ECOChain

White Paper

Version 2.0

--- Reshaping Ecological Consensus with Blockchain ---

Produced by the ECOC Foundation

ecoc.io

Contents

01 Application Value of Blockchain

A long time ago, people regarded the blockchain as a ledger on a peer-to-peer network. All data usage will be recorded on "blocks". Blocks are cryptographically created and connected to form a chain structure and broadcasted to all nodes on the network. The nodes form a consensus through a protocol mechanism. Node members can view all records without any restriction (permission less) , which guarantees the transparency property. On the other hand, any single node cannot easily control and change the data of the entire network.

Overview Of Blockchain

In 2008, Satoshi Nakamoto published the paper “Bitcoin: A Peer-to-Peer Electronic Cash System.” The article proposes that it is possible of a new type of electronic payment system to be crated. This system is based on cryptographic principles rather than credibility (trust less) so that any two parties who have reached an agreement can directly make payments without the participation of a third-party intermediary.

The paper spawned the first type of decentralised virtual currency, Bitcoin, marking a major step forward in the monetary system of human society. Using bitcoin, no third party is needed for transactions

In Satoshi Nakamoto’s original paper, the words “block” and “chain” were used separately, and when they were widely used, they were collectively referred to as block-chain. Word: “Blockchain.” In August 2014, Bitcoin’s blockchain file size reached 20 gigabytes. It was proposed in Satoshi’s white paper that Satoshi created the first block, the “ Genesis Block”. Bitcoin then entered a period of rapid development and eventually led to the birth of the blockchain.

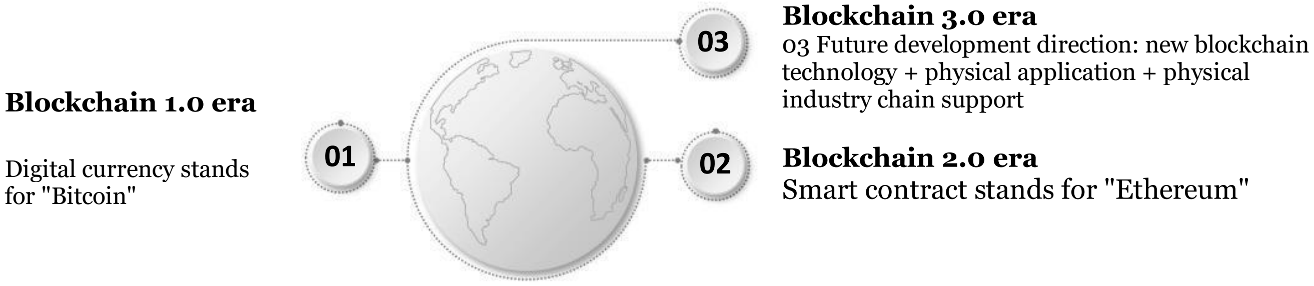
In the following years, the blockchain became the core component of electronic money Bitcoin: as a public ledger for all transactions. By using a peer-to-peer network and UTXO model, the blockchain database can be autonomously managed. The blockchain invented for Bitcoin made it the first digital currency to solve the problem of every day’s financial transactions. Bitcoin’s design has become a source of inspiration for the other applications. The blockchain architecture was first applied to Bitcoin as a solution to make databases secure without the need centralised entities.

In a narrow sense, a blockchain is a chain data structure that combines data blocks in a sequential manner in a chronological order, and it is a cryptographically-immutable and unforgeable distributed ledger. In a broad sense, blockchain technology uses the blockchain data structure to verify and store data, uses distributed node consensus algorithms to generate and update data, uses cryptography to ensure the security of data transmission and access, and uses automated scripting. A new type of distributed infrastructure and computing paradigm in which smart contracts composed of code are used to program and manipulate data.

Development History of Blockchain Technology

Blockchain is a decentralized core security technology. Using decentralized data security technology can improve data security reduce data maintenance costs and promote the intelligent development of organizations. In the future, it will be used in banking, auditing ,the Internet of Things, notarization and copyright. It is widely used in management and other fields and is given an "overweight" rating.

There are many weak points in traditional market centralized data, and blockchain technology is expected to become a saviour. The concentration of data in the era of big data and cloud computing is relatively high, which leads to excessive manipulation power of the cloud centre, increasing the risk of collective data leakage, and all data passing through the cloud, with low efficiency and high cost. Blockchain technology can achieve decentralized storage of data on the premise of ensuring that the content is not tampered with, and fundamentally solve the above problems. Bitcoin supported by the blockchain has been running securely for ten years, which is enough to verify the reliability of the technology. Beyond Bitcoin, the blockchain will embrace the wider world of finance, culture, and society in the future.



Blockchain 1.0 era

Digital currency stands for "Bitcoin"

Blockchain 2.0 era

Smart contract stands for "Ethereum"

Blockchain 3.0 era

03 Future development direction: new blockchain technology + physical application + physical industry chain support

At present, the blockchain is still mainly used in currency (blockchain 1.0). At present, the technologies mastered by many enterprises have been applied to the financial field beyond blockchain (blockchain 2.0), and even beyond social notarization and intelligence in the financial field (block chain 3.0). Overseas traditional industry giants have been deploying blockchain since 2014: major banks around the world have established a blockchain alliance, Deloitte and other well-known accounting firms have developed blockchain auditing technologies, NASDAQ has first launched blockchain securities genealogical members. Blockchain has specific market opportunities in the following areas:

Advantage 1: Blockchain can reduce trust risk

Blockchain technology is open source and transparent. Participants in the system can know the operating rules of the system, verify the authenticity and integrity of the contents of the ledger and the history of the ledger structure, and ensure that the data and history of related information are reliable. The result is to improving the traceability of the system and reducing the trust risk of the system.

Advantage 2: Survivability of data

In case of fully Decentralized applications, or even for simple individual transactions, when the owner (deployer of smart contracts) goes out of business the data stay on ledger (blockchain) forever, in contrast of using a traditional database, when a company stops operating all the data all lost and operations shut down. So blockchain guarantees the **Survivability of data**. In fully decentralized applications the operation can continue even when the company cease to exist. This fact forms an expectation for end users: whatever is going to happen, their data are safe (and in some cases operation will not stop). That adds value, attracting more users for the product and increasing the loyalty. So a company can benefit using the blockchain because of the survivability of data (and in some cases the product itself).

Advantage 3: Blockchain can reduce costs

Immutability of the ledger, combined with digital signing brings on table properties that can make the operation possible even without forcing identification of the users. When regulations do not demand some kind of proof of physical identity (KYC) the applications can operate completely anonymous. Irreversibility of transactions (immutability) and anonymous ID verification (digital signing based on cryptography) in many cases can completely skip the verification costs and other costs as well (for example escrow costs).

Advantage 4: Blockchain can prevent network failures and attacks

The current chaotic and inefficient management status and the opacity of centralized information have greatly increased the risks of management and exchange. The blockchain has many distributed nodes and computer servers on the point-to-point network to support it. If any part fails, it will not affect the overall operation, and each node keeps a copy of the blockchain data. The built-in smart contract of the blockchain is the key core circulation business, which has extremely high reliability and fault tolerance.

Advantage 5: Blockchain can realize a "programmable society"

Since all files or information data can be embodied in the form of codes or ledgers, by setting the data processing program on the blockchain, the exchange may be realized on the blockchain. For example, smart contracts can write the basic information of the users into the protocol to ensure the automatic execution of the code.

Records stored on the blockchain have the characteristics of transparency, traceability, and immutability. Any record, once written to the blockchain, is permanently stored and cannot be tampered with. The records of people anywhere can be tracked and queried.

02 ECOChain --- Distributed Ecological Public Chain

2.1 What is ECOChain?

ECOChain, also known as decentralized public chain, is a permission-less, secure, scalable blockchain. It carries all advantages of a public blockchain: immutability, transparency, transaction capability. Additionally, embedding a virtual machine (VM), it makes it a platform to host Turing complete code (smart contracts). It is the bridge that connects applied technology and real-world markets based on blockchain . It brings a brand-new solution for the Economy and businesses. ECOChain is a truly fast, and economically friendly decentralized public chain that uses Ethereum smart contracts executed in a virtual machine(EVM). Initiated by a well-known international blockchain team it uses blockchain technology as a basis to explore the integration of the global economic market and the blockchain world, and build a global decentralized distributed ecosystem.

2.2 Mission of ECOChain

In the development of the future economic market system, ECO has its own mission explores fully the advantages of the blockchain, uses the traditional economic market system, reshapes the new economic ecosystem, and achieves a good, trustworthy, and fast financially and friendly decentralized ecosystem.

At the same time it lets more people having a secure and high-quality distributed security network, enables the healthy and trustworthy development and incentives of the market to be realized through the ECOChain. This is also the ECOChain team's mission.

2.3 Unique Characteristics of ECOChain

At the technical level, the ECO chain is built using blockchain technology (communication protocols, cryptography etc.) to ensure that there are no obstacles to the connection between users. It has the following unique advantages:

1. **High Performance**

(1) Users can experience a high transaction speed

The ECOChain takes advantage of long known communication protocols to maximize their benefits. Various model analysis and pressure testing shoes that it can support up to 650 transactions per second (see yellow paper for details).

(2) An efficient adaptive consensus algorithm is a blockchain protocol provided by ECOC. This adaptive algorithm guarantees efficient and concurrent processing of the public chain most of the time and accurately handles the problem of node errors and network connection problems.

(3) Fast transaction confirmation. ECOC uses an efficient and adaptive consensus algorithm to ensure the completion of transactions, that is, transaction confirmations, and to optimize other properties in the transaction confirmation process, such as cryptographic secure signature algorithms and ledger storage methods.

(4) For storage, ECOC supports local database storage, file system storage and cloud storage. Local storage achieves hot and cold separation, database storage uses a database and table model, and cloud storage supports expansion in accordance with cloud cluster rules.

2. High Speed Access

ECOC is based on the principle of minimizing the development circle of business applications, meeting the existing development knowledge of programmers and promoting the deployment and maintenance of the it with high security. So it has achieved a lot of compatibility in terms of user business development, deployment, and security. The ecosystem provides many clients (different wallet types) and tools (SDKs), for users and developers who can choose how they connect to blockchain having a good UI experience, high security, lower costs and fast speed. SPV (simple verification payments) clients can be also used , making possible many operation without the need to run a full node but also not use a third-party service (trust less operation).

3. High Security

(1) Reliable and consistent storage

ECOC guarantees that service requests will not be tampered with during the transmission process through asymmetric encryption and digital signatures (public cryptography) and stores the data of each node through a consensus mechanism. For stored data records, self-tests within nodes and quasi-real-time multi-node data verification are used to ensure that stored data records cannot be modified.

(2) User Privacy and Transaction Confidentiality

The user real identity and blockchain public address in ECOC are isolated. Public addresses are pseudonymous. Associated user information cannot be obtained from the record store of each node. The user information store has multiple layers of protection, such as permission control, access authentication and encrypted storage. Users with higher transaction confidentiality can also choose a transaction- independent mechanism. Each transaction of the same user is mapped to a different address on the blockchain, thus ensuring that multiple records of the user cannot be obtained on the ledger (untraceability).

(3) Security Key Management System

In the ECOC key management solution, key security and user account delegation functions are provided to ensure the security of keys. The key safe uses user information to encrypt the private keys. The key safe cannot be accessed under normal business processes. CLI and GUI tools exist to save the keys offline (cold storage). Hierarchical deterministic key generation and restore are also possible. The user, if he wishes he can use a hardware wallet. Additionally, inside consensus algorithm the staker can co-sign using different accounts from the same wallet when it forms the block (Coinbase transactions). This enhances the security for the staker.

(4) Operation Efficiency

The ECOChain builds GUI and CLI tools for metrics (analytics) of data. Depending on the need of the application and business Dapp, smart contract's storage and blockchain data can be tested, inspected, filtered or customized for producing any kind of report. Also, enhanced compiler exists for code compilation. Additional tools for security analysis, cost and performance of the smart contracts exist. All these belong to ECO chain's ecosystem.

The ECOChain provides universal and efficient information collection components, which are deployed at the business layer, consensus node layer, and ledger storage layer. The information collection component integrates the system information of the machine (such as CPU, memory, hard disk, and network status) and the node usage status (such as node visits, time spent, node health, etc.) and business usage (business visits, success rate, time-consuming distribution, etc.) are displayed on the monitoring interface in real time to facilitate management of the entire system.

2.4 Ecosystem expansion of ECOChain

With the continuous improvements, expansions and development of the ECOChain ecosystem more and more use cases can be solved, and the ECO chain will increase in usability, which will bring higher circulation and unavoidably higher value.

Use case 1: Trading Market Mall

The economic transaction market mall not only brings convenience to people, but also brings huge traffic. The ECO chain will build a decentralized online economic market trading platform, with a variety of items displayed on these platforms.

The buyer and seller agree on a smart contract on the ECOChain platform. The buyer puts a certain amount of tokens on the blockchain. After the seller confirms that the item is received correctly, the token on the blockchain will be automatically sent to the seller's account.

Otherwise, if the buyer has not received the item or has not confirmed it, according to the agreement of the smart contract, the token on the blockchain will be returned to the buyer's account. For some large- value transactions, multiple protection measures are required. Artificial intelligence technology can be used to protect the property rights of items that are recorded on the chain to avoid contract breach between the two parties. A certain amount of deposit (guarantee) is required. This type of buying and selling process is not only secure, but also protects the rights of both buyers and sellers.

Use case 2: Cross Chain Transactions and Interoperability

There are many flavours of blockchains today with different architecture, properties and goals. Some will survive, others not. But is it possible to connect them in a decentralized way ?

Decentralized connection of chains (cross-chaining) adds value to the connected chains and to blockchain industry sector in general. Applications can be used universally; the network effect increases their usability and decentralization (trust less property) is preserved.

ECOChain is already working on this. Atomic swaps code is under implementation as open source and the repository is published on GitHub (GitHub source code) . The first target is Ethereum, because it is a big platform with a rich ecosystem. Other platform will follow. Atomic swaps are asset swapping in a completely decentralized way, meaning coin or token swapping between different chains take place without a need of third parties or custodians.

In the future, interoperability between ECOChain and other chains that run virtual machines will be implemented. A yellow paper on cross-chaining is also underway.

Use case 3: Separate Protocol (Consensus) for Oracles

The virtual machine is a deterministic state machine. It is isolated from the outer world. That means that it can't access any data from outside. The only way to get the data is as input from someone who has access to write to the smart contract (through contract functions). The entities who have access to these functions can make the VM code useful. A usual example for this is exchange rates data. This is how the term "oracle" is born.

An entity that has special access to the smart contract and feeds it periodically with real world data is an oracle. The term stems probably form the fact that this entity (usually a server) is highly trusted from the users of the application. That way the decentralized applications can operate for real world use cases.

The above reveals a serious problem, the so called "oracle problem". The oracle must be highly **trusted**. But this defeats the whole logic and philosophy of decentralized apps

and blockchain. If you need trust, then better implement a solution the traditional way (centralized). This problem can be solved with a system of oracles. A special protocol must be used to handle byzantine oracles, so the consensus algorithm must be byzantine. This system runs independently of the blockchain and ensures that the data feeding takes place in a decentralized way.
ECOChain already finished research on this. There is a yellow paper for the oracles which is published.

The paper explains how the system and consensus works and contains mathematical proof for the soundness of the protocol. Because it is independent of blockchain it can be used by anyone who wants to run an oracle system.

Use Case 4: Application of Proof of Location (PoL)

Use case 3 can be used to support PoL. Proof of Location is the problem that an entity must prove to others about its real (physical) location. GPS system provides information to someone to self-compute its location with a small error. The problem is that this GPS information can't be used to convince others. So the whole problem is how someone can prove to any other that he doesn't fake its location at a given time.

The most usual case of PoL is application on the logistic chain. About critical products, such as food and drugs, the problem is even more urgent. There other use cases, also.

There is no general solution for PoL. Fortunately, use cases are specific and location bound. At these places special hardware can be used from different entities. The oracle system we referred as use case 3 can be used here to provide PoL in a completely trust less way. Hardware, oracle consensus and a mesh network at the point of interests can provide a viable solution.

A whitepaper for PoL is under way.

03 ECOChain System Technology

The ECOChain core is in the heart of the ecosystem. The architecture focuses on decentralization and security, but also allows the maximum transaction speed that hardware and telecommunication technology allows today. Before designing architecture , analysis based on mathematics was considered and concepts got proved, under some assumptions, to be certain that the final product will be solid. All ecosystem is based on the core, and this is true for every blockchain. A weak architecture can attract attackers and decrease trust. A technological solid product based on sound financial fundamentals is the best option for real world uses cases and applications. That's why in our analysis we consider the cost factor for both dApps, users and network preserves (people running a node).

The most important concepts are included in the yellow paper that is published on Ecochain's website. A part of it is republished here.

3.1 Transaction Speed

Of interest for a chain which plans to host many dApps is the capacity of the chain; that is, how many transaction per second (TpS) it can receive. Here we must separate two variables: the maximum TpS and the sustainable TpS, that is, the average TpS in the long run which can keep the chain usable.

Let’s analyse the maximum TpS first. We are going to show on which parameters it depends and what restrictions exist in real world and put a limit to the transaction speed.

Maximum TPS

Now, let:
h be the number of hops
b be the bandwidth in bits per second
s be the maximum block size in bytes
n be the number of nodes
c be the number of outbound connections for each node
ts be the desired transaction speed (TpS)
l be the average transaction size in bytes

First, we are going to compute the number of hops required until all the nodes get the data. Because the number of connections is fixed, c , and because each node that has the data (block) broadcasts to the other nodes that it is connected, the flow is following a ”snowball” effect. This, in mathematics is a geometric progression:

$$a_h = a_0 r^{h-1}$$

where ah is the number of nodes that are informed after h – 1 hopes. Here we assume that a0 = 1,because a0 is the node who forms (wins) the block and is ready to start broadcasting. The total informed nodes n after the h hops will be

$$\sum \alpha_h = \frac{\alpha_0(1-c^{h)}}{1-c} \Rightarrow \sum \alpha_h = \frac{1-c^h}{1-c} \quad (1)$$

and for all nodes to be informed the hopes h can be computed from the inequality

$\sum \alpha_h \geq n$

$$\sum \alpha_h \geq n \Longrightarrow \frac{1-c^h}{1-c} \geq n \Leftrightarrow \frac{c^h-1}{c-1} \geq n$$

and because $c > 1 \Leftrightarrow c - 1 > 0$ we have:

$$\frac{c^h-1}{c-1} \geq n \wedge c > 1 \Longrightarrow c^h \geq n(c-1)+1 \Leftrightarrow \log_c(nc-n+1) \Leftrightarrow$$

$$\Leftrightarrow h \geq \log_c(nc-n+1)$$

We must keep in mind that the number of hops h is an integer and also the first hop is actually happening for the term a1 → a2 of the geometric progression.

In Short, $h = \lfloor h \rfloor + 1 - 1 \Leftrightarrow h = \lfloor h \rfloor \Longrightarrow h = \lfloor \log_c(nc - n + 1) \rfloor$. So we finally have

$$h = \lfloor \log_c(nc - n + 1) \rfloor \quad (2)$$

We know h now , so we can continue to find what is the lowest bandwidth requirement b to achieve the desired transaction speed ts, where ts is the number of maximum transactions per second. Here we assume that the maximum block sizes is very large compared to block header, that is $\frac{bl}{s} \approx 0$,where bl is the length of the block header. Obviously, the maximum transactions per block are $tr \approx \frac{s}{l}$. Let’s define *bt* as the target(average) block creation time in seconds.

We have:

$$tr \approx \frac{s}{l}$$

The propagation time required for one ”push”, that is, one hop is :

Ti = Tl + Tp

where Ti is the total time in seconds required for each hop to complete , Tl is the latency and Tp the time needed to broadcast the block data. This time depends on the upload bandwidth of broadcasters and the download bandwidth of the receivers. Latency mainly depends on the location of the nodes (physical topology of the network). Let’s assume for now that for large block size data, Tp is significantly larger than Tl, in other words assume that Ti ≈ Tp. This is not very accurate, but it will help the simplification of analysis.

For a hop *hi* the maximum time $T_i \approx T_p = 8\frac{s}{b}$ because a byte equals 8 bits and *s* is measured in bytes. The total propagation time , let’s say *tT* is

$$\mathrm{t}_{\mathcal{T}} = \sum \mathrm{T}_{i} \approx \sum \mathrm{T}_{\mathcal{P}} = \sum 8\frac{\mathcal{S}}{\mathcal{b}} = \sum \frac{s}{b}$$

We can make one more assumption here, that each hop *hi* needs the same propagation time, because all the conditions are the same (average bandwidth, block size to be propagated). Consequently

$$\mathrm{t}_{\mathcal{T}} \approx 8\sum_{i=1}^{h} \frac{s}{b} = 8h\frac{s}{b}$$

We have already proved that h = log c (nc − n + 1) , so

$$\mathrm{t}_{\mathcal{T}} \approx 8h\frac{s}{b} \approx \frac{8s\left\lfloor \log_{c}(nc - n + 1)\right\rfloor}{b} \quad (3)$$

Computing the above approximation was not hard at all, but is beneficial: It clearly shows that the total time tT depends on the maximum block size s , the number of connections c , the number of nodes n and the average network speed (bandwidth) b. So it is NOT depending on the block creation time bt. But bt sets an obvious limitation:

$$tT < bt \; (4)$$

And is very easy to see why. The nodes should have enough time to ”get” (download) the block data. So , while it is tolerable for some nodes to get the data from previous blocks while new ones are created, this is not safe to carry on for long; total propagation time should be lower than the average creation time of a block.

Combining (3) and (4) we get

$$\mathrm{t}_{\mathcal{T}} \approx \frac{8s\left\lfloor \log_c(nc - n + 1)\right\rfloor}{b} \Longrightarrow \mathrm{bt} > \frac{8s\left\lfloor \log_c(nc - n + 1)\right\rfloor}{b} \Leftrightarrow$$

$$\Leftrightarrow b > \frac{8s\left\lfloor \log_c(nc - n + 1)\right\rfloor}{bt} \Leftrightarrow$$

$$\Leftrightarrow b_{min} > \frac{8s\left\lfloor \log_c(nc - n + 1)\right\rfloor}{bt} \quad (5)$$

Equality (5) shows clearly the lowest bandwidth b_{min} in that the network must have to sustain a block size of size s in bytes. It is also worth noting that the propagation of data is easily scalable because there is a

logarithmic relation between the number of nodes of the network n and the number of connections c. In other words, the number of hops h(n) is O(log n). The reason of this efficiency is that the propagation is based on the gossip *protocol* [1]. Bitcoin and Ecochain follow the gossip protocol with a (default) number of connections c = 8. That can be easily seen in the code in the file **src/net.h**:

```
static const int MAX_OUTBOUND_CONNECTIONS = 8;
```

From the above we conclude that for Ecochain c = 8. As a side note, we must stress the point that any node is free to change the outbound number of connections; that is, c is not a parameter of the consensus protocol. Just changing the above line of code from 8 to any number is acceptable by the network, as it is not really detectable. For example, a node may have a high upload bandwidth and also may want to help the network, so chooses to set c to 100. Or the node is selfish or malicious and sets c to zero, not broad casting anything. In short, changing c is an easy soft fork. We can safely assume here that the vast majority of nodes are not going to change c as they don't have an incentive to do so. If the default value of c is set to a value greater than 8 that does not necessarily brings faster propagation time; there are restrictions of disk writing time when the database is committed and of CPU delay because of the needed validation time when the number of transactions is large. So Ecochain keeps c = 8 , which as we already mentioned is not restricting for the nodes; each node can change it very easily.

Let's see an example in numbers: for a maximum block size s = 4Mbytes, block time bt = 32sec, number of nodes n = 4, 000 and number of connections c = 8 the minimum network speed (bandwidth) from equation (5) should be

$$b_{min} > \frac{8s\left\lfloor log_{c}\left(nc - n + 1\right)\right\rfloor}{bt} = \frac{8 * 4000000 * \left\lfloor log_{s}\left(4000 * 8 - 4000 + 1\right)\right\rfloor}{32}\frac{bits}{sec} =$$

$$= 1000000 * \lfloor log_{8} 28001\rfloor\frac{bits}{sec} = 1000000 * \lfloor 4.92439691020751\rfloor\frac{bits}{sec} =$$

$$= 1000000 * 4\frac{bits}{sec} = 4000000 = 4Mbps$$

As we have already seen the function $b_{min}(n)$is logarithmic. So with the same parameters but with a larger number of nodes n = 30, 000 for example we have

$$b_{min} > \frac{8s\left\lfloor log_{c}\left(nc - n + 1\right)\right\rfloor}{bt} = \frac{8 * 4000000 * \left\lfloor log_{s}\left(30000 * 8 - 30000 + 1\right)\right\rfloor}{32}\frac{bits}{sec} =$$

$$= 1000000 * \lfloor log_{8} 210001\rfloor\frac{bits}{sec} = 1000000 * \lfloor 5.8933455574294\rfloor\frac{bits}{sec} =$$

$$= 1000000 * 5\frac{bits}{sec} = 5000000 = 5Mbps$$

Today's (Q4 2018) average global bandwidth is around 10Mbps. Also, we must keep in mind that as the telecommunication's technology advances the bandwidth will get higher. There is a belief that the increase in bandwidth follows Nielsen's Law [*?*], which states that global bandwidth increases around 50% every year. This prediction is somewhat optimistic, as historical data show a slower annual rate increase. But the truth is that the increase rate is significant. Consequently, even if some people think that 4Mbps or 5Mbps is marginally achievable today it must be clear that it could be easily achievable in the near future.

Let us finally compute the TpS for the above parameters. For block size s = 4MB, block time *bt* = 32*seconds* and assuming that the average length of a transaction in bytes is *l* ≈200 we get a maximum transaction speed of

$$ts \geq \frac{tr}{bt} \approx \frac{\frac{s}{l}}{bt} = \frac{s}{l * bt} \approx \frac{4 * 10^6}{200 * 32} = \frac{10^6}{200 * 8} = \frac{10^6}{1600} \approx 625$$

So maximum TpS *ts* ≈ 625 transactions/second. This is the speed in theory. In practice, we measured around 560 transactions per second. The tests were run on a low number of nodes (n = 100) on AWS cloud. A real network is far less ideal as there may be greater deviation of bandwidth, more often disconnects etc. For this reason the network protocol has built-in capability to avoid long timeouts. If a node doesn't get a response or receives very slow connection for longer than 2 seconds it disconnects and connects to another node; that way it avoids slow propagation time.

The reader must keep in mind that all the above is an approximation; we conclude these results under certain assumptions to simplify the analysis. For example, we assumed that the block header size is negligible compared to its body size (which is true). We also assumed that the latency time Tl is very short compared to the time to transmit the data T_p. This deserves more attention. The protocol in use is the TCP, which demands the well-known ”three-way handshake” (SYN,SYN-ACK,ACK). We assume here that the node connections are trans-continental, so the latency is usually between 80–120*ms* (milliseconds). Some connections would be intercontinental. For these few transactions the latency would be around 200ms. If the network has technical problems (very often connections and disconnections of nodes) the latency will be greater, which may play a minor role in the final TpS result. For a network with large number of nodes a large-scale latency (high latency infecting many nodes) is unprovable; in practise it is not possible for most nodes to have connection problems. The third assumption we made is the average transaction size. The most common transaction has a vin and two vouts (one receiver and the ”change” that return to the owner). This is usually 191 bytes long. But there will surely be transactions with more vouts. There is also the case of smart contracts(for example, when a long bytecode smart contract is deployed). It is really difficult to predict the average transaction size. What is measurable is the throughput and not the transactions. If the estimation of the average transaction size of 200bytes is optimistic then TpS may be somewhat lower.

A final note why we choose a high block size limit. The maximum size of the block can be set lower in the peer's code without any problem, in fact other peers have no way to know the size limit that has been set internally in each node. In sort, a soft fork can lower the block size just changing a line inside the code of **src/ecoc/ecoc.h** file:

```
const int blockSizeLimit = 4000000 ; // block size limit
```

The opposite is NOT true. If the node wants to increase the block size limit it can really not. Just increasing the size, mining and forming a block beyond the common accepted limit will lead to rejection from the other nodes, as it violates the consensus protocol rules. In other words, increasing the block size limit demands a hard fork; that is, everyone must update their client version so the change can take effect. This is an additional reason that we initially prefer a high block size limit.

Sustainable TPS

It is time to talk about the scalability issue in the economic sense. In the previous section we analysed the technical restrictions for blockchain's capacity. In this section we are going to analyse the restrictions that the real economy sets. There are real world costs to run a full node, which grows linearly following the total size of the blockchain. The data of the public chain grow with a pace. This pace depends on average transactions per second and is measured in bytes per second. If the size's growth per unit of time is high, then three problems arise for the preservers of the chain(nodes):

(a) the initial download time may take too long
(b) much RAM is needed
(c) much storage (disk space) is needed

Let's see each of these problems closely. For (**a**), the problem is that when a node wishes to join the public chain for the first time, he must download all the data (history). If the size is very large and the node has low download speed, then it may take long time (several days) until the initial download completes.

This may discourage new nodes to join the public chain.

For (**b**), because UTXO model needs RAM linear to the transactions number, a large chain demands from the nodes a capability of high RAM (memory) usage. RAM is expensive, much more expensive than disk storage. So, considering the memory swap option, it looks natural for a node to use virtual memory (disk space as RAM). All operating systems for desktops today (Windows, Linux, Mac and all *nix systems) offer this capability. But there is a pitfall: disk is much slower than memory. This fact brings the following problem: the staker needs more time to validate a block, so he must delay some seconds before he starts minting(staking). While this is a problem in PoW protocol it does not pose a real problem in PoS if the granularity is longer than the validation time; that is, it does not put the staker in a disadvantage. We can assume that this problem , (b), given that virtual memory will be used, is equivalent with (c), which we are going to present immediately.

(c) The growth rate of chain's size depends on the actual (average) trans- action speed. For example , if the average transaction speed is 50 transactions per second, and assuming an average length of 200 bytes per transaction , then in one year the size data will by larger by (we do not count block header in the equation as it is very small compared to the body)

$$\triangle S=tps*l*t=50*200*60*60*24*365=315360000000 \text{ bytes} \approx 315Gb$$

which is a considerable amount of data. So we must find the sustainable TpS that can keep the nodes in the network, preserving decentralization. As a side node here, because it was never mentioned before, we must stress the point that for the staker to get the opportunity to mint and gain some profit he must run a full node. So a staker has an incentive to join the network running a node as far as his expected gains from minting are greater than his costs(rational economic behaviour). The costs are the hardware (basically the disk space) and the telecommunication costs. The decisive factor here is the cost of disk space. As we have already explained the RAM restriction resources can be converted to disk space resources. While we cannot predict exactly the future costs or the staker's profits - which depend on coin's price - we can try to find the connection between the chain's size growth rate with relevance to the declining costs of disk storage as technology advances. That is , we can , under some assumptions, find a cost function c(c0, y) , the value of which must be lower than the maximum acceptable cost for the staker, let's say *cmax*. Here *c0* is the cost at the time the staker joins the network and y the years after the time that the cost is c0. So our first restriction is:

$$c_{max} > c(c_0, y) \quad (6)$$

Now, let:

Cmax,i be the maximum acceptable cost for the staker *i*(let's say in USD)

C0 be the cost to run a node for at first join time (USD)

s_0 the minimum disk size for the node to run at starting year in GBytes d*c* the cost of disk storage (in USD/Gbyte)

Sy the minimum disk size for the node to run at year *y* in GBytes (*y* years after joining)
gr the growth rate of the chain (measured in GBytes/year)

Obviously, *gr* = *tps* ∗ *l* , where tps stands for average transaction speed and *l* for average transaction length. We also consider that $\frac{b_h}{b_b} \approx 0$, where b_h is the block header size and b_b the body size. Obviously, *c(c0, 0)* = *c0* by definition .
The new cost after a year for the node will be

$$c1 = c0 - \delta cy0{-}{>}y1 + \delta sy0{-}{>}y1 * dc1$$

c1 is the cost to run a node after on year of first join (in USD)
δcy0−>y1 is the declined cost because of technologic advance - that is, cost storage lowers over time. *δsy 0−>y1* is the extra chain data size after a year
dc1 the cost of disk storage (in USD/Gbyte) at y1
The new maximum accepted cost is *cmax,1* which can be higher or lower than cmax,0 as the price of the coin can be lower or the staker’s balance may be lower giving him lower expected staking rewards. We are going to symbolize the annually cost difference and maximum accepted cost difference at year y as *δcy,y−1* and *δcmaxy*, *y−1* perceptively.

The first think to notice is that stakers who have a very low balance (close to zero) do not have an economic motivation to run a full node. That is, at any time y, for a staker with a total current balance *bi*, staking reward *r per* year and an exchange rate e between the coin and USD , to run a node the following inequality appears:

$$\delta c_{y,y-1} < b_i * r * e \quad (7)$$

In plain English , the annual profit must cover the extra cost added per year. While it is clear that the profit is depending on the exchange rate e we must not conclude that is depending on the staking reward r because e is not independent from *r; e(r)* is a monotonic declining function because r creates inflation driving the exchange rate down. In other words a higher value of r does not guarantee higher profits for the staker. As a side note, *δcy,y−1* may be negative. This may seem strange at first glance; how the cost for a node can decline when the chain data increase? But if a technology breakthrough take place, the storage cost *dcy* will fall dramatically. In this case, if

$$\delta c_{y-1->y} > \delta s_{y-1->y_y} * dc_y$$

then

$$c_y = c_{y-1} - \delta c_{y-1->y1} + \delta s_{y-1->y} * dc_y \wedge \delta c_{y-1->y} > \delta s_{y-1->y_y} * dc_{y \Rightarrow}$$

$$\Rightarrow c_y < c_{y-1} \Leftrightarrow c_y - c_{y-1} < 0 \Leftrightarrow +\delta s_{y-1->y} < 0$$

So it is clear that the total cost may even decrease with the pass off time while chain size increases. In this case, even if the yearly profit decreases, but less than the cost annual reduction, it is still profitable for the staker to stay and run a full node. In short, the important factor is the annual **marginal** cost and the annual **marginal** profit from minting. By marginal here we mean the annual difference in values.

Let us be more precise. The staker does not know his future reward nor the future cost. So we are talking about the **expected** annual profit and **expected** annual cost. From the economic theory we know that for a rational economic behaviour the marginal cost should be less or at least equal to the marginal profit (after the first initial investment in equipment). So the follow inequality holds for a stakeholder:

$$M\overline{c_y} < M\overline{pr_y} \quad (8)$$

The marginal annual profit for a staker $i \ M\overline{pr_{y,i}}$ depends, as we have already seen, on his balance b_{yi} , the current exchange rate e_y and the annual staking reward *r*. On the other hand the annual marginal cost depends on the growth rate of the public chain gr and the new cost per unit of disc storage dc_y . So the above inequality transforms to

$$M\overline{c(gr, dc_y)} < Mp\overline{r(b_{y_\iota}, r, e_\iota)} \quad (9)$$

Being more analytic for $M\overline{c(gr, dc_y)}$ we have:

$$\overline{c(gr, dc_y)} = c_y - c_{y-1} \wedge c_y = c_{y-1} - \delta dc * s_{y-1} + \delta s_y * dc_y \Longrightarrow$$

$$\Longrightarrow M\overline{c(gr, dc_y)} = \delta s_y * dc_y - \delta dc * s_{y-1} \Leftrightarrow$$

$$M\overline{c(gr, dc_y)} = gr * dc_y - \delta dc * s_{y-1} \Leftrightarrow$$

gr is the growth rate of the chain, *dcy* the storage cost at year y, *δdc* is the technological cost decrease per unit storage and *sy* −1 is the storage size of the previous year. So finally we have:

$$M\overline{pr(b_{y_\iota}, r, e_\iota)} = gr * dc_y - \delta dc * s_{y-1} \quad (10)$$

For every rational staker to keep staking, that is, continue running a full node, the above inequality must hold. So his decision is based on his stake (his account balance), the exchange rate and annually reward on staking, the growth rate of the chain and the decrease cost factor of disk storage (which depends on the technology evolving). Unfortunately , we cannot make more simplifications as this may lead us to inaccurate results.

Let's see an example. Suppose that the growth of the chain was for the last year *gr* = 315Gb (like us previous example), the cost of 1Gb on the current moment (year) is dc ∗ *Sy* = $0.04 , the cost of the previous year was *dc∗Sy-1* = $0.05 and the total size of the chain the previous year was, let's say, *sy −1 = 1.5T b*. So his marginal cost for the last year is

$$M\overline{c(gr, dc_y)} \ \ = gr * \ dc_y - \ \delta dc \ * \ s_{y-1} \Leftrightarrow$$

$$M\overline{c(gr, dc_y)} \ \ = \ 315 \ Gb * \ 0.04\$/Gb - (0.05\$ - 0.04\$)\$/Gb * 1.5 \ * 1000 \Leftrightarrow$$

$$\Leftrightarrow M\overline{c(gr, dc_y)} \ \ = \ -2.4\$USD$$

In the present example we see that the extra annual cost is negative, so it is lower from the last year's cost by 2.4$ So extra profit for the last year can be lower but no more than 2.4$:

$$M\overline{pr(b_{y_\iota}, r, e_\iota)} \ > \ -2.4\$ \ \Longrightarrow \ pr_y - \ pr_{y-1} > \ -2.4\$ \ \Leftrightarrow \ pr_y + 2.4\$ > pr_{y-1}$$

Usually the marginal cost will be positive, except in the case of a great unexpected tech innovation in storage or in the case that the growth rate of the data of the chain will be too low. In any case , the extra profit should cover the extra cost.

Let as check, for the above example, the maximum cost for a staker to join the network for first time. We have cmax,0 = s0 ∗ dc0 ⇒ cmax,0 = 1.5T b ∗ 0.05USD/Gb ⇔ cm a x ,0= 1.5∗1000∗0.05USD ⇔ cm a x ,0 = 75USD ⇒ *prm* in,0 = 75USD. So his expected profit should be more than 75USD to decide running a node.

In our analysis so far, we have excluded the networking costs. This simplification makes our job simpler but more inaccurate. The truth is that for many machines the user pays for network traffic either way. In this case his network cost is zero. A typical example is a desktop user who already uses internet for his personal use or a server who is running doing various other things and has much bandwidth unused. There is also an "irrational behaviour" in real world; a staker may have enough balance to his account but decide not to run a node or the opposite, to decide running a node even if he suffers a minor loss. Also, our equations and inequalities depend on future exchange rates which are impossible to predict.

In this section we have just shown mathematically the relation between the factors who play a major role to a rational decisional if and when he will join the chain or when he will have incentive to stop running a node.

What we must keep in mind is that decentralization depends on the number of nodes, which in turn depend on the value of the coin (the higher, the more nodes join) and the storage cost decreasing rate (again, the higher the decreasing cost rate, the more nodes join). There is ”Kryder's Law” [*?*], which is not actually a law, but a prediction of the disk storage costs for the year 2020. The prediction is somewhat about 40% decreasing rate per year. Until now his prediction has been seen as overoptimistic, but the fact is that the storage cost is really decreasing, although with an unpredictable pace. It is not unlike that somewhere in the future a sharp decline of cost may arise, for example a great innovation in the field of

quantum storage or DNA use.

The takeover is that growth rate of the chain can increase the cost for the staker no more than his marginal (extra) profit. In this section we proved that this greatly depends on the declining storage costs.

3.2 Block creation time

Let's describe in short how PoS architecture reaches consensus. It is an imitation of the PoW process. The difference is that in PoS the ”miner” cannot pass any value(argument) to the hash function, as it is the case in PoW. He can only pass time (timestamp) and his public address (which must have a positive account balance). Off course, until the formation of the next block transactions cannot take place, so public address is also fixed. His only option is to change the timestamp. When the timestamp changes, a hash is produced. The necessary condition to win the block is :

$$h(c1, c2, ..., cn, ts, pa) < t * b$$

where :

h is result of the hash function

c1,c2,...,cn are arguments that can't be changed

ts is the timestamp (the only thing that staker can change)

pa is his public address

t is a value (target) that is set by the difficulty (like PoW) and got reset every fixed number of blocks

b is the balance in his public address.

When the above inequality is true the stakeholder can claim and form the next block. The probability for each individual stakeholder to win the block at each different values of timestamp is $p_i = p * b_i$ where pi is the probability of the individual to win the block proportionally to the balance bi he has in his account. The probability at each timestamp (second), let's say each "tick", for the total network to form a block is of course

$$P = p_1 + p_2 + p_3 + \ldots + p_s = \sum_{1}^{s} p_i = \sum_{1}^{s} p * b_i = p \sum_{1}^{s} b_i = p * B$$

where s subscript is the individual stakeholder (identified by his public address), B is the total balance of all stakeholders that participate in the consensus, that is, try to form ("win") the next block.

Until now, we didn't discuss how much is the probability p, so to be able to calculate the final probability P which the chain has to form a block at next "tick". Additionally, we are talking about the next tick and not the next second. True, we can force each stakeholder to try not every second but every $g + 1$ seconds; we are going to call g as granularity from now on. $g + 1$ is integer of course, and not only that but it has the form of $g+1=2k \Leftrightarrow g=2k-1$, where k is also integer. For $k = 0$ we have the maximum granularity, that is, $g = 0$, which means that the staker can submit a hash each second.

First, we are going to give more details of how granularity works. And after that, we are going to explain why granularity adds security for the chain and what is the trade-off. To force the stakers to compute a hash every $g + 1$ seconds and not every second we must mask the timestamp. This can be easily done if a NAND logic operation is used with timestamp. For example, if we want 4 sequential timestamps to give the same hash (rendering the 3 timestamp useless, as it they will give the same hash as the input will be the same) we can just do an AND operation of the last two bits of the timestamp with 0 (that is, binary xb00). So , doing a NAND with binary 11 (that is, 3) we mask the timestamps (setting the last two bits to zero) , transforming all 4 timestamps to the same value. Below we can see how this is implemented in the code(C++):

```
nTime Block &= ~STAKE_TIMESTAMP_MASK;
```

It is clear why granularity has the form 2n – 1. It is to mask the last n bits of the timestamp.

Low granularity (high g values) helps to prevent stake-grinding attacks. It is much harder for the attacker to perform a successful attack. The implications of low granularity is higher variation for the block creation time. We are going to examine the mean creation time and variation of block time.

It is easy to see which probability distribution our model fits. Stakers can try to form a block every g +1seconds,where *g ∈{0,1,3,7,15,31,...,2n−1}.g+1* is a power of 2. So every *g+1* seconds they try to form a block. We are interesting for the mean time and cumulative distribution (CDF) of stakers to form a block, so we must calculate the p probability for a block to be formed. The tries make our distribution model discrete and not continuous (as it is in bitcoin or any other PoW consensus). The correct probability distribution to pick is the **geometric distribution** [5] or **GD** [5] for short. Under the assumption that for each try the total stacking balance is about the same and the difficulty changes to readjust the mean time to be fixed (target time), we assume that we already know the mean value (mean = target time). The geometric distribution is a discrete probability distribution which computes the distribution of X Bernoulli trials needed to get the first success after i number of tries. Keeping in mind that we have g and target already known, and clarifying which distribution model describes exactly our model we can calculate the probability p, the cumulative probability to form a block after *i* tries and more.

We know from mathematics that for **GD** the mean is:

$$E[p] = \frac{1}{p}$$

So we have: $E[p] = \frac{1}{p} \Longrightarrow \frac{target}{g+1} = \frac{1}{p} \Leftrightarrow p = \frac{g+1}{target}$

The first occurrence of a success attempt, that is, the creation of block after *i* tries is

$$P(X = i) = (1 - P)^{i-1p}$$

For example, the probability for *g = 7 , target = 128 sec and i = 1 (first try) is:*

$$P(X = i) = (1 - p)^{i}p \Longrightarrow P(X = 1) = (1 - 0.0625)^{1-1} * 0.0625 \Leftrightarrow$$

$$\Leftrightarrow P(X = 1) = 1 * 0.0625 \ \Leftrightarrow P(X = 1) = 6.25\%$$

Now, let $k = \frac{target}{g+1}$ We are interesting in the case where *i* ≤ *k*, because this is where the average block time stands, or where the block must be created most of the time. Much longer than that is, obviously, less desirable. The probability that the block will be formed until the target time can be easily computed from the cumulative distribution function (CDF) for GD. We have

$$Fx(x) = P(X \leq x) \Longrightarrow Fx(k) = 1 - (1-p)^k \Longrightarrow Fx(k) = 1 - (1 - \frac{g+1}{target})^{\frac{target}{g+1}} \Leftrightarrow$$

$$\Leftrightarrow Fx(k) = 1 - (1 - \frac{target - g - 1}{target})^{\frac{target}{g+1}}$$

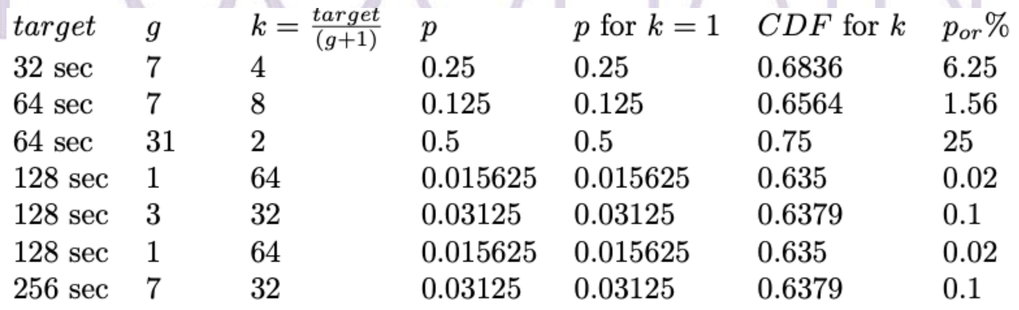
For the above example $(g = 7, target\ = 128)\ k = \frac{target}{g+1} = \frac{128}{7+1} = 16$ *and*

$$Fx(16) = 1 - (\frac{128 - 7 - 1}{128})^{\frac{128}{7+1}} = 1 - (\frac{120}{128})^{16} \approx 64.39\%$$

So we expect the block to be formed at the average time or before with a probability of 65.6%.

Before we move to the next section to study the effectiveness and security, we can make some observations from the table below, which shows that everything is depending on k (if we assume no latency for the network). That is, $k = \frac{target}{g+1}$, the number of tries each stakeholder has until the target time, is the most decisive factor. For low values of k the CDF is a bit higher , which is desirable. It is also safer, as it restricts the stakers, making grind type attacks harder. Unfortunately, it also produces more orphaned blocks (see below), which have a negative impact in network efficiency and security.

Finally, we must not forget that we assumed no latency or propagation time. In real world the latency may be considerable and there is also the propagation time (time for the block to be ”pushed”). That means that transmission of data is not instant. A research [4] showed that for bitcoin - a network with many nodes around all the globe - the median propagation time is 6.5 seconds, while the average time is 12.6 second. That is natural as some nodes will take longer than normal to respond (or even lose connection). In section 2.1 we made our own analysis and tests of the propagation time. The reader should study this section to have a better idea about the network behaviour of ECOChain.



$target$	g	$k = \frac{target}{(g+1)}$	p	p for $k = 1$	CDF for k	$p_{or}\%$
32 sec	7	4	0.25	0.25	0.6836	6.25
64 sec	7	8	0.125	0.125	0.6564	1.56
64 sec	31	2	0.5	0.5	0.75	25
128 sec	1	64	0.015625	0.015625	0.635	0.02
128 sec	3	32	0.03125	0.03125	0.6379	0.1
128 sec	1	64	0.015625	0.015625	0.635	0.02
256 sec	7	32	0.03125	0.03125	0.6379	0.1

Figure 1: probability distribution of block creation time

3.3 Network Effectiveness and Security

What is the probability of the creation of at least one orphaned block? The probability for a node *n1* to find one block in the next interval (”tick”), is

$$P(X=1)=(1-P)^{1-1}P=(1-P)^{0}P=1*P=P$$

where *P* is the total probability of all stakeholders. Assuming a great distribution of the coin (stakes) , the probability for a second stakeholder, lets says *n2*, to find another valid block in the same period (before the next interval) is around *P* also. That is because, as we have seen from above

$$P=p\sum_{1}^{s}b_i=p*B$$

Taken the fact that *n1* with balance *bn1* has found a valid block, the probability that another can be found is:

$$P^{I}=p\sum_{1}^{n_1-1}b_i+p\sum_{n_1+1}^{s}b_i=p\sum_{1}^{n_1-1}b_i+p*b_{n1}+p\sum_{n_1+1}^{s}b_i-p*b_{n_1}=$$

$$=p\sum_{1}^{s}-p*b_{n1}=p*B-p*b_{n_1}=P-p*b_{n_1}\approx P$$

since $\frac{b_{n_1}}{B}\approx 0$ (we have assumed large distribution to stakeholders). In short, the probability Por for an orphaned blocked to be formed will be

$$P_{or}=P*P'\approx P*P=P^2$$

Example: With a target of 64 sec of blockcreation and granularity $g=7$ we have $k=\frac{target}{g+1}=\frac{64}{7+1}=8$, so $P=\frac{1}{k}=\frac{1}{8}$ and $P_{or}\approx P^2=\frac{1^2}{8^2}=\frac{1}{64}=1.5625\%$ So the orphaned blocks aren’t so many - only one orphaned block out of 64 will be created if $k=8$. But what happens if $k=4$. In this occation, $P_{or}\approx\frac{1}{k^2}=\frac{1}{4^2}=\frac{1}{16}=6.25\%$

A question arises why we should care about the percentage of orphaned blocks. Orphaned blocks influence the efficiency of the network, which in turn has an impact on the security of the chain. But just for a moments let’s assume that there aren’t any orphaned blocks. How stakeholders can successfully attack the chain? In PoS if an entity or group has more than 50% of the coins, he can launch a successful attack, reversing blocks and rewriting history. It is not very difficult to see why this is happening. Let’s say that an attacker a has Ba balance in his account(s). He wants to reverse the previous n blocks, so he is ”going back” and starts staking from the desired point. As the algorithm approves the longer chain his personal chain is not validated because he is n block back in history. But because he stakes only in his chain, now the rest of the stakeholders have not P probability but less than P as the total available balance now is Br = B – Ba , where B is the total amount of coins. Simply

$$B_a > \frac{B}{2} \Leftrightarrow p * B_a > p * \frac{B}{2} \Rightarrow p * B_a > p * B' \Leftrightarrow P_a > P_r$$

where *Pa* and *Pr* is the probability to form a block for attacker and the rest of the network respectively. As time passes the attacker will form new blocks more often than the rest of the network until his chain finally passes in length the original chain length. At this point the consensus algorithm will consider his chain as valid and the original chain as invalid. So he successfully reversed (rewritten) n blocks.

This kind of attack, which in fact is also possible in PoW consensus protocol, can be even easier if there are orphaned blocks. Let us define the efficiency of the network as a function *ef (o) = 1 – o* , where *o* is the percentage of orphaned blocks. The limit for the previous attack to take place will be

$$s(ef) = \frac{ef}{1+ef}$$

where s is safety function and if the efficiency function. For example , in case of absence of orphaned blocks we have

$$o = 0, ef(o) = 1 - o = 1 - 0 = 1$$

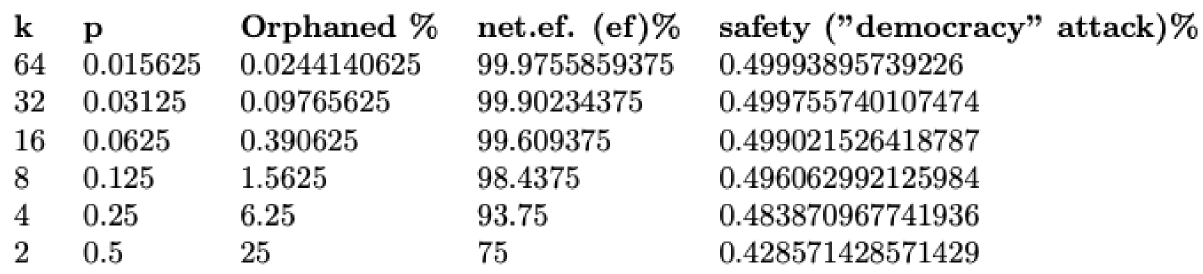
$$s(ef) = \frac{ef}{1+ef} \Leftarrow s(1) = \frac{1}{1+1} \Leftrightarrow s(1) = 0.5$$

So without orphaned blocks an attacker needs more than 50% of the coin. But, for o = 6.25% we have *ef (0.0625) = 1 – 0.0625 = 0.9375 = 93.75%* and the safety limit is:

$$s(ef) = \frac{ef}{1+ef} = \frac{0.9375}{1+0.9375} \approx 0.4839 = 48.39\%$$

It is clear that the safety of the system is lower now.

In the above table we can see how orphaned blocks are related to the security of the chain.



k	p	Orphaned %	net.ef. (ef)%	safety ("democracy" attack)%
64	0.015625	0.0244140625	99.9755859375	0.49993895739226
32	0.03125	0.09765625	99.90234375	0.499755740107474
16	0.0625	0.390625	99.609375	0.499021526418787
8	0.125	1.5625	98.4375	0.496062992125984
4	0.25	6.25	93.75	0.483870967741936
2	0.5	25	75	0.428571428571429

Table 1: orphaned blocks , network efficiency and safety

04 History and Roadmap

Milestone	Description
2017	ECOC project was initiated and core team was formed
February 2018	Research on blockchain and VMs
March 2018	Designing architecture for ECOChain
September 2018	First published open source code
May 2019	Yellow paper published officially
September 2019	First release of the core is ready. Test Net is up and running. Formalizing deployment processes.
October 2019	Successful launch of Main Net
April 2020	Successful Listing on MXC and Boboo Exchange
August 2020	ECOC Fan Meet up
End of 2020	Oracles, POL and Cross Chain 1st phase testing
2021+	Full implementation of decentralized Apps on ECOChain and expanding ecosystem.
2022+	Achieving a Universal Ecosystem Services and ecosystem for ECOC

05 Future Vision Planning of ECOChain

In the not-too-distant future, it is foreseeable that billions of people will save their wealth in the form of digital assets. These wealth are not only money in the narrow sense, physical assets, but also virtual assets. The activities you live in, whether they are public welfare activities or commercial activities, will bring benefits or carry out economic activities. There will be a strong market potential. People will get new virtual assets at the same time they acquire the asset chain. The ECOChain will cater to this trend, change the traditional economic market structure and bring an innovative universal service to the new economic market model.

In the new blockchain economic inheritance system, the younger generation has become the most anticipated "growing giant". The younger generation participates in the economic market industry with a more intuitive, more economical, material and spiritual concept. The plot of the digital asset world and the economy is parallel and closely integrated.

Under the ECOChain system the digital assets can gain value. Under the current model of digital assets, circulation generates value. It has a complete structure and unique encrypted digital currency on ECO chain, and has the potential for asset appreciation, obtaining the corresponding number of tokens, and one-to-one correspondence with the value of the real asset (tokenization). Blockchain technology provides a security mechanism for this and at the same time allows digital assets to reach unlimited interaction between different periods and different scenarios, so that Tokens also have clear ownership and tradable abilities. Eco chain has the capability of smart contracts, so anything can be programmed with computer code.

The ECOChain embraces the trend and gets deep insight into the value of digital assets. The ECOChain tokens have capabilities that gives them competitive advantage , making them preferable from other digital assets on other chains.

With the increase in the number of users, the increase in the use of ECOChain, and the continuous increase in circulation, the value of ECOChain is getting higher (network effect, the Metcalfe's law). It is not just a digital asset that appears in the blockchain world. It is a connection to the economy. The new proposition of the market, the new world.

5.1Coin Policy

In this document we describe the monetary policy of ECOC coins, we provide formulas for the circulation and destruction coins and the reasons and effect they will bring to ECOC price and ECOChain ecosystem. We wish the price to have a positive impact for the ecosystem in the long run.

5.2 Monetary Analysis

We are going to see the forces that change the price level. Our arguments are based on existing macroeconomic rules, such as the quantity theory of money and price rigidity .

5.2.1 Impact of Quantity of Coins

The change rate of the circulating coins affect the price. There is a connection between $\frac{\Delta y}{\Delta t}$ and $\frac{\Delta P}{\Delta t}$. The first is the growth rate of the quantity of money (coins) while the second is the price change for a period *t*.

When

$$\frac{y_t+1}{y_t} > \frac{P_t+1}{P_t} ,$$

the price declines. This is because the circulation of coins increase with a rate higher than the utility of coins. Similarly, when

$$\frac{y_t+1}{y_t} < \frac{P_t+1}{P_t}$$

,the price increases. In a stable economic environment the best thing is a balance to achieve, namely

$$\frac{y_t+1}{y_t} = \frac{P_t+1}{P_t} ,$$

At this point the price reaches equilibrium.

5.2.2 Price Rigidity

Price rigidity is the phenomenon that appears in practice that the prices or exchange rates don’t move immediately to the equilibrium point. The reasons for this are many and include internal and external factors. Decision (reaction) and action time can be considered as internal factors from the view of the investor. Imperfect information and process duration belong to external factors. Regardless of the classification the fact remains. There is price rigidity, some time is needed for the current prices to match (or at least close enough to) the equilibrium point.

5.2.3 Important Monetary Factors

For deciding the correct monetary policy we must consider which factors play a major role of forming the price. We are going to consider three factors:

- Response time of monetary policy until its goal completion.
- Velocity of money (circulation speed of the coins)
- Expected outcome of the rules

5.3 Monetary Policy

The end goal of the policy is stability, which is beneficial for ECOChain's ecosystem. Because it is difficult to regulate the economy based solely on markets, at least in the early stages, ECOC's official policy is going to use monetary regulation tools to achieve the desired goal.

5.3.1 Monetary Regulation Tools

ECOChain technology uses three different tools to enforce its monetary policy:

- PoS Consensus Staking Rewards handling of the official accounts
- Intervention in changing the quantity of money in circulation
- Direct buy or sell orders in exchange markets

Each of the above have a different degree of impact on the price and stability of the coin. The first is long term because it sets the expectation of the final total circulation of coins; the second has a mid-term, forming expectations as the circulation quantity changes. Finally the last is the most immediate, as it can instantly change the price, moving it to the desired stability point.

5.3.2 POS Consensus Staking Rewards Handling

Proof of Stake (POS) is vital for ecochain to work. Staking is necessary to motivate the coin holders to run a full node. Running a node supports the blockchain and decentralizes it. It also makes it more secure. There is a small cost to run a node (server cost), so the reward must overcover this. Of course, the staking reward is also a compensation for the risk of the investor.

While staking rewards for investor and users is desirable and fair, it is not desirable for official accounts , if they use them for profit. The staking rewards of the official accounts are going to be used for regulation only and finally (after the chain reaches the market cap) the staked coins of the official accounts are going to be destroyed. That way they will never be able to enter circulation after the cap is reached.

Until that point they can be used as a tool to regulate the price.

5.3.3 Rate Release Policy

This tool can be used by officials to release coins into circulation, changing the circulating supply. That changes the expectation of the users. Larger circulation of coins creates inflation, lowering the price. Officials have the power to do that because of the large staking rewards. So, depending on the needs of stabilization, they can change the rate that they release their staked coins to the public. Cutting significantly the rate will bring expectation on the users , raising the price. If the price is too high they can increase the release rate. So the release rate is signalling to the public the direction that the price must take. This tool can also be used when external unexpected events take place, that can affect significantly the market and coin price.

5.3.4 Open Market Business

This is the most direct way, and consequently, the most powerful and effective monetary tool. Direct selling has an immediate effect on lowering the price. Of course , buying coins has the opposite effect, raising the price. This is a direct intervention in exchange platforms or any other open market.

5.4 Math Formulas for Total Money Supply

5.4.1 Release Mechanism Effect

Proof of stake (PoS) consensus algorithms are based on staking. That means that the owners of the coins, while running a full node, have a probability to ”win” a reward at each block. The probability is proportional to the coins they hold. This reward is given as a motivation to anyone who holds coins to run a node. Without running nodes a blockchain cannot exist. The stakers support the chain and also help in decentralization. For that reason, they are rewarded with coins.

There was the initial session (which was not PoS) and four epochs of PoS. First session starts with a reward of 50 ECOC/block. At each epoch the reward is doubled.

The initial epoch lasted 10,000 block. After that , the first PoS epoch started. Each epoch lasts 2,500,000 block except of the last one, which is a little shorter (2,312,500) because there is a coin cap (max) of 2,000,000,000 (2 billions). Consequently, at block height 9,822,500 the last PoS reward will be given and the cap of 2 billions will be reached. After that point the stakers will get as a benefit only what they collect from the transaction fees.

The target time for creating a block is 32 seconds. That means that the epochs will totally last ten years. Give that the genesis block has been created at October 28 in 2019, the last PoS reward is expected to be given in the end of October of the year 2029.

Let's create the formulas for the reward. Let h be the block height, r the reward and e_1, e_2, e_3, e_4 the epochs. For every given block height h of the reward of the block is:

$$r_h = 50 * \left\lceil \frac{h - 10000}{2500000} \right\rceil \quad (1)$$

under the restriction of $h \leq 9822500$
The total PoS reward rt given until block height h is:

$$rt_h = \sum_{i=10001}^{i=max(h,9822500} r_h = \sum_{i=10001}^{i=max(h,9822500} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil \quad (2)$$

Finally, we can compute the annual average return as follows:
The expected number of blocks b_y to be formed in a year is, obviously:
$b_y = \frac{60*60*24*265}{32} = \frac{315360}{32} = 985500$, because the average time for forming a block is 32 seconds. Also, in the initial phase the coins that have been produced was $c_0 = 200000$. The expected return at a block height h is the total coins that will be staked for the following year divided but the total coins circulating at block h. Let R be the expected return. We have:

$$\overline{R(h)} = \frac{rt_{h+b_y} - rt_h}{c_0 + rt_h} = \frac{\sum_{i=10001}^{i=max(h+b_y,9822500)} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil - \sum_{i=10001}^{i=max(h,9822500)} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil}{20000 + \sum_{i=10001}^{i=max(h,9822500)} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil}$$

$$\frac{\sum_{i=h+1}^{i=max(h+b_y,9822500)} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil}{20000 + \sum_{i=10001}^{i=max(h,9822500)} 50 * \left\lceil \frac{i-10000}{2500000} \right\rceil}$$

5.4.2 Expected coins to be destructed at the end of staking

ECOC coins can't be destroyed in a protocol level. Still, there are techniques to get them destroys. Sending them to "zero" (or any other recognizable pattern) address, locking them in smart contracts or sending them in smart contracts and then destroying the smart contract. Regardless the method, it can be carried out in practice.
As an example, let's suppose that the three big wallets decide to destroy the coins they stake when the 4th epoch ends. Assuming that the starting block is h = 500,000 then until the last staking block and using equation (2) we get:

$$rth, last = \sum_{i=10000}^{i=9822500} 50 * \left\lceil \frac{i - 1000}{250000} \right\rceil - \sum_{i=10001}^{i=50000} 50 * \left\lceil \frac{i - 1000}{2500000} \right\rceil$$
$$= 1800000000 - 245000000 = 1775500000(4)$$

The three wallets have a balance of 198,000,000 ECOC. That means that at block height h = 500,000 their staking power *sp* is

$$SP_{h=50000} = \frac{balance}{totalcoins} = \frac{198000000}{224500000} \approx 0.882 \quad (5)$$

sp = 88,2%. Under the assumption that all coin holders are going to stake, then this percentage will be the same as time passes because the probability of forming a block (the staking power) of the holder is proportional to the quantity of the coins. The expected staked coins *sc* until the cap will be:
$\overline{sc}$ = 1,775,500,000 ∗ 88,2% = 1,565,991,000 (6)
The three wallets may decide to keep 5% of the 200,000,000 of initial phase for their costs for the ten year run. Let *cr* = 0.05 is the cost rate, *d* the coins to be destroyed and *ic* = 200,000,000 the coins of the initial phase. The destroyed ECOC coins will be: *d* = *sc* – *ic* ∗ *cr* = 1,565,991,000 – 0.05 ∗ 200,000,000 = 1,555,991,000 (7) ECOC expected to be burned.

5.4.3 Final Liquidity Formula

Total circulation of coins can be measured at different sizes (M1,M2,M3). Coin (money) supply M1 is the total circulating supply of the coins. The M2 type include M1 plus coins in smart contracts and exchange platforms. M3 includes all the above plus derivatives which are placed on ECOC.
Calculating M1 is very easy. After the destruction of the coins the total circulation *tc* will be:
tc = *cap* – *d* = 2,000,000,000 – 1,555,991,000 = 444,009,000 (8)

5.5 Expected Outcome of Monetary Policy

It is clear from the above that the monetary policy uses the right tools to intervene, changing the quantity of circulating coins (increasing or decreasing) , which in turn impact the ECOC price, stabilizing the coin. The excess or scarce coin circulation is countered by intervening in the markets by buying or selling. The final cap is regulated by the destruction of the coins.

06 Team Introduction

The members of the core team of the ECOChain have experienced blockchain senior technical personnel, the world's top professional technical developers, professional investment and financial analysts, management talents, and business consultants. They have top experts and consultants in the artificial intelligence industry. The ECOChain team can be called a full-scale team, with members from elites in multiple industries such as artificial intelligence, finance, blockchain technology, market management, and big data analysis. Its technology leader is mainly responsible for blockchain application technology research and development, system research and development, system security, vulnerability upgrades, patented technology development, etc., and concentrates on researching blockchain market applications in economic markets to open up a new value ecology.

【Core team members】

Dom Teh
CEO

Graduated from the Singapore Institute of Management with a Master‘s degree in Engineering Business Management. Stayed and worked in the States for a couple of years. Having an extensive international language knowledge of many countries and with many years of rich experiences in financial investment and specialty on return on assets. In recent years, he has conducted in-depth research on public blockchains and has rich experience in blockchain technology.

Albert Shi
CBO

Graduated from Charles, Australia with Master’s in Economics, , independent investor, director of European blockchain Joint Committee, Director of Thailand blockchain Research Centre

Akis Chalkidis
CTO

ECOC’s Public Chain Chief Technology Officer and Core Developer, mathematics expert, graduated from the Massachusetts Institute of Technology computer major, CTO and core developer of dApp Blockchain Store Co., Ltd., has 15 years of software development experience in the field of cryptography Extensive knowledge

Bilal Waebuesa
R&D Director

Graduated with a Bachelor of Engineering (Electrical and Mechanical Engineering) from Prince of Songkhla University in Thailand. He has more than 8 years of experience in web application and software development. He is proficient in Python, Java, C, C ++, Solidity and other languages, and has rich code writing capabilities.

Kei Kaneda
CMTO

Graduated from Korea University with a major in marketing, has many years of marketing experience in Germany and the United States. It has marketing techniques such as precision promotion, precision marketing, big data analysis, and intelligent analysis.

Jay Pichitsurakij
Programmer

Master of Computer Science, programmer, has deep research on Go language, C language, C ++ language and so on.

Antonatos Nikolas
Advisors on Economics

Studied Economics and Finance. He has experience in the fields of finance and risk management, digital marketing and actuarial science. He is capable to mathematically formalize, analyse and solve problems of economic nature. He also has knowledge and interest in blockchain and digital assets.

Sotiris Kravvaritis
Back-End Developer

Skills expertise: python, web3, solidity

John Stavropulos
Back-End Developers,

Skills expertise: php, Nodejs, database architect, web3, solidity

07 Risk warning

7.1 Disclaimer

This document is for informational purposes only and does not constitute a relevant opinion on trading of shares or securities of ECOChain companies. The above information does not constitute investment advice, suggested decisions or specific recommendations. This document does not constitute any investment advice, investment intention or solicitation of investment in the form of securities. This document does not constitute and is not to be construed as providing any buying, holding or selling behaviour, or any invitation to buy or sell, any form of securities, nor is it any form of contract or promise.

Given the unpredictable circumstances, the goals outlined in this white paper may change. Although the team will do its best to achieve all the goals of this white paper, all individuals and teams that purchase ECOC will do so at their own risk. Part of the content of the document may be adjusted accordingly in the new version of the white paper as the project progresses. The team will publish the updated content to the public by publishing an announcement or new version of the white paper on the website.

ECOChain makes it clear that it will not bear any direct or indirect losses caused by participating in this project, including:

(1) The reliability of all third-party information provided in this document
(2) any errors, negligence or inaccurate information arising therefrom
(3) or any action caused by it.

The ECOChain team will strive to achieve the goals mentioned in the document. Due to the force majeure, the team cannot fully make the commitment. ECOC is a tool for efficiency in ECOChain platforms. It is not an investment. ECOC is not an ownership or control right. Holding ECOC does not represent ownership of the ECO chain or ECO chain applications, and the ECO chain does not grant any rights to participate in, control, and make decisions about ECO chains and ECO chain applications.

ECOC is a digital asset credit that uses ECO chain as one of its usage scenarios. ECO chain cannot guarantee that ECOC will add 100% value, and it may also have a price drop under certain circumstances. ECOC has no ownership or control. The purchase of ECOC does not represent ownership of the ECOC or ECOC application, and ECOC does not grant any individual any right to participate, control, or make any decision regarding ECOC and ECOC applications.

To the maximum extent permitted by applicable law, the team is not liable for damages and risks arising from participation, including but not limited to direct or indirect personal damage, loss of commercial profits, loss of business information, or any other economic loss . The ECOChain platform clearly communicates the possible risks to the participants. Once participating in the ECOC issue, it represents that it has confirmed that it understands and agrees to the terms and conditions in the detailed rules, accepts the potential risks of the platform, and bears the consequences.

7.2 Risk Warning

In order to develop and construct a ECOChain and govern a transparent mechanism, advocate and promote the smooth progress of ECOChain work, promote the safe and harmonious development of an open source ecological society, and monitor and manage funds, and serve as a resource integration platform to support the global economic market ecology Circle construction, the ECOChain established a ECOChain foundation overseas.

The ECOChain Foundation will strictly in accordance with the laws and regulations of the company's locality, conduct swaps to specific groups in an appropriate manner, and give digital assets ECOC. Due to legal restrictions of national citizens or groups, digital asset points ECOC will not conduct public crowdfunding or public offerings in certain countries and regions. Digital asset ECOC, as a virtual commodity with practical uses, is not a security or a speculative investment tool.

The ECOChain foundation's income from the ECOC swap of digital assets will be used by the ECO chain foundation for technology development, marketing, community construction, financial auditing, and business cooperation.

The ECOChain platform is still likely to be questioned and regulated by competent authorities in different countries around the world. In order to meet and comply with local laws and regulations, the ECOC platform may not provide normal services in some regions.

This document is only for the purpose of conveying information and does not constitute related opinions or investment opinions on the purchase and sale of native digital assets in the future, nor is it any form of contract or commitment.

Once an investor participates in private placement and sales, it means that they understands and accepts the risks of the project and is willing to personally bear all the corresponding results or consequences for this. The platform expressly does not assume any direct or indirect losses caused by participating in the platform project.

The native digital asset involved in this project is an encrypted digital code used on the platform and does not represent the equity, creditor's rights, income rights or control rights of the platform project.

7.3 Systemic Risk

It refers to the possible change in returns due to a global common factor, which affects the returns of all securities in the same way. For example, policy risk-At present, the country's regulatory policy for blockchain projects to be financed in tokens is unclear, and there is a possibility of losses for participants due to policy reasons. In market risk, if the overall value of the digital asset market is Overestimation, then the investment risk will increase, and participants may expect the growth of blockchain application projects to be too high, but these high expectations may not be achieved. At the same time, systemic risks also include a series of force majeure factors, including but not limited to natural disasters, large-scale failures of computer networks worldwide, political turmoil, a pandemic etc.

7.4 Regulation Absence Risk

Digital asset transactions, mainly represented by BTC, have extremely high uncertainty. Due to the lack of strong supervision in the digital asset trading field, there is a risk that the tokens will skyrocket and plunge or be manipulated by the dealer. After the individual participants enter the market, without experience, it may be difficult to resist asset shocks and psychological pressure caused by market instability. Although academic experts, official media, etc. have always given suggestions for cautious participation, there is no written regulatory method and provisions, so at present such risks are difficult to effectively be avoided.

7.5 Regulatory Risks

It is undeniable that in the foreseeable future, there will be regulatory regulations to restrict and regulate the field of blockchain and tokens. If the regulatory body regulates the field, the purchased tokens may be affected, including but not limited to fluctuations or restrictions in terms of price and ease of sale. Other unknown risks: With the continuous development of blockchain technology and the overall situation of the industry, ECOC may face some unexpected risks. Participants are requested to fully understand the team background, understand the overall framework and ideas of the project, reasonably adjust their vision, and participate rationally before making participation decisions.

Appendix:

【References】

1. https://bitcoin.org/bitcoin.pdf , Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2008
2. https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf , Chain Interoperability , Vitalik Buterin, 2016
3. https://en.wikipedia.org/wiki/Gossip_protocol , Gossip protocol
4. https://ecoc.io/wp-content/uploads/docs/yp.pdf , ECOChain 's yellow paper
5. Blockchain-based Proof of Location , Giacomo Brambilla, Michele Amoretti, Francesco Medioli, Francesco Zanichelli , 2016
6. https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts , Hash Time Locked Contracts
7. https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v3g.pdf , Joseph Abadi and Markus Brunnermeier , 2018
8. http://elit.lnu.edu.ua/pdf/9_10.pdf , Pros and Cons of consensus algorithm proof of stake , O. Vashchuk, R. Shuwar , 2018
9. Economics of Proof-of-Stake Payment Systems, Giulia Fanti, Leonid Kogan, Pramod Viswanath , 2019