. Multiple Inheritance and Multilevel Inheritance, UCF, webcourses.ucf.edu/courses/1249560/pages/multiple-inheritance-and-multilevel-inheritance.

[28] "Block." Block - Bitcoin, Bitcoin, en.bitcoin.it/wiki/Block

[29] "Confirmed Transactions Per Day." Blockchain.com, www.blockchain.com/en/charts/n-transactions

[30] Szabgab. "Multi Dimensional Hashes in Perl." Perl Maven, Gabor Szabo, perlmaven.com/multi-dimensional-hashes.

[31] BBC Bitesize. (2019). The CPU and the fetch-execute cycle. [online] Available at: <https://www.bbc.com/bitesize/guides/zws8d2p/revision/2>.

[32] ShabirmeanShabirmean 11811 silver badge44 bronze badges, and BivBiv 8. "How Long Does a Good AES Encryption Take?" Cryptography Stack Exchange, crypto.stackexchange.com/questions/44927/how-long-does-a-good-aes-encryption-take.

- [33] Ethereum, ethereum. "Ethereum/Wiki." GitHub, Ethereum, github.com/ethereum/wiki/wiki/White-Paper.
- [34] columbia.edu. (2019). An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. [online] Available at: http://www1.cs.columbia.edu/~salman/publications/skype1_4.pdf
- [35] Toxcore Documentation". GitHub. Retrieved 7 November 2015.
- [36] " Bittorrent.com. (2019). BitTorrent (BTT) White Paper. [online] Available at: https://www.bittorrent.com/btt/btt-docs/BitTorrent_Token_Whitepaper.pdf
- [37] NYC Mesh Docs. (2019). Supernode Architecture - NYC Mesh Docs. [online] Available at: <https://docs.nycmesh.net/networking/supernode-architecture/>
- [38] Ietf.org. (2019). Load balancing models for DHTbased Peer-to-Peer Networks. [online] Available at: <https://www.ietf.org/proceedings/76/slides/p2psip-2.pdf> [Accessed 22 Jul. 2019].
- [39] Bankrate. (2019). Cryptocurrency Definition. [online] Available at: <https://www.bankrate.com/glossary/c/cryptocurrency/>.
- [40] sebastianraschka. (2019). Machine Learning FAQ. [online] Available at: <https://sebastianraschka.com/faq/docs/deeplearn-vs-svm-randomforest.html>.

Additional Bibliography

[1] "What Is Proof of Work? (PoW): Lisk Academy." Lisk, lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-work.

[2] "What Is a Peer to Peer Network?" Lisk, lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-a-peer-to-peer-network.

[3] Konheim, Alan (2010). "7. HASHING FOR STORAGE: DATA MANAGEMENT". Hashing in Computer Science: Fifty Years of Slicing and Dicing. Wiley-Interscience. ISBN 9780470344736.

[4] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A (1996). Handbook of Applied Cryptography. CRC Press. ISBN 978-0849385230.

[5] Paul, Eliza (12 September 2017). "What is Digital Signature- How it works, Benefits, Objectives, Concept". EMP Trust HR.

[6] Pdos.csail.mit.edu. (2019). [online] Available at:
https://pdos.csail.mit.edu/papers/chord:sigcomm01/chord_sigcomm.pdf

[7] Cs.cmu.edu. (2019). [online] Available at: <https://www.cs.cmu.edu/~dga/15-744/S07/lectures/16-dht.pdf> [Accessed 22 Jul. 2019].

[8] Medium. (2019). Distributed Hash Tables And Why They Are Better Than Blockchain For Exchanging Health Records. [online] Available at:
https://medium.com/@michael.dufel_10220/distributed-hash-tables-and-why-they-are-better-than-blockchain-for-exchanging-health-records-d469534cc2a5.

- [9] Crypto.stanford.edu. (2019). *Cryptography - Zero-Knowledge Proofs*. [online] Available at: <https://crypto.stanford.edu/pbc/notes/crypto/zk.html>
- [10] CoinDesk. (2019). *What is the Difference Between Public and Permissioned Blockchains?* - CoinDesk. [online] Available at: <https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains>.
- [11] Blockstack.org. (2019). *Blockstack Technical Whitepaper v 2.0*. [online] Available at: <https://blockstack.org/whitepaper.pdf>
- [12] Hackernoon.com. (2019). *Creating Truly Modular Code with No Dependencies* - By Konrad Gadzinowski. [online] Available at: <https://hackernoon.com/creating-truly-modular-code-with-no-dependencies-16f8f784d4a6>.
- [13] Kothagal, K. (n.d.). *Modular programming in Java 9*.
- [14] Bhargavan, K., Fournet, C. and Gordon, A. (2010). Modular verification of security protocol code by typing. *ACM SIGPLAN Notices*, 45(1), p.445.
- [15] Benmccormick.org. (2019). [online] Available at: <https://benmccormick.org/2016/06/04/what-are-mutable-and-immutable-data-structures-2>
- [16] Hackernoon.com. (2019). *5 Benefits of Immutable Objects Worth Considering for Your Next Project* - By. [online] Available at: <https://hackernoon.com/5-benefits-of-immutable-objects-worth-considering-for-your-next-project-f98e7e85b6ac>.

- [17] Ieeexplore.ieee.org. (2019). HIERAS: a DHT based hierarchical P2P routing algorithm - IEEE Conference Publication. [online] Available at:
<https://ieeexplore.ieee.org/abstract/document/1240580/>
- [18] Mdpi.com. (2019). A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks. [online] Available at: <https://www.mdpi.com/1424-8220/19/4/970/pdf>
- [19] Oak.cs.ucla.edu. (2019). *Searching the Web*. [online] Available at:
<https://oak.cs.ucla.edu/~cho/papers/cho-toit01.pdf>
- [20] M. (2019). *OPEN CONNECTIVITY FOUNDATION (OCF)*. [online] Open Connectivity Foundation (OCF). Available at: <https://openconnectivity.org/>
- [21] TheStartupFounder.com. (2019). Blockchain: What are Nodes and SuperNodes? - TheStartupFounder.com. [online] Available at:
<https://www.thestartupfounder.com/blockchain-what-are-nodes-and-supernodes/>
- [22] ieeexplore-ieee-org. (2019). An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function. [online] Available at: <https://ieeexplore-ieee-org.ezproxy.libproxy.db.erau.edu/document/6781303> [Accessed 22 Jul. 2019].
- [23] Cisco Meraki. (2019). Site-to-site VPN Settings. [online] Available at:
https://documentation.meraki.com/MX/Site-to-site_VPN/Site-to-site_VPN_Settings.