# LondonCoin: Reinventing cryptocurrencies

Myongsu Choe, Ph.D.
Email: myongsu.choe@gmail.com

## Abstract

We reinvent current cryptocurrencies with LondonCoin by analyzing inherently existing vulnerabilities and by proposing our innovative solutions. Our insights indicate that by determining good nodes and bad ones, and by seamlessly integrating traditional currencies with our cryptocurrency, major properties of scalability, security, and safety can be enforced to significantly match the current financial system and be placed in a pivotal position between traditional currency and cryptocurrency.

Key words: cryptocurrency, blockchain, trust, consensus, proof of trust, scalability, security, safety, gold backed cryptocurrency, biometric system on-card.

# 1 Introduction

A Bitcoin: a forerunner cryptocurrency based on a blockchain has been introduced into the market around 2009. Since then, it created a new market and caused the generation of more than 1050 coins such as Ethereum, Litecoin, Ripple, iota, etc., known as Bitcoin alternatives or alternate coins (altcoins), and made a market capacity worth 123 billion dollars [1] exponentially. What does it bring to the market? Rather than trading one cryptocurrency, the fundamental concept of a blockchain may have enormous potential so that it will change from the current Internet of Information to the Internet of Value 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 the traditional services provided by the middle man [1, 2].

Since nearly a decade of their existence, cryptocurrencies are used to some extent and traded in a market. People can transfer the cryptocurrency to someone who lives in a foreign country and who does not even have a bank account; thereby paying lower transfer fees that

[1] https://coinmarketcap.com/

are not comparable with the middle man like the 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 US or Euro dollars with the Internet or an ATM equipment in certain regions. Numerous applications based on the blockchain are not limited to the currency but are expanding in many areas, namely in the arts, gaming industry, music, intellectual properties, land registration certificates, agricultural products, etc.

On the other hand, excessively speculative trading market conditions are unexpectedly fluctuating so that they can reluctantly accept the cryptocurrency as actual money. In addition, 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 payment, which brought about investigations from law enforcement authorities. Due to the lack of security, a Bitcoin exchange called Mt. Gox was hacked and all the Bitcoins assigned and stored from the customers were gone, resulting in the bankruptcy of the exchange. Presently, some governments such as Japan and the Unites States are acknowledging cryptocurrencies as an alternative of the current fiat currency and want to monitor them and introduce regulations and taxation like securities for all of the transactions, in order to prevent investors from fraud and loss.

Therefore, we are proposing an innovative approach for our coin called LondonCoin (also known as, LDC), thereby clearly resolving the aforementioned issues.

# 2 Critical issues

We have to examine all the major cryptocurrencies in comparison with the traditional ones called fiat currency and analyze its pros and cons in order to reinvent an innovative form of cryptocurrency. Therefore, we extract major essential properties such as safety, security, and scalability, which are required for a new cryptocurrency implementation.

## 2. 1 Safety

We do not expect that the traditional currency will be wiped out and that the cryptocurrency will suddenly substitute it in the near future. Thus, the cryptocurrency has to coexist with the fiat one. People can freely use their cryptocurrencies like the traditional one when buying and exchanging, paying, transferring, withdrawing their money from the ATM and more. In addition, its exchange price in a market has to be stable while most cryptocurrencies are unexpectedly fluctuating so that it can be traded in a cryptocurrency market to a certain degree. In a real market, it is difficult to trade them since merchants are reluctant to accept the currencies due to the uncertainty of the traded price. These are the real challenges that most cryptocurrency supporters do not want to acknowledge.

Our solution: We want to issue a gold backed cryptocurrency which is reminiscent of a historical event that occurred on August 1971 when the US government unilaterally terminated the convertibility of the US dollar to gold. Another solution is to integrate it with normal cryptocurrency, which can be also used in entertainment and gaming as usual. For both of the cryptocurrencies, by reflecting the current price of gold, the US dollar, and Euro dollar, which is a similar way to determine the present fiat currency's exchange rate, we will add some degree of control in order to make our cryptocurrency stabilized within a constrained exchange rate.

## 2.2 Security

A computer that connects to the cryptocurrency network is called a node. In the case of Bitcoin, there are nodes that fully enforce all of the rules of the Bitcoin called full nodes. In addition to the node, a digital wallet consisting of a file containing keys and the amount is stored in a smartphone or a notebook 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. Because there are no limits for the number of nodes that can participate in the cryptocurrency network, all the nodes may not have a definite chance to update the same software version at the same time, which commonly results in a permanent divergence in the blockchain known as hardware fork and coin fragmentation. Even in the worst case possible, it may occur that two different coins are separately traded.

All the nodes participating as a peer-to-peer based cryptocurrency network may cause some vulnerabilities in terms of security. 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 degrade the whole trust in the network. Some nodes may act as a host for masquerading DoS.

In addition, all the digital wallets stored in a mobile device like a smartphone and a notebook might be lost so that anyone can illegally steal and use it. And the digital wallet itself has some limitations when it comes to buying and selling some merchandises and services via the mobile devices.

Our solution: We want to control nodes in the cryptocurrency network to countermeasure security threats by determining a node's trust into a good node or a bad one. And a digital hardware wallet known as a SSEN[2] credit card which is a biometric system on-card that integrates a current EMV chip credit card by adding a fingerprint sensor and a display, which is going to be issued for bridging a fiat currency and 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 [3]. For example, suppose that a cryptocurrency is designed to cover up worldwide economic transactions including cash. To provide global transactions, we need to know our competitor's 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. In addition, to be able to withstand DoS attacks, it implies that our currency will be set to a target comparable to Visa's.

Our solution: LondonCoin will match Visa's performance.

## 3 LondonCoin

### 3. 1 Partly distributed control

As a centralized network and a peer-to-peer (or fully distributed) based network are shown in Figure 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, which mediates and relays as a middle man. All the nodes in a (pure or full) peer-to-peer network are working in an autonomous way and all 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

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

failure, while the distributed one is the most difficult to maintain. When it comes to fault tolerance and stability, the centralized one is highly unstable because the center node is down, which results in the whole network not working, but 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 very low scalability and the distributed one has high scalability.

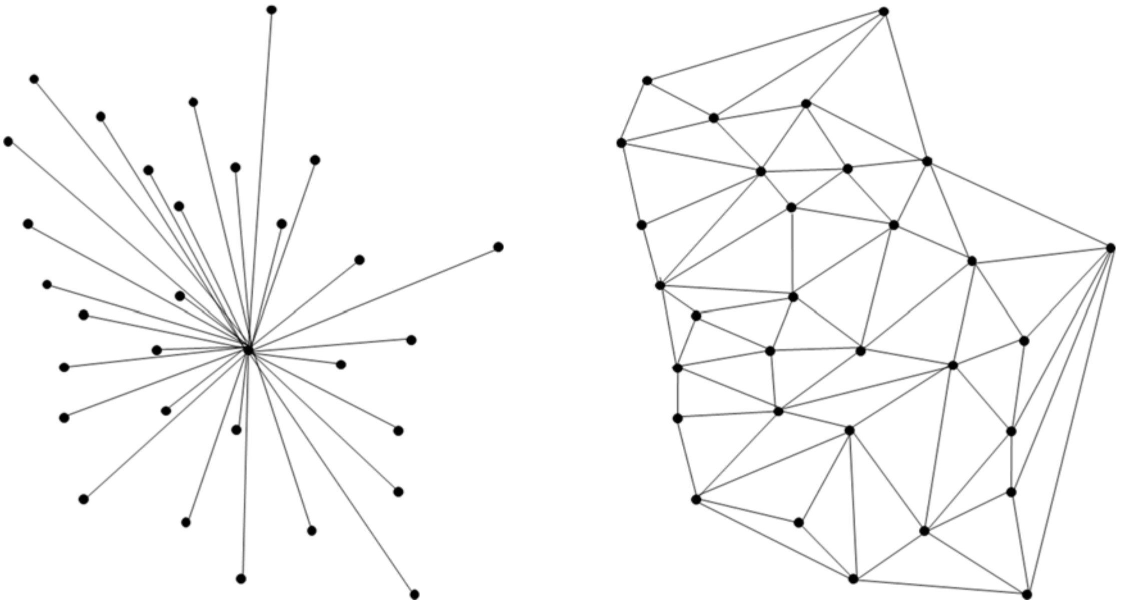

Figure 1: A centralized network and a peer-to-peer (fully distributed) one

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 (or fully distributed) 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 teams), from which we schematically represent the partly distributed network in Figure 2. The dotted circle 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 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 is formed as a clique (or complete graph) to rapidly exchange messages among nodes where each pair of nodes is directly connected by an edge with one diameter.

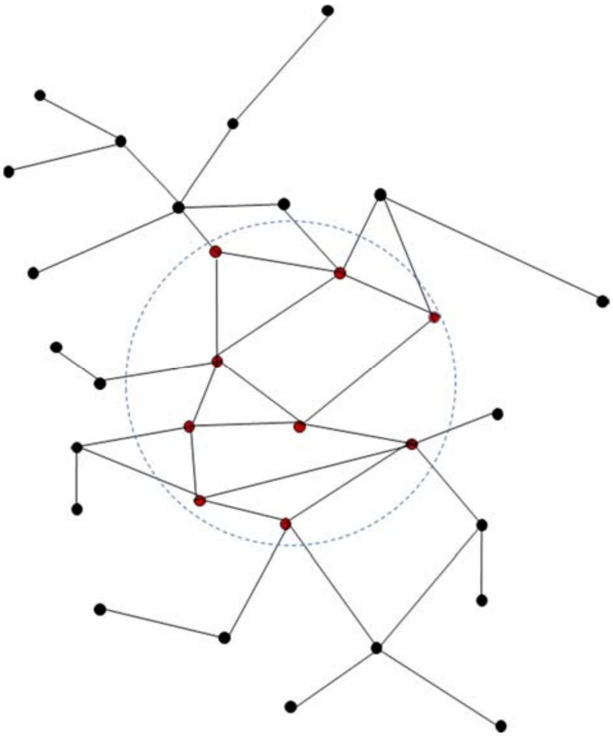

Figure 2: Partly distributed (clustered or hybrid) network

## 3.2 Deciding the Good, the Bad and the Ugly[3]

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 LondonCoin protocol. A decision process consists of three steps: Global snapshot, Election, and Consensus. The global snapshot is to construct explicitly a system-wide (or network-wide) global configuration consisting of local states (snapshot states) of each process. 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 is a process to choose

[3] 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.

an arbitrary node from the whole node set and all the nodes can be legitimately chosen depending on the satisfaction of qualifications. The consensus is a process where all the nodes are reaching 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. Global snapshot

The notion of a cut underlies the construction of global snapshot algorithms [7, 8, 9]. As shown in Figure 3, 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.

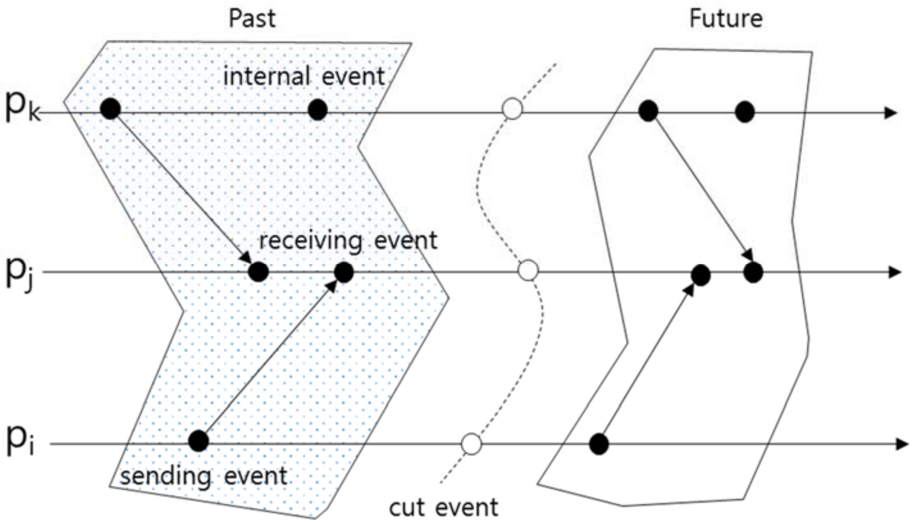

Figure 3: A cut message

Lai and Yang [8] 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 black when taking a local snapshot, (2) every message sent by a white (black) process is colored white (black), and (3) every process takes a local snapshot before a black message is received. Ensuring that a local snapshot is taken before a black 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 black, 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 black, *i.e.*, upon receipt of a control message, a process colors itself black as illustrated in Figure 4.

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 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 black 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.

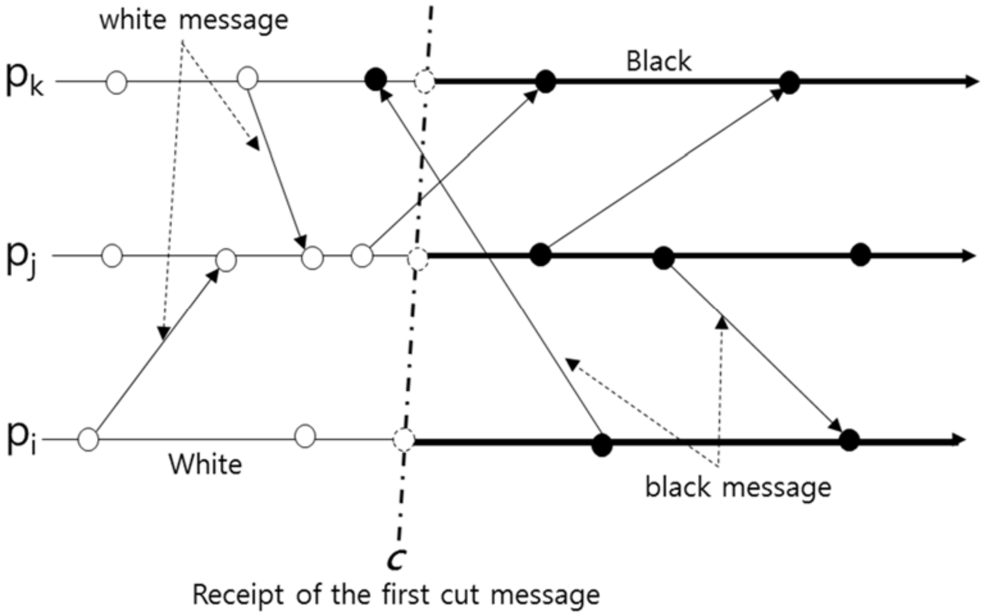

Figure 4: Global snapshot

## B. Election

Initially, all the nodes are qualified to become a chosen node. 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. Unchosen nodes work as a wallet or a SPV (Simple Payment Verification) in a Bitcoin jargon, and the nodes are not participating in mining (proof of work or proof of stake, in the case of LondonCoin, we name it as proof of trust). The total number of chosen nodes *N* are fixed in advance or varied upon the number of wallets and 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 payment transit instead of issuing new coins, thereby preventing excessive competition and resulting in saving computing power and electric energy, while it provides proof of the transactions' correctness.

## C. 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.

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 purged from the elected node set [4, 6].

As proven by Fisher et al. [5], 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 3$f$+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 3$f$+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.

$$3f+1 \leq \text{number of elected nodes} \leq N \tag{1}$$

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.

$$f+1 \leq \text{number of rounds of cut message} \tag{2}$$

# 4 Protocol

## 4.1 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; it can only support to send and receive to adjacent elected nodes. It is similar to SPV in Bitcoin.
- Digital hardware wallet: This wallet has a form factor of a credit card with an EMV chipset having compatibility to a NFC chip, a fingerprint sensor, and a display, and it stores and manages the owner’s keys and the account amount in its secret

memory. It can be used just for the ATM and the merchant's credit card terminal or LondonCoin.

- 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.

## 4. 2 Procedures

We explain some details about four major procedures relevant to LondonCoin cryptocurrency.

A. 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 2 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.

B. Election

- Initially, some nodes with a high trust level are accepted and then they become elected nodes until it reaches the 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.

C. 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 broadcast (flooding) for making a decision given a condition of $f$ faulty nodes.

- Due to global snapshot, a node causing a timing error can be eliminated.

D. Proof of Trust

- In a blockchain, block size is dynamically varied upon the number of transactions in the corresponding time interval.
- There are no incentives for nodes, which can provide mining services for proof of trust. Instead, when money is transferred to and from cryptocurrencies and the fiat ones, a minimum transfer fee will be shared for the elected nodes.
- The whole distributed ledger at each elected node can be stored by compression for efficiency.
- An average block time which is required to validate current block and add it to a distributed ledger is designed to be within two seconds, while Bitcoins corresponds to 10 min., Ethereum 15 sec., Ripple 3.5 sec., and 2.5 min for Litecoin.

## 4. 3 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 $\mathcal{GT}(t)$ be the approximate *GT* as computed by our protocol at time $t$.

THEOREM 4.1 (SAFETY) Let $t$ be the instant at which $\mathcal{GT}(t)$ is computed. The $\mathcal{GT}(t) \leq GT(t)$.

PROOF. $\mathcal{GT}(t)$ is computed by the initiator ⇔ $count = 0$. $count = 0$ ⇔ there are no white messages in transit. Hence, we need only concern ourselves with the timestamps of black messages in transit when computing the *GT*, *i.e., $GT(t) = min$*{timestamp of all nodes at time t, timestamps of black messages in transit at time $t$}. From the protocol,

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

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 black message since each node became black. The $min(ts) \leq$ timestamps of all black messages in transit at $t$ since the black messages in transit at time $t$ form a subset of all the black messages sent since each node became black. Furthermore, at time $t$, no $lt$ can be less than the minimum timestamp of the black 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 $\mathcal{GT}(t) \leq GT(t)$. ■

We now establish the liveness of the protocol.

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

PROOF. After the computation of $\mathcal{GT}(t_1)$, it is possible for one of the nodes to be rolled back by a black message, but not by a white message (the white messages have all arrived). However, the minimum timestamp of the black messages in transit is included in the definition of $\mathcal{GT}(t)$ and by virtue of this definition, the $\mathcal{GT}(t_2)$ cannot decrease subsequent to the computation of $\mathcal{GT}(t_1)$, 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 $\leq N\delta+\varepsilon$. ■

# 5 Conclusion

In this paper, we introduced a partly distributed control and a decision of good nodes and bad ones based on the cooperation amongst nodes in the whole network. Unlike other cryptocurrencies, only the chosen nodes, which satisfy some trust level maintains its number of nodes by adding or purging nodes in the set. Basically, some nodes with powerful computing resources may collude with other nodes, which may be not an elected node or may be purged from the elected node list. By taking the example of Bitcoin, we are not encouraging competitive mining from all the nodes, in order to save the Earth; whereas only one node can have additional Bitcoins as incentives and can receive compensation by enormously consuming electric energy. Only the chosen nodes that are trustworthy can participate in the proof of trust for providing the trust of LondonCoin and these nodes have a minimal amount of transfer payment as incentives. We expect that our cryptocurrency outperforms better than others.

To be able to realistically apply LondonCoin into our lives, we aim to create a cryptocurrency that is capable of converting gold, that can also use a biometric (owner's fingerprint) system on-card as a digital hardware wallet, and to integrate a currency exchange rate by replicating the financial process, which executes the current currency market, in order to guarantee stable trading and transactions, which are highly emphasized. Shortly, we expect to make a debut of LondonCoin.

# 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. Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", http://bitcoin.org, 2008.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. Lai, T. and Yang, T., "On Distributed Snapshots", Information Processing Letters, Vol.

25, No. 1, pages 153-158, 1987.

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