FreitX Network
Blockchain as a Service for Supply Chain Management Powered by a Stable Coin and Scalable Blockchain

The FreitX Network Team (hello@freitx.network)
White paper version: 1.9
14th November 2018

Abstract

Supply chains are all around the world. Everything that we buy, eat, touch or use every day was part of some supply chain and has its own journey of history. Supply chains literally connect the world and are one of the most powerful competitive tools in today's globalizing business economy.

Data management, especially one that is properly done, is crucial for the success of any organizations. Enterprise resource planning (ERP[1]) and supply chain management (SCM[2]) are two of the most widely implemented software types in many corporations and organizations today. They are responsible for proper data management starting from the basic stage of production of goods to their handover to the customer. Companies operating in supply chains establish processes and data integration through the specialized intermediary companies, whose role is to establish interoperability by mapping and integrating company-specific data for various organizations and systems. This has typically caused high integration costs, and diffusion is slow.

The developments of Blockchain has provided new opportunities not only for better SCM and ERP but also to transform the supply chain. The blockchain-based integrated management provides us with opportunities to increase the value and decrease the waste of SCM[3]. In this paper, we present a new blockchain based SCM tool: ***Freitx Network***. We design a new architecture which presents a stable, simple, useful, auditable, scalable, transparent, distributed and decentralized mechanism for SCM. *FreitX Network* is designed to be a powerful tool for every participant in any supply chain.

Keywords: Supply chain, Supply chain management (SCM), Blockchain, Decentralized, Distributed, Lean.

---

1. Preface

After the creation of Bitcoin[4], Blockchain showed us not only its ability to be used for financial transaction applications but also its even greater potential to be deployed into and transform many other industries such as banking, security, identity management, healthcare, and supply chain. While Blockchain technology is still developing, every day we see the emergence of numerous new blockchain projects. Many projects hold promise with their attractive ideas of blockchain integration options. Despite the fact that we have many technological promises and talks about future development, blockchain technology is rather new, and still lacks match points between theoretical and practical sides. In this paper, we present *FreitX Network* as a versatile and practical SCM tool, where we strike to balance blockchain as an innovative technology that is practically adoptable in a real-world environment.

2. Supply Chain

There are billions of products being manufactured every day. Every product has a story and at times a profound one. However, we, the consumers, are usually not aware of this. Our product knowledge is primarily limited to the country of manufacturing and product brand and label. Despite our lack of knowledge, we endow our trust to retailers we deem reputable and trust that the product is safe for consumption. Inherent in our trust is the assumption that proper safety and inspection steps have occurred in the background. This background, which is also responsible for the successful and timely delivery of any product to us, is the global supply chain network. The supply chain is an elaborate and multifaceted system that extends to all parts of the world. The supply chain consists of many direct and indirect participants, sometimes from different continents, whose workflow coordination is vital to the successful and timely delivery of products. The complexity arises not only from the enormous number of parties involved but also from the requirements that many events from all aspects of supply chain need to be well coordinated. There are always many questions on any product in any supply chain, such as how, when and where does a product originate from, was it manufactured and was it processed throughout its life cycle. Before reaching the end consumers, products pass through direct supply chain participants (with actual contacts with the products) including the producers, transport companies (e.g. truck, cargo ship, and air freight), wholesalers, distributors and retailers (Figure 1). Additional stakeholders include intermediaries who may not have had actual contacts with the physical products but are nevertheless key. These include authoritative entities such as customs, regulatory and compliance entities, and facilitating businesses such as insurance and finance companies (Figure 1).

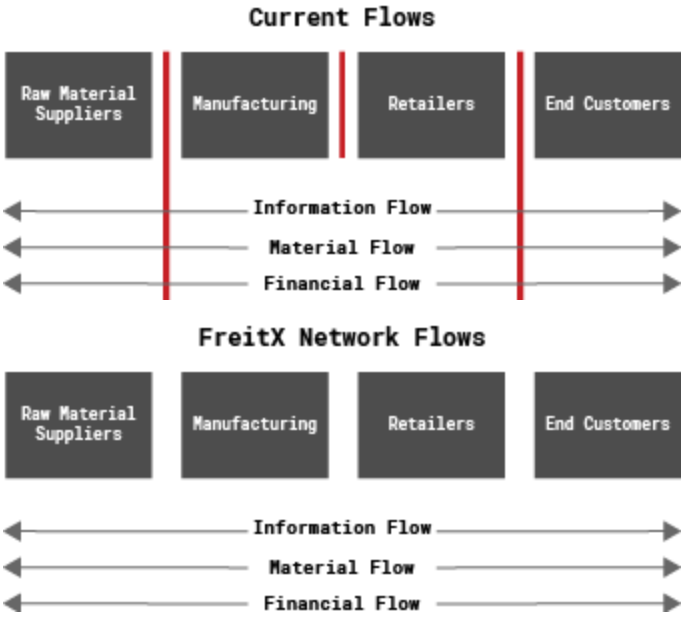

Figure 1: Supply chain main flows.

Coordinating the flow of materials, information, and finance through each component of the supply chain involves many challenges. Most of these processes further need quick actions. Many supply chain participants function as silos, with limited information sharing between parties, as document sharing could be time and resource consuming. In some cases, document sharing between parties is well done with the help of existing software(s) such as ERPs. With the inherent complexity of any supply chain, there lacks a transparent overview of product flow and relevant information for supply chain participants and intermediaries. There also exist information asymmetry within the supply chain. Larger and resource-rich participants have access to more information, via in-house data or other information management system, allowing them to be more efficient supply chain participants. In contrast, smaller or resource-limited participants, e.g. a private transport company, have less overview or information about the product, and may not have the resources to manage the required workflow at all. Having the relevant overview and information will help all players become better participants, benefiting the entire supply chain. In the event of an emergency food outbreak or safety recall, where fast response is required, having a product and supply chain overview will certainly facilitate the tracking and tracing of the ingredients or parts along the supply chain and back to all consumers involved. This could be life-saving in a critical situation.

3. Blockchain and Artificial Intelligence

FreitX Network believes in the power of blockchain technology to transform the global supply chain network. The efficiency of any supply chain greatly depends on the seamless teamwork and solid, and usually long-term, partnerships between supply chain partners. Trust is key to all long-term successful partnerships. Trust, in turn, requires

transparency. *FreitX Network* envisions using blockchain technology, with its key features: decentralization, transparency, trustless, immutability and timestamp, to transform supply chain into one with increased transparency and trust that promises economic, social, environmental, and at times life-saving, impacts. Our versatile *FreitX Network* Blockchain platform could be applied to any situations along the supply chain, including applications such as tracking and tracing ingredient(s), the payment flow, the freight storage, and transport conditions and customs declarations. If the supply chain were an orchestra, blockchain enables the supply chain as the conductor. *FreitX Network* blockchain also offers practical opportunities for a leaner and more efficient supply chain by saving time and cost and reducing manual paperwork.

FreitX Network envisions using our platform for better data management including data collection and integration to empower supply chain management. From globalization to compliance, data management is key to any successful supply chain planning and a critical asset to any modern organization. In many supply chain situations, basic data collection or having the information itself is still not a given and needs to be established. Furthermore, raw information coming from suppliers, partners, and even customers are often composed of both structured and unstructured data with varying degrees of fragmentations, making data management and further analytics and insights generation a challenge for enterprises. Our capability will allow for the processing and transformation of raw information into compatible formats required by different supply chain management systems to ensure their seamless flow. A successfully-implemented platform allows for interaction between flows of information, materials, workers, capital equipment and infrastructures. Having the information alone is not sufficient, proper management of the information itself is critical for any useful and actionable data analysis, interpretation and insights generation. Proper data management includes data capture, search, storage and capacity management. With the *FreitX Network* blockchain platform, we will further capitalize the platform using artificial intelligence[5](AI)-driven data analytics for purposes such as diagnosis, analysis, and prediction using diverse analytic tools including visualization, statistics, and modeling algorithms.

FreitX Network aims to help create a supply chain with increased sustainability, where resources are more efficiently and wisely used, while waste is being reduced. Having an overview of the supply chain is very valuable. For example, supply chain transportation control blockchain containing a detailed overview of freight and product conditions allows for greater transparency, connecting all relevant parties to information with insights, and allows for informed decision making within the transportation chain. Empty trips and lead times could be minimized while resource capacity is maximized. We believe in the empowerment of the supply chain participants including the “upstream” ingredient suppliers and “downstream” consumers, who usually do not participate actively in the supply chain. Ingredient suppliers could use our platform to document their data and work process, e.g. for efficient track and trace. Importantly, our platform will also provide visibility and recognition to these important group of supply chain

participants. We aim to empower consumers by providing access to important product knowledge. This includes better appreciating the products by having awareness of the work involved in making the end product, knowing and connecting to the farmers and certifying that what consumers assume are indeed true, e.g. the organic origin of a specific ingredient. Finally, our blockchain platform will help our users maximize their potential and contributions for any supply chain.

4. Model and Design

FreitX Network is designed based on lean principles. A lean[6] organization observes user-focused value and is oriented on its key processes to permanent increase. The main goal is to provide value to customers with the help of perfect value creation process with zero waste. Lean changes the focus of management from optimizing separate technologies and assets to optimizing the flow of products and services through whole value streams that flow across technologies and assets to customers.

One of its main characteristics is stability. It gives the confidence to provide different kinds of partnerships within the network. Currently, there is a lack of a stable system that provides a clear vision of how one's potential contributions will function in the future.

The network seeks to have simple supply chain management service development skills that is user-friendly. Simplicity and accessibility are two main components that play a huge role in *FreitX Network* success. We try to avoid all options that include complexity in its function. Multiplex optimization will only be accepted if it provides benefits.

The main aim is to stay applicable while having guaranteed capabilities and flexibilities for future development. We can count applicability as one of the most important fundamental parts of ***FreitX Network*** design philosophy. The function that we want to serve for our project ensures the possibilities for future features development.

As the industry grows faster than we could imagine, we have to take full control over the technologies that we use for development. While the goal is to stay focused on the innovative way of thinking, one needs to have a clear vision of risk probabilities. By having quick development skill and being agile, we will strive to overcome challenges encountered along the way.

To provide confidence to all users of our Network, we will ensure that the network is secured. The ecosystem that we create with the help of our tools is powered by transparent operations, which will perceive and detect all risks, thus providing our customers safety and security .

We will not have any prioritized participant in any provided operation. We design a network with regulating tools to avoid damage and not attempt to oppose specific

undesirable applications. All rights are strictly controlled and the ecosystem is powered by equal opportunity within the network.

5. Blockchain Technical Overview

Freitx Network Blockchain is a permissionless blockchain based on a dual token system, designed to be scalable for enterprises, individual or IoT[7] applications requirements. In *FreitX Network* Blockchain we are not trying to reinvent the wheel, most components of our blockchain are well tested already in current projects like as Ethereum[8], Zerocash[9], and Nano[10]. We believe our synths of blockchain have the ability to adopt new customers from around the world and reveal the full potential of blockchain technology.

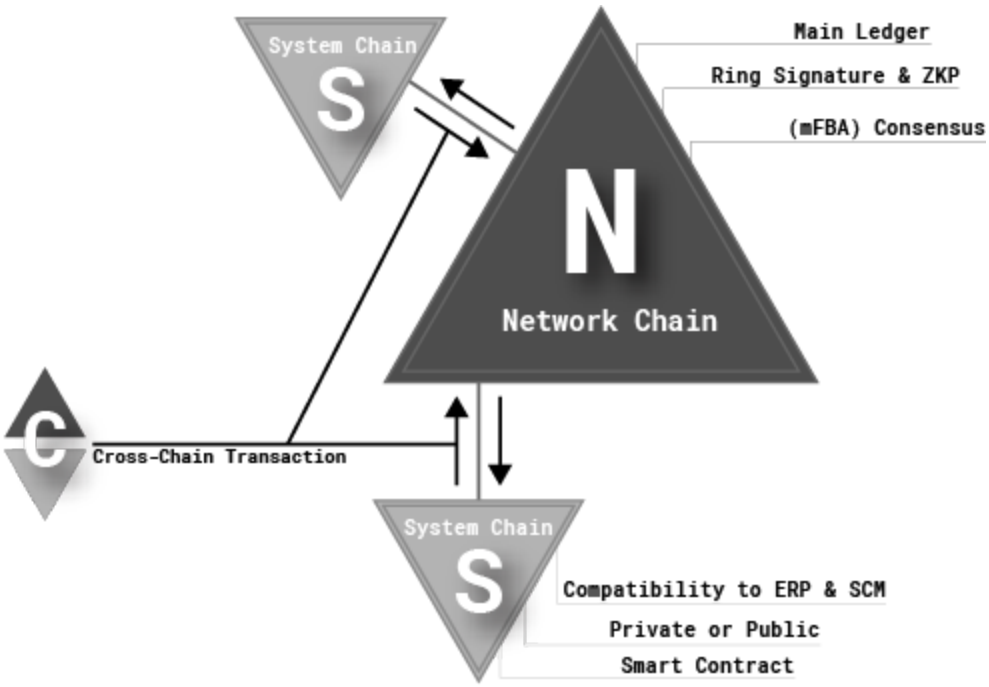

Figure 2: Freitx network blockchain architecture.

FreitX Network Blockchain is a network of multiple independent blockchains that run in parallel. The main blockchain in this network, which we term the Network Chain, connects multiple blockchains termed System Chain. The Network Chain is a public blockchain and operates as the main ledger that achieves interdependence and interoperability between system chains. The main ledger is a place which captured transactions and token movements between system chains, and is the ledger for the entire network. The Network Chain is responsible for all types of tokens that are active in our ecosystem. The System Chain is well suited and could be modified to fit any type of customer requirements. The System Chain could be a private or public blockchain which supports smart contracts execution, account management, and privacy. Cross-chain is a distributed coordination assignment where multiple parties exchange assets across

multiple system chains. In FreitX Network, cross chains transfer tokens between system chains through to the network chain. In the next sections (6 to 13), we define all details and components of *FreitX Network* Blockchain.

6. Cryptography Layer

Blockchain technology requires the use of cryptography, which we could imagine as a major tool for trust in Blockchain. In this section, we introduce the security and efficiency aspects and the basic cryptographic techniques used in the *Freitx Network*. We use Elliptic Curve Cryptography (ECC[11]) public-key algorithms for digital signatures, while for the hash function, ***Freitx Network*** uses the Blake2b[12] cryptographic hash function.

6.1. Hash function

Freitx Network employs Blake2b as a hashing function. The hash function is based around a HAIFA[13] structure that incorporates a variation of the ChaCha[14] stream cipher by Bernstein. The hash function is notable for its high performance on x86-64 architecture, being faster for short messages than SHA-256[15] despite being considered as having a much higher security margin at 14-rounds. More details and comparisons of Blake2 and other hashing functions are presented in Figure 3.

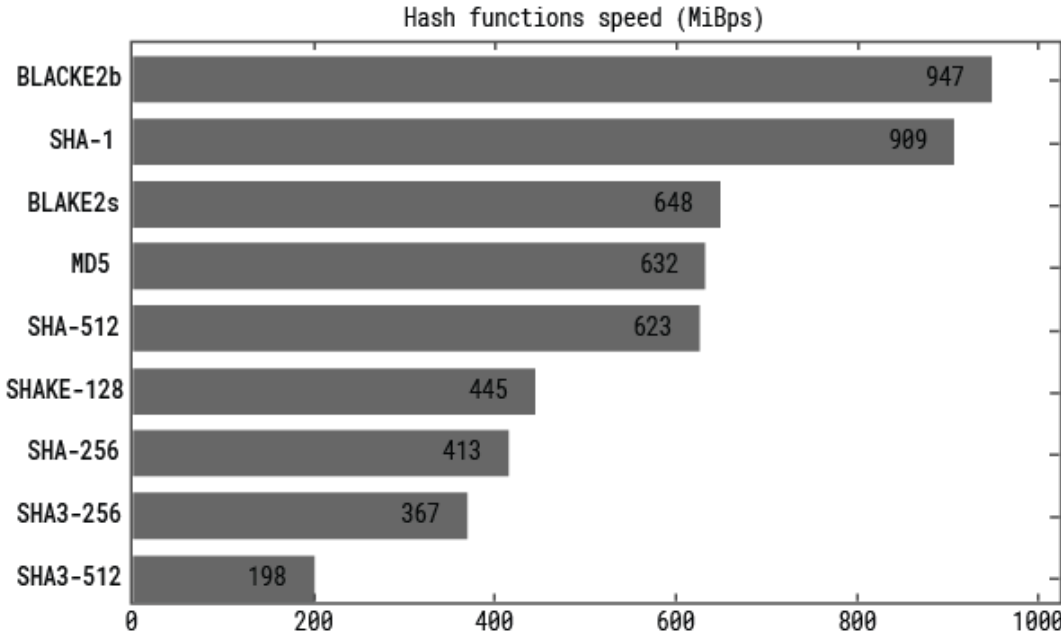

Figure 3: Hash functions speed comparisons

6.2. Elliptic-curve

There are variations of algorithms for public-key digital signatures. Algorithms based on elliptic curves have gained wide interest because the size of keys and signatures is

significantly lower than those in the RSA[16] alternatives. *FreitX Network* uses Edwards-curve Digital Signature Algorithm (EdDSA[17]) for the signing algorithm, it is a modification of the Schnorr signature algorithm system that makes use of Twisted Edwards Curves. In EdDSA family we use an Ed25519[18] instance of the digital signature scheme, which is widely used in numerous security protocols, networks, products and is also specified in RFC 8032[19]. Choosing Ed25519 has numerous attractive convenient features as described below.

6.2.1. Comparison, Security, and Speed

In Blockchain technology one of the most popular ECC is Elliptic Curve Digital Signature Algorithm (ECDSA) family member Secp256k1[20] instance, which is currently used in Bitcoin and Ethereum. Ed25519 is claimed to be more side-channel resistant than Secp256k1, not just in terms of resisting software side-channels i.e. featuring constant timing. Also, the default signature format for Ed25519 allows batch signature verification, which gives us double the faster performance of the Digital Signature Algorithm (DSA) than Secp256k1. Ed25519 is recognized as one of the most secure elliptic curves by top cryptographers. The security of Ed25519 algorithms is generally based on the Discrete Logarithm Problem (DLP[21]) which is currently one of the widely used in, many popular modern crypto-algorithms. Ed25519 is more efficient and fast than Secp256k1.

Curve	Complete single-scalar formulas	Complete multi-scalar formulas	Number of points of order 2	Number of points of order 4
Ed25519	✓ True	✓True	1	2
Secp256k1	✗ False	✗False	0	0

Figure 4: Safe curve comparison between Ed25519 and Secp256k1.

In ***Freitx Network*** Ed25519 was chosen for its better designs with respect to security, distribution, flexibility and fast performance. It is one of the most suitable algorithms for the Internet of Things (IoT[22]) applications and it allows us flexibility in the Smart Contract[23] area. The exact Ed25519 and Secp256k1 comparisons in security and benchmark are provided in Figure 4 and Figure 5.

Phase	Secp256k1 ECDSA	Ed25519
Key size	33 bytes	**32 bytes**
Signature size	~71 bytes	**64 bytes**
Security target	2^{128}	2^{128}
Security Tests	7 of 11	**11 of 11**

Figure 5: Security test[24] comparison between Ed25519 and Secp256k1.

6.2.2. Suitability

In *FreitX Network*, IoT is one of the active research fields with many practical applications for supply chain management emerging. Internet of Things (IoT) applications and resources sparse platforms such as Radio-frequency identification (RFID[25]) tags and sensor nodes consider ECC exclusively for their (exceptional) public-key requirements. This does not come as a surprise knowing that working in fields with size 160 bits or so is considered to be at least as secure as RSA with size around 1200 bits. This belonging often results in implementations of smaller memory/area footprints and lower power/energy consumption.

7. Network Layer

7.1. Peer-to-peer

Peer-to-peer (P2P[26]) network is one of the most important decentralization and blockchain network functions. As an example, P2P based systems had previously been used in many popular sharing platforms, allowing data exchange among a large number of users without the use of a centralized administrative system. In the Freitx Network, like most other cryptocurrency projects, we have two main functions for a P2P network, first to allow the synchronization of the nodes of the network and second to distribute nodes data in order to enable nodes to reenter the network after a disconnect.

7.2. Time synchronization

Freitx Network relies on timestamps for transactions and blocks data. In the network, time synchronization is critical because of every aspect including managing, securing, and implementing, a network plus network stability itself involves determining when events happen. Time also provides the only frame of reference between all nodes on the network. Without synchronized time, accurate synchronization of data between nodes is difficult, or even impossible. Based on this, we need to have a right time synchronize protocol to ensure stability working on the network. The *Freitx Network* develops custom time protocol based on the P2P network, which could reduce synchronization offsets to times of the order of a few milliseconds over the P2P network.

7.3. Internet protocol

In *FreitX Network,* we are using two widely known internet communication protocols. UDP[27] (User Datagram Protocol) uses a simple connectionless transmission model with on minimum protocol mechanism. Generally, UDP used for real-time communication, in *FreitX Network* UDP uses for node discovery and new peers for blockchain synchronize. TCP[28] (Transmission Control Protocol) uses for data sharing between nodes in the blockchain.

7.4. Latency

Currently, several projects aim to improve the speed of block generation. Most of the time, these projects focus only on limiting the size of data in the block that needs to be broadcasted over the network or on relaying speeds to cut the time before it takes for block generation. For example, in Bitcoin and Ethereum P2P networks, nodes randomly connect to the other nodes and transmit data over this network until each has received all required data. This method is termed "Random Neighbors Selecting" (RNS[29]). A node must maintain a list of neighbors when it is a member of a blockchain network. The classic and simplified procedure when this happens is shown as follows.

#	Connection	Latency(ms)
0	(0,6)	1431
1	(1,5)	1252
2	(2,4)	1258
3	(3,4)	948
4	(4,2)	1258
5	(4,3)	948
6	(5,1)	1252
7	(5,8)	1471
8	(6,0)	1431
9	(7,9)	1445
10	(8,5)	1471
11	(9,7)	1445

Figure 6: Current method nodes connection in P2P network and their latency.

List of **RNS** method steps:

1) Initiate neighbors list when a node first connects or reconnects to the network,

2) Refresh its neighbor'(s) list while the node finds a new neighbor or a lost neighbor,

3) Send messages via selected neighbors to the rest of the blockchain network.

The RNS method for the P2P network is relatively slow and inefficient for a fast and scalable blockchain.

In *Freitx Network*, we examine a new method to optimize transmission latency between nodes, by choosing the closest neighbors and using them to spread messages in the network. This method, which we term "Closest Neighbors Selecting" (CNS[30]) contains several steps as follows.

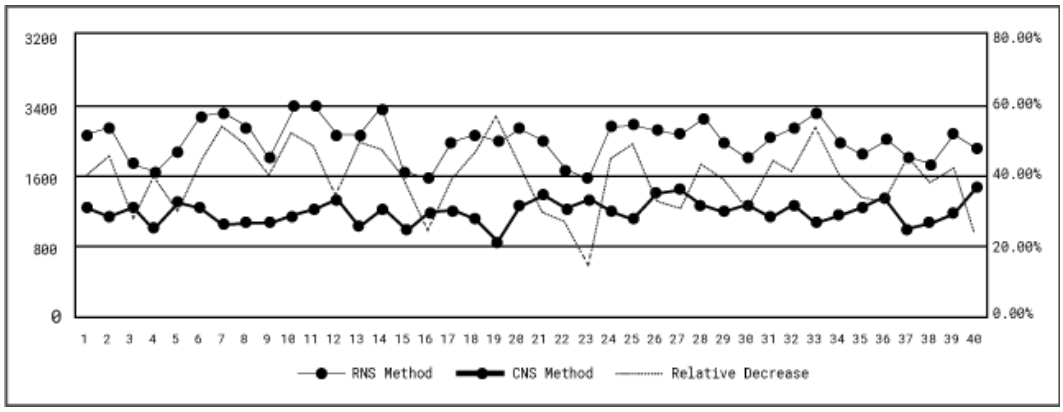

Figure 7: Neighbors' average latency in a 40-node simulation network.

List of **CNS** method steps:

1) Initiate a potential neighbors list, where each neighbor is associated with an infinite latency value.

2) Refresh the list of neighbors when new nodes are discovered or old nodes are lost and refresh each neighbor's latency value via round-trip-time (RTT[31]) measurement,

3) Sort the neighbors in the list by its latency value, with the smaller values being first,

4) Send messages by selecting neighbors based on the list order to nodes all over the network.

Besides the similarities of the mentioned methods, we could also see a difference that plays an important role to understand the whole mechanism. CNS appears to have different functions, and they could be divided into several stages as showing the distance, identifying the value of nodes with the help of RTT and selecting neighbors by priority.

These changes are implemented by using different tools and abilities within the software by using a simple data list, which is refreshed as the network fluctuates. The generic sorting algorithm is the solution for the list sorted by RTT starting from the smallest with increasing values. Classic network measurement including RTT measuring between a pair of nodes could be solved with individual measurement packets. To solve this problem, one has to first identify and observe existing traffics. The accurate RNS and CNS method differences and results are provided in Figure 7.

8. Data Layer

8.1. Accounts, addresses, and states

8.1.1. Accounts

FreitX Network is an account-based model (such as Ethereum), each address is seen as an account with a balance, and transactions are transfers of value from one account to another. In *FreitX Network*, there are three types of accounts: Major account, linked account, and public or private contract account. The major account contains a public-key (address) portion of a Digital Signature Algorithm (DSA[32]) generated by Ed25519 private key. The linked account is created and guided by the major account. Public and private contract accounts are for a smart contract which is generated by major account.

8.1.2. Account Management

FreitX Network uses an account management system, which allows the users to create both the major and linked accounts. The major account has the ability to generate linked accounts and edit permissions, which appears to be an important tool for customers. This major and linked accounts then establish the hierarchical system. In supply chain management operations, every step should be planned in accordance with account needs. Planned activities lead to targets for each account and help to provide relevant products.

8.1.3. Account State

Each account is associated with an account statement. Account state is the key which itself contains different states with values and functions. It stores every value which is associated with its account and contains the following components:

1) **address (64 bits):** The address generated from the account public key with Ed25519. The main identification tool for the account owner.
2) **balance (64 bits):** Balance is the positive value where tokens are stored. While account receives or sends tokens to another account operations directly affect account balance. Received or reduced amounts of tokens are immediately shown on the account balance.
3) **account nonce (64 bits):** The nonce is a zero-initialized counter that can provide with the transactions, transfers, and creations of all types of accounts.
4) **account timestamp (32 bits):** The timestamp includes a part which is termed "created". Created is time identification that shows the time required for the creation of all kinds of accounts.
5) **created (32 bits):** Created by is responsible to observe the creation history and provide information about the creator. It identifies major account which creates a contract account or linked account.

8.2. Transaction

A transaction in programming systems could be defined as a sequence of information exchange and work that is related to and treated as a unit for fulfilling a request for enabling database integrity.

1) **transaction hash (64 bits):** The main identification hash which digests data that reaches signature.

2) **sender address (64 bits):** The one who sends transaction and address is for his identification.
3) **receiver address (64 bits):** The one who receives transaction and address is for his identification.
4) **confirmations (64 bits):** The process of observation where the system confirms the transaction sending and receiving information within the current location.
5) **block hash (64 bits):** The classification of blocks which shows in which blocks transactions are stored.
6) **network fee (32 bits):** The cost of proceeding transaction and activating operation.
7) **type (32 bits):** The type of transaction which is activated and transacted. Transactions contain four major types of actions: Asset, bond, contract, and vote transactions.
8) **timestamp (32 bits):** The time exactly when the transaction has been provided.
9) **amount (64 bits):** Amount identifies how many tokens are in process or have already been transacted.
10) **status (32 bits):** Every transaction has its own status which provides information on transaction type and whether it was successfully executed or not.
11) **nonce (64 bits):** The zero-initialized counter and the equal number of transactions sent by the sender of this transaction.

8.2.1. Cross-chain transactions

Cross-chain[33] is a distributed coordination assignment where multiple parties exchange assets across multiple blockchains. In *FreitX Network*, cross-chain transfers tokens between system chains through network chain.

When X tokens are transferred between system chains, e.g., from Rick account on M system chain to account Morty on V system chain through with network chain, the network chain must verify a number of events:

1) The account is in possession of X tokens.
2) Morty's account expects to receive X tokens from Rick's account (either because the Rick and Morty agreed to the transfer).
3) The Morty's account will not use the X tokens dedicated for the transfer in a different way (by transferring them to another account on M or by transferring them to a third system chain V).

In Figure 8 shown the following steps, example cross chain transaction between Rick and Morty.

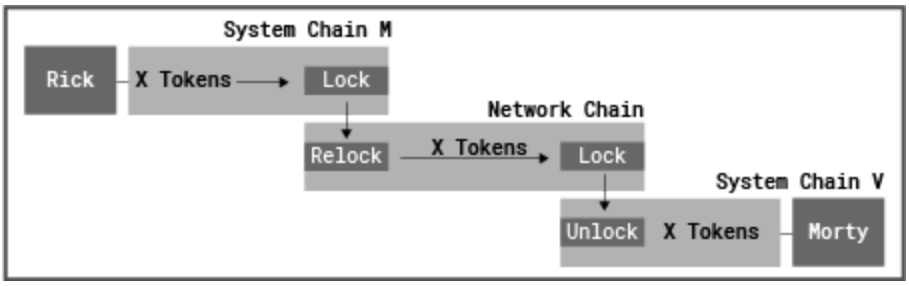

Figure 8: Cross-chain transaction example between Rick and Morty.

8.3. Blocks

Block is the collection of diverse types of information that includes two main components: i) the Block header, where information about a block is stored, and ii) Block body, where all transactions provided in this block are visible or stored. The block structure shown in figure 9.

Block header contains the following data:

1) **block hash (256 bits):** The *BLAKE2b-256* hash digest of the block header.
2) **parent hash(256 bits):** The *BLAKE2b-256* digest of its previous block header.
3) **timestamp (32 bits):** The time when the block was generated.
4) **version (32 bits):** Current version of the block.
5) **block number (32 bits):** The number of the block after genesis block number (0).
6) **reward (32 bits):** The amount of token reward for the block produce.
7) **total fee (32 bits):** The total amount of fee used in this block body provided operations.
8) **size (64 bits):** Size shows all amounts of bits that were used while the transactions were transacted in this block.
9) **producer public key (180 bits):** The Ed25519 public key of the producer who generated the block.

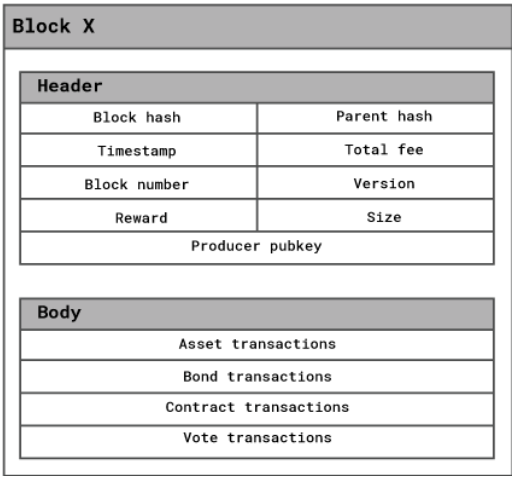

Figure 9: Block structure..

9. Consensus Layer

Blockchain projects use a variety of consensus models which are Proof of Work (PoW[34]) and Practical Byzantine Fault Tolerance (PBFT[35]) in their original form or modifications of it presenting several improvements desired over the original model. Bold new models are also introduced, such as Proof-of-Stake (PoS[36]) and Proof-of-elapsed-Time (PoeT[37]) and variations of PBFT appear as viable alternatives.

Achieving consensus in a distributed system is challenging. Consensus algorithms have to be flexible to failures of nodes, partitioning of the network, message delays, messages reaching out-of-order and corrupted messages. They also have to deal with selfish and deliberately malicious nodes. Several algorithms are proposed in the research literature to solve this, with each algorithm making the required set of assumptions in terms of synchrony, message broadcasts, failures, malicious nodes, performance and security of the messages exchanged. For a blockchain network, achieving consensus ensures that all nodes in the network agree upon a consistent global state of the blockchain. We believe that this is down to four principles, which serve as a key to choosing the right consensus mechanism in *FreitX Network*:

1) **High-level decentralization:** Anyone can be a participant in the network. There are no limitations from the central authority who dictates whose approval is required for consensus.
2) **Low latency:** Consensus agreement can be achieved in a few seconds.
3) **Flexible trust:** Participants are free to determine what other nodes they trust, without any limitations.
4) **Asymptotic security:** Digital signatures and hash families are used in a way to protect the network even against adversaries with unimaginably vast computing power.

9.1. Background

9.1.1. Proof of Work (PoW)

Proof of Work[38] (PoW) is the most famous decentralized consensus scheme and is currently used in two most popular cryptocurrencies: Bitcoin and Ethereum. PoW consensus requires its participants to perform some form of work to participate. PoW has limitations and weaknesses. It consumes resources, one estimate from 2014, Bitcoin might consume a huge amount of electric power. Secure transaction settlement suffers from expected latencies in the minutes or tens of minutes. Mining centralization is a weakness in Bitcoin where a large number of ASICs were cheaply produced to perform hashing operations at very high rates, thereby outnumbering and outperforming the general-purpose computer hardware by a very large margin. This allowed select powerful entities, such as large companies to create mining pools, with a very high hashing rate and which in turn allowed them to dominate a large portion of the computing power of the network.

9.1.2. Proof of Stake (PoS)

Proof-of-Stake[39] algorithms are intended to overcome the limitations of PoW algorithms in terms of the high electricity usage involved in mining operations. PoS simply replaces the mining operation with an alternative approach involving a user's stake or ownership of virtual currency in the blockchain system. PoS[40] has randomly determined a set of node vote on the next block, and their votes are weighted based on the size of stakes. However, PoS algorithms suffer from a problem possibility called "Nothing at Stake".

PoS does not provide right incentives for nodes to vote on the correct block. Nodes can vote on multiple blocks that support multiple forks to increase their chances of winning a reward as they do not "expend" anything in working process as opposed to in PoW, the node would split its resources to vote on multiple forks. Implementation of PoS opens the possibility of "nothing at stake" attacks, in which parties that previously posted deposit but later cashed it in and spent the money can go back and revise records from a point where they still had a stake.

9.1.3. Practical Byzantine Fault Tolerance (PBFT)

Another approach to consensus is the Byzantine agreement[41], where the most widely known modification is the Practical Byzantine Fault Tolerance (PBFT). PBFT algorithm, introduced by Miguel Castro and Barbara Liskov, was the first practical solution to achieving consensus in the face of Byzantine failures. It uses the concept of the replicated state machine and voting by replicas for state changes. It also offers several important optimizations, such as signing and encryption of messages exchanged between replicas and clients, reducing the size and number of messages exchanged, for the system to be practical in the face of Byzantine faults. Exactly, it rests on three series of message exchange before reaching an agreement. This guarantees that 3f + 1 nodes can reach consensus also in the presence of Byzantine nodes; this is proved to be optimal. Many other BFT algorithms have been introduced, largely for improving PBFT performance;

among others, we can cite Q/U, HQ, Zyzzyva, Aardvark, see the survey in for more parts of each solution.

9.1.4. Federated Byzantine Agreement

In a Federated Byzantine Agreement (FBA[42]), such as the Stellar Consensus Protocol (SCP[43]), a number of participants seek to agree on a common piece of data in the behavior of all types of fault (e.g. death, malicious lying and random error). In Stellar, this is accomplished by allowing each participant to choose multiple quorum sets of other participants with whom they would like to agree with, should the rest of that set agree. Each participant governs within by agreeing with the first quorum set that agrees. Each node chooses which other nodes to trust. The sum of all these individual choices is a system level quorum of consensus.

9.2. The Consensus In FreitX Network

We envision a scalable and efficient consensus mechanism by instant block finality that is well suited for SCM and IoT. *FreitX Network* Blockchain achieves consensus with modern asynchronous modified Federated Byzantine Agreement (mFBA) consensus algorithm. The algorithm will be inspired and combined by the SCP, Tendermint[44], FBA and Dynamic Quorum[45]. mFBA protocol operates using four phases Proposal, Prepare, Commit and Externalize.

The mFBA consists of changing digitally-signed messages connected to the nodes' quorum slices. In addition to quorum slices, messages compactly carry votes on sets of conceptual statements. The core technique of voting with quorum slices is termed federated voting. We describe federated voting, followed by details of mFBA messages in the subsections that follow.

9.2.1. Federated voting

Federated voting is a process through which nodes confirm statements. Not every attempt at federated voting may succeed. An attempt to vote on some statement "a" may get stuck, with the result that nodes can confirm neither "a" nor its negation "!a". However, when a node succeeds in confirming a statement "a", federated voting guarantees two things:

1) No two well-behaved nodes will confirm contradictory statements in any configuration and failure scenario in which any protocol can guarantee safety for the two nodes (i.e., quorum intersection for the two nodes holds despite ill-behaved nodes).

2) If a node that is guaranteed safety by #1 confirms a statement "a", and that node is a member of one or more quorums consisting entirely of well-behaved nodes, then eventually every member of every such a quorum will also confirm "a".

9.2.2. Proposal

mFBA starts in a ***Proposal*** phase whose goal is to devise one or more candidate output values for the consensus protocol. In this phase, nodes send proposal messages comprising a monotonically growing set of values:

```
struct Nomination
        {
          Value voted<>;      // X
          Value accepted<>;   // Y
        };
```

9.2.3. Ballots

Once there is a candidate on which to try to reach consensus, a node moves through three phases of balloting: ***Prepare***, ***Commit*** and ***Externalize***. Balloting uses federated voting to choose between commit and aborts statements for ballots. A ballot is a pair consisting of a counter and candidate value:

```
// Structure representing ballot <n, x>
        struct SCPBallot
        {
          uint32 counter; // n
          Value value;    // x
        };
```

9.2.4. Prepare

The first phase of balloting is the prepare phase. During this phase, as soon as a node has a valid candidate value (see the rules for ballot.value below), it begins sending the following message:

```
struct SCPPrepare
        {
          SCPBallot ballot;        // b
          SCPBallot *prepared;     // p
          SCPBallot *preparedPrime; // p'
          uint32 hCounter;         // h.counter or 0 if h == NULL
          uint32 cCounter;         // c.counter or 0 if c == NULL
        };
```

9.2.5. Commit

In the commit phase, a node has accepted commit “b” for some ballot “b” and must confirm that statement to act on the value in b.counter. A node sends the following message in this phase:

```
struct SCPCommit
        {
          SCPBallot ballot;      // b
          uint32 preparedCounter; // prepared.counter
```

```
    uint32 hCounter;       // h.counter
    uint32 cCounter;       // c.counter
};
```

9.2.6. Externalize

A node enters the Externalize phase when it confirms commit b for any ballot b. As soon as this happens, SCP outputs b.value as the value of the current slot. In order to help other nodes achieve consensus on the slot more quickly, a node reaching this phase also sends the following message:

```
struct SCPExternalize
    {
      SCPBallot commit;        // c
      uint32 hCounter;         // h.counter
    };
```

9.2.7. Summary of phases

Here, we summarize the phases of mBFA. The Proposal and Prepare phases begin concurrently. However, a node initially does not send the "Prepare" messages but only listens for ballot messages in case accept prepare(b) reaches the blocking threshold for some ballot b. The Commit and Externalize phases then run in turn after the Prepare phase ends. A node may externalize (act upon) a value as soon as it enters the Externalize phase.

The point of Externalize messages is to help struggling nodes catch up more quickly. As such, the Externalize phase never ends. Rather, a node should archive an Externalize message for as long as it retains the slot state.

10. Data Privacy Layer

FreitX Network uses cryptography to prevent all except the party relevant to the transaction from detecting sensitive data. ***FreitX Network*** employed the method of privacy inspired by Quorum and Tezos blockchain projects. The block validation method is adjusted such that all nodes validate both public and any private transactions they are a party of by performing the contract code connected with the transactions. For other private transactions, a node will skip the contract code execution method. The segmentation of the state database, i.e. the state database is divided into a private state database and a public state database. Below, we introduce the three most known ways to achieve this: Ring signatures, Stealth addresses and non-interactive zero-knowledge (NIZK).

10.1. Ring Signature

Ring signatures[46] validate against a set of public keys, enabling individuals to determine that they are part of a group, without disclosing specifically which public key matches to the private key that they control. Any two signatures created by the same party are

interchangeable from signatures produced by two different parties in the ring. Linkable ring signatures subvert this property and are appended with a linking tag, which is the same across any signatures created by the same party in the same ring. These tags do not show the identity of the signer, but only show whether or not the signer has already produced a signature for that ring. Using linkable ring signatures, we can create a transaction mixer, which several parties can deposit funds into, and either withdraw themselves, in order to obfuscate the trail of their transactions or allow a receiver party to withdraw from, in order to transfer tokens in an unlinkable method. We use unique ring signatures. One of the main benefits of ring signatures is that they are relatively simpler to implement than NIZK and rely on more sophisticated cryptographic primitives.

10.2. Non-Interactive Zero-knowledge

We use the account-based model to implement transactions and smart contract privacy we put forward a homomorphic encryption scheme with the form like Pedersen commitment and construct a concrete NIZK[47] scheme to prove the validity of transactions. In our NIZK argument system, the public parameter works as the general source string which is only produced once for multi proofs. With respect to the security, we can achieve the zero-knowledge property in the standard CRS model, while the soundness can be obtained under the RO model. We also show the practical performance of the NIZK scheme on a personal computer. The result gives us confidence in applying our scheme in practice. The NIZK scheme employed a range of proofs. There has been a lot of research on the range proof so far such as [References]. A future direction is to utilize a new range of proof to obtain more efficiency without losing security. In the range proof, we utilize the weak Boneh-Boyen signature scheme. It is also a way to develop our scheme to use alternative signature schemes in the range proof.

10.3. Stealth Addresses

Stealth[48] address derivation generates addresses that are interchangeable from random, with the guarantee that only the holder of the master private key is able to use tokens from any address received from the master public key. For a long-term, or master, Ed25519 public key pair mpk and msk, derived stealth keys spk and ssk are created as explained below.

With elliptic curve group E(Fq), generator G, H a hash function with output in Zq, long-term master key pair mpk, msk and secret v shared among the sender and receiver address and its key pair spk, ssk are constructed as follows:

$=\Rightarrow spk = mpk + H(v) \cdot G$ (1)

$=\Rightarrow ssk = msk + H(v)$ (2)

In dual-key stealth addresses, the secret v is formed by the payer generating a temporary key pair of b and B, with B being broadcasted to the intended receiver. The secret is then formed $v = b \cdot mpk = msk \cdot B$. Stealth addresses with one amortized information (in which v is communicated), with n a sequence number, mpk the long-term public key of

the recipient, are formed + H(vmpk||n) · G. Here, v acts as a viewing key, allowing the account owner to provide others with the ability to deanonymize specific transactions, without the ability to spend the funds in the given account.
For A wishing to make a transfer to B, cooperation are as follows:

1) A uses B's long-term mpkB, nonce m, and secret v to form spkB.
2) A forms the transaction to deposit both spkB and the agreed denomination of funds into the smart contract.
3) When the required number of participants have joined, or a predefined number of blocks has been mined, the smart contract broadcasts a notification processed by A. A tells B (off-chain) that the contract is ready, and sends him the contract address.
4) B fetches ring description pki from the contract, derives sskB, using v and m, and constructs the linkable ring signature.
5) B creates a new address and sends the correctly formed ring signature to the contract, triggering the withdrawal of funds.

11. Smart Contract Layer

A smart contract is an event–condition–action stateful network program, executed between two or more parties that are resistant to trust each other unconditionally. Smart contracts have the ability to automate complex, multi-party workflows in the supply chain without a representative, while transparently recording transaction history on the blockchain. Smart contracts are usually written in a high-level language such as Ethereum's Solidity, and translated to compressed low-level bytecode for deployment on the blockchain. Once deployed, the bytecode is autonomously executed, usually by a virtual machine. Today, there are various developers in the Ethereum area, and numerous smart contracts are implemented based on Solidity[49] and EVM[50]. Therefore, we have determined to implement EVM compatibility and support of Solidity-based smart contracts in ***FreitX Network*** Blockchain. In the future, we intend to develop extra virtual machines and develop our own virtual machine.

12. Application Layer

FreitX Network is developing SCM tools based on *FreitX Network* Blockchain, defined by a flexible platform design that allows specific implementations to meet desired use-case conditions beyond various supply chains. Flexibility allows settings to be improved over time, with new features being introduced as *Freitx Network* Blockchain advance further. Taking advantage of modern microservice design patterns, the platform architecture helps future-proof an enterprise's investment in the blockchain. The platform hub consists of various layers, each including various sub-service, with many customizable layers via pluggable interfaces.

When deciding to develop new SCM tools based on blockchain technology, it is necessary to examine the ease of use and the network, developing applications with

best-in-class tools, and integration with existing enterprise systems. Our blockchain structure comprises interfaces that present the required functionality to achieve these purposes, thus improving overall ease of use.

13. Use Cases

FreitX Network Blockchain platform is adaptable to any supply chain applications in all industries. Our platform could be deployed to manage the workflow of existing processes and documents related to transport, customs, regulatory, import, export, certifications and others. Our flexible and scalable platform will allow international corporate companies to manage both internal and external supply chain processes. In addition, we aim to pursue and test new innovative ideas, such as using our platform to create a marketplace for smallholder farmers (see 13.2.2) and for soon to be expired food (see 13.2.3). Below, we illustrate several use case concepts in pharmaceutical, healthcare, agriculture and food industries.

13.1. Pharmaceutical and Healthcare Industries

13.1.1. Falsified Medicine

The supply chain of the pharmaceutical and healthcare segments is a complex system with many requirements (e.g. Current Good Manufacturing Practice (CGMP) regulations enforced by the Food and Drug Administration for medicines imported into the United States) to ensure safety and quality. The requirements are well established, strict and specific, and even include details such as the source and specific batch of an ingredient used and the temperature of the shipping container. Even with such strict regulations, falsified medicine is still a global health issue resulting in hundreds of thousands of deaths each year. WHO estimates ~700,000 deaths each year because of falsified malaria and tuberculosis medicines [51]. Patients and doctors rarely have access to such medicine processes and its documents in the supply chain. *FreitX Network* aims to help create a transparent medicine supply chain blockchain for tracking, tracing and certifying the authenticity of the basic ingredients and medicines. Having an overview of the medicine supply chain history will benefit everyone within the supply chain. There are numerous blockchain activities relevant to pharmaceutical industries. These include new projects: i) One Network is using blockchain to help secure medical supply and prevents counterfeit drugs, and ii) Ambrosus[52] and Modum[53] are using blockchain to address drug shipping condition to ensure that the medicine is intact throughout the supply chain process and meets the regulatory requirement. Pharmaceutical industry leading players such as drug distributors (e.g. McKesson Corporation) and pharmaceutical companies (e.g. Roche and Pfizer) are also actively participating in blockchain projects, such as the Medi Ledger Project, where blockchain is used to help the pharmaceutical industries to comply with regulations and improve the security of the supply chain. By partnering with pharmaceutical companies, NGO, hospitals, clinics and government, *FreitX Network*

blockchain platform will provide benefits to all parties involved, including in the generic drug industries, where an increase in visibility and transparency will be impactful.

13.1.2. Medicine Distribution Chain

The medicine distribution chain differs between developed and developing countries, with a few big firms controlling a majority of the primary wholesale markets in western Europe, the US, and Japan. However, in developing countries, medicine distribution poses a huge challenge, to the point that supply chain inefficiency causes cost increase, making medicinesless affordable. The first challenge is that hundreds, if not thousands, of companies, control tiny shares of the wholesale markets, and significantly more intermediaries are involved in developing countries. The supply chain is rather fragmented and information sharing is inefficient. The second challenge is that the final leg of the distribution chain to the clinics or hospital could be expensive and inefficient in developing countries. The impact of creating an efficient drug distribution chain to transform medicine availability and affordability has been well documented. In a three-year program in Senegal supported by MSD for Mothers, the Bill and Melinda Gates Foundation and other partners, where the supply chain logistics of family planning medicines was outsourced to private third-party operators, the proportion of public health facilities experiencing family planning medicines stock-outs decreased from over 80% to less than 2% in a 3-year period. The translated to the impact of allowing all patients needing family planning medicines being provided with the medicine, instead of just 20-40% of the patients. By working with relevant partners including pharmaceuticals companies, clinics, suppliers and NGOs, *FreitX Network* envisions the creation of a decentralized medicine ledger and SCM to introduce transparency and increase connections between all parties within the medicine distribution chain. Our platform could be used for both basic data collection and management and advanced data analytics to improve medicine availability for the patients while increasing efficiency for medicine distribution chain participants. Our work promises a huge impact to improve the health outcome for all patients.

13.1.3. Access to healthcare in the resource-limited area

Access is the greatest challenge to health care delivery in Africa, with fewer than 50% of Africans having access to modern health facilities. Causes for healthcare access challenges include a shortage of nurses and doctors and the lack of good health facilities and its maintenance, which at times is worsened by poor management, lack of transparency and corruption. the clinic is used to provides access to hard to reach populations. Our platform could be used to help manage the daily operations of such health facilities, including its maintenance, supply inventories, and interactions with external parties such as vendors, suppliers, and patients. In developing countries, frequently, fewer resources are set aside for equipment breakdowns or facility maintenance. Our applications could have additional functions to ensure timely checkup and maintenance of many expensive medical equipments. By doing so, we envision improving the efficiency of the daily operation and general condition of any health

facilities, and also reducing the cost of running such healthcare facilities. Healthcare access challenge is also due to the fact that many patients live in hard-to-reach rural areas. One important phenomenon in the current digital age is that despite the lack of access and infrastructure challenges, the majority of the resource-limited area population own or have access to mobile phones. Just like how mobile phone-based banking services (e.g. M-pesa) allow population in the hard-to-reach area taking a leap to not even needing a bank, *FreitX Network* envisions using blockchain to help the same hard-to-reach population take a transformational leap for access to healthcare using mobile phones. For this population, we could develop mobile phone applications that enable patients to consult doctors remotely (for non-life-threatening situations), make appointments and access their medical records and medicine. From the same application platform, with the proper consent of patients, health care workers could have an overview of the patient medical records, including those external to their own clinics. Having a holistic overview of a patient medical record within and outside one's practice is crucial for proper diagnosis and treatment.

13.2. Agriculture and Food Security

13.2.1. Food Fraud/Ingredient Authenticity

Food fraud costs the global industry many billions of USD every year and is a global issue that results in illness and death annually. *FreitX Network* aims to develop applications to improve the transparency in the food supply chain. The tracking, tracing and certifying the authenticity of an ingredient (e.g. organic cocoa, tea, and coffee) along the entire supply chain is critical. By partnering with partners such as farmers, food manufacturers, regulatory authorities or consumer organizations, *FreitX Network* blockchain platform could connect participants along the supply chain and provide an overview with increased visibility of the actual workflow and participants involved. Our platform is adaptable to use cases with varying degrees of complexity. *FreitX Network* could be developed as a full fledge SCM for an entire organization and its partner, and it is also versatile enough to be used as SCM for a family-owned transport company communicating with partners. Our platform could also be used to help monitor and provide data analytics for the production process, helping to guarantee qualities and freshness along the entire production process. Consumers are generally unaware of the source and ingredient of the food they consume. Our platform could serve as a go-to center for consumers to learn about the food they consume and to confirm the authenticity of the food. Our platform will help raise consumer awareness and provide benefits to all parties involved.

13.2.2. The smallholder farmers marketplace for sales, credits and improved agricultural yield

Smallholder farmers provide up to 80% of food in Asia and sub-Saharan Africa and 70% of food worldwide, respectively [54]. Smallholder farmers are farmers who rely primarily on family labors to grow one or two cash crops on a small plot of land. Many of these farmers have limited resources, lack a credit history, work with cash only, and do not

have access to a big pool of buyers. Many of them also live in rather remote settings, making access to modern infrastructures or technologies challenging. Co-op structures to try to pool resources for smallholder farmers is rather fragmented. Blockchain promises transformational impacts for smallholder farmers. *FreitX Network* envisions a blockchain-based, transparent and trustless financial marketplace that would allow smallholder farmers to get more value out for their products by connecting the farmers to a larger marketplace and by providing access to financial services. For perishable food that needs to be sold within a defined timeframe, smallholder farmers could use our blockchain-based marketplace to access a much larger pool of interested buyers. For those farmers who previously work with cash only, with our token system, the farmers could now have the confidence of being paid, and this will empower them to choose the buyer with the best bids, instead of one with cash but with a lower bid. Another challenge these smallholder farmers face is access to and affordability of modern farming technology, such as the use of higher-priced seeds and machines to enhance yield or harvest efficiency. Our blockchain financial marketplace will serve both as a credit-based financial services platform and also a social one for technology access and exchange. This would enable the smallholder farmers to use new agriculture practice resulting in improved yield and sustainability. We are providing farmers with opportunities to transform their agricultural practice. Furthermore, we aim to use our platform to increase the visibility of the smallholder farmers' sustainable farming practice, with the hope to facilitate the sales of their higher-priced, but well-justified products. Importantly, in many cases, visibilities of farming communities and their products in resource-limited areas have a crucial social impact of ensuring the preservation of indigenous communities and their cultures. Along the same line, in fact, the appreciation of the effort of farmers, be it smallholders or larger farm, is a gap in the modern agriculture and food industries. Consumers are rarely aware of the identities and where the source of the products they consume. We aim to connect farmers of all scales to the world, especially the consumers, by providing them a platform to make their identity and notable effort known and visible. This is a mutual benefit scenario, as farmers could get recognition for their efforts (which in some cases are their cultures), and the consumers are made aware of the farmers whose effort gave rise to the food we consumed daily.

13.2.3. Food Waste

Food waste is a resource liability for the sustainability of our planet earth, with roughly a third of food produced in the world (± 1.3 billion tonnes) being wasted each year [55]. This is especially a large loss for the earth considering that a considerable proportion of the world population experiences famine, hunger, and malnutrition. Food waste occurs along the entire supply chains but the waste pattern differs between developed and developing countries. In developing countries, it occurs more during the production process, "early" in the supply chain, while in developed countries, it occurs more at the "end" of the supply chain, frequently at the hand of the consumers [56]. *FreitX Network* envisions several opportunities along the supply chain to help reduce food waste. Our platform could be used to strengthen the "early" part of the supply chain where a large amount of

food loss and waste occur in developing countries. For example, our platform could be used to improve the visibility and timeline for produce for both the farmers, buyers, food packaging and transport companies. Another way we could help is for smallholder farmers to use our smallholder farmers marketplace to find the interested buyer sooner or be connected to a larger pool of interested buyers, increasing the chance of produce being sold, thus reducing food waste. In contrast, in more wealthy countries, food wastes occur at the retailer level and include soon-to-be expired produce and products whose quality and taste is at standard, but whose visual properties (e.g. cucumber that is too curly, red pepper that is not of the wrong color, or apple that is too small) do not meet the requirement. There are many innovative efforts to try to convert produce that would otherwise go to waste into food. La Soupe is a non-profit organization making soup from leftover produce from retailers and farm to feed families and those in need, while Rubies in the Rubble uses fruits and vegetables that would otherwise go to waste, most often for aesthetic reasons, to make condiments such as ketchup and relishes. To further help reduce food waste, we aim to use our platform to create an alternative leftover produce marketplace to facilitate reduction of food waste by enabling the sale of such produce rescued from various parts of the supply chain. Our platform will hopefully create access for distributors and retailers to offer their products to interested buyers, who could make use such products to make longer shelf life food such as canned food and preserved vegetables.

13.3. Implementation of Artificial Intelligence and Data Analytics for further value extractions

Blockchain Technology offers enormous opportunities to transform supply chain management. In the future, we envision using AI-driven data analytics for diagnostic and predictive purposes to further provide value to our customers. Data analytics could be applied to any *FreitX Network* applications, as our user-friendly platform has been designed for fast and compatible data retrieval. We envision using diverse tools for data analytics, including AI. For example, for access to healthcare use cases described in 12.1.3, with patients' consent, AI-driven data analytics could help the healthcare ecosystem and hospitals to predict demands for human resources, medicines, equipment, and other supplies, improving the efficiency and cost saving of the entire supply chain system. For smallholder farmers described in 13.2.2., our platform could further increase the work process and sales of smallholder farmers by helping them predict demands, price bids and prospective buyers, while to reduce food waste (described in 13.2.3), we could use our blockchain platform data to help the retailers and distributors to predict the timing of sales to the alternative marketplace instead of taking the risk to have the produce go to waste, by keep selling the produce in conventional markets. We are confident that data analytics would further generate value for our customers.

14. Robust Economic Model

14.1. Onex

OneX in *FreitX Network* ecosystem is one type of token which is a reflection of the dual token system. What makes this token special is that it is stable and could not be affected by any external or internal factors. OneX is pegged to fiat, thus this token is always equal to U.S dollar. Without OneX one cannot provide operation such as transaction producing, smart contract creating and payment processing. This is the main reason why OneX is the fuel for blockchain technology that we use in our ecosystem. To become a useful currency like the fiat U.S dollar, a currency must satisfy the criteria to achieve stability. In general, the stable coin is a price-stable cryptocurrency stabilized by one of the three most widely used methods: fiat-collateralized, crypto-collateralized or uncollateralized stable. It is a global digital currency that possesses the characteristics of having low volatility despite market conditions, thus allowing for practical utility. It has significant implications for multiple stakeholders. *FreitX Network* chooses to stabilize OneX stable coin with the crypto-collateralized method. Stability and tangibility of gold render it an attractive option in an unpredictable market. Gold brings balance to the crypto force.

14.1.1. Collateralized Debt Positions (CDP)

Owners of collateral assets can leverage them to generate OneX on the *FreitX Network* ecosystem through FreitX smart contracts known as collateralized debt positions (CDP). CDPs hold collateral assets deposited by a consumer and permit this consumer to generate OneX, but generating it also accrues debt. This debt effectively locks the accumulated collateral assets inside the CDP until it is covered by paying back an equivalent amount of OneX, where the owner can again withdraw their collateral. In excess, CDPs have always collateralized it means that the value of the collateral is higher than the amount of the debt.

14.2. FRX

FRX token is the cryptographic currency, the major component that drives the *FreitX Network*. FRX holders get voting priority for governance in the Network ecosystem. FRX is designed as fuel for using specific functions on *FreitX Network*. FRX empowers users to contribute and maintain the ecosystem. Token will be used as the unit of exchange between participants on the network. Ownership of FRX carries no rights other than the right to use FRX as a means to enable usage of and interaction with the *FreitX Network*. We provide fixed token supply, thus the total amount of tokens have been decided before the first FRX coin was created. After FreitX Blockchain Mainnet Launch, FRX will be swapped on FreitX Blockchain.

15. Governance Model

The *FreitX Network* governance model underlines the main characteristics of the governing system. Organizational structure is the choice of platform creator with respect to the types of user segmentation. Defined roles and responsibilities of all ecosystem

participants appear to be core instruction of interaction. Below mentioned characteristics help to have a network with common guidance function that ensures both high values in time for collaborative developments and better results.

Defined organizational structure - Plays the leading role in governance efforts. Participants know who are the teams and how do they interrelate within the platform. It could be a hierarchy of groups, a network, or different combinations.

Defined roles and responsibilities - As soon as roles and responsibilities are defined, we face critical guidance. This aspect of governance helps to understand who does what and how what are their responsibilities and when they have to interact with one another for collaboration.

Common guidance - provides a clear understanding of how to correspond to active processes, standards, and guidelines. This is a way to build supported and collaboratively developed governance model.

15.1. Board and Community

FreitX Network provides a governance model with a defined organizational structure, common guidance, defined roles, and responsibilities. The platform has a hierarchy of groups under their participation activities and token amounts. The system which enables users to do their jobs more effectively is the best opportunity to fulfill their needs and requirements. On *FreitX Network* we divide our participants into two types such as **A** roles and **B** roles.

Both of them have defined roles and responsibilities that are mutually beneficial. Their participation, contribution, and implementation should affect the ecosystem and help in sight setting, scoping and systemizing. Also, involvement and diversity of people in the network help to reach innovativeness, ambidexterity, traceability, and transdisciplinarity. According to implementations of hierarchically split groups, *FreitX Network* chooses work items which are prioritized and added to the stack.

Board is found on teams depending on the scale faced by the team.
Community roles are filled on a temporary basis to address scaling issues.

Board

1) **Executives**

Executives are actively contributing their skills and experience, and are engaged in the business model, marketing plan, funds and token management, white paper and website updates, technical development and business challenge. Executives have to be engaged in all provided processes. There is also the range of experience required includes previous participation in successful ICOs and experience in general marketing, business planning, budgeting, investor relations, and scenario modeling.

2) **Team**

The team member is responsible for producing an actual solution for consumers. There are different ecosystems where team members are employed. They could be engaged in testing, architecture, programming, analysis, design, planning and many more activities as required throughout the project lifetime.

Community

1) Stakeholder

A stakeholder is a person who is materially impacted by the outcome of the solution. The stakeholder could be an indirect or direct user, staff member or supporter. Everyone who is identified as a token owner remains a stakeholder.

2) Community

The community is a group of platform participants who use the service, find interests and benefit from provided operations.

15.2. Activity

We provide governance activity for implementation of processes and structures to inform, direct, manage and monitor the activities of our network. To achieve this, its objectives must be beneficial for our customers and ecosystem participants.

In each quarter, token holders who decide to lock FRX will have the power to participate in the governance activity. Each quarter has its own development areas, as indicated in the development timeline. Participants who have relevant skills and are sure that they could effectively contribute in the chosen quarter could lock their tokens in the same quarter. While the tokens are locked, if a participant managed to make an official proposal which was implemented into the network development, *FreitX Network* will offer the participant additional tokens for successful activity. This reward tokens could also be used after lock date has passed.

FreitX Network empowers FRX holders with capabilities to contribute to its ecosystem development and updates. We seek to empower and nurture contributing users who are effective and prolific, and who could uphold the platform by continuously finding the best issues to contribute to. Primary role FRX token owners, who are also the decision-makers, have the power to upvote or downvote after FRX secondary role owners make their final proposal.

We divide the official proposal creation process into several stages. The first stage is to make a pre-proposal, which is publicly viewable and active until it reaches indicated amounts of votes that decide its final status. To become a proposer, the pre-proposal should gain official proposal status, which provides the proposer the right to implement project improvements and modifications.

16. Economic Model

Given the non-fungible nature of supply chain data moved by FreitX Network, it is essential to facilitate liquidity and stability of the market. One of the main prerequisites for this is both a stable medium of exchange and accurate price discovery mechanism. Former is being addressed by native OneX stable coin, which provides much-needed stability and security for the somewhat conservative transportation industry. FreitX Network allows data originators and data consumers to freely negotiate fees and data that are being exchanged; this enables the ecosystem to discover price given the value of the data in each unique case, as well as contribute to the liquidity of the market.

For the network to function, the fee structure should be simple, while creating incentives for both suppliers and consumers to join. Each data consumer provides pre-negotiated payments linked to each instance of requesting data. Allowing for fee fluctuations helps absorb the shock produced by the difference in the value of each unique data point with respect to each of the consumers.

After defining incentives to join the network, it is essential to identify and promote compliant behavior for each of the stakeholders. First, it is essential for data produced to place valuable information onto the blockchain and abstract from spamming it. Thus a fee is associated with uploading data onto the blockchain, which will be covered in case there is sufficient demand for the data point. The second type of compliant behavior is the provision of the data consistent with the frequency outlined in the contract. To incentivize data originator to adhere to this requirements, the party is required to pledge collateral during the lifetime of the contract. Thanks to the stability provided by OneX, there is no exchange rate risk associated with collateral requirements. The total amount of funds in collateral scales with the growth of the network, which helps reduce the velocity of the token further strengthening the stability of the price.

17. Possible Future Directions and Research

There are many ways and possibilities for us to choose the right directions and make choices for suitable future developments. Here, we explore future directions of research to further improve the *FreitX Network* ecosystem.

We expect that all technologies that are used as building blocks for our network will be modified and improvised from time to time. As the industry grows and evolves, we encounter new situations that need to be followed in a beneficial way. The complex structure may not always lead to complications, however, sometimes the complexity remains the essential characteristic. Regarding the development process, we envision to be limitless and adaptable for as many functions as possible.

Adaptation is always crucial but at the same time, evolving and improving on current development allow us to take control of existing operations. *FreitX Network* tries to provide solutions to supply chain management problems with the identification of the

needs and trends of the market. We believe that research for the ways of broad adoption and integration is the primary key to our success.

The main philosophies of our platform design, which also is the main characteristics of our network, is to have a secure decentralized ecosystem, user-centric system, suitable services, and operations. This will make our platform more flexible to every environmental change.

References

1. "ERP Overview." 1 Jan. 2000, https://faculty.ist.psu.edu/yen/421/erp.pdf. Accessed 11 Nov. 2018.
2. "Supply Chain Management.indd - PFRI." https://www.pfri.uniri.hr/knjiznica/documents/Supply_Chain_Management.pdf. Accessed 11 Nov. 2018.
3. "Fundamentals of Supply Chain Management.pdf - Kenyatta University ...." http://library.ku.ac.ke/wp-content/downloads/2011/08/Bookboon/Magement%20andOrganisation/fundamentals-of-supply-chain-management.pdf. Accessed 11 Nov. 2018.
4. "Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org." https://bitcoin.org/bitcoin.pdf. Accessed 11 Nov. 2018.
5. "What is Artificial Intelligence (AI)?." https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-825-techniques-in-artificial-intelligence-sma-5504-fall-2002/lecture-notes/Lecture1Final.pdf. Accessed 11 Nov. 2018.
6. "Lean Management - McKinsey & Company." https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/financial%20services/latest%20thinking/reports/lean_management_new_frontiers_for_financial_institutions.ashx. Accessed 11 Nov. 2018.
7. "(PDF) The Internet of Things (IoT) Applications and ... - ResearchGate." 31 Jul. 2018, https://www.researchgate.net/publication/286573266_The_Internet_of_Things_IoT_Applications_and_Communication_Enabling_Technology_Standards_An_Overview. Accessed 11 Nov. 2018.
8. "White Paper · ethereum/wiki Wiki - GitHub." 21 Aug. 2014, https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 11 Nov. 2018.
9. "Zerocash: Decentralized Anonymous Payments from Bitcoin ...." 18 May. 2014, http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf. Accessed 11 Nov. 2018.
10. "Whitepaper - Nano.org." https://nano.org/en/whitepaper. Accessed 11 Nov. 2018.
11. "Elliptic Curve Cryptography." https://ocw.mit.edu/courses/mathematics/18-704-seminar-in-algebra-and-number-theory-rational-points-on-elliptic-curves-fall-2004/projects/asarina.pdf. Accessed 11 Nov. 2018.
12. "BLAKE2: simpler, smaller, fast as MD5." 29 Jan. 2013, https://blake2.net/blake2_20130129.pdf. Accessed 11 Nov. 2018.
13. "A Framework for Iterative Hash Functions — HAIFA - Cryptology ePrint ...." https://eprint.iacr.org/2007/278.pdf. Accessed 11 Nov. 2018.
14. "ChaCha, a variant of Salsa20." 28 Jan. 2008, https://cr.yp.to/chacha/chacha-20080128.pdf. Accessed 11 Nov. 2018.
15. "Descriptions of SHA-256, SHA-384, and SHA-512." http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf. Accessed 11 Nov. 2018.
16. "The RSA Algorithm." 3 Jun. 2009, https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf. Accessed 11 Nov. 2018.
17. "EdDSA for more curves." 4 Jul. 2015, https://eprint.iacr.org/2015/677.pdf. Accessed 11 Nov. 2018.
18. "High-speed high-security signatures - Ed25519." 26 Sep. 2011, https://ed25519.cr.yp.to/ed25519-20110926.pdf. Accessed 11 Nov. 2018.
19. "RFC 8032 - Edwards-Curve Digital Signature Algorithm ... - IETF Tools." https://tools.ietf.org/html/rfc8032. Accessed 11 Nov. 2018.
20. "Secp256k1 - Bitcoin Wiki." 19 Jul. 2018, https://en.bitcoin.it/wiki/Secp256k1. Accessed 11 Nov. 2018.
21. "Discrete Logarithm Problem." http://www-math.ucdenver.edu/~wcherowi/courses/m5410/dlp.pdf. Accessed 11 Nov. 2018.
22. "Understanding the Internet of Things (IoT) - GSMA." https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf. Accessed 11 Nov. 2018.

23. "The Blockchain Model of Cryptography and Privacy-Preserving Smart ...." https://www.cs.umd.edu/sites/default/files/scholarly_papers/Kosba.pdf. Accessed 11 Nov. 2018.
24. "SafeCurves." https://safecurves.cr.yp.to/. Accessed 11 Nov. 2018.
25. "RFID Technology Principles, Advantages, Limitations & Its ... - ijcee." 1 Feb. 2011, http://www.ijcee.org/papers/306-E794.pdf. Accessed 11 Nov. 2018.
26. "PEER-TO-PEER NETWORK." https://www.infosec.gov.hk/english/technical/files/peer.pdf. Accessed 11 Nov. 2018.
27. "User Datagram Protocol (UDP) - NC State: WWW4 Server." http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture5.pdf. Accessed 11 Nov. 2018.
28. "An Introduction to TCP/IP." https://www.jameco.com/Jameco/Products/ProdDS/320733%20(TCP%20IP)%20Intro.pdf. Accessed 11 Nov. 2018.
29. "An Accelerated Method for Message Propagation in Blockchain ...." 3 Sep. 2018, https://arxiv.org/abs/1809.00455. Accessed 11 Nov. 2018.
30. "An Accelerated Method for Message Propagation in Blockchain ...." 3 Sep. 2018, https://arxiv.org/abs/1809.00455. Accessed 11 Nov. 2018.
31. "Measuring Round Trip Times to Determine the Distance between ...." https://symonics.com/publications/papers/hoene_paper2.pdf. Accessed 11 Nov. 2018.
32. "The Digital Signature Algorithm (DSA) Johannes ... - CRYPTREC." 15 Dec. 2001, http://www.cryptrec.go.jp/exreport/cryptrec-ex-1003-2001.pdf. Accessed 11 Nov. 2018.
33. "Atomic Cross-Chain Swaps." 29 Jan. 2018, https://arxiv.org/abs/1801.09515. Accessed 11 Nov. 2018.
34. "On the Security and Performance of Proof of Work Blockchains." https://eprint.iacr.org/2016/555.pdf. Accessed 11 Nov. 2018.
35. "Practical Byzantine Fault Tolerance - Programming Methodology Group." http://pmg.csail.mit.edu/papers/osdi99.pdf. Accessed 11 Nov. 2018.
36. "Proof of Stake." https://vitalik.ca/files/technion2.pdf. Accessed 11 Nov. 2018.
37. "What is Proof of Elapsed Time Consensus? (PoET) - Blockonomi." 11 Sep. 2018, https://blockonomi.com/proof-of-elapsed-time-consensus/. Accessed 11 Nov. 2018.
38. "Proof of Work and Blockchains - IBM Research | Zurich." https://www.zurich.ibm.com/dccl/papers/eyal_dccl_slides.pdf. Accessed 11 Nov. 2018.
39. "Proof of Stake." https://vitalik.ca/files/technion2.pdf. Accessed 11 Nov. 2018.
40. "Light Clients and Proof of Stake - Ethereum Blog - Ethereum.org." 9 Jan. 2015, https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/. Accessed 11 Nov. 2018.
41. "The Byzantine Generals Problem - EECS at UC Berkeley." https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf. Accessed 11 Nov. 2018.
42. "The Stellar Consensus Protocol: A Federated Model for Internet-level ...." https://www.stellar.org/papers/stellar-consensus-protocol.pdf. Accessed 11 Nov. 2018.
43. "The Stellar Consensus Protocol: A Federated Model for Internet-level ...." https://www.stellar.org/papers/stellar-consensus-protocol.pdf. Accessed 11 Nov. 2018.
44. "Tendermint: Consensus without Mining." https://tendermint.com/static/docs/tendermint.pdf. Accessed 11 Nov. 2018.
45. "Scalable and Dynamic Quorum Systems - CiteSeerX." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.6437&rep=rep1&type=pdf. Accessed 11 Nov. 2018.
46. "A Framework for Unique Ring Signatures. - Cryptology ePrint Archive." 23 Mar. 2017, https://eprint.iacr.org/2012/577.pdf. Accessed 11 Nov. 2018.
47. "Non-Interactive Zero-Knowledge Proofs for Composite Statements." https://eprint.iacr.org/2018/557.pdf. Accessed 11 Nov. 2018.
48. "Stealth Address and Key Management Techniques in ... - SciTePress." http://www.scitepress.org/Papers/2017/62700/62700.pdf. Accessed 11 Nov. 2018.
49. "Solidity Documentation - Read the Docs." https://media.readthedocs.org/pdf/solidity/develop/solidity.pdf. Accessed 11 Nov. 2018.

50. "Ethereum EVM illustrated - GitHub Pages." https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf. Accessed 11 Nov. 2018.
51. "Blockchain for Social Impact | Stanford Graduate School of Business." 11 Apr. 2018, https://www.gsb.stanford.edu/faculty-research/publications/blockchain-social-impact. Accessed 11 Nov. 2018.
52. "White Paper - Ambrosus." https://ambrosus.com/assets/en/Ambrosus-White-Paper.pdf. Accessed 11 Nov. 2018.
53. "Whitepaper - Modum.io." https://modum.io/sites/default/files/documents/2018-05/modum-whitepaper-v.-1.0.pdf. Accessed 11 Nov. 2018.
54. "smallholders and family farmers - Food and Agriculture Organization ...." http://www.fao.org/fileadmin/templates/nr/sustainability_pathways/docs/Factsheet_SMALLHOLDERS.pdf. Accessed 11 Nov. 2018.
55. "Key facts on food loss and waste you ...." http://www.fao.org/save-food/resources/keyfindings/en/. Accessed 11 Nov. 2018.
56. "Food Loss and Food Waste | FAO | Food and Agriculture Organization ...." http://www.fao.org/food-loss-and-food-waste/en/. Accessed 11 Nov. 2018.