# LONDONCOIN: THE ULTIMATE CRYPTOCURRENCY

Myongsu Choe, Ph.D.
Email: myongsu.choe@ssencorp.com
(v1.5, updated on March 25, 2018)

## Abstract

We reinvent current cryptocurrencies by analyzing inherently existing vulnerabilities and issues such as real-time payment and transactions, security threats and weaknesses from current centralized basis exchanges as well as wallets, and the lack of an intrinsic value of cryptocurrencies. Therefore, we propose a reference model for a cryptoecosystem and we build up an innovative cryptoecosystem by containing SSENCORE as a high performance core engine for processing LONDONCOIN (also known as, LDX) cryptocurrency, which realizes real-time payments and transactions, SSENDEX which is a decentralized exchange, making it possible to trade without the presence of the current exchange via a smartphone, and SSENWallet, which is embodied in a biometric-based HW wallet. Our insights indicate that the major properties of scalability, security, and safety can be enforced to significantly match or outperform the current financial system and to be placed in a pivotal position between the traditional economy and cryptoeconomy.

Key words: cryptocurrency, blockchain, directed acyclic graph (DAG), consensus, trust, proof of trust, byzantine failure tolerance (BFT), scalability, security, stability, gold-backed cryptocurrency, value creating cryptocurrency, LONDONCOIN, LDX, decentralized exchange (DEX), SSENCORE, SSEN[1] DEX, biometric based card, fingerprint, SSENWallet.

Proof of Trust
*Don't employ anyone who is suspicious. If someone is employed, do not suspect him*[2] (Korean proverb)

# 1 Introduction

Bitcoin as a forerunner cryptocurrency based on a blockchain technology has been

[1] SSEN (쎈) means *strong* or *powerful* in Korean.

[2] 의인막용 용인물의 (疑人莫用 用人勿疑), 명심보감 성심편 (明心寶鑑 省心篇)

introduced into the market around 2009. Since then, it created a new market and caused the production of more than 1583 coins such as Ethereum, Litecoin, Ripple, iota, etc., which are known as Bitcoin alternatives or alternate coins (altcoins), and it developed a market capacity worth 327 billion dollars[3] exponentially. What does it bring to the market and how does it make an impact on our society and daily lives? The fundamental concept of a blockchain may have more potential than by solely trading a cryptocurrency; so that it may change from the current Internet of information to the Internet of value (or money), or from a worldwide web to a worldwide ledger by eliminating a middle man such as a government, a bank, a big corporation, or even high-tech based traditional big companies by guaranteeing privacy, safety, transparency, and integrity rather than all of the traditional services provided by the middle man [1, 2].

Since nearly a decade of their existence, cryptocurrencies are used to some extent and they are traded in a market. Even so, people can transfer the cryptocurrency to someone who lives in a foreign country and even to those who do not even own a bank account; thereby paying lower transfer fees that are not comparable to the fees of the middle man such as traditional banks, Western Union, PayPal, and more. Moreover, people can also buy commodities via a cryptocurrency or exchange a cryptocurrency to a fiat currency like the USD or Euro dollars and vice versa via the Internet or ATM equipment in certain regions. Numerous applications based on the blockchain are not limited to the currency but they are expanding in many areas, namely in the sector of the arts, gaming industry, music, intellectual properties, land registration certificates, agricultural products, etc.

We wish to further investigate on whether obstacles still exist or not when using cryptocurrency in the real world. Generally, merchants may not be willing to receive the cryptocurrency from their customers since its nominal price can fluctuate unexpectedly and it takes a considerable amount of time to receive confirmation for the transactions. In the case of Bitcoin, every 10 minutes, a block is created and confirmed, and with additional time, it takes theoretically about an hour to resolve forks. If many transactions occur at the same time, then more time than one hour is needed. On the other hand, excessively speculative trading market conditions are unexpectedly fluctuating, resulting in the reluctant acceptance of cryptocurrency as actual money. If these cases are not resolved soon, then the future of cryptocurrency may not be promising.

In addition, when cryptocurrencies are traded at a centralized exchange, since the

[3] https://coinmarketcap.com/

exchange manages all of the sensitive information, all of the security incidents can be occurred at an exchange. For example, a Bitcoin exchange called Mt. Gox was hacked and all the Bitcoins that were assigned and stored from the investors were gone, finally resulting in the bankruptcy of the exchange. This incident occurred due to the lack of security at the exchange, instead of security flaws existing in a blockchain technology.

Presently, some governments such as Japan and the Unites States are considering cryptocurrencies as an alternative of the current fiat currency and they wish to monitor them and introduce regulations and tax-related securities for all of the transactions, in order to prevent investors from fraud and loss. More specifically, sudden bankruptcies of some issued currencies caused enormous losses for investors, and the illegal use of the currencies for the trafficking of drugs and weapons, gambling, and ransom payments, resulted in the investigations by law enforcement authorities. On the other hand, the Chinese government placed a ban on the ICO (Initial Coin Offering) and the Korean government is considering to follow the example of the Chinese government by pressuring the speculative frenzy related to cryptocurrency.

Therefore, we wish to propose an innovative cryptoecosystem to clearly resolve the aforementioned issues.

# 2 A CryptoEcosystem

Ethereum developer Vlad Zamfir states that cryptoeconomics is “A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.” The blockchain technology runs on the principles of cryptoeconomics as implied by the word Cryptoeconomics coming from the combination of both words; Cryptography and Economics. The cryptoeconomy consists of cryptoeconomic approaches by combining cryptography and economics to create robust and decentralized peer-to-peer networks that thrive over time despite the adversaries that attempt to disrupt the network. The cryptography aspect underlying these systems is what makes the peer-to-peer communications within the networks secure. The economics aspect is what incentivizes all actors to contribute to the network so that it thrives over time and to be applicable to traditional economic activities as well as newly created ones in terms

of users, distributed capital markets, applications, services, micro payments, live collaboration, and auctions.

We define a reference model about a CryptoEcosystem consisting of three layers required to drive a CryptoEconomy, in which a service layer provides various markets, users, applications, and services; an exchange layer that provides the role of trading and arbitrage, arbitration, an mediation between services and distributed ledgers; and a distributed ledger layer that plays a pivotal role in managing all of the transactions and confirming them in a controlled peer-to-peer communications even under a Byzantine failure model as illustrated by Figure 2.1.

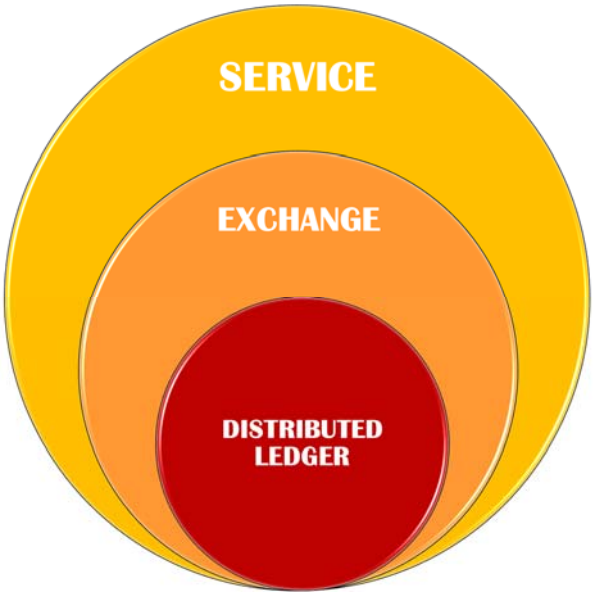



Figure 2.1: A reference model of a CryptoEcosystem

Our solutions for the corresponding layers range from a distributed layer to a service layer through an exchange layer, which is working as a middle layer shown in Figure 2.2. As an embodiment of the cryptocurrency, LONDONCOIN is processed and transacted at a distributed ledger layer on top of a core engine called SSENCORE, which aims for real-time payment based on a ledger without a blockchain structure. At the second layer, a decentralized exchange called SSENDEX is processed within a person-to-person trading and transactions on the top of a peer-to-peer computer network. Finally, a biometric-based SSEN Wallet provides secure authentication and user friendliness for all of the services and applications in a top layer.

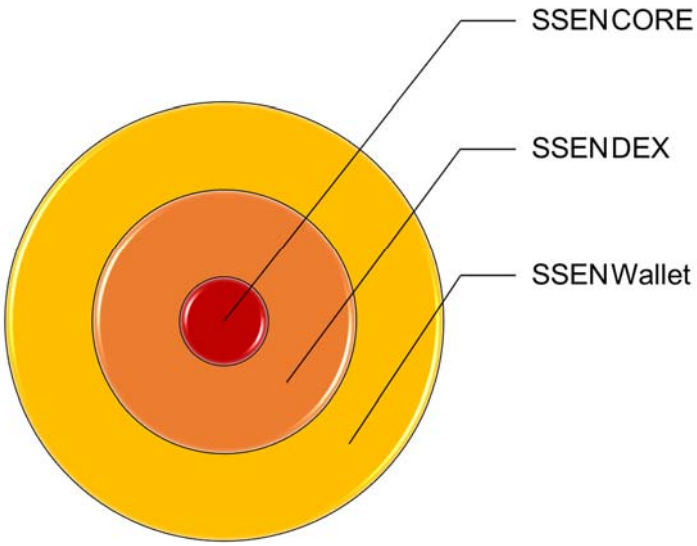



Figure 2.2: Our solutions

By examining all of the major cryptocurrencies in comparison with the traditional one, which is called a fiat currency, and analyzing their pros and cons, we propose three major properties such as stability, security, and scalability from the CryptoEcosystem as shown in Figure 2.3.

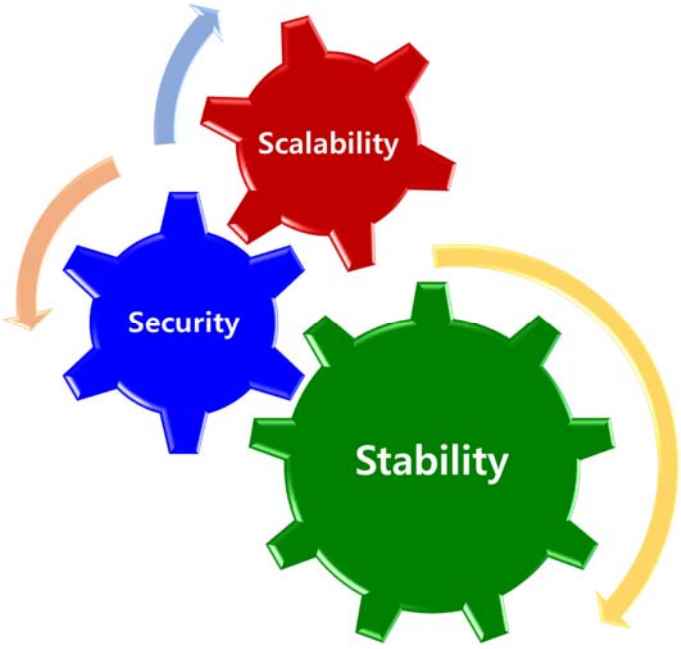



Figure 2.3: Essential functionality in a CryptoEcosystem

## 2.1 Stability

We do not expect for the traditional currency to be wiped out completely and replaced by

the cryptocurrency in the nearby future. Thus, the cryptocurrency will coexist with the fiat currency for the time being, and people may freely use their cryptocurrencies like the fiat currency such as buying and exchanging, paying, transferring, withdrawing money from an ATM or banks. In order for things to properly work under this scenario, the exchange price of the cryptocurrency in a market has to be stable in accordance with a case of the fiat currency. In an actual market, the prices of most cryptocurrencies are unexpectedly fluctuating. Thus, it makes it difficult to trade them since merchants are reluctant to accept them due to the uncertainty of the traded price. Therefore, maintaining stability is an important and challenging objective. However, most cryptocurrency supporters do not want to acknowledge this reality.

**Our solution**: We raise a primitive question on whether a cryptocurrency has its own intrinsic value, and how the cryptocurrency is endowed with some acknowledgeable value. Some people say that an expense itself that is invested for mining cryptocurrency such as electricity and mining rigs is of value, but we believe that it is only a number that exists in a cyber world. At present, prices of cryptocurrencies including Bitcoin are skyrocketing due to the speculative frenzy that is similar to the case of the tulip trade in 1637. But if the values are decreasing, how can they protect their values?

We want to bring back a gold-backed cryptocurrency, which is reminiscent of a historical event that occurred in August 1971 when the US government unilaterally terminated the convertibility of the US dollar to gold. There are two alternatives for this issue.

The first solution is to integrate gold with a cryptocurrency. As usual, there are no mining fees in our cryptocurrency unlike other cryptocurrencies on the market, and transaction fees are only collected during the confirmation of transactions. 10% of the fees are given to computer nodes, which participate in consensus works as an incentive, and the rest of the fees can be used to purchase gold and to deposit it. As the LONDONCOIN is traded and transacted, the amount of the deposited gold also increases. Thus, compared to others, our cryptocurrency always creates value, as well as the ability to stabilize the prices. Gold can usually be traded at an exchange by a unit of an ounce or a gram (or kg). The second one is to make our cryptocurrency pegged to gold. In this case, a basic unit of the cryptocurrency is set to a 1/10 of a gold gram. Once we start an ICO, we will then publish an elaborate plan. As an analogy, can you imagine buying a cup of coffee at Starbucks by paying 0.1gram of gold or 1.0 LONDONCOIN?

## 2.2 Security

We enumerate all the computers and devices, which are participating in a cryptocurrency network, thereby expecting potential security vulnerabilities from various attacks. A computer that connects to the cryptocurrency network is called a node. In the case of Bitcoin, there are full nodes that fully enforce all of the rules of the Bitcoin, and a SPV (Simple Payment Verification) node, which is a client that only downloads the headers of blocks during the initial syncing process and then requests transactions from the full nodes as needed. And a Bitcoin wallet can refer to either a wallet program or a wallet file. Wallet programs create public keys to receive Bitcoin and use the corresponding private keys to spend those Bitcoins. Wallet files store private keys and (optionally) other information related to transactions for the wallet program.

Because there are no limits for the number of nodes that can participate in the cryptocurrency network, all of the nodes may not have a definite chance to update to the same software version and commit transactions at the same time, commonly resulting in a permanent divergence in the blockchain known as hardware fork, coin fragmentation, and double spending. All of the nodes that are participating in a peer-to-peer based cryptocurrency network may cause some security vulnerabilities. Some of the nodes may be working in a malicious manner, and other nodes with powerful computing resources may collude to the proof of work and disrupt the whole trust in the network. Some nodes may act as a host for masquerading DoS (Denial of Service).

Cisco estimates that smartphone traffic will exceed PC traffic by 2021 and traffic from wireless and mobile devices will account for more than 63 percent of total IP traffic by 2021 [4]. Therefore, it means that a wallet device is shifting from a PC or a notebook to a smartphone where the device has a limited amount of computing power and storage. The wallet device usually connects to an adjacent node in the cryptocurrency network to make transactions. Thus, all of the digital wallets stored in a mobile device like a smartphone might get lost, resulting in the illegal theft and usage of it.

Aside from nodes and wallets, which are used for cryptocurrency transactions, there exists a set of computer nodes at an exchange, which can be used for trading. It was an exchange that failed due to the equivalences of a bank run, and exchanges failed because the operators of the exchange were frauds, and also due to numerous break-ins. In fact, the statistics are not encouraging, but a study in 2013 found that 18 out of 40 Bitcoin exchanges

closed due to failure or due to an inability to pay out the money that the exchange had promised to pay out. The most famous example of this is the Mt. Gox case. Mt. Gox used to be the largest Bitcoin exchange, and it eventually became insolvent, and it was unable to pay out the money that it owed. Mt. Gox was a Japanese company, and it declared bankruptcy, which left a lot of people wondering where their money had gone. So this is an example of a cautionary tale concerning the user of exchanges. Connecting this idea back to the banks, we do not see a 45 percent failure rate for banks in most developed countries, which is partly due to regulations; governments regulate traditional banks in various ways. Governments often impose a minimum reserve requirement on banks. In the United States, the fraction of demand deposits that banks are required to have in liquid form is typically 3-10 percent, so that the bank can handle a surge of withdrawals if necessary. In exchange for the application of these forms of regulations, governments typically try to help banks or to help their depositors. First, governments issue deposit insurance. That is, the government promises the depositors that if a bank that follows these regulations encounters financial problems, the government will return at least a portion of these deposits. Moreover, governments sometimes act as a "lender of last resort." If a bank experiences difficulty but remains solvent, the government may step in and give a loan to the bank to tide it over until it can move money around as much as necessary to get itself out of the current situation. So traditional banks are regulated this way but cryptocurrency exchanges are not. Unlike the banks, without any regulations and reserves how can we trust an exchange?

**Our solution**: We want to control nodes in a cryptocurrency network to countermeasure security threats by determining a node's trust into a good node or a bad one. As a separate issue, it is known that moral hazards, collusions, and security weaknesses are mainly generated from the current centralized-based exchange site, and not from a blockchain technology, and we propose a decentralized one to prevent it from security incidents and threats that occur at the centralized exchange. We separate a wallet device into two parts to enhance the security level. The upper part is a smartphone with an app which supports trading and transactions with a public key, and the lower part has a digital hardware-based wallet known as a SSEN Wallet, which is a biometric system on-card that integrates a current EMV (Europay, Mastercard and Visa) chip credit card by embedding a fingerprint sensor and a display with a secret key. It is going to bridge the fiat currency with a cryptocurrency at the same time.

## 2.3 Scalability

A scalability is defined as the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged, in order to accommodate that growth [5]. For example, suppose that a cryptocurrency is designed to cover up worldwide economic transactions including cash. To provide global financial services, we need to know our competitor's transaction performance. For example, in the case of Visa, it handles around 2,000 transactions per second (tps), 4,000 tps in a daily peak, and 56,000 in a peak capacity. Visa itself never achieves more than about a third of 56,000 even during peak shopping periods. PayPal processed an average transaction rate of 50-100 tps in late 2014. The Bitcoin is designed to process about 7 tps.

To be able to withstand DoS attacks, this implies that at least our currency will be set to a target comparable to Visa's or even more. In order to achieve high performance computing and real-time payment comparable to Visa's transaction processing speed, several exemplary protocols are thoroughly reviewed such as iota [14], Algorand [15], PBFT [17], ripple [18], and hashgraph [16] protocols because these candidates are to some degree known to produce phenomenal results even though the simulation and testing results were set up and tested in a limited testing environment.

**Our solution**: To provide real-time payment and transactions, we have been devising an extraordinary consensus mechanism based on an asynchronous Byzantine Fault Tolerance and a directed acyclic graph (DAG), not a generic PoW (Proof of Work) or PoS (Proof of Stake) based consensus and a blockchain structure. We add some functionality by reinforcing gossiping (or rumor spreading) with push and (conditional) pull features in order to accelerate information dissemination, and to promptly reach consensus with the aid of a snapshot and an election with extinction. SSENCORE's performance will outperform that of Visa's and Hashgraph, targeting 200,000 transactions per second within 7 seconds and serving a global coverage.

# 3 SSENCORE

## 3.1 Partly distributed control

A centralized network and a peer-to-peer (or fully distributed) based network are shown

in Figure 3.1 for comparison purposes. The centralized network consists of a central node and the rest of the nodes, which are linked to the central one. On the other hand, a pure peer-to-peer network as an overlay on top of the Internet has distinguished features such as self-organization and swarming where there is no centralized node, and in which it mediates and relays as a middle man. All of the nodes in a (pure or full) peer-to-peer network are working in an autonomous way and all of the nodes are equally considered. In terms of the points of failure and maintenance, the centralized network is easier to maintain as there is only a single point of failure, while the distributed one is the most difficult one to maintain. When it comes to fault tolerance and stability, the centralized one is highly unstable since in the case where the center node is down, it results in the whole network not functioning. However, the distributed network is very stable and a single node failure does not have any effects on the operations. In regards to scalability, the centralized one has a very low scalability and the distributed one has a high scalability.

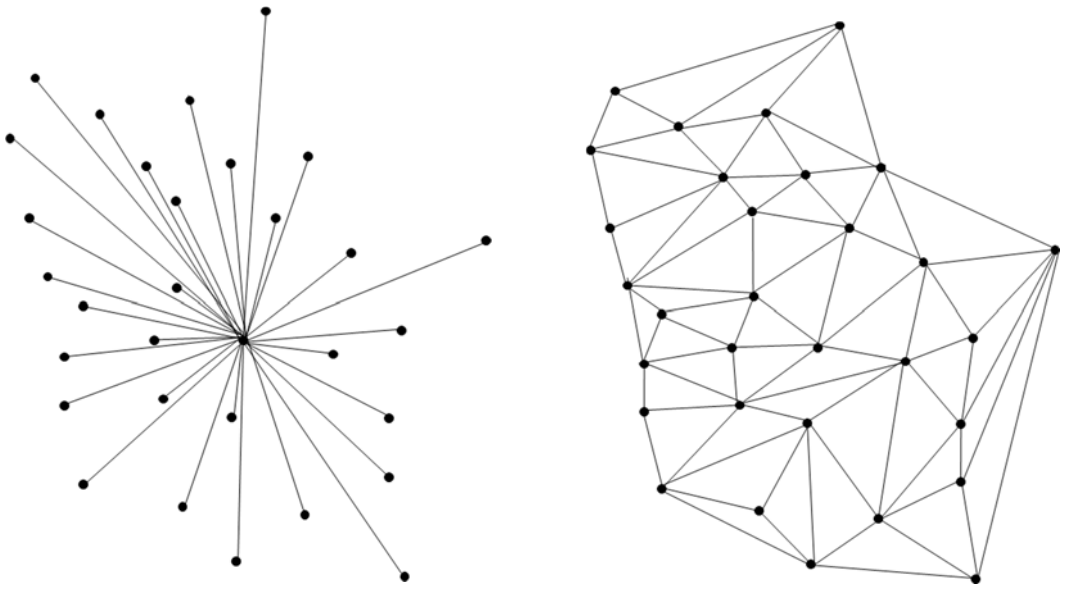


Figure 3.1: A centralized network and a peer-to-peer (fully distributed) one

In general, each node in a pure peer-to-peer network usually has overly excessive freedom and it runs its own control by communicating adjacent nodes and exchanging information such as control, data, and states, thereby resulting in too many traffic flows in the whole network and a late convergence in the whole network. To reduce the excessive messages and controls over the network, running the pure peer-to-peer network is not a clever idea. Instead, a small network consisting of a part or a subset of a node set called a partly distributed (clustered or team or hybrid) network, which is obtained by partitioning

the whole network, can be a better choice due to the actual experiences obtained from a mobile ad-hoc or a mesh network, wherein a node communicates to other nodes without using any aids or relays via any special central node.

The partly distributed network consists of a set of clusters (or regions, groups, teams, shards), from which we schematically represent the partly distributed network in Figure 3.2. The dotted polygonal line represents an elected set of nodes, precisely a leader or a cluster head in each partitioned network. The leader node is the elected node depending on the satisfaction of certain conditions in each partitioned network. When the node is rejected to the election, then we call the node as a non-leader (plain) node, and the non-leader node can communicate with other nodes in its internal networks via its leader node working, which in turn works as a network gateway. And the non-leader node can also communicate with other nodes located at other partitioned networks via its leader node functioning as a network gateway. If possible, a set of the elected nodes can be formed as a clique (or complete graph) to rapidly exchange messages amongst nodes where each pair of nodes is directly connected by an edge with one diameter.

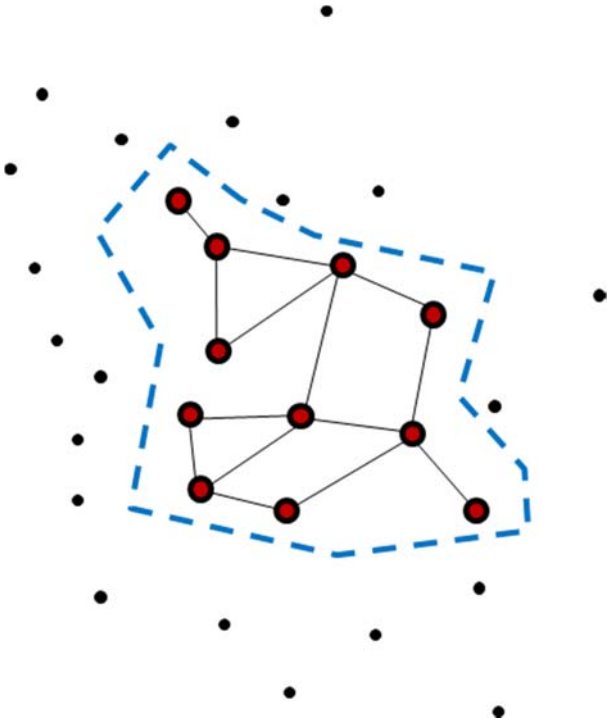


Figure 3.2: Partly distributed (clustered or hybrid) network

## 3.2 Deciding the Good, the Bad and the Ugly[4]

Unlike other cryptocurrencies, deciding good (honest) nodes or bad (dishonest) ones in the course of forming the partly distributed network topology is a core concept of the SSENCORE protocol. A decision process consists of four steps: Dissemination, Global snapshot, Election by extinction, and Consensus. The dissemination stage consists of the sharing amongst all nodes to have consistent information by using a gossip (or rumor) message. The global snapshot stage contains constructing explicitly a system-wide (or network-wide) global configuration featuring local states (snapshot states) of each process and channel states. Using the distributed snapshot, we can find the total number of elected nodes, the global timestamp, the trust level of the network, and more in a snapshot instant. The election by extinction stage is a process to choose an arbitrary node from the whole node set and all the nodes can be legitimately chosen depending on the satisfaction of qualifications. Within a finite time, part or all of the nodes that started the election process can finally be determined as one elected node so that the election process is faster than the normal election one and a certain node is not required to play the role as a designated node in advance. Finally, the consensus stage is a process where all the nodes reach an agreement. A node showing faults will be excluded from the chosen node set or it cannot be selected to belong to the chosen node set.

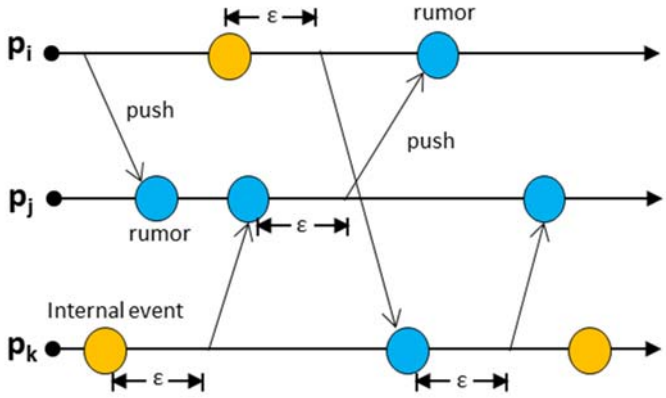
### A. Dissemination

When a transaction has occurred, then the information of the transaction has to be shared amongst all the nodes in a system. We are using a gossip (or a rumor) and a gossip about gossip (a rumor about rumor) to share the information because gossiping (or rumor spreading) is an efficient way of spreading in comparison with broadcast and flooding [13]. We extend to an information dissemination protocol by using a push and (conditional) pull gossip message in order to reach fast convergence for all the nodes to have the same consistent information.

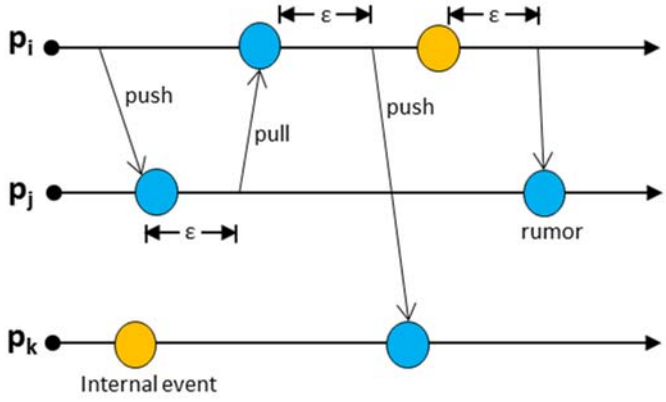
As shown in Figure 3.3(a), when a transaction known as an internal event (or a self-event) is created at a node $P_i$, and then the $P_i$ randomly chooses adjacent node $P_j$ and sends its local information to $P_j$ within a time interval ε. At node $P_j$, when the gossip message receives, then it combines its own local information with the information from

[4] We quoted the title of a famous 1966 Spaghetti Western film directed by Sergio Leone and starring Clint Eastwood, Lee Van Cleef, and Eli Wallach in their respective title roles since it matches with our metaphor.

a remote node $P_i$. In Figure 3.3(b), $P_i$ sends to a randomly chosen node $P_j$. If $P_j$ knows that $P_i$ have the same consistent information, then $P_j$ does not respond to its gossip message anymore until the next gossip message has arrived. Otherwise, within an interval ε, node $P_j$ packs its unshared information into a gossip message and sends it back to the sending node $P_i$.




(a) Push




(b) Push and conditional Pull

Figure 3.3: Gossiping (or rumor spreading)

The dissemination via gossiping autonomously proceeds without control from a certain node called the leader, and all the nodes voluntarily take participation in the dissemination process. There is no distinction between control and gossip messages. By piggybacking a gossip message with a special tag «*m*, *tag*», where *m* is a gossip message and a *tag* a special tagged information, our dissemination process can be extended to estimate a network size using aggregation computations and detect

termination of rounds for Byzantine Fault Tolerance (BFT). When it reaches to detect the termination of rounds, it can finally perform self-voting and confirm all the transactions just prior to an instant of the termination detection.

## B. Global snapshot

The notion of a cut underlies the construction of global snapshot algorithms [9, 10, 11, 12]. As shown in Figure 3.4, a cut essentially divides the events of a system into those occurring before the cut and those occurring after the cut. Messages then travel between the "past" and the "future", as defined by the cut. A consistent cut is one in which no messages from the future travel into the past. Otherwise, we consider the cut inconsistent. In order to obtain a global snapshot, local snapshots are gathered from individual processes "along the cut". In order for the global snapshot to be meaningful, it is necessary that the protocol satisfies a consistent cut.

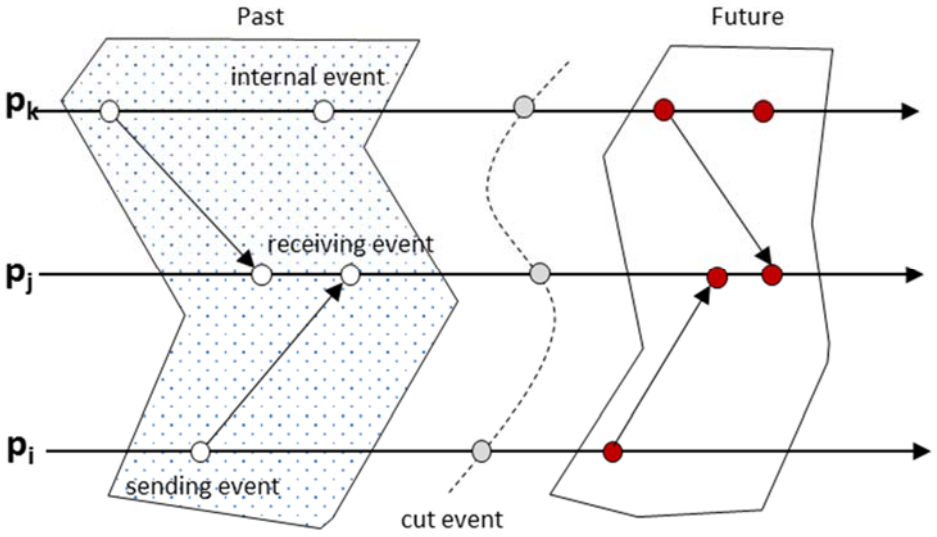


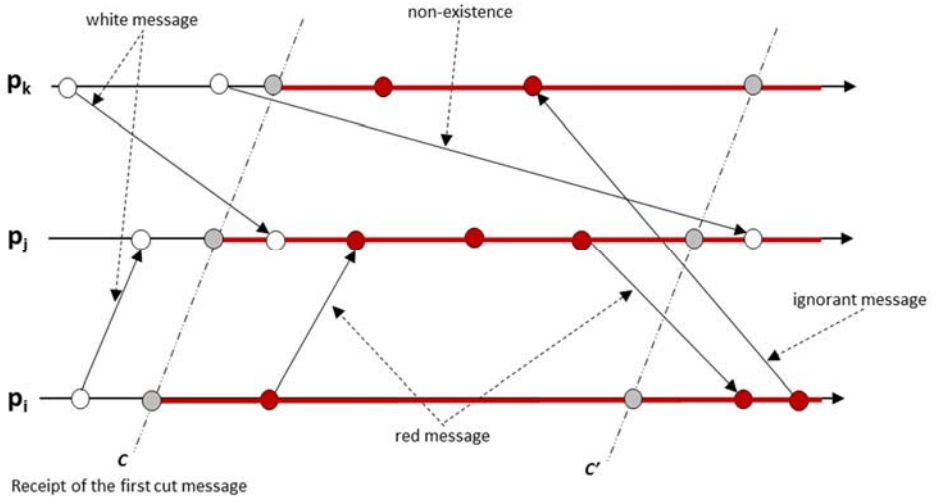

Figure 3.4: A cut message

Lai and Yang [11] developed an elegant algorithm for obtaining such a cut. Their algorithm applies to non-FIFO systems, and only invokes the piggybacking of status information in one bit onto all messages. The algorithm is as follows: (1) every process is initially white and turns red when taking a local snapshot, (2) every message sent by a white (red) process is colored white (red), and (3) every process takes a local snapshot before a red message is received. Ensuring that a local snapshot is taken before a red message is received at a process is accomplished by examining the color of the messages before processing them. In the event that a message is red, the local snapshot

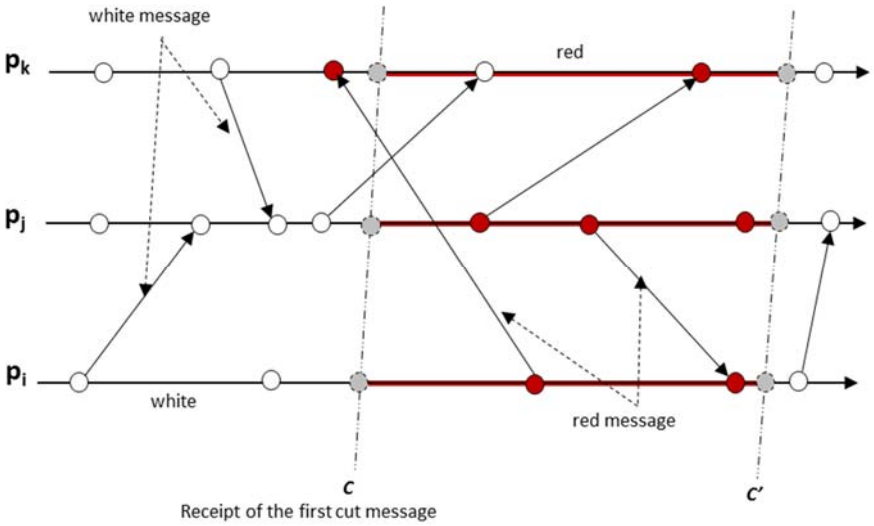
is taken prior to processing the message. One way of implementing the algorithm is to circulate a control message, which colors each of the visited processes in red, *i.e.*, upon receipt of a control message, a process colors itself red as illustrated in Figure 3.5.

At the same time, the local state of the process can be appended to the control message (or sent directly to the process initiating the algorithms). However, it is possible that the white messages are in transit while the local snapshots are being collected. Consequently, it is necessary to record the states of the channels (or links). A way of doing this is for red processes to send copies of these messages to the initiator and to use termination detection algorithms to determine when they have all arrived. When the cut message is traversing all the nodes in an elected node set and gathers local snapshot and messages in transit, all the nodes have their own local and global information. Each node always maintains and announces its local information called a trust level for a node proof, which contains information like a node's computing power, history information, etc., when it performs its local snapshot. By a global snapshot, all the nodes share the total number of elected nodes and the current global time since a recent global snapshot.

When a node wants to participate in the election, it may be accepted or rejected according to its trust level. When a set of elected nodes needs to decide some actions, then based on all of the gathered local and global snapshot information, nodes can vote for some decisions based on the collected information.




(a) An inconsistent cut message




(b) A consistent cut message

Figure 3.5: Global snapshot

## C. Election by extinction

Initially, all the nodes are qualified to become a chosen node within a finite time. During the extinction, only a node can be chosen as a final leader. If a node or a link shows some failures, *i.e.*, the node itself and nodes connecting to the link are not working properly, then the nodes automatically lose their qualifications to be chosen. Once a node belongs to the set of the elected nodes, it will keep its status until it does not meet its trust qualifications during the run. Unelected nodes do not participate in a consensus work because in the case of SSENCORE, we basically use a proof of trust mechanism. The total number of chosen nodes $N$ in a cluster is fixed in advance or can be varied upon the number of faulty nodes or required number of transactions. Initially, a low bound number of nodes is chosen for preventing faulty nodes from joining, and during the run, the number of chosen nodes is increasing till it reaches $N$. The chosen nodes are shared and compensated by a minimal amount of transaction fee instead of issuing new coins like a Bitcoin, thereby preventing excessive competition for mining and resulting in saving computing power and electric energy, while it provides a proof of the transactions' correctness.

## D. Consensus

There exist five types of failure modes as follows:

- Link failure: A link is said to be a fail if it remains inactive and the network gets

disconnected.

- Initially-dead process: A process is called initially dead if it does not execute a single step of its local program.
- Crash: A process is said to crash if it executes its local program correctly up to a certain moment, and does not execute any step thereafter.
- Byzantine behavior: A process is said to be Byzantine if it executes steps that are arbitrary steps and, not in accordance with its local program. In particular, the Byzantine process sends messages with an arbitrary content.
- Timing error: There is an additional failure in synchronous distributed systems, where a process executes correct steps but at the wrong time due to a slow or fast clock of the process.

Fischer et al.'s impossibility result shows that under some conditions, which include the nodes acting in a deterministic manner, they proved that consensus is impossible with even a single faulty process. The impossibility result was proven for a specific model [2]. First, it introduces the idea of incentives, which is novel for a distributed consensus protocol. This is only possible in Bitcoin because it is a currency and therefore has a natural mechanism to incentivize participants to act honestly. So Bitcoin does not quite solve the distributed consensus problems in a general sense, but it solves it in the specific context of a currency system. Second, Bitcoin embraces the notion of randomness. Also, it does away with the notion of a specific starting point and ending point for consensus. Instead, consensus takes place over a long time, about an hour in the practical system.

Let $f$ be the maximum number of faulty nodes. An initially-dead process is no longer a problem because it cannot be chosen and there are no initially-dead nodes in the elected node set. In the case of a link failure, it is impossible to reach consensus even in the synchronous case, and even if one only wants to tolerate a single link failure. Fortunately, the node with a link failure or unreliable link cannot be chosen as an elected node or it can be purged from the elected node set [6, 8].

As proven by Fisher et al. [7], there are no asynchronous, deterministic 1-crash robust consensus protocols known as the impossibility of consensus. To determine crash failures, at least $f$+1 rounds of message broadcast (or flooding) and $f$+1 number of elected nodes are required while in the Byzantine failure, $f$+1 rounds of

message broadcast and $3f+1$ number of elected nodes are also needed. To determine a minimal number of nodes to be chosen as an elected node initially, at least $3f+1$ nodes are required. The number of elected nodes can be explicitly indicated in an expression (1) where $N$ is the total number of nodes in an elected node pool.

$$3f+1 \leq \text{number of elected nodes} \leq N \quad (1)$$

After broadcasting (flooding) messages in $f+1$ number of rounds, every non-faulty node knows about all the values of all other participating nodes, thereby deciding the same value even under the occurrence of crash and Byzantine failures at nodes.

$$f+1 \leq \text{number of rounds of cut message} \quad (2)$$

## 3.3 Protocol

### A. Configuration

We describe configurations in our cryptocurrency network as follows:

- (Elected) Node: Once a node is elected, then the node runs entire functions requiring for the cryptocurrency processing.
- Unelected node: Although it is capable of running all the functions, it is not chosen as an elected node due to the limited number of available nodes at that instant. Once an elected node is to be proven that it is faulty or that it has crashed, then an unelected node can challenge to become a node again.
- Wallet device: A wallet has a two tier configuration, which consists of a smartphone and a credit card with an EMV chipset with a NFC chip, a fingerprint sensor, and a display. The device can be used to contact an ATM, a merchant's credit card terminal, and a smartphone installed with a LONDONCOIN's wallet app.
- Distributed ledger: The ledger containing all the transactions are recorded in a repository of the elected nodes where all the transaction records are stored in a chronological sequence and opened to all the users and unelected nodes. The whole distributed ledger at each elected node can be stored by compression for efficiency.

## B. Procedures

We explain some of the details about 4 major procedures relevant to LONDONCOIN cryptocurrency.

- **Dissemination**
  - A push and (conditional) pull gossip message is sent to the randomly chosen node.
  - By piggybacking, network size and termination detection of rounds can be determined for fast confirmations on transactions.
  - For disseminating information, it is not required to elect a special node as a leader.

- **Global snapshot**
  - Cut messages periodically are traversed from the message initiator to the rest of the elected nodes. When the cut message visits each node, it records its local state and visits adjacent nodes till it returns to its initiator.
  - During the cut message transversal, all the local states are collected and shared amongst the whole nodes. We are set to a one second time lapse for each global snapshot. During the interval, the global snapshot and consensus agreement are performing to obtain common information and detect node failure.

- **Election by extinction**
  - By introducing a concept of extinction, the number of required message to determine the elected nodes can be reduced.
  - Initially, some nodes with a high trust level as a proof of trust are only accepted and then they become elected nodes until it reaches the total number of nodes *N* in an elected node pool. All the works needed for cryptocurrency are processed among elected nodes.
  - Some malicious nodes can be screened by the election process.
  - By reducing unnecessary nodes and overly excessive freedom, performance will be enhanced.
  - It can be extensible to permissioned (public) and unpermissioned blockchain

systems.

- There are incentives for elected nodes, which can provide confirmation services for proof of trust. When LONDONCOIN is transferred to other cryptocurrencies or fiat currency ones, part of a transaction fee will be shared for the elected nodes.

➢ **Consensus**

- During the global snapshot, node failure can be detected via the elected nodes by circulating rounds of cut messages.
- Some internal and external threats can be eliminated by consensus.
- Consensus gives a low bound of minimal number of nodes and number of rounds of message gossiping (or rumor spreading) for making a decision given a condition of *f* faulty nodes.
- Due to global snapshot, a node causing a timing error can be eliminated.

## C. Correctness proof

We proved the correctness of the protocol by establishing the safety and the liveness of the protocol. Safety corresponds to the protocol producing an estimate, which is less than (or equal to) the exact global time *GT*. Liveness corresponds to the protocol producing monotonically increasing estimates. We first establish the safety property. Let *GT(t)* be the exact *GT* at time *t* and *GT(t)* be the approximate *GT* as computed by our protocol at time *t.*

THEOREM 4.1 (SAFETY) Let *t* be the instant at which *GT(t)* is computed. The $GT(t) \leq GT(t)$. PROOF. *GT(t)* is computed by the initiator $\Leftrightarrow$ *count* = 0. *count* = 0 $\Leftrightarrow$ there are no white messages in transit. Hence, we need only concern ourselves with the timestamps of red messages in transit when computing the *GT*, *i.e., GT(t)* = *min*{timestamp of all nodes at time t, timestamps of red messages in transit at time *t*}. From the protocol,

$$GT(t) = min\{min(lt), min(ts)\}$$

where *min(lt)* = minimum of the nodes' timestamps for all the nodes, *i.e.*, *lt* = each local node's timestamp, and *min(ts)* = minimum timestamps of all of the red message since each node became red. The *min(ts)* $\leq$ timestamps of all red messages in transit at *t* since the red messages in transit at time *t* form a subset of all the red messages sent since each node became red. Furthermore, at time *t,* no *lt* can be less than the minimum timestamp of the red messages in transit at time *t*. (These are the only messages which can roll back a node since

the cut message has visited all of the nodes except the initiator prior to time $t$.) Hence, we conclude that $GT(t) \leq GT(t)$. ■

We now establish the liveness of the protocol.

THEOREM 4.2 (LIVENESS) *if* $t_1 < t_2$, then $GT(t_1) \leq GT(t_2)$.

PROOF. After the computation of $GT(t_1)$, it is possible for one of the nodes to be rolled back by a red message, but not by a white message (the white messages have all arrived). However, the minimum timestamp of the red messages in transit is included in the definition of $GT(t)$ and by virtue of this definition, the $GT(t_2)$ cannot decrease subsequent to the computation of $GT(t_1)$, the theorem follows. ■

THEOREM 4.3 Node coloring and choosing a leader in the course of node election can be achieved within a finite time.

PROOF. Suppose that the channels in the network have a finite transmission time, that transmission is fault-free, and that a node takes finite time $\delta$ to be colored. If all of the nodes begin to color at the same instant, the time for coloring will be $\delta$. Otherwise, if the nodes are colored sequentially, in the worst case, it takes $N\delta+\varepsilon$, where$\varepsilon$is the time for the cut event to traverse the network and $N$ total number of nodes participating in the snapshot. Therefore, choosing a leader requires time $\leq N\delta+\varepsilon$. ■

## 3.4 Comparisons

Table 3.1 compares a traditional approach based on a central server, Bitcoin blockchain, and ours. SSENCORE is providing preventions of all the failures, thereby guaranteeing to run well under even any kinds of network configurations and security threats.

Table 3.1 Comparison of features

| Features | Traditional approach (Central Server) | Bitcoin Blockchain | **SSENCORE** |
|---|---|---|---|
| Fairness | No | Yes | Yes |
| Low computation | Yes | No | Yes |
| Resilience to DoS | No | Yes | Yes |

| | | | |
|---|---|---|---|
| No single point of failure | No | Yes | Yes |
| Network configuration | Static | Dynamic | Adaptive |
| Cryptographic proof of receipt | No | No | Yes |
| Cryptographic proof of transmission | Yes | Yes | Yes |
| Trusted consensus timestamps | No | No | Yes |
| Scalable | Yes | No | Yes |
| Immutable record for audits | No | Yes | Yes |
| Distributed trust | No | Yes (Power of Work) | Yes (Asynchronous BFT) |
| Reliable storage and high availability | No | Yes | Yes |
| Preventing failures (Link failure, Crash, Byzantine behavior, Timing error) | No | Byzantine behavior | All the failures |
| Actions for security threats | Passive | Passive | Active |
| Performance (tps) | Visa 2,000 (within 7 seconds processing)<br>-Daily peak: 4,000<br>-Peak capacity: 56,000<br>-Peak shopping period: 18,700<br>PayPal: 50-100 | 7 | 200,000 (global coverage and within 7 seconds processing) |

# 4 Conclusions

In this paper, we introduced a cryptoecosytem consisting of a core cryptocurrency, a decentralized exchange, and a biometric-based hardware wallet. In order to create a cryptoeconomy based on a cryptoecosystem, realizing factors such as scalability, security, and stability as a steamroller can provide dominant features into the cryptoeconomy.

First of all, our cryptocurrency LONDONCOIN is designed to enable and to support real-time payments and transactions, which is more powerful than VISA's current processing rate by focusing on the scalability aspect. To realize the goal, we are using the following SSENCORE protocol: 1) extending to an unpermissioned (or public) blockchain system only from a permissioned one, by using a partly distributed control which can decide between good nodes and bad ones based on the cooperation amongst nodes in the whole network; 2) unlike other

cryptocurrencies, only the chosen nodes satisfying a certain trust level can maintain its number of active nodes by adding or purging nodes in the set. Basically, if some nodes with powerful computing resources may collude with other nodes, then they may be not elected or purged from the elected active node list; 3) rapidly reaching to information dissemination by changing from a push-based gossip to a push and (conditional) pull based gossiping (or rumor spreading); and 4) promptly deciding to reach a consensus by a global snapshot.

Secondly, we are reinforcing a security level to guard anti-threats and protect privacy by providing a biometric-based fingerprint card as a digital hardware wallet as well as a decentralized exchange, in which it does not have a single point of failure such as centralized servers or databases that are prone to hacks. Furthermore, this exchange could continuously operate, no matter the political climate of a nation, such as governments shutting down the exchanges (*i.e.* the Chinese exchange shutdowns), and the exchange can respect the privacy of its users and not ask for numerous registrations and KYC (Know Your Customer) verifications.

Finally, we are not encouraging competitive mining from all the participating nodes. In a PoW based consensus, only one node can have additional Bitcoins as eventual winning compensation by enormously consuming electric energy and computing resources. On the other hand, only the chosen nodes that are proven to be trustworthy can participate in the proof of trust, and all of the nodes share a transaction fee for transfer payment and a node fee for connecting nodes to access a blockchain as incentives.

Maintaining stability as a currency is a very important aspect. The main reason why current cryptocurrency cannot be exchanged like fiat currencies such as the dollars or the euros is due to the lack of stability regarding the exchange rate. To prevent this, our cryptocurrency is to be endowed with an intrinsic value. 10% of the transaction fees are paid out for all the nodes as a form of compensation, and the rest will be deposited as gold. The deposited gold can be representing as a stake that is proportional to the number of fully owned LONDONCOINs in order to guarantee stable trading and transactions. Once the transactions continue, then the value of our deposited gold also accumulates. Thus, the LONDONCOIN can be defined as a value-creating currency unlike other cryptocurrencies. We expect our cryptoecosystem to act as a unity that outperforms better than other individual solutions such as a cryptocurrency, an exchange or a wallet.

Shortly, we expect to make a debut for our cryptoecosystem soon. For instance, a prototype of our wallets was issued in late 2017 and a marketable wallet and a DApp called

FlySafe will be released in 2018. Moreover, we have been implementing a decentralized exchange and a core coin platform. Finally we hope that our cryptoecosystem can bring bold changes that will break down the many uncertainties and concerns that exist in the current market of cryptocurrencies and even fiat ones.

# OUR OTHER PROJECTS

## A. SSENDEX

### A.1 Exchanges

Prior to the introduction of a centralized exchange, we briefly need to understand what a web portal site is in retrospect. A portal is a term that is generally synonymous with gateway for a World Wide Web (WWW) site that is or proposes to be a major starting site for users when they are connected to the Web or that users tend to visit as an anchor site. There are general portals as well as specialized or niche ones. For instance, some major general portals include Yahoo, Excite, Naver, Daum, etc. Examples of niche portals include Fool.com (for investors), and TechCrunch.com (for the latest technology news and information). A number of large access providers offer portals to the Web for their own users. Most portals have adopted the Yahoo style of content categories with a text-intensive, faster loading page that visitors will find easier to use and to return to. Companies with portal sites have attracted more stock market investors' interests because portals are viewed as being able to command large audiences and numbers of advertising viewers. Typical services offered by portal sites include a directory of websites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum. Before a web browser that was based on a graphic user interface was introduced, only a small minority of people like engineers, researchers, and scientists used the Internet at that time. The majority of the general public did not have easy access to the Internet because all of the applications and services were designed by a command line interface. Since the first graphical web browser known as NCSA's Mosaic has been introduced to the public in 1993, they prefer to access the portal sites instead of visiting certain specific sites by search due to the fact that the portal site has all of the information that they need.

The situation that we have encountered at present seems to have a *déjà vu* effect, since there has been a very similar situation in the early 1990s. When people want to trade cryptocurrencies, it is not easy to find a proper marketplace or traders in a peer-to-peer network environment nor to get accustomed to a new technology. Thus, they definitely prefer to visit a centralized exchange site like a portal site, which can easily access an order book with buy/sell prices and quantities, trading patterns, and charts. Although Satoshi Nakamoto insisted that "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly

from one party to another without going through a financial institution" in his/her or their whitepaper [3], at present, most trading is still processed through a financial institution called an exchange as shown in Figure A.1. All of the security breaches and accidents mainly derive from the centralized exchange rather than being the flaws that exist in cryptocurrencies. We want to solve the issues by introducing a decentralized exchange.

A person who wants to trade cryptocurrencies must register at an exchange site in advance. Then the site automatically generates a wallet including a pair of keys with a private key and a public one for its newly registered customers and maintains all the wallets' information for its customers. Offered data such as buy and sell information provided by traders is shared amongst all the traders. The exchange performs trading by using its trading algorithm.

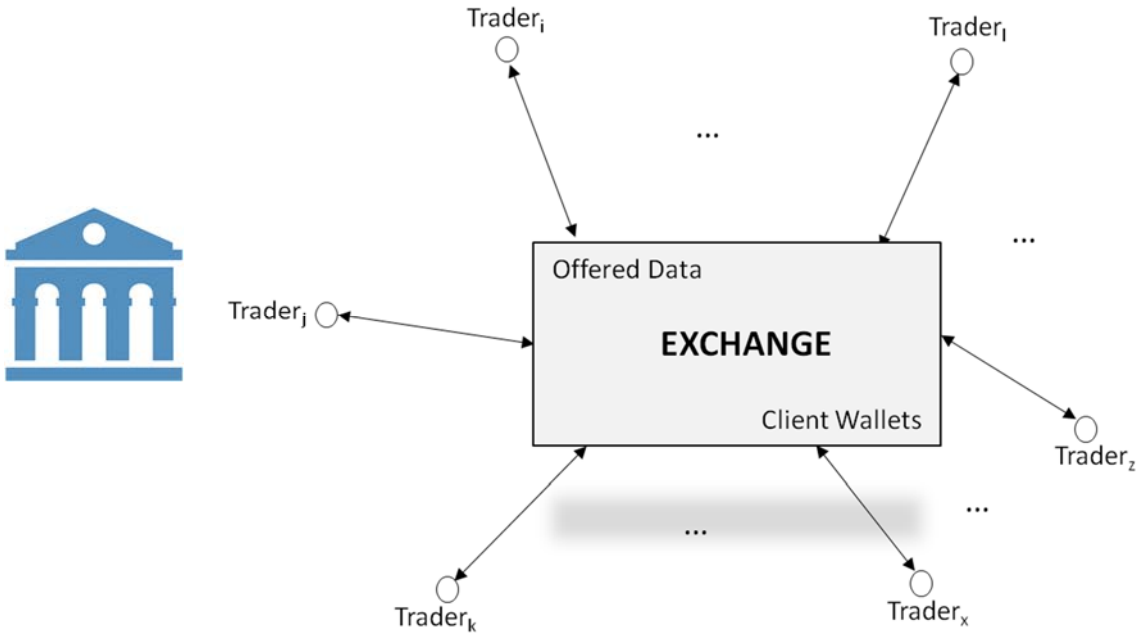



Figure A.1: A traditional exchange

There are pros and cons to using centralized exchanges. One of the big advantages is that exchanges help connect the cryptoeconomy and the flows of cryptocurrencies with the fiat currency economy, so that it is easy to transfer the value back and forth. The disadvantage is a risk. You encounter the same kinds of risk that you face with banks. The first risk is the risk of a bank run. A run occurs when many people show up at the same time and they demand their money back. Since the bank maintains only fractional reserves, it might be unable to cope with the simultaneous withdrawals. The danger stems from the general panic behavior. Once the

rumor starts to circulate that a bank or exchange might be in trouble and might start refusing to honor withdrawals, then people stampede in, in order to try to withdraw their money ahead of the crowd, and as a result, there is an avalanche of demands. The second risk is that the owners of the banks might have fraudulent intentions by running a Ponzi scheme. This is a scheme when an individual gets people to give them money in exchange for profits in the future, but instead, they take their money and use it to pay out the profits to people who have bought previously. Such a scheme is doomed to eventually fail and cause a lot of people to lose a massive amount of money. The third risk is that of a hack. The risk that someone, perhaps even an employee of the exchange, will manage to penetrate into the security of the exchange. Since exchanges store key information that controls large numbers of cryptocurrencies, they need to be careful about their software security and their procedures, as well as how they manage their cold and hot storage. If something goes wrong, your money could get stolen from the exchange.

To understand cyrptocurrency exchanges, we are looking back at how banks or bank-like services operate in the traditional economy. You deposit your money at a bank and the bank promises to give you back that money later. In fact, the bank does not solely take your money and put it in a box in the bank's vault. All that the bank does is to maintain a promise; that is if you ask for the money, then they will give it back to you. The bank typically invests the money somewhere else. In addition, the bank keeps some money in reserve to make sure that it can pay out the demand for withdrawals on a typical day, or maybe even on an unusual day. Many banks typically maintain a reserve called a fractional reserve. Thus, they keep a certain fraction of all demand deposits in the reserve just in case [2].

A cryptocurrency exchange performs businesses that function in a similar way to that of a bank. They accept deposits of cryptocurrencies and they will maintain a promise to give them back when demanded later on. You can also transfer fiat currency into an exchange by transferring from your bank account. The exchange promises to pay back either or both types of currency on demand and the exchange lets you do various banking-like activities. You can make and receive cryptocurrency payments. That is, you can direct the exchange to pay out some of the cryptocurrencies to a particular party, or you can ask someone else to deposit funds into the particular exchange on your behalf, and put the coins into your account. You can also exchange for fiat currency or vice versa. Typically, cryptocurrency exchanges complete the exchange by finding a customer who wants to purchase cryptocurrencies with dollars and another customer who wants to sell cryptocurrencies for dollars, and to match them up. In other words, they try to find customers that are willing to take opposite positions in a transaction. If

there is a mutually acceptable price, they will complete that transaction.

A decentralized exchange is different from the centralized one, which is illustrated from Figure A.2. First, the decentralized exchange presented in a dotted line does not share any information such as wallets and offered data about traders. Each trader has his/her own wallet and offered data, and the offered data is shared across amongst all the traders by using an information dissemination protocol. For example, offered data of a $Trader_i$ has to be transferred to the rest of the traders' offered data while offered data of the rest of traders are to be simultaneously exchanged to the $Trader_i$.

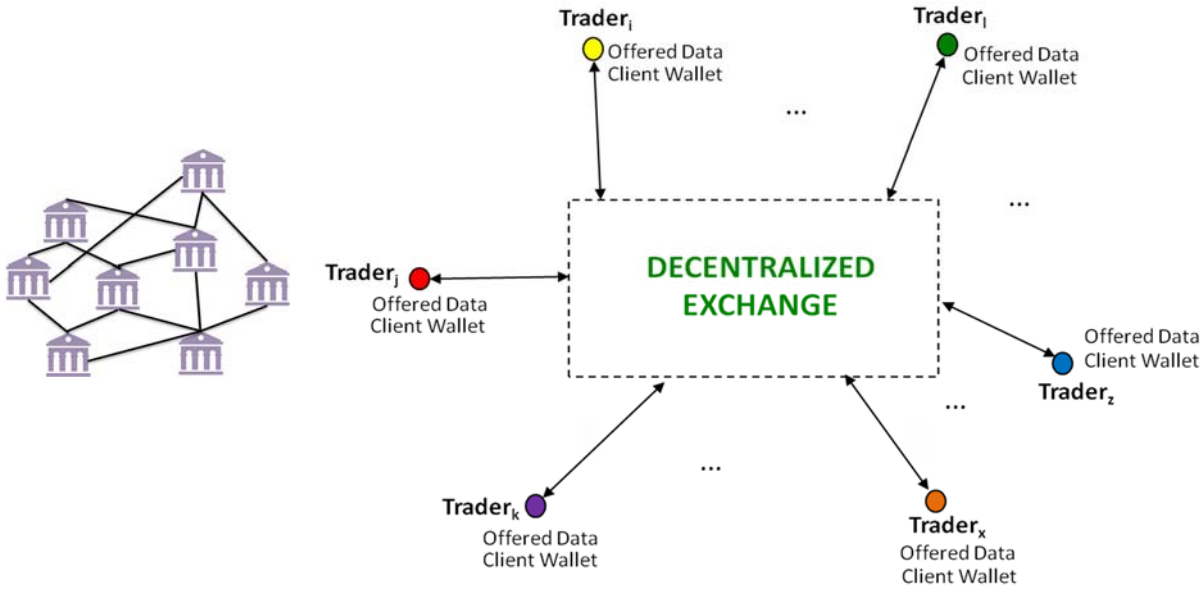



Figure A.2: Our decentralized exchange, SSEN DEX

## A.2 Sharing a virtual order book

In a centralized exchange, all of the offered data given by each trader is stored and managed as an order book. If a trader wants to trade cryptocurrencies, then he/she offers the same or similar trading conditions such as a buy or a sell, buy or sell price and quantity, etc. by referencing an order book, a balance, current exchange rates, real-time charts and trends. Then the offered data is to be matched and traded by an exchange's trading algorithm.

A decentralized exchange is completely different from the centralized one as shown in Figure A.3. The decentralized exchange does not have any information relevant to trading about other traders. Each trader has their own wallet and intentions for trading. Our most

distinguished feature is a method to disperse the trader's intentions and to consistently share them amongst all the traders as soon as possible. Therefore, this means that all of the traders have the same virtual order book, from which each trader has the same view of information as the centralized exchange. We call the intention data for trading as a virtual (simulated or intentional) order book, which is slightly different from an actual order book in a centralized exchange. The trader who composes the intention data disseminates it, which is signed by the sender's secret key to prevent a forgery of the data. The detailed format is shown in Figure A.4. The shaded part represents the encrypted data signed by a sender. Except for the sender's ID, all the data is signed by a sender's secret key. In particular, a valid time-to-live field is allowed for a trader's intention to exist during a finite time period in a peer-to-peer network and a trader's mobile device.

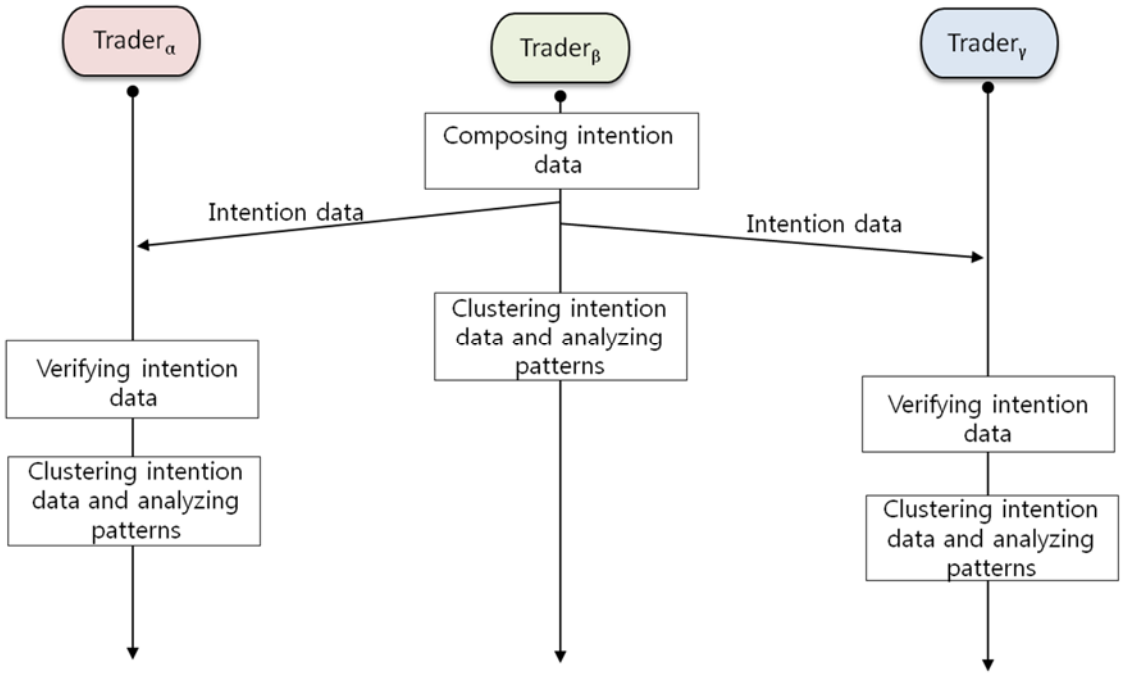



Figure A.3: Spreading and sharing buy/sell (or bid/ask) intention data

If a Trader$_\beta$ wants to buy or sell cryptocurrencies, then the trader composes the intention data and disperses the data by a gossiping or rumor spreading protocol. By using the same dissemination protocol based on a push and (conditional) pull message spread used in a SSENCORE, the intention data is distributed to all of the traders. When the rest of the traders receive the intention data, each trader verifies the intention data by decrypting a sender's identifier and computes data clustering of the intention data and analyzes its relevant trading patterns in order to support precise and foreseeable trading. To do trading, the trader's mobile

device has to install an app called an *ssendex* agent, which has an inherent trading program.

For each trader to have the same consistent offered data, each trader who has intention to complete trading in advance has to publish his/her intention to the rest of the traders in a periodic interval or an event basis.

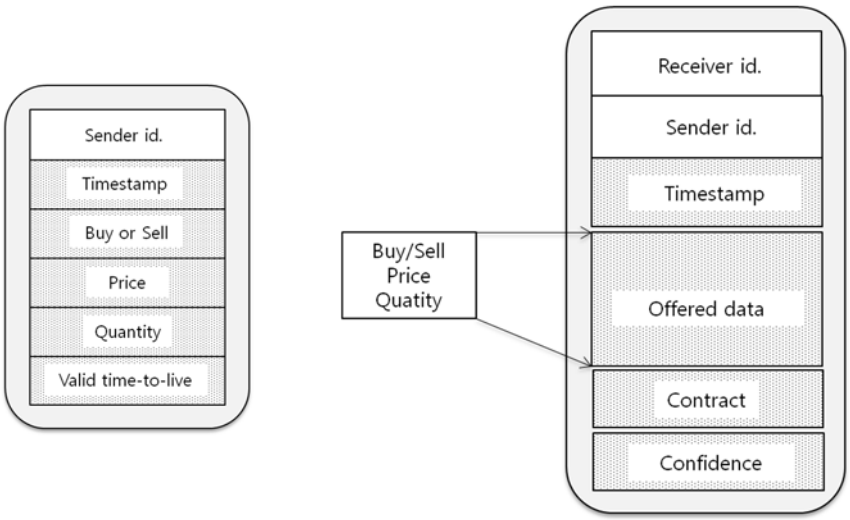



Figure A.4: Packet formats of Intention and Offered data

## A.3 Trading

Based on the virtual order book, if $\text{Trader}_{\alpha}$ decides to trade with $\text{Trader}_{\beta}$, the trading process in a consecutive sequence is illustrated by Figure A.5. The $\text{Trader}_{\alpha}$ prepares offered data for the trading and sends it to his/her trading partner $\text{Trader}_{\beta}$ directly. When the receiving partner receives the offered data, the $\text{Trader}_{\beta}$ is verifying against forgery and any integrity disaccords from the received offered data. If $\text{Trader}_{\beta}$ finally decides to proceed with the offered trading, then the trading result is sent to $\text{Trader}_{\alpha}$ and the corresponding traded offer can be submitted to the traded cryptocurrency's distributed ledger and it will be confirmed at the ledger. Therefore, we are aiming for our decentralized exchange to be designed not solely for a specific cryptocurrency, but for one that is applicable to all types of cryptocurrencies.

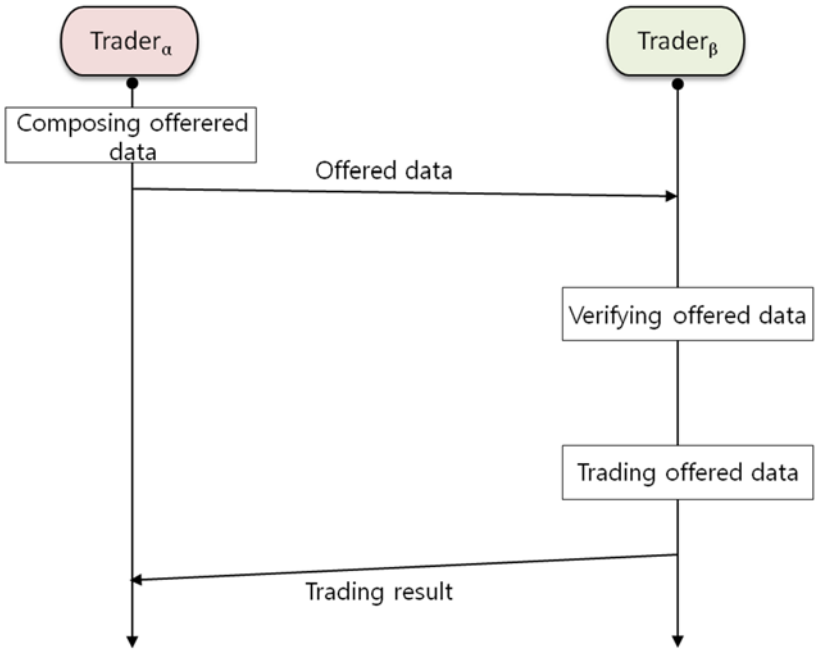



Figure A.5: Trading process

# B. SSEN WALLET

In general, cryptocurrencies do not exist in a user's computer or a smartphone; rather they exist as an entry in a distributed ledger. The ledger holds the amount of funds available for each address and an address is like a bank account. The private key associated with an address is used to sign a transaction spending the funds from that address. A cryptocurrency wallet is simply a collection of private keys. Although a wallet derives its name from an analogy with a physical wallet, a wallet is a piece of software that allows the spending of funds from the addresses in a wallet and to manage the wallet. The tasks performed by the wallet software usually include the following:

- Querying the distributed ledger and presenting to the user a total of the funds available
- Generating new addresses to receive new funds, or to receive the change coming from transactions performed by the wallet software
- Interfacing with the user, for instance, generating or reading QR codes represented by addresses, and transactions, etc.
- Allowing the user to send funds to chosen addresses. To accomplish this, the wallet must gather addresses with enough funds under its control, assemble a transaction that is spending the funds from these addresses or to select an existing one to send back the change, sign the transaction with all of the private keys, and to publish the transaction to the distributed ledger
- Tracking transactions' confirmation status
- Making a backup of the wallet
- Restoring a backup into the wallet

If you want to store your cryptocurrencies locally, you usually use a wallet which can keep track of your coins, contain your keys and manage them, and make things more convenient when using it. A wallet gives you a simple interface that tells you how much is in your wallet. When you want to spend cryptocurrencies, your wallet handles all the details of which keys to use, how to generate new addresses, and so on. When figuring out how to store, manage, and use the keys, three goals are to be considered [2].

- Availability: being able to actually spend your coins when you want to use it
- Security: making sure that nobody else can spend your coins

- Convenience: managing your keys should be relatively easy

Our biometric-based hardware wallet called SSEN Wallet is shown in Figure B.1. Unlike a USB-based dongle type device for a PC or a notebook, it achieves the aforementioned goals by solely focusing on a wireless mobile communication device, such as a smartphone. Moreover, it implements a hierarchical deterministic wallet amongst several types of wallets, which allows the cold side (a card with a credit card form factor) to use an essentially unbounded number of addresses, but also a hot side (a smartphone) with a trading algorithm and a user interface to only know about these addresses with only a short, one-time secret communication between the two parties.


Figure B.1: A HW based wallet with a biometric fingerprint sensor

The wallet implemented by a patented technology consists of a tamper-resistant EMV chipset, a fingerprint sensor, a built-in rechargeable battery with a reinforced battery life time comparable to the usual credit card's expiration terms such as 5 years' usage, a tiny display, a NFC enabled communication means, and an ambient light detection sensor, and a private key that is stored at the HW-based card and a public one that is maintained within a smartphone. When a user takes out of his/her SSEN wallet, then the wallet detects ambient lighting and works automatically. By scanning a fingerprint, it will be operating for a fixed, temporary time period. Once it passes the authentication test, then the user can use the wallet after, and a display window can display a quick response (QR) code that expresses the key for easy transaction. In addition, this wallet device can also be used as a general credit card or an entry card requiring identity authentication and authorization. For this specific application, we release a SSEN Card based on the same platform for this kind of market.

# References

1. Tapscott, D. and Tapscott, A., "BLOCKCHAIN REVOLUTION: How the Technology behind Bitcoin is Changing Money, Business, and the World", Penguin Random House LLC, 2016.

2. Narayanan, A. et al., "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, 2016.

3. Nakamoto, Satoshi, "*Bitcoin: A Peer-to-Peer Electronic Cash System*", https://bitcoin.org/bitcoin.pdf, 2008.

4. CISCO, "*Visual Networking Index: Forecast and Methodology, 2016-2021*", June 2017.

5. Bondi, A., "*Characteristics of scalability and their impact on performance",* Proceedings of the second international workshop on Software and performance, WOSP '00, page 195, 2000.

6. Lamport, L., Shostak, R. and Pease, M., "*The Byzantine Generals Problems*", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pages 382-401, 1982.

7. Fischer, M., Lynch, N. and Paterson, M., "*Impossibility of Distributed Consensus with One Faulty*", Journal of the ACM, Vol. 32, No. 2, pages 374-382, 1985.

8. Attiya, C., Dolev, D., and Gill, J., "*Asynchronous Byzantine Agreement*", In Proceedings, the 3rd Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, pages 119-133, 1984.

9. Lamport, L., "*Time, clocks, and the ordering of events in a distributed system*", Communications of the ACM, vol. 21, pages 558-565, 1978.

10. Chandy, M. and Lamport, L., "*Distributed Snapshots: Determining Global States of Distributed Systems*", ACM Trans. on Computer Systems, Vol. 3, No. 1, pages 63-75, 1985.

11. Lai, T. and Yang, T., "*On Distributed Snapshots*", Information Processing Letters, Vol. 25, No. 1, pages 153-158, 1987.

12. Mattern, F., "*Efficient Algorithms for Distributed Snapshots and Global Virtual Time Approximation*", Journal of Parallel and Distributed Computing, Vol. 18, pages 423-434, 1993.

13. Demers, A. et al., "*Epidemic Algorithms for Replicated Database Maintenance*". Proceedings of the Sixth Annual ACM Symposium on Principles of Distributed Computing (PODC), pages 1-12, 1987.

14. Popov, Serguei, "*The Tangle*", https://iota.org/IOTA_Whitepaper.pdf, 2017.

15. Micali, Sylvio, "*ALGORAND The Efficient Public Ledger*", CSAIL, MIT, https://arxiv.org/pdf/1607.01341v7.pdf, 2016.

16. Baird, Leemon et al., "*Hedera: A Governing Council and Public Hashgraph Network*", https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.0-180313.pdf, Mar. 2018.

17. Castro, M. and Liskov, B., "*Practical Byzantine Fault Tolerance*", Proceedings of the Third Symposium on Operating Systems Design and Implementation, Feb. 1999.

18. Schwartz, D. et al., "*The Ripple Protocol Consensus Algorithm*", Ripple Labs Inc., https://ripple.com/files/ripple_consensus_whitepaper.pdf, 2014.