University of Amsterdam

Feasibility of Cryptocurrency on Mobile devices

MSc System and Network Engineering
Research Project 1

Sander Lentink & Anas Younis
sander.lentink@os3.nl anas.younis@os3.nl

Abstract

This research focuses on the use of cryptocurrencies on mobile devices, which is a subset of possible applications of a distributed ledger. This paper gives an overview of consensus mechanisms available when designing a practical cryptocurrency for mobile devices. The focus is on permissionless designs to reach consensus and keep in sync with the distributed ledger.

For this we looked into chain linking, SPV (Simple Payment Verification), SCP (Stellar Consensus Protocol), Skipchains and the tangle. The first three are consensus mechanisms for blockchain ledgers and the last is a consensus mechanism designed with a DAG (Directed Acyclic Graph) ledger. These consensus mechanisms were explored as options since they enable faster transaction times than traditional payment processes, which take around 30 seconds [1]. Besides the transaction time, we look at techniques that allow a device to determine the balance of a wallet. These synchronization techniques are dependent on the consensus mechanisms.

We conclude that acceptable transaction times and efficient usage of a mobile device's power resource can be achieved with the researched techniques. Future work notes that this is a non-exhaustive list and mentions other requirements for mobile cryptocurrencies, such as privacy.

Contents

1 Introduction

Blockchain technology has enabled permissionless (public) digital currencies as an alternative to permissioned (private) digital fiat currencies. One of the shared principles of permissionless blockchains is the limited processing speed of transactions and the need to be synchronized with the blockchain to verify account balance. The requirement to be synchronized with the blockchain requires a node to be constantly connected to the internet, which is not feasible for mobile devices. This currently prevents blockchain technology to be effective on mobile devices, somewhat limiting its use. Cryptocurrencies are governed through algorithms, which prevent manual reconciliation, resulting in faster and cheaper transaction settlements [2].

In this paper we will explore techniques that enable the practical use of cryptocurrencies on mobile devices. We look at the consensus mechanisms that allow for prompt transactions speeds and ways to get an offline wallet in sync again. The goal of this research is to provide a literary overview of the different aspects of making blockchain technology practical on mobile.

2 Related work

Previous research looked into aspects that contribute to making blockchain technology practical on mobile devices. Sirinlabs has looked into relevant security aspects, which they state that the current generation of smart devices compromises on user security. The main focus nowadays is for the most part on user experience, at a huge cost in fraud and cybercrime.

To address the relevant security aspects, Sirinlabs has developed a device called a "FINNEY" device. These are the first cyber-protected, blockchain-enabled mobile phone devices and personal computers [3]. Sirinlabs states that all FINNEY devices will form an independent blockchain network. The network operates without centralized backbones or mining centers which clutter up the transaction process.

Nikitin et al. wrote a research paper about Chainiac. Chainiac introduces SkipChains, a cryptographically-traversable, offline- and peer-to-peer-verifiable blockchain structure, which can be used for blockchain technology. In addition to back links, which are cryptographic hashes of past blocks that are already standard in blockchains [4], Chainiac introduces collectively-signed forward links. They are cryptographic signatures of future blocks, which are added retroactively when the target block appears. With these links, any party can securely "catch up" on a Chainiac blockchain via peer-to-peer communication with any party who is more up-to-date. A prerequisite hereby is that the party, who is more up-to-date has actually stored and can forward all the intervening block headers and forward links.

When creating a new block with Chainiac, that block does not just include one hash link to the immediately prior block, but also additional hash links to that point further back in time. By taking this approach, any party can find, or prove the integrity of, an old transaction anywhere prior to the history of its blockchain with a small (logarithmic) number of hash-link steps. This long-distance back-link refinement is not new or unique to Chainiac as other blockchain and hash-chain designs have already incorporated this idea for backward links.

The new and unique aspect of Chainiac is to provide the long-distance forward links as well via collective signatures. When adapting both long-distance forward and backward links, a SkipChain becomes cryptographically traversable in both directions. This enables one party to efficiently prove the correctness of a transaction anywhere in time while taking the reference point of the other party. This is achieved in a logarithmic number of steps, regardless of which party has a more up-to-date view of the blockchain.

With current public blockchains such as Bitcoin and Ethereum, verifying that a transaction is part of the blockchain requires a device to;

- be online with a working connection to the Internet,
- keep connection with multiple ”full nodes” on the overlay network of the blockchain,
- regularly synchronize with the blockchain.

With SkipChains, a mobile device can securely catch up when it comes online [5, 6].

Suankaewmane et al. conducted a performance analysis and application of mobile blockchain. They state that mobile security has become more and more important due to the boom of mobile commerce (m-commerce) and that blockchain has been introduced as an effective security solution in many applications in practice. The absence of blockchain technology in m-commerce is due to the requirement of standard computing units for mining. They introduce a new m-commerce application using blockchain technology named MobiChain. MobiChain is used to secure transactions in the m-commerce and can be executed efficiently on mobile devices using their proposed Android core module. Their performance results show that blockchain is an efficient security solution for m-commerce [7].

Satoshi Nakamoto, the person or group behind Bitcoin, described a technique called SPV (Simplified Payment Validation) which is being used in mobile Bitcoin clients. With SPV, a client maintains connections with one or several full nodes and only needs to keep a copy of the block headers (which are around 80 bytes) rather than full blocks. While this is more economical than running a full node by downloading the full block, it still needs to be online to verify transactions [8, 5].

3 Research question

This research focuses on the possibilities for blockchain on mobile devices by looking into the various techniques used in different blockchain technologies.

The goal for this research is to provide a literary overview of the different techniques available and what problem they solve for disconnected devices participating or connecting to a distributed ledger.

For this we formulated the following research question:

- Which aspects are required to make cryptocurrency feasible on mobile devices?

The following sub questions support the research question:

- Which consensus methods exist and how do they compare to each other on mobile devices?
- Which techniques are available to keep mobile devices in sync with the blockchain, and how do they perform?

4 Cryptocurrency attributes

Permissioned vs. permissionless To understand this attribute of a cryptocurrency in depth, we need to explore the motivation for the concept, cryptocurrency, at first.

The first popular cryptocurrency was introduced with Bitcoin. After Nakamoto lost trust in the financial structure during the banking crisis, he presented an open source alternative for financial transactions that enables a trustless system. This is, at the heart of the cryptocurrency revolution, not having an authority that is able to manipulate or control the system, also called a permissionless system. It allows anyone to join without a party approving. A permissionless system is transparent, everyone can verify the code and the validity of the ledger. The data stored on the ledger is immutable and the data is stored redundant on multiple participating entities. Another aspect of trust is auditability. When a ledger is publicly verifiable, it enables trust to be shared instead of centralized.

On the opposite side is a trusted or so called permissioned system, in which the founders keep some form of influence on the cryptocurrency [9], up to the extent of the current banking system, in which they control the inflation, credibility, privacy, security etc.

Consensus mechanism Bitcoin uses a distributed ledger that is maintained by miners through PoW (Proof-of-Work); this is an implementation of *dynamic membership multi-party signature* (or DMMS) [10]. This enables all nodes on the ledger to reach consensus over the state of the ledger. While this permissionless system was a technological break through, it did not allow the same processing speed as traditional credit card payments. To enable prompt crypto payments, there are different consensus mechanisms. We will look into feasible consensus mechanisms for mobile devices, described in section 5.

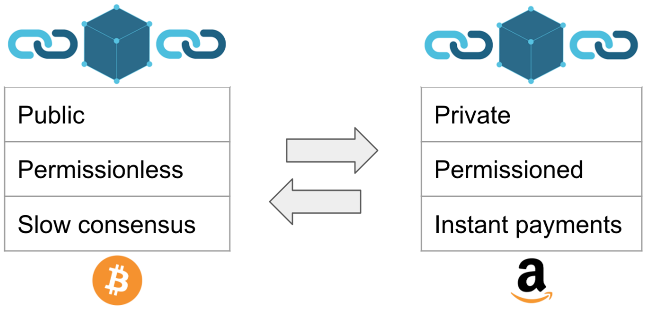

Figure 1: Example use case of chain linking: speedy transactions with a private blockchain

Sidechain enabled When one has crypto assets on one blockchain (e.g. Bitcoin) and wants to use a different consensus mechanisms (e.g. permissioned for instant payments), one can transfer the assets from one chain to another (if both support this). This enables assets of blockchain X to be transferred using the consensus mechanism of blockchain Y. Figure 1 shows an example use case of this. See section 5.1 for more information.

Traceability This attribute has two aspects to it, the ability to trace a wallet or transaction to a user and the ability to correlate different transactions.

Scalability For permissionless blockchains, the block size and block interval are limiting transaction throughput. When it comes to permissioned systems, the security and throughput are determined by the protocol and the entity controlling it.

Speed of transaction The processing speed of global consensus mechanisms (permissionless blockchains) that use PoW (Proof-of-Work) is insufficient when comparing it to traditional digital payment methods. Permissioned systems however, enable faster transaction settlements [2]. We note that the speed of a transaction can be seen in two ways; the regular instant transaction via card at a point of sale and the payment finality (when no chargebacks can occur), which can take years for traditional financial systems [11] and up to thirty minutes for Bitcoin.

5 Techniques

This section explores the various techniques that could be used when designing a system that allows mobile payments using cryptocurrencies. Figure 2 shows an overview of the cryptocurrency consensus mechanisms we will be looking into.

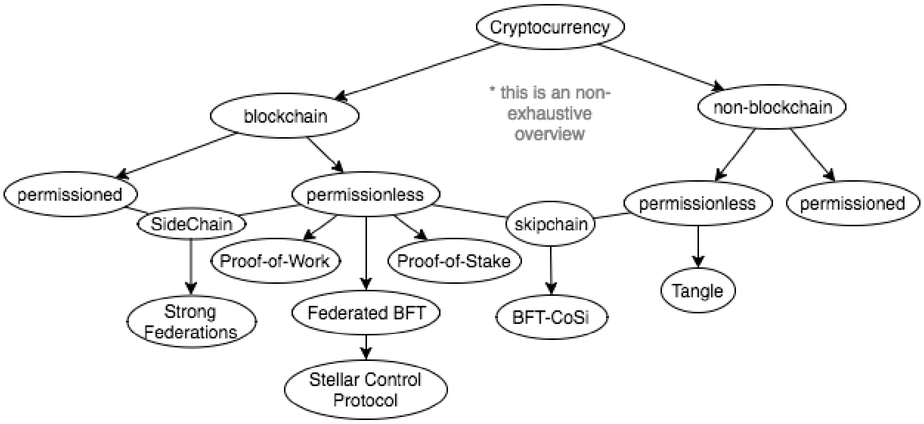

Figure 2: Overview of cryptocurrency consensus mechanisms

We start with blockchain techniques, followed by implementations that use DAG (Directed Acyclic Graph). For this we looked into chain linking, SPV (Simple Payment Verification), SCP (Stellar Consensus Protocol), Skipchains and the tangle.

5.1 Sidechain

Customers pay at retailers with standardized fiat currencies, together with gift-cards, coupons and reduction/discount structures. For cryptocurrencies, a similar structure can exists through smart contracts.

The major difference with cryptocurrencies is the shared fiat currency. Every retailer can add his own discount logic in addition to the fiat currency. For cryptocurrencies, the rules are dictated by the altcoin (alternative cryptocurrency, not Bitcoin) it is part of, and every altcoin has its own currency.

Modern webshops accept multiple fiat currencies, which is feasible since there is a limited set of fiat currencies and there is less fluctuation in value than cryptocurrencies. To reduce the number of crypto assets one needs to pay in different stores, Back et al. proposed to link chains, allowing currency X to be spend with the rules and on chain Y [10]. This allows one blockchain to be the asset container, while the assets are transferred from party A to B using the rules of another blockchain. The asset will be locked on the main chain in a special wallet, which is controlled by the sidechain, giving the sidechain the authorization of those assets. Just as dollars and pounds used to be backed by physical gold, the sidechain is backed by the main chain.

This allows a company to have its own private blockchain without a separate currency and ICO (Initial Coin Offering). Their blockchain will be a sidechain to a chain that holds value, such as Bitcoin. This allows a company to be payed in cryptocurrencies without having their own altcoin. Customers transfer a part of their assets on the main blockchain (e.g. Bitcoin) to the managed blockchain, sacrificing a trustless system for other features, such as faster transactions, enhanced privacy and ring signatures.

When it comes to mobile payments, chain linking reduces the amount of currencies a user owns, but the assets will be spread across multiple chains. Fast transactions times are possible with currencies that naturally have a slow transaction speed, such as Bitcoin.

Sidechains add complexity, implementation requirements and new attack vectors, requiring extra security. Therefore, it is important to choose trustworthy custodians. Wallets and blockchains need to implement the new features. For Bitcoin, this would require a soft fork [10]. When chains can use the asset of the main chain, the sidechain security becomes more important since the assets it managed are more relevant. To increase the strength of a sidechain network, the mining capacity could be increased with merged mining [12].

5.2 Simple Payment Verification

Cryptocurrencies that make use of blockchain need to be up-to-date with the ledger to determine the wallet balance. This implies that clients (mobile devices) that are offline cannot state their wallet balance with certainty. However, if one trusts that it is the only one with access to its private key and the system has not been compromised and is up and running, it can confidently initiate a transaction at a point of sale. This can be compared to current payment systems, where the card and PIN are the private key and the *non compromised system that is up and running* represents the banking infrastructure, which has seen downtime through DDoS attacks [13].

SPV (Simple Payment Verification) has been proposed in the original Bitcoin whitepaper and was specified in detail in BIP-37 [14]. A client that uses this is considered a light node. A light node first requests the headers from its last known point, followed by requesting the blocks linked to the wallet of the client. By not downloading the full blockchain, the light node requires less disk space and synchronization time. This separates full nodes from light nodes, which enables mobile devices to only care about the transactions it is interested in.

Proof-of-Stake Bitcoin uses PoW (Proof-of-Work), which is limiting the transaction speed. Current Bitcoin transactions can take up to 30 minutes to be considered final. Before looking at SPV for wallet synchronization, the consensus mechanism of the blockchain should be considered.

PoS (Proof-of-Stake) is an alternative to PoW. It does not demand the miners to invest computational power, but in the cryptocurrency itself (own a stake). This mechanism assures honesty of miners, not by computational investment, but in the currency, making it waste less energy. The transaction time improves [15] since there is no bruteforce mining.

5.3 Stellar Consensus Protocol

D. Mazires et al. presented FBA (federated Byzantine agreement), a model suitable for worldwide consensus. This section focuses on the design of the FBA model and the implementation of the model in a protocol called SCP (Stellar Consensus Protocol) [16].

5.3.1 Syncing and consensus

Federated Byzantine Agreement FBA is used for reaching consensus worldwide. With FBA, each participant knows of other nodes it trusts. The participant waits for the majority of the trusted nodes, with whom it is participating, to agree on any transaction before settling the transaction. Those trusted nodes only agree to the transaction until the participants they trust agree as well.

By taking this approach, it becomes infeasible for an attacker to roll a transaction back if the majority of the network accepts the transaction. The FBA consensus protocol is derived from the traditional Byzantine agreement.

Traditional Byzantine agreement guarantees achieving consensus despite arbitrary behavior of some fraction of the participants. The Byzantine agreement has two properties, reaching consensus fast and efficient, and decoupling trust from resource ownership. Membership in Byzantine agreement is controlled by a central authority or closed negotiation, which makes it permissioned. The members are known and are added to the group based on permission. This is done to ensure that none of the members of the group can undermine the shared consensus regarding the status of the transactions. This makes the consensus protocol fast as only the central authority stores all data. There were prior attempts to reach decentralized consensus with the Byzantine agreement, but they had to give up some benefits. Ripple took an approach to publish a starter membership list that participants of the Ripple network can edit for themselves, with the hope that people's edits are reproduced by an overwhelming fraction of the participants. But users of the Ripple network are holding back to edit the list in practice, because divergent lists invalidate safety guarantees [16].

Alchieri et al. introduces Byzantine Fault Tolerance-CUP (BFT-CUP), which was a similar approach like the researchers of FBA. However, they did not take a Sybil attack into account, where malicious users try to join multiple times to exceed the system's failure tolerance [16, 17].

Stellar Consensus Protocol The Byzantine agreement is an approach to efficiently achieve consensus among distributed systems. FBA tackles the issue of updating replicated state of a transaction ledger like traditional Byzantine agreement and other techniques described in this paper.

Updating a distributed ledger with a transaction tree like the tangle is also an option, which is discussed further on in section 5.5. However this is done by trusting designated participants. Bitcoin introduced the revolution of decentralized consensus with blockchain technology, which led to many new system and research challenges. David Mazires introduces SCP (Stellar Consensus Protocol) which is based on FBA. It preserves the traditional benefits of the Byzantine agreement while it achieves decentralized consensus.

For updating the transaction ledger, each update is identified by a unique slot. An FBA system ensures that nodes agree on slot contents by running a consensus protocol. A node v can apply update x in slot i, when node v has safely applied updates on all slots upon which i depends. Additionally it assumes that all correctly functioning nodes will eventually agree on x for slot i.

The challenging part of implementing an attack-proof Byzantine agreement system is that malicious nodes can join many times and outnumber honest nodes to reach consensus with a malicious central authority. For this particular issue, FBA determines "quorums" in a decentralized way, by each node selecting "quorum slices" to reach consensus. A quorum is defined as the set of nodes which are sufficient to reach an agreement. A quorum slice is the subset of a quorum, which convinces one particular node of agreement [18].

With a consensus protocol, nodes exchange messages asserting statements about slots. If a node notices that a sufficient set of nodes asserts a particular statement, it will assume that no functioning node will contradict that statement. This sufficient set of nodes represents the quorum slice. By having each node choose its own quorum slices, there is no centralized authority; individual nodes decide whom to trust [16, 19].

5.3.2 Transactions

Transaction confirmation time and speed Transactions are processed fast with the SCP protocol. This is achieved by letting the trusted nodes in the network do all the required hard work, like maintaining an expansive ledger and processing high-throughput low-latency transactions. At a Stellar meet up in Singapore, Lightyear program manager Lindsay Lin's presentation mentions that the Stellar network can handle more than 1000 transactions per second [20]. Transaction confirmation time with Stellar takes just a few seconds. This is possible by the central authority's computational power, whom a node trusts depending on the node's quorum slice [21].

Transaction fees At the same Stellar meet-up, it was presented that the transaction fee is less than 0.01$. This is achieved by eliminating gaps between closed systems [20].

5.3.3 MobileCoin

To provide a feasible solution for mobile devices, a team of experts have set up a cryptocurrency called MobileCoin. MobileCoin is a cryptocurrency, fully based on SCP [22].

Design The MobileCoin network is made up of nodes, where each node serves users. The nodes in the network do all the required hard work like maintaining an expansive ledger and processing high-throughput low-latency transaction. The nodes are designed such that a node operator should never have access to the funds of the users it is serving nor learn anything about their balances and transaction history. The intention of all MobileCoin nodes is to keep them running in a SGX secure enclave. A SGX enclave is isolated from the host OS in hardware-encrypted RAM. SGX is a set of new CPU instructions that can be used by applications to set aside private regions of code and data [23]. This keeps the node operator from having the ability to see into the enclave.

The ledger is public and distributed to all MobileCoin nodes and will also never be accessible or viewable by humans (MobileCoin operators included), because the entire MobileCoin ledger is designed to remain sealed within SGX enclaves across the entire network. The open approach of MobileCoin, by the help of SCP based on FBA, is to eliminate permissioned Byzantine. Mobile applications do not have the ability to synchronize a multi-gigabyte blockchain and desire transactions that are equal or faster than traditional payment methods, which take around 30 seconds [1]. To eliminate these issues, attempts were made to build a cryptocurrency with a better user experience, but unfortunately this led to trusting a third-party service to manage keys and validate transactions [22].

Security By running MobileCoin in an SGX enclave, it enables the ability to securely manage keys for users. A client can perform remote attestation to its MobileCoin node before transmitting its keys into the remote SGX enclave by giving up a short recovery PIN. Remote attestation allows a remote client to determine that a server is indeed running a specific piece of software inside a SGX enclave over the network. The node can then rate limited authenticated access to the keys, while the enclave prevents the node operator or anyone who attempts to compromise the node from circumventing the software and attempting to brute force access to the keys directly. The user can reside his key safely in a node and survive reinstalls or lost devices, without having to trust the node operator or the security of the node computer. Memorizing or safely storing extremely long recovery phrases is also not necessary to be able to reside the users' key[22].

Privacy To achieve privacy, MobileCoin does not only rely on SGX for maintaining transaction privacy, but transactions are also designed to use CryptoNote one-time addresses and one-time ring signatures. This way, MobileCoin will maintain transaction privacy through unlinkable addresses, even if an attacker is able to defeat SGX and view transactions that happen across the network [22].

Consensus and Syncing MobileCoin nodes are designed to use SCP to synchronize with a ledger. This allows sub-second transaction under normal circumstance with decentralized control and flexible trust. In paragraph 5.3.2 we highlight the transaction times which are achieved by SCP. By letting the SGX nodes do all the hard work, it allows user nodes to avoid storing a full blockchain history. It is only necessary to maintain a ledger of address value mappings, and the list of used key images to prevent double spending.

To maintain privacy, all transaction and balance information is kept private by the SGX enclaves across the network. In addition to this, privacy is further protected with so called "CryptoNote" one-time addresses and one-time ring signatures. With this addition, attackers cannot compromise private information even if they are able to forge SGX remote attestation [22, 24].

By having the SGX nodes validate the transaction, the number of participating nodes needed to validate each transaction is low, which leads to high scalability.

5.4 Skipchains

To achieve tamper evidence, consistency and search efficiency of a timeline, Chainiac introduces Skipchains. Skipchains enable clients to efficiently traverse long update timelines, both forward and backward. This is made possible by implementing forward-links in addition to back-links, the latter are cryptographic hashes of a past block that are already standard in blockchains. Chainiac introduces collectively-signed forward links.

They are cryptographic signatures of future blocks, which are added retroactively when the target block appears. With these links, any party can securely sync on a Chainiac blockchain via peer-to-peer communication with any party who is more up-to-date. A prerequisite hereby is that the party, who is more up-to-date has actually stored and can forward all the intervening block headers and forward links. When creating a new block with Chainiac, that block does not only include one hash link to the immediately prior block, but also additional hash links to that point further backward in time. This is illustrated in figure 3.

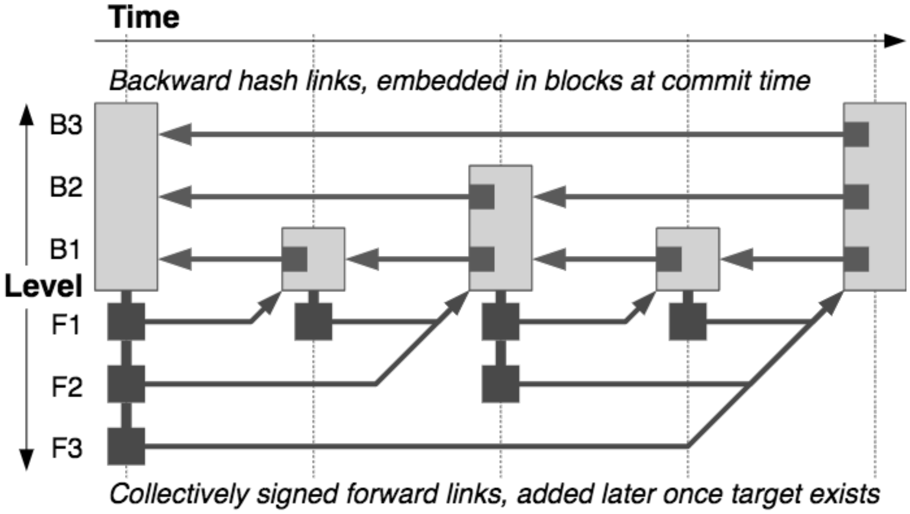
Time
Backward hash links, embedded in blocks at commit time
B3
B2
B1
Level
F1
F2
F3
Collectively signed forward links, added later once target exists

Figure 3: Skipchains' back- and forward-links [5]

As a result of Skipchains, resource constrained clients like mobile and IoT devices can efficiently obtain and validate updates in the ledger. Clients making use of Skipchains do not need to continuously keep track of a release chain, like in the case of a Bitcoin full-node. Skipchains clients can privately exchange and independently validate newer and older blocks on demand. Skipchains enable this through forward and backward links, which are offline verifiable [6, 5].

5.4.1 Syncing and consensus

Skipchains makes use of the BFT-CoSi (Byzantine Fault Tolerance Collective Signing) consensus algorithm. Eleftherios Kokoris-Kogias et al. introduce ByzCoin [25], a Bitcoin-like cryptocurrency which implements the BFT-CoSi consensus algorithm. BFT-CoSi is based on the principles of the PBFT (Practical Byzantine Fault Tolerance) consensus algorithm, combined with the CoSi protocol to reach scalable collective signing. This allows a trusted central authority to publicly validate statements made by nodes. BFT in this context is the same technique as the traditional BA (Byzantine agreement), which is discussed in section 5.3.1 about FBA.

To bring PBFT's strong consistency to cryptocurrencies, BFT-CoSi addresses four key challenges:

- Open membership
- Scalability to hundreds of replicas
- Proof of work block conflict

- Transaction commitment rate

The design of PBFT does not allow for scalability to large consensus groups, the deployments and experiments often employ a minimum of four replicas and have not explored scalability levels beyond 16 replicas.

Chainiac has managed to make permissioned BFT more open. To achieve this, the researchers had to eliminate two conflicting challenges. The first challenge is that conventional BFT schemes rely on well-defined consensus groups. The other challenge is that Sybil attacks can trivially break any open-membership protocol involving security thresholds, like in PBFT, where the assumption is that at most f out of $3f + 1$ members are honest [26].

Practical Byzantine Fault Tolerance The Byzantine Generals' Problem describes the situation where one or several components of a distributed system fail, which prevents from reaching an agreement. The Practical Byzantine Fault Tolerance (PBFT) algorithm was the first efficient solution to the Byzantine Generals' problem in reaching consensus that works in weakly synchronous environments such as the internet.

PBFT also has limitations. It assumes a fixed, well-defined group of replicas, by which it contradicts Bitcoin's basis principle of being decentralized and open for anyone to participate. Next to this, each PBFT replica communicates directly with every other replica during each consensus round, resulting in O(n^2) communication complexity. This becomes impractical if n represent hundreds or thousands of Bitcoin nodes. The last issue is that a client must communicate with a majority of the replicas in order to confirm the transaction has been committed and to learn its outcome after submitting a transaction to a PBFT service, which makes secure transaction verification unscalable [27].

Collective Signing The Collective Signing (CoSi) protocol has been created to reach scalable collective signing, which enables an authority or leader to request that statements be publicly validated and (co-)signed by a decentralized group of witnesses. Each protocol run delivers a collective signature with the size and verification cost comparable to an individual signature, but which compactly confirms that both the leader and his (many) witnesses have signed the declaration and agreed to sign the statement.

CoSi combines Schnorr multi signatures [28] with communication trees. The protocol initially assumes that signature verifiers know the public keys of the leader. Each message has to be collectively signed, the leader initiates a CoSi four-phase protocol which requires two round trips over the communication tree between the leader and its witnesses [6, 26].

5.4.2 Transactions

Transaction fees As PBFT's consensus group has been made more open towards a permissionless solution with the help of the CoSi protocol, it can no longer be assumed there is voluntary participation in a closed group of trustees.

There is need for an incentive for nodes to obtain shares in the consensus group and remain active. To achieve this, the researchers adapted Bitcoin's existing incentives of mining awards and transaction fees. Instead of letting all these rewards go to the miner of the most recent block, this block's rewards and fees are split across all members of the current consensus group, in proportion to the number of shares each miner holds.

The consequence of this is that if a miner has devoted more hash power within the current window, the more shares the miner holds, which leads to more revenue the miner receives during payouts in the current window. By splitting the rewards, it creates incentives for consensus group members to remain live and participate, because they only receive their share of the rewards for a new block if they continually participate [26].

Transaction confirmation time and speed By using a PBFT-like mechanism, BFT-CoSi transactions can take place within seconds, rather than a fixed time like with the current blockchain for Bitcoin. Eleftherios Kokoris-Kogias et al. have measured a network throughput up to ≈ 700 transactions per second [26].

5.5 Tangle

IOTA is a cryptocurrency for the Internet-of-Things (IoT) industry. The main feature of IOTA is the tangle, a DAG (Directed Acyclic Graph) for storing transactions, instead of a global blockchain.

The tangle is an alternative to the blockchain, because it offers features that are required to establish a machine-to-machine micropayment system [29].

5.5.1 Syncing and consensus

The DAG consists of sites which are transactions represented on the tangle graph, issued by nodes. The edge set of the tangle is obtained by letting a new transaction approve two previous transactions. These approvals are represented by directed edges from site to site. Because a DAG is acyclic, it means that the same transaction can never be encountered for the second time.

The transactions are issued and validated by nodes. Users must work to approve other transactions. Thus these users are contributing to the security of the network by approving transactions.

A direct path between two transactions means they can directly approve each other. If there is no direct path between two transactions, but there is a path of at least two between them, that means the transactions indirectly approve each other. For example, in figure 4. there is a directed edge between A and B, meaning that A directly approves B. The path between A and F is indirect, A approves B, which in turn approves F. The nodes check if the approved transactions are not conflicting. If a node finds a transaction which conflicts with the tangle history, it will not be approved in either a direct or indirect manner.

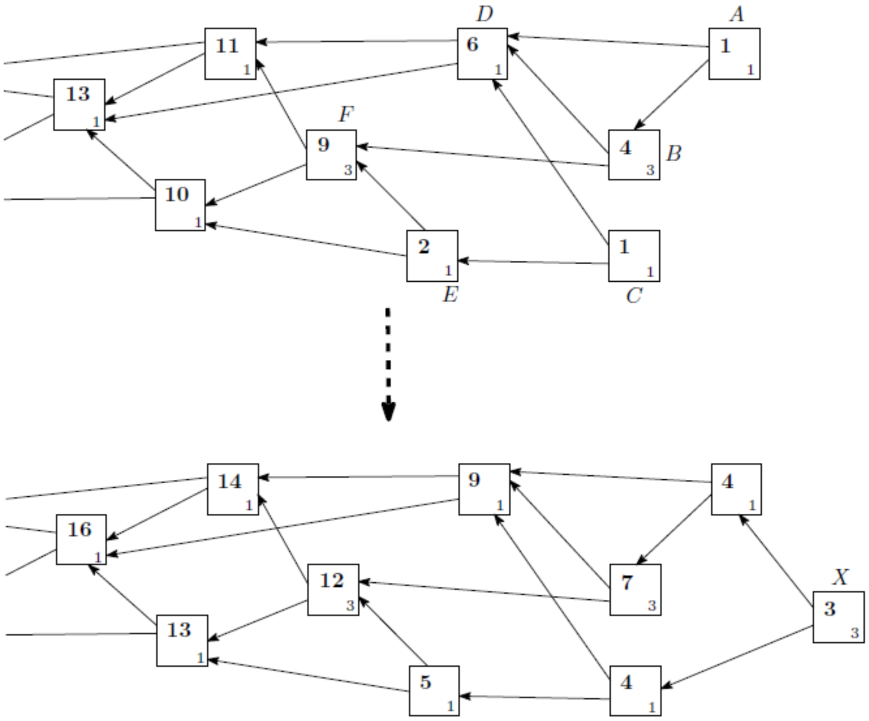

Figure 4: DAG with weight assignments before and after a newly issued transaction, X. The boxes represent transactions, the small number in the SE corner of each box denotes own weight, and the bold number denotes the cumulative weight [29]

To issue a transaction, a node chooses two other transactions to approve according to the MCMC algorithm [30]. The node also checks if the two transactions which are chosen by the algorithm are not conflicting. To finally issue a valid transaction, the node has to solve a cryptographic puzzle similar to the PoW approach of blockchain. The node has to find a nonce such that the hash of that nonce concatenated with some data from the approved transaction has a particular form.

To avoid spamming, conflicts and other attack styles, a transaction has a weight and a cumulative weight. In figure 4. the top-left corner indicates the cumulative weight and the small number in the bottom-right corner of each transaction box denotes its own weight. The own weight of a transaction box has a positive integer n, which correlates to the amount of work that the issuing node has invested into it. It is irrelevant to determine how a transaction's own weight has been obtained, it is only important to know that it has a weight attached to it.

The cumulative weight is more important than the own weight. It is the own weight of a particular transaction plus the sum of own weight of all transactions that directly or indirectly approve this transaction in the tangle. For example, the cumulative weight F is calculated as follows. Since transactions A and C indirectly approve transaction F, and transactions B and E directly approve transaction F, their weight is added to the own weight of F, which is $1(A) + 3(B) + 1(C) + 1(E) + 3(F) = 9$. The bottom tangle snapshot of figure 4 shows what happens when a new transaction is being added to the tangle. The bottom tangle shows how the weight of the new transaction "X" distributes itself among other transactions their cumulative weights. Because X is the "tip" of this part of the tangle, all other transactions are directly or indirectly approved by it. A "tip" is an unapproved transaction in the tangle graph. The top tangle snapshot in figure 4. shows that A and C are the tips. In the bottom tangle snapshot, transaction X becomes the new and only tip. The cumulative weight helps in particular with avoiding the double-spending problem, by having every node approve two other transactions before making its own transaction.

With the case of two conflicting transactions, Tx1 and Tx2 which are recorded in the tangle ledger. The cumulative weight of these transactions decides which one gets to stay, which is the transaction with the most cumulative weight. The IOTA network is asynchronous; the nodes in the IOTA network do not have to see the same set of transactions, which means that the ledger does not have to come to an agreement at the end of the day. With blockchain there is a miner who decides which transaction gets to stay in order to make the ledger synchronous [29, 31].

Eventually, IOTA should be completely decentralized, not requiring any regulated central. For now, the transactions which are selected to validate other transactions are regulated by a central authority, called a coordinator. The coordinator, which is a full node in a secret location, helps to verify transactions and is run by the IOTA Foundation. This is done by the IOTA Foundation to withstand attacks on the tangle network, because the current IOTA network is not strong enough yet. There have to be a lot of nodes and users doing transactions on IOTA continuously and concurrently (every second of the day) to be considered a secure network. It would not be a good choice to shut down the coordinators at this moment; the network would be susceptible to attacks when the activity is low. However, a user can always set up own full node(s) to make it as decentralized as the user needs [32, 33].

Next to this, IOTA's tangle network is not private, yet. The team behind IOTA is researching this aspect [34, 35].

5.5.2 Transactions

Transaction confirmation time and speed All nodes have a different version of the transaction history, by confirming two random transactions in the network; this links every transaction with other which creates a shared history of all the transactions in the network. A node can quickly verify if a transaction is valid when it sees a new transaction, without having to store all the data [36].

A user can choose to run a light client or a full node. When running a light client, the responsibilities of running a full node will be delegated to a third party. The user trusts the third party to perform critical functions, such as; providing accurate balances and wallet transaction history, and broadcasting your transactions to the rest of the network [37].

The reason to connect to a full node is because a mobile device does not have the computing power, or its usage would not be efficient, to search the entire tangle for figuring out the wallet balance. The full balance will be on the wallet after it asks the node it is connected to [38, 29].

In our case a light client is desired for the most efficient solution in order to achieve a practical use of cryptocurrency on mobile devices. The main benefit of using a tangle rather than a blockchain is its scalability. The transaction confirmation time gets faster the more nodes join, which is shown in figure 5. By having a sender who validates two transactions for each transaction, the more transactions can be confirmed, because the number of validating transactions increases with more users. Thus, the system becomes faster instead of slower the more users it has, in contradiction to blockchain where it can only maintain a certain number of transactions at a time [39, 40, 41].

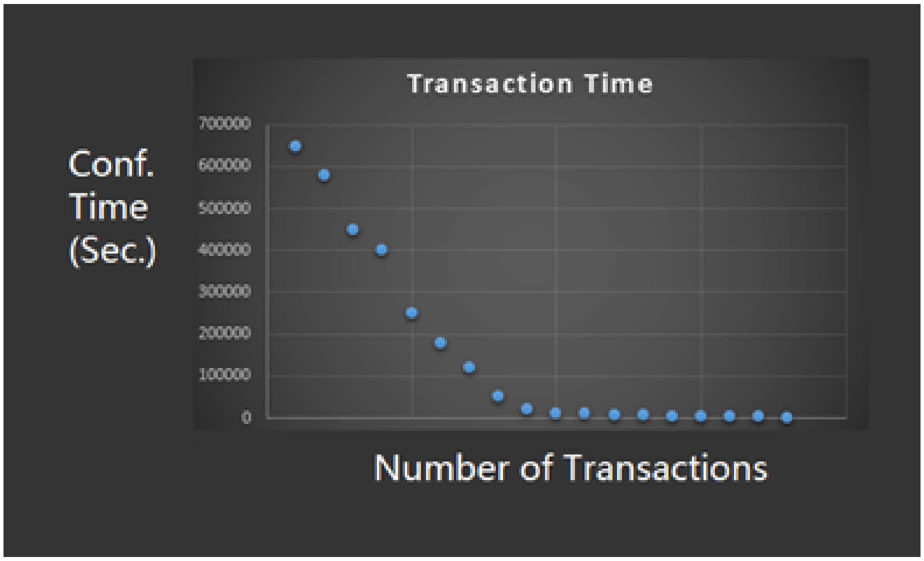

Figure 5: Number of transactions made versus transaction confirmation time [39]

The transaction times are inversely related to the numbers of transactions being issued on the tangle. The confirmation time of a transaction will be quicker with more transactions on the network. The transaction times will eventually approach the network propagation time if the number of transactions will still increase, which is shown in figure 5. IOTA's tangle already exceeds 500 transactions per second [42, 43]. [39]. Figure 6 shows that the capacity of the tangle network increases the more nodes join, which makes the tangle very scalable.

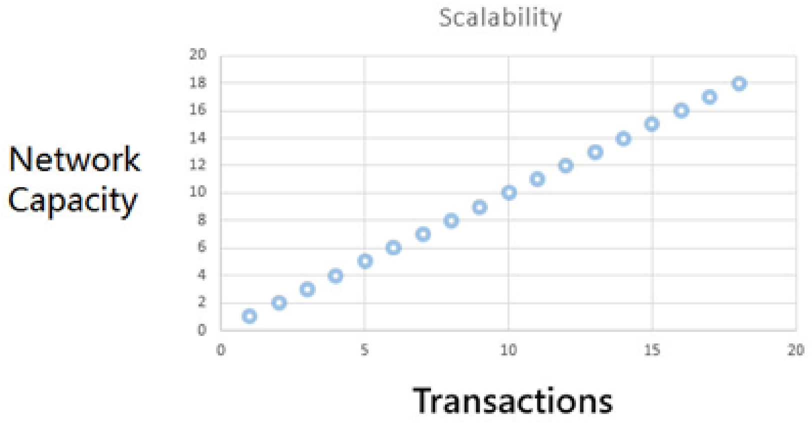

Figure 6: IOTA's tangle network capacity versus the number of transactions being verified [39]

Next to this, making offline transactions is also possible with IOTA's tangle. It is possible for a user to issue transaction offline by creating an offline sub-tangle which can be attached to the main tangle when coming online. The transactions will be valid if the online addresses hold the required balances according to the offline transaction. When the sender comes online, the sub-tangle merges with the main tangle. Other users will then start accepting the sub-tangle [44, 45]. Bear in mind that some kind of trust is needed in the case of an offline transaction, for example in the form of a contract.

Transaction fees Serguei Popov states that one notable drawback of Bitcoin is the concept of a transaction fee for transactions of any value. It is not logical having a situation where the amount of the fee is larger than the amount of the transaction being transferred. Getting rid of the fee is not easy as they serve as an incentive for the creators of the blocks. Unlike Bitcoin, IOTA does not have any transaction fees. Achieves consensus with IOTA is based on the validity of transaction. The entire network of participants (i.e. the devices making transactions) are directly involved in the approval of transactions, instead of a smaller subset of the network being responsible for the overall consensus (i.e. without involvement of any miners). The total supply of IOTA is fixed by the founders in the genesis transaction; no tokens will be created in the future. This results in the fact that there are no miners who receive monetary awards. There is basically no option to mine for more IOTA tokens. Therefore, based on this, there are no transaction fees.

Because it is a fee-less system, it enables users to even transact sub-cent values Peer-to-Peer without any form of a transaction fee for either the sender or the recipient [29].

5.5.3 SirinLabs

IOTA's tangle technology has been fully adapted by the company SirinLabs. They have developed the first cyber-protected mobile phone device, called a "FINNEY" which makes use of IOTA's tangle technology. They use it for the development of their cryptocurrency, Sirin Labs (SRN) tokens [3].

6 Conclusion

In Table 1 we highlight and compare different aspects for the consensus mechanisms we discussed.

	PoW	PoS	SCP	BFT	BFT-CoSi	Tangle
permissionless	X	X	X		X	X
tx time $\leq$ traditional methods		X	X	X	X	X
miners	X	X	X	X	X	
incremental throughput						X

Table 1: Comparison of consensus mechanisms

Every technique except for traditional BFT is based on a permissionless design. The consensus mechanism used in Bitcoin, PoW, is unable to provide the same transaction speed as traditional payment methods, which take around 30 seconds [1].

An alternative to PoW is PoS, which requires miners to invest in the currency instead of computational power. The absence of a computational puzzle enables an increased block interval, resulting in faster transaction times [15].

Transaction confirmation time with SCP takes just a few seconds. This is possible by the central authority's computational power, which a node trusts depending on the node's quorum slice, which is in turn accomplished by the SCP consensus protocol that uses the federated BA consensus algorithm.

Skipchains is also based on a variation of BFT, which is the same as the BA consensus algorithm SCP looked into. The central authority does all the required computational power. Besides this, a mobile device can traverse the blockchain very efficiently to confirm a transaction thanks to back- and forward signing links, where the latter is achieved by implementing CoSi next to BFT. It publicly validates statements made to make this technique permissionless. BFT on its own is already fast due to its centralized design, but as it is not permissionless, it does not fit in the recommendations of our research. Transaction confirmation time with the tangle becomes faster as the network grows. This is possible due to the fashion of how the tangle works. For every transaction that is assigned, two other transactions have to be validated.

We also need to take the efficiency into account for mobile devices, as these devices have finite power and resources.

Skipchains is efficient as there is no need to store the whole blockchain because of the efficient confirmation by traversing through the blockchain with the back- and forward signing links, the latter which is possible by implementing CoSi next to BFT. Next to this, all the computational labor is done by the the party, which is trusted using BFT, but still is permissonless as CoSi ensures that the trusted central authority has to request that all statement made are publicly validated by the forward signing links.

Efficiency is possible with SCP, because it is not the mobile device that does all the hard work, but the designated trusted party, which is trusted by the node's quorum slice. The tangle is efficient for mobile devices, if they are run as a light client instead of a full node. The computational intensive operations are delegated to the trusted third party, the full node. An example is the traversal over the tangle to determine the wallet balance. If a user does not trust a third party, the user could choose to set up a full node.

For the mining aspect, the tangle is the only method, which does not take mining into account. The entire network of participants are directly involved in the approval of transactions, instead of a smaller subset of the network being responsible for the overall consensus. Besides this, the organization cryptocurrency IOTA which makes use of the tangle, has released a fixed amount of coins. This means that it is not possible to mine more coins.

Incremental throughput of the network is only possible with the tangle. It requires every node to validate two other transactions before it can make a transaction, resulting in faster throughput when more participants join the network. This leads to a faster tangle network.

Besides looking at transaction speeds, we mentioned SPV, which originated from the original Bitcoin whitepaper. It allows clients to determine the balance of their wallet, without downloading the full blockchain.

7 Discussion and future work

This section contains relevant aspects related to the feasibility of mobile payments using cryptocurrencies, which we did not cover in this paper.

Consensus mechanisms The described consensus mechanisms in this paper are a non-exhaustive list. Other useful techniques are SegWit (Segregated Witness) [46], having masternodes, Spectre (DAG based) [47, 48] and others in the list of Bitcoin Improvement Proposals. These topics could extend our research.

Traceability In this paper we did not focus on the privacy aspect of cryptocurrencies. We do acknowledge that this is mandatory for real world application, since a user should not expose his previous spending pattern to everyone one makes a payment to.

There are multiple altcoins such as Monero that have anonymity by default [49], while others such as Dash have it as an option [50]. The danger of using anonymity as an optional feature is that it makes them non-fungible. Further research could look into techniques used to provide privacy for users.

Image The Proof-of-Work consensus model used in Bitcoin provides a mechanism for distributing new coins (instead of buying coins and making one party rich, miners earn them). However, it wastes a lot of energy, which could be an issue for green companies [1].

Some techniques used in coins have a strong image associated with it, such as demurrage used in Freicoin, which benefits the proletariat instead of the capitalist [51]. There are multiple labels cryptocurrencies can have; *how green, secure, traceable, controlled etc. is a cryptocurrency?* These inherit attributes effect the image of a cryptocurrency. Future research could classify these attributes and match them on techniques used in cryptocurrencies.

Addresses The internet is accessible through the Domain Name System (DNS). This allows for flexible mapping of human readable names to addresses that are hard to remember. Others systems use the users' email address or phone number for identifying a user.

For cryptocurrencies, this is also an issue [52]. Users change wallet addresses, which makes it difficult to transfer money or set up recurring payments. Future work could look at generic solutions to this problem, optional requirements could be the fungibility of coins and anonymity/privacy of users.

Secure storage and backup This topic is all about convenience vs. security. Cloud wallets offer users key management, in exchange for a different security model and fees [53]. When users manage their private keys on their device, backup and security (e.g. by password protecting the keys) of the keys becomes an important aspect. Before mobile cryptocurrencies become mainstream, users should know what their options are and decide if they want convenience vs. security.

Fungibility of coins The first blockchain, Bitcoin, enables everyone to see the history of a coin. This also enables the black listing of certain coins that have once been used for illegal activities [54]. For money, this is an undesirable property, however, this uniqueness can also be used for identification of smart property through the concept of 'colored coins' [55]. Future research could compare methods that enable the fungibility of coins.

[1] A green company claims to act in a way which minimizes damage to the environment.

Cloud wallet There are third parties that make it easier for users to start using cryptocurrencies. Future research could look at the security implications and usability of cloud solutions that allow the user to manage the private key.

Education In day to day life, people are facilitated by banks, which provide them knowledge about their products. For cryptocurrencies, users are expected to gather knowledge themselves. The knowledge provided by the entity that provides a cryptocurrency cannot always be trusted [56]. Just as banks educate users to not click on spam links, users should also be educated for this new financial system.

References

[1] M. Polasik, J. Górka, G. Wilczewski, J. Kunkowski, K. Przenajkowska, and N. Tetkowska, “Time efficiency of point-of-sale payment methods: Empirical results for cash, cards and mobile payments,” in *International Conference on Enterprise Information Systems.* Springer, 2012, pp. 306–320, accessed in Jan. 2018. [Online]. Available: https://www.researchgate.net/profile/Michal_Polasik/publication/228150256_Time_Efficiency_of_Point-of-Sale_Payment_Methods_Empirical_Results_for_Cash_Cards_and_Mobile_Payments/links/55c4bf2708aeca747d617ce8/Time-Efficiency-of-Point-of-Sale-Payment-Methods-Empirical-Results-for-Cash-Cards-and-Mobile-Paym
pdf

[2] D. Brandon, “The blockchain: the future of business information systems,” *International Journal of the Academic Business World*, vol. 10, no. 2, pp. 33–40, 2016.

[3] Sirinlabs. Mission. Accessed in Jan. 2018. [Online]. Available: https://sirinlabs.com

[4] R. Bohme and T. Okamoto, *Financial Cryptography and Data Security.* Mairdumont Gmbh Co Kg, 7 2015.

[5] B. Ford, “How do you know it’s on the blockchain? with a skipchain.” accessed in Jan. 2018. [Online]. Available: http://bford.github.io/2017/08/01/skipchain

[6] K. Nikitin, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, I. Khof, J. Cappos, , and B. Ford, “Chainiac: Proactive software-update transparency via collectively signed skipchains and veried builds,” accessed in Jan. 2018. [Online]. Available: https://eprint.iacr.org/2017/648.pdf

[7] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, “Performance analysis and application of mobile blockchain,” accessed in Jan. 2018. [Online]. Available: https://arxiv.org/pdf/1712.03659.pdf

[8] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008, accessed in Jan. 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] E. research, “initial coin offerings,” 2017, accessed in Jan. 2018. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf

[10] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling blockchain innovations with pegged sidechains,”

URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014, accessed in Jan. 2018. [Online]. Available: https://blockstream.com/sidechains.pdf

[11] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, "Strong federations: An interoperable blockchain solution to centralized third party risks," *arXiv preprint arXiv:1612.05491*, 2016, accessed in Jan. 2018. [Online]. Available: https://arxiv.org/pdf/1612.05491.pdf

[12] ZmnSCPxj, "Driveproof: Sidechain headers on mainchain (shm)," 2017, accessed in Jan. 2018. [Online]. Available: https://zmnscpxj.github.io/sidechain/driveproof/index.html

[13] R. Turner, "Tackling the ddos threat to banking in 2014," *White Paper of Alamai*, 2014, accessed in Jan. 2018. [Online]. Available: https://www.cio.co.uk/cmsdata/whitepapers/3594184/wp_ovum_ddos_jan14.pdf

[14] M. C. Mike Hearn, "Connection bloom filtering," accessed in Jan. 2018. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki

[15] V. Zamfir, "Introducing casper the friendly ghost," 2015, accessed in Jan. 2018. [Online]. Available: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost

[16] D. Mazires, "The stellar consensus protocol: A federated model for internet-level consensus," accessed in Jan. 2018. [Online]. Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[17] M. Swan. Blockchain consensus protocols. Accessed in Jan. 2018. [Online]. Available: https://www.slideshare.net/lablogga/blockchain-consensus-protocols

[18] M. Koller. The stellar consensus protocol: Decentralization explained. Accessed in Jan. 2018. [Online]. Available: https://itnext.io/the-stellar-consensus-protocol-decentralization-explained-338b374d0d72

[19] ——. On worldwide consensus. Accessed in Jan. 2018. [Online]. Available: https://medium.com/a-stellar-journey/on-worldwide-consensus-359e9eb3e949

[20] Stellar meetup in singapore. Accessed in Jan. 2018. [Online]. Available: https://stellarcommunity.org/t/stellar-meetup-in-singapore/1665/2

[21] How does the stellar network compare to bitcoin? Stellar Development Foundation. Accessed in Jan. 2018. [Online]. Available: https://www.stellar.org/faq/

[22] "Mobilecoin," accessed in Jan. 2018. [Online]. Available: https://www.mobilecoin.com/whitepaper-en.pdf

[23] H. Matthew. Intel sgx design objectives. Accessed in Jan. 2018. [Online]. Available: https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx

[24] N. van Saberhagen, "Cryptonote v2.0," 2013, accessed in Jan. 2018. [Online]. Available: https://cryptonote.org/whitepaper.pdf

[25] P. Jovanovic. Byzcoin: Securely scaling blockchains. Accessed in Jan. 2018. [Online]. Available: http://hackingdistributed.com/2016/08/04/byzcoin

[26] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," *Proceedings of the 25th USENIX Security Symposium*, 2016, accessed in Jan. 2018. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kokoris-kogias.pdf

[27] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 1999, accessed in Jan. 2018. [Online]. Available: http://pmg.csail.mit.edu/papers/osdi99.pdf

[28] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuill, "Simple schnorr multi-signatures with applications to bitcoin," 2018, accessed on 17 January 2018. [Online]. Available: https://eprint.iacr.org/2018/068.pdf

[29] S. Popov, "The tangle," 2017, accessed in Jan. 2018. [Online]. Available: https://iota.org/IOTA_Whitepaper.pdf

[30] S. Brooks, A. Gelman, G. L. Jones, and X.-L. Meng, *Handbook of Markov Chain Monte Carlo*. Chapman and Hall, 5 2011. [Online]. Available: http://www.mcmchandbook.net

[31] A. Jain. Iota and the double-spending problem. Accessed in Jan. 2018. [Online]. Available: https://www.commonlounge.com/discussion/24c33e56808747b0a2b7eef7b0318177

[32] Is there an eta for full decentralization? Accessed in Jan. 2018. [Online]. Available: https://www.reddit.com/r/Iota/comments/7pvbla/is_there_an_eta_for_full_decentralization

[33] K. P'ng. Is iota decentralized? Accessed in Jan. 2018. [Online]. Available: https://www.quora.com/Is-IOTA-decentralized

[34] D. Snsteb. Iota development roadmap. Accessed in Jan. 2018. [Online]. Available: https://blog.iota.org/iota-development-roadmap-74741f37ed01

[35] L. Tennant. Research on private transactions in iota. Accessed in Jan. 2018. [Online]. Available: https://blog.iota.org/research-on-private-transactions-in-iota-cd546751e2c4

[36] How does iota store transactions. Accessed in Jan. 2018. [Online]. Available: https://thecrypto.pub/t/how-does-iota-store-transactions/2172

[37] Limo. The incentive to run a full node for iota and to perform pow without monetary compensation. The Tangler. Accessed in Jan. 2018. [Online]. Available: http://www.tangleblog.com/2017/06/27/incentive-run-fullnode-iota

[38] Node scalability vs tangle scalability. Accessed in Jan. 2018. [Online]. Available: https://www.reddit.com/r/Iota/comments/7dzkg2/node_scalability_vs_tangle_scalability

[39] An introduction to iota. IOTA Support. Accessed in Jan. 2018. [Online]. Available: https://iotasupport.com/whatisiota.shtml

[40] Transaction speed. IOTA. Accessed in Jan. 2018. [Online]. Available: https://forum.iota.org/t/transaction-speed/3881

[41] J. MacAvoy. Iota: A cryptocurrency with infinite scalability and no fees. Interesting Engineering. Accessed in Jan. 2018. [Online]. Available: https://interestingengineering.com/iota-a-cryptocurrency-with-infinite-scalability-and-no-fees

[42] Everything you need to know about the iota cryptocurrency. 5to9News. Accessed in Jan. 2018. [Online]. Available: https://www.5to9news.com/everything-need-know-iota-cryptocurrency.html

[43] Transaction speed - bitcoin, visa, iota, paypal. Steem. Accessed in Jan. 2018. [Online]. Available: https://steemit.com/cryptocurrency/@steemhoops99/transaction-speed-bitcoin-visa-iota-paypal

[44] Making a transaction. IOTA. Accessed in Jan. 2018. [Online]. Available: https://iota.readme.io/docs/making-a-transaction

[45] Iota and the tangle: The future backbone of the iot. Hackernoon. Accessed in Jan. 2018. [Online]. Available: https://hackernoon.com/iota-the-tangle-the-future-backbone-of-the-iot-e7e417d5d86b

[46] P. W. Eric Lombrozo, Johnson Lau, "Segregated witness (consensus layer)," accessed in Jan. 2018. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[47] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: A fast and scalable cryptocurrency protocol." *IACR Cryptology ePrint Archive*, vol. 2016, p. 1159, 2016, accessed in Jan. 2018. [Online]. Available: https://eprint.iacr.org/2016/1159.pdf

[48] A. Zohar, "Spectre: Serialization of proof-of-work events, confirming transactions via recursive elections." accessed in Jan. 2018. [Online]. Available: https://medium.com/@avivzohar/the-spectre-protocol-7dbbebb707b5

[49] A. Kandpal. Monero - an anonymous cryptocurrency. Accessed in Jan. 2018. [Online]. Available: https://medium.com/@harrypotter0/how-does-monero-work-17f18ea37652

[50] Dash.org. (2017) Interview with ryan taylor, ceo of dash. Accessed in Jan. 2018. [Online]. Available: https://www.dash.org/2017/10/09/interviewryan.html

[51] F. Developers, "What is freicoin?" 2016, accessed in Jan. 2018. [Online]. Available: http://freico.in/about

[52] A. B. Johnson. How can digital cash become accessible to all? episode 6. DASH School. Accessed in Jan. 2018. [Online]. Available: https://youtu.be/vFwXeFk6VO8?t=47s

[53] "Bankruptcy; stolen bitcoin," accessed in Jan. 2018. [Online]. Available: https://en.wikipedia.org/wiki/Mt._Gox

[54] M. Moser, R. Bohme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *eCrime Researchers Summit (eCRS), 2013*. IEEE, 2013, pp. 1–14.

[55] M. Rosenfeld, "Overview of colored coins," *White paper, bitcoil. co. il*, p. 41, 2012, accessed in Jan. 2018.

[56] D. Patel, "6 red flags of an ico scam," 2017, accessed in Jan. 2018. [Online]. Available: https://techcrunch.com/2017/12/07/6-red-flags-of-an-ico-scam