Journal of Network and Computer Applications 149 (2020) 102471

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Sidechain technologies in blockchain networks: An examination and state-of-the-art review

Amritraj Singh [a], Kelly Click [a], Reza M. Parizi [a], Qi Zhang [b], Ali Dehghantanha [3], Kim-Kwang Raymond Choo [4,*]

[a] Department of Software Engineering and Game Development, Kennesaw State University, GA, 30060, USA
[b] IBM Thomas J. Watson Research Center, Yorktown Heights, NY, 10598, USA
[3] Cyber Science Lab, School of Computer Science, University of Guelph, Ontario, Canada
[4] Department of Information Systems and Cyber Security, University of Texas at San Antonio, Texas, USA

ARTICLE INFO

Keywords:
Blockchains
Sidechains
Smart contracts
Decentralized applications
Decentralized ledger
Digital assets
Cryptocurrency

ABSTRACT

In the last decade, blockchain has emerged as one of the most influential innovations in software architecture and technology. Ideally, blockchains are designed to be architecturally and politically decentralized, similar to the Internet. In recent times, however, blockchain-based systems have faced stumbling blocks in the form of challenges related to scalability, privacy, security, etc. Several new methods have been proposed both by the research and professional communities to mitigate these challenges. One such recent advancement proposed is the use of *sidechains*. A sidechain is a secondary blockchain connected to the main blockchain with a two-way peg. Sidechains may have their own consensus protocols, which could be completely different from the mainchain's protocol. Theoretically, a sidechain can add new functionalities, improve privacy, and security of traditionally vanilla blockchains. To this date, however, little is known or discussed regarding factors related to design choices, feasibility, limitations and other issues in adopting the sidechain technology. Moreover, there is a lack of studies discussing how and where it can effectively be integrated into blockchains to remedy current issues in a clear context. Hence, this paper provides the first comprehensive review of the state-of-the-art sidechains and platforms, identifying current advancements and analyzing their impact from various viewpoints, highlighting their limitations and discussing possible remedies for the overall improvement of the blockchain domain.

1. Introduction

Blockchains have come a long way since their initial proposal in 2008 as the backbone of Bitcoin (Nakamoto, 2008) cryptocurrency. They enable trusted transactions among several untrusted participants on a network without a need for a trusted central authority or a third party. As a result of this, blockchains are now employed in various computing and business domains such as cloud computing, supply chains, Internet of Things (IoT), finance, and many others (Miller, 2018), (Fiaidhi et al., 2018), (Zhou et al., 2018), (Mylrea and Gourisetti, 2018). Alongside its industrial counterpart, academic research in the domain is also increasing rapidly, especially in applying blockchain technology for developing decentralized solutions and applications (Yu et al., 2018), (Lou et al., 2018), (Kan et al., 2018), (Robinson, 2018), and also in recognizing its technical challenges (PariziAmritraj and Dehghantanha, 2018), (Atzei et al., 2017), (Giagliset al., 2017) by providing possible remedies including, formal verification of smart contracts (Bhargavanet al., 2016), (Amani et al., 2018), (Abdellatif and Brousmiche, 2018), scalability improvement of blockchains (Dennis et al., 2016) and defining atomic cross-chain swap protocols (Herlihy, 2018).

There are, however, a number of challenges in blockchain-based applications, especially on public and permissionless blockchains such as Ethereum (Wood, 2014), (Buterin, 2014) and Bitcoin, for example in terms of scalability (Nadiya et al., 2018), (Chauhan et al., 2018), performance (Anish Dev, 2014), privacy (Henry et al., 2018) and security (Halpin and Piekarska, 2017), (Keenan, 2017), (Kovalchuk et al., 2017). Most of the proposed solutions (Bala and Manoharan, 2018), (Ehmke et al., 2018) to address these issues require a change in protocol of these public blockchains, which is extremely difficult to implement due to their decentralized nature. A change in protocol needs to be agreed upon by all

* Corresponding author.
E-mail addresses: amritra@students.kennesaw.edu (A. Singh), kclick@students.kennesaw.edu (K. Click), rparizi1@kennesaw.edu (R.M. Parizi), q.zhang@ibm.com (Q. Zhang), adehghan@uoguelph.ca (A. Dehghantanha), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.jnca.2019.102471
Received 17 February 2019; Received in revised form 10 July 2019; Accepted 20 October 2019
Available online 24 October 2019
1084-8045/

the peers on the blockchain network, otherwise it may result in a hard-fork, which may ultimately reduce its value. This makes it extremely difficult to test changes to a pre-existing blockchain protocol or to add new functionality to it. Additionally, there has been a huge surge in blockchain-based systems in recent years, for instance Bitcoin primarily supports peer-to-peer payment network, Ethereum is used for the deployment of decentralized applications and Hyperledger Fabric (Androulakiet al., 2018) is used for the enhancement of supply-chains.[1] Thus, it is hard to envision a single blockchain 'to rule them all' for the future. It would be more worthwhile instead to make these disparate blockchains interoperable, so that they can communicate and interact with one another.

In 2014, realizing this hindrance in the growth and further adoption of blockchains for building advanced, complicated and scalable software systems, Back et al. (Backet al., 2014) proposed a new and innovative method for improving the versatility and interoperability of traditional blockchains. In their paper, they proposed the idea of "sidechains" for the Bitcoin blockchain.

Sidechains are secondary blockchains which are connected to other blockchains by means of a two-way peg. A two-way peg is a mechanism that allows bidirectional transfer of assets between the mainchain and the sidechain at a fixed or pre-deterministic exchange rate. Sidechains may have their own protocol and implementation, which can be completely different from the main blockchain. Such adjustability provides the users flexibility to access various other functionalities and features offered on a sidechain by using the assets they already own on the main blockchain. Furthermore, sidechains are isolated from the main blockchain in such a way that in the case of a cryptographic break (or a maliciously designed sidechain), the damage is entirely confined to the sidechain itself.

Although promising, the sidechain technology is still relatively new and immature. There is a lack of comparative and empirical studies both in academic and industrial environments to analyze such multi-blockchain systems in a comprehensive manner. Hence, the motivation of this research is to provide the first comprehensive review of the state-of-the-art sidechain platforms (which represent the most commonly used implementations of sidechain technology - hereafter referred to as sidechains) to understand the design choices, advancements, use cases, and limitations of sidechains. The specific contributions of this research are as follows:

- Analyze the most common two-way peg design choices for sidechain technologies by highlighting their advantages and disadvantages (Section 2).
- Provide a comprehensive review of current state-of-the-art sidechain platforms based on their technical use cases, consensus mechanisms, asset transfer protocols and limitations with horizontal comparison (Section 3).
- Identify open issues and discuss possible solutions to mitigate those issues with state-of-the-art sidechain platforms (Section 4).

The rest of this paper is structured as follows: Section 2 provides an overview of sidechain design and implementation based on an example usage. Section 3 introduces and discusses state-of-the-art sidechain platforms based on their use cases, consensus mechanism, asset transfer protocol and limitation. We also discuss some of new and upcoming sidechain projects and scalable frameworks proposed in the community. Section 4 highlights general open issues with these sidechain platforms and discusses possible ways to tackle such issues. Finally, Section 5 provides a conclusion of our work.

[1] https://cointelegraph.com/news/walmart-ibm-blockchain-initiative-aims-to-track-global-food-supply-chain.

2. Two-way peg implementation and design choices

In this section, we demonstrate the core working of a two-way peg based on an example described below (Section 2.1). We then visualize and analyze current design choices for implementing two-way pegs for asset portability in sidechain technologies (Section 2.2).

2.1. How does a two-way peg work?

To understand the fundamentals and design choices for implementing a two-way peg enabled sidechain, we will discuss a trivial example in this section. Let us assume a sidechain is attached to a public and permisionless primary blockchain with a two-way peg. The primary blockchain: 1) operates a cryptocurrency called *MainCoin* and 2) cannot execute non-trivial smart contracts due to the absence of a Turing complete Virtual Machine. The sidechain: 1) operates its own cryptocurrency of named *SideCoin*, 2) has the capability of executing non-trivial smart contracts and 3) offers significantly higher transaction rate (i.e. higher transactions per second) than the mainchain. For the sake of simplicity in such multi-blockchain environment, the primary blockchain is called the *parent blockchain (or mainchain)* and the sidechain attached to it is called a *secondary chain* (the terms sidechain and secondary chains will be used interchangeably throughout the rest of this paper). In our example, a two-way peg allows the transfer of *MainCoins* from the mainchain to the sidechain and vice versa at a fixed rate of 1 *MainCoin* = 1 *SideCoin*. Suppose a user wishes to transfer 5 *MainCoins* from the mainchain to the sidechain to play a rock, paper and scissor game with another random user based on a smart contract (where winner takes all and a draw results in no exchange of coins) implemented on the sidechain, then this system could work in the following abstract manner:

1. The user sends 5 *MainCoins* to a special address (also known as a lock-box) where the coins are locked and can only be unlocked once funds on sidechain are locked and transferred back to the mainchain.
2. Once the funds locked on the mainchain, 5 *SideCoins* are created on the sidechain.
3. The user can now use these *SideCoins* to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of *SideCoins*.
4. Depending on the outcome of the game, 10 *SideCoins* are transferred to the winner or 5 *SideCoins* are transferred back to their respective owners (in case of a draw).
5. The user(s) can then transfer their funds back to the mainchain, which essentially means that the *SideCoins* will be locked/destroyed on the sidechain and an equivalent number of *MainCoins* will be unlocked on the mainchain from the lock-box (in step 1) after *SideCoins* are destroyed on the sidechain.

The above steps are summarized in Fig. 1 and can vary depending on the way in which a two-way peg has been implemented for the sidechain (Section 2.2). With this model the total number of *MainCoins* in the mainchain ecosystem remains conserved whilst adding new functionality to it, i.e. execution of non-trivial smart contracts and faster transaction rates. Moreover, the implementation of these new features with sidechains do not require any major change in the core features or consensus protocol of the mainchain itself.

2.2. Two-way peg design choices for sidechains

Based on our analysis, currently there exist three major design choices for implementing a two-way peg for transferring assets from the mainchain to the sidechain and vice versa. These design choices are discussed below.

2.2.1. Centralized two-way pegs

The simplest way to implement a two-way peg is to have a trusted

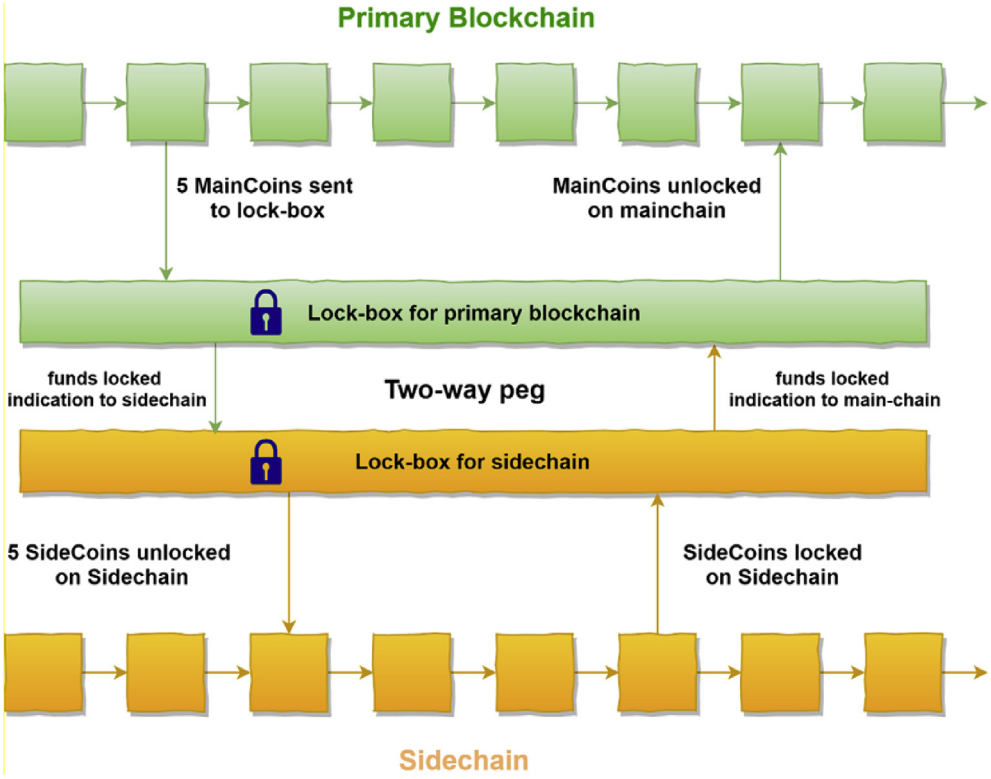

Fig. 1. Transfer of funds between mainchain and sidechain with a two-way peg.

third entity hold custody of the locked funds. In this design, the trusted entity is solely responsible for locking and unlocking of funds on both the mainchain and its sidechain. Fig. 2 shows the relevant steps in which the entire process of fund transfer takes place, both from the mainchain to the sidechain and vice versa.

Based on this two-way peg design, the steps for fund transfer (based on our example in Section 2.1) are modified in the following manner:

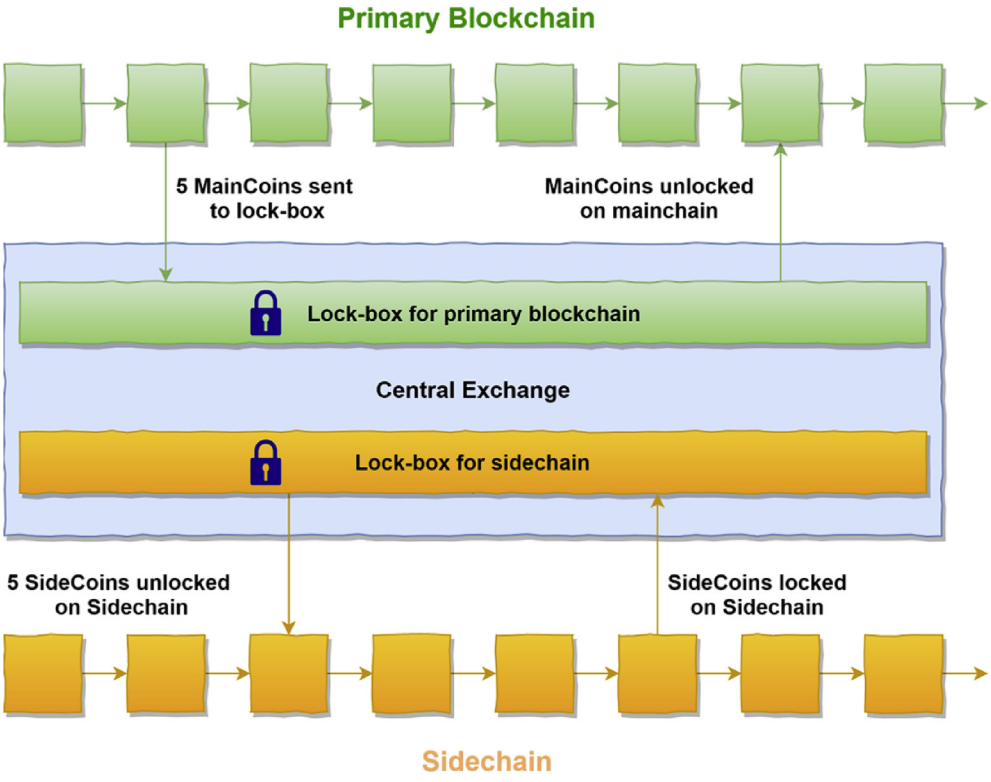

Fig. 2. Centralized two-way peg implementation.

1. The user sends 5 *MainCoins* to a lock-box address maintained by a *trusted centralized entity* meant for regulating fund transfer between the two blockchains.
2. The trusted entity then generates 5 *SideCoins* on the sidechain and sends these funds to the user's requested address.
3. The user can now use these *SideCoins* to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of *SideCoins*.
4. Depending on the outcome of the game, 10 *SideCoins* are transferred to the winner or 5 *SideCoins* are transferred back to their respective owners (in case of a draw).
5. The user(s) can then transfer their funds back to the mainchain, by sending their *SideCoins* to the lock-box address on the sidechain which is also maintained by the same *trusted central entity*. The user(s) also specify the address where the funds need to be sent on the mainchain.
6. The trusted central entity destroys the *SideCoins* on the sidechain and sends the equivalent number of *MainCoins* to address specified by the user(s).

Advantages of centralized two-way pegs: There are two major advantages of using a centralized two-way peg design: 1) Centralized two-way pegs are easy to visualize and implement due to their simplistic design which involves just one entity to oversee the transfer of assets between blockchains. 2) the design could provide extremely fast transfer of funds from the parent blockchain to its sidechain and vice versa as the central entity generally requires a simple proof of locked funds in the lockbox, which they can verify themselves at any given time.

Disadvantages of centralized two-way pegs: Using a trusted central entity comes with its own drawbacks, such as: 1) Public blockchains such as Bitcoin and Ethereum are designed to improve political decentralization and using such a two-way peg design introduces a degree of political centralization as one has to trust a single entity to manage fund transfer from a primary blockchain to a sidechain and vice versa. 2) Using a centralized two-way peg design introduces a single point of failure in such multi-blockchain ecosystems as unforeseen circumstances such as power failures, hardware failures or natural disasters would temporarily or permanently cease asset transfers between the blockchains, which would cripple the sidechain network and 3) If the centralized entity is rogue or malicious, it can steal all the funds stored in the lock-box.

2.2.2. *Multi-signature or federated two-way pegs*

An improvement over centralized two-way pegs are the federated two-way pegs (Backet al., 2014), (Dilley et al., 2016). In such a design, a group of entities or notaries control the lock-box rather than just one central entity. Consequently, the entire federation or group collectively holds custody of the locked funds and regulates fund transfer between the primary blockchain and its sidechain. The fund transfer takes place only when the majority of the entities i.e. 'n' out of 'm' entities (where 'n' is the majority and 'm' is the total number of entities in the federation) within the federation sign the transaction (Deng et al., 2018). Fig. 3 demonstrates the sequential steps with which fund transfer takes place between the two blockchains using a federated two-way peg.

Based on a federated two-way peg design, the steps for fund transfer (based on our example in Section 2.1) are modified as follows:

1. The user sends 5 *MainCoins* to a lock-box address maintained by a *federation of entities* meant for regulating fund transfer between the two blockchains. The entities of the federation then sign this transaction after verifying that the funds have been received in the lock-box.
2. If the majority of the entities within the federation sign the transaction, then the federation generates 5 *SideCoins* on the sidechain and sends these funds to the user's requested address.
3. The user can now use these *SideCoins* to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of *SideCoins*.
4. Depending on the outcome of the game, 10 *SideCoins* are transferred to the winner or 5 *SideCoins* are transferred back to their respective owners (in case of a draw).
5. The user(s) can then transfer their funds back to the mainchain, by sending their *SideCoins* to the lock-box address on the sidechain which is also maintained by the same *federation of entities*. The user(s) also specify the address where the funds need to be sent on the mainchain.
6. The entities of the federation again sign the transaction after verifying that the funds have been received in the lock-box on the sidechain.

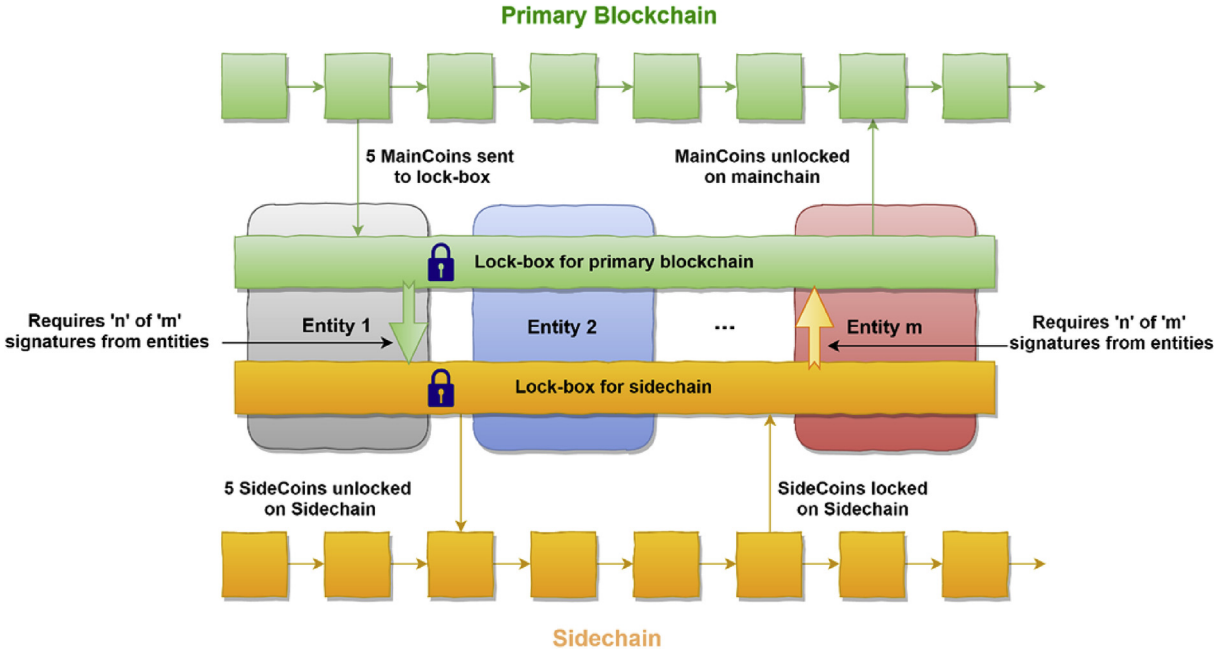

Fig. 3. Federated two-way peg implementation.

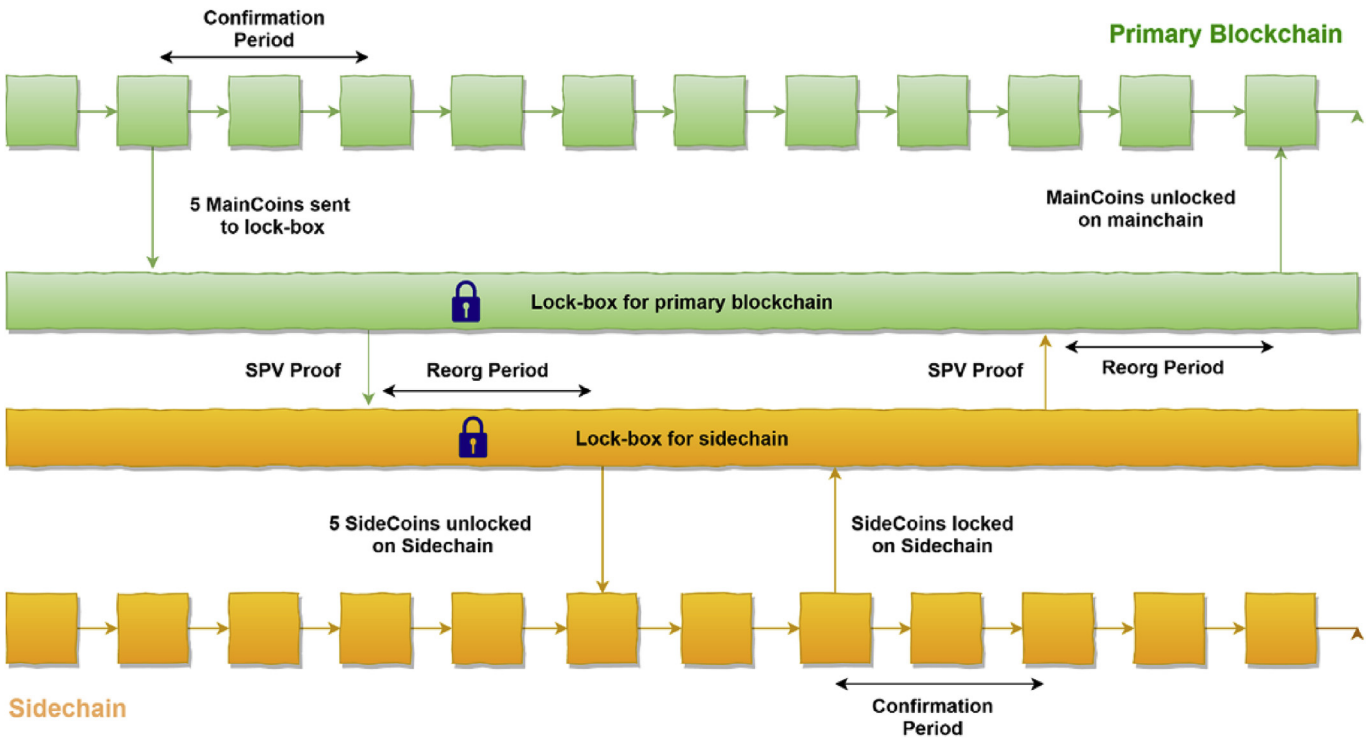

Fig. 4. Two-way peg based on SPV proofs.

7. If the majority of the entities sign the transaction, then the federation destroys the *SideCoins* on the sidechain and sends the equivalent number of *MainCoins* to address specified by the user(s).
8. In the case when the majority of the entities within the federation do not reach an agreement regarding a transaction, then the funds are sent back to their respective owners on either chain.

Advantages of federated two-way pegs: The advantages of using a federated two-way peg design are: 1) It improves upon centralized two-way peg design by improving the political decentralization of such multi-blockchain systems to some extent and 2) These designs could be implemented with specialized federation protocols for fast transfer of funds between the blockchains. Some of these protocols are *Strong Federations* (Dilley et al., 2016) (which is discussed further in Section 3.3 B).

Disadvantages of federated two-way pegs: Federated two-way pegs can have drawbacks such as: 1) Such design does not entirely eliminate the political centralization problem as this design still relies on a small group of entities to regulate and manage fund transfer between blockchains and 2) Funds in the lock-box could be stolen if the majority of the entities of a federation lose their private keys due to a malicious internet attack or social engineering.

2.2.3. Simplified Payment Verification

Simplified Payment Verification (SPV) allows a lightweight[2] client to prove that a given transaction was included in a legitimate block of the longest Proof-of-Work (PoW) blockchain, without having to download the entire chain from the genesis block itself. These lightweight (or SPV) clients are only required to download the block headers of the entire blockchain, which are much smaller in size than the actual block itself. To verify if a given transaction was included in a legitimate block, an SPV client requests a proof of inclusion, in the form of a Merkle branch of that transaction. Fig. 4 demonstrates the entire process of transfer of funds from the mainchain to the sidechain and vice versa based on two-way peg implemented with SPV proofs.

SPV proofs indirect proofs in the sense that a given transaction is not proven to be consistent with the entire blockchain from the genesis block itself. Instead it is shown to be a part of valid block upon which miners have mined newer blocks, subsequently forming the longest chain. The way in which this is done is as follows:

1. After a transaction is submitted for the transfer of funds from the mainchain to the sidechain or vice versa (i.e. the funds are locked in the lockbox), there is a confirmation period, which is strategically in place to allow miners to mine on top of the last block which consequently, allows the generation and submission of SPV proof.
2. The SPV proof is then submitted by the user and the block in which the his/her transaction is recorded is located.
3. The user then provides the hashes along the Merkle tree branch on which his/her transaction lies. This is done in the following manner:
   a. Suppose a user is looking to validate Transaction 2 (Fig. 5), he/she can obtain the hash of Transaction 1 and a combined hash of Transaction 3 and 4 i.e. Transaction (3, 4) from a number of other full nodes.
   b. With this information the user can compute the root hash of the Merkle tree in the block.
4. If these hashes all collectively hash to the original Merkle root of the transaction hash tree in that block, then the transaction is valid.

After an SPV proof is submitted there is a reorganization or reorg period in which other users may submit their own SPV proofs to contradict the user's transaction. The SPV proof in which more blocks have been mined is considered to be the correct proof and decides the fate of the transaction.

Given an SPV based two-way peg design, the steps for fund transfer (based on our example in Section 2.1) are modified as follows:

1. The user sends 5 *MainCoins* to a lock-box address which is usually maintained by the miners of the network. Once the coins are locked on the mainchain, the user has to wait for a predetermined

[2] https://www.mycryptopedia.com/full-node-lightweight-node/.

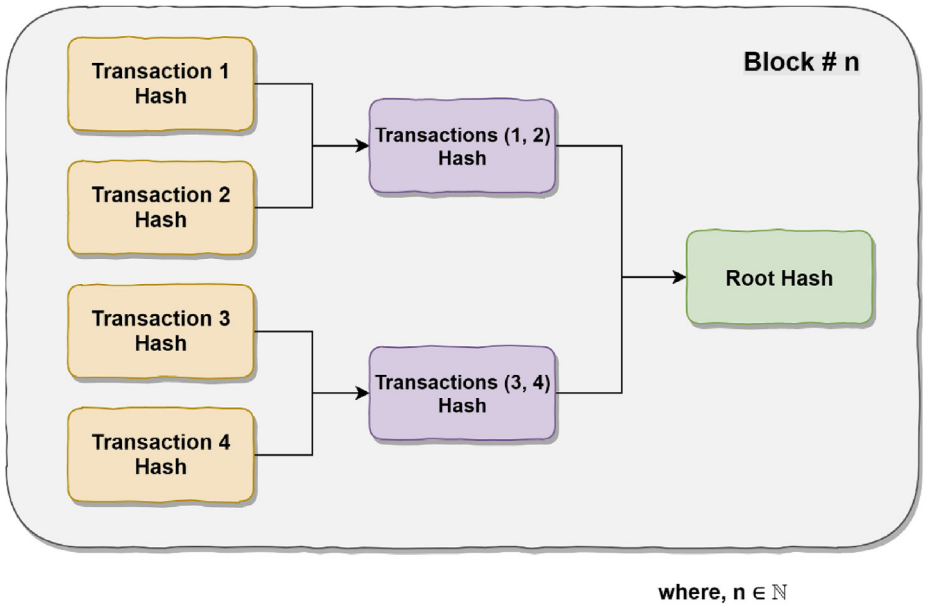

Fig. 5. A block of transaction hash Merkle tree.

confirmation period to allow the mines to create new blocks to create SPV proofs.
2. Once sufficient blocks are created by the miners, the user can submit an SPV proof verifying that the coins were locked on the mainchain.
3. After the SPV proof is submitted, the user has to wait for the reorg-period where other users can submit their SPV proofs to nullify a fraudulent transactions, in case one has taken place.
4. After the SPV proof is verified 5 SideCoins are unlocked on the sidechain.
5. The user can now use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of *SideCoins*.
6. Depending on the outcome of the game, 10 *SideCoins* are transferred to the winner or 5 *SideCoins* are transferred back to their respective owners (in case of a draw).
7. The user(s) can then transfer their funds back to the mainchain, by sending their *SideCoins* to the lock-box address on the sidechain and repeating the same process mentioned in steps 1–4 on the sidechain side.

Advantages of SPV based two-way pegs: The main advantage of an SPV based two-way peg is that it eliminates the third party required for fund transfer between two blockchains as in case of Centralized and Federated two-way pegs.

Disadvantages of SPV based two-way pegs: A disadvantage of an SPV based design is that, these designs tend to be slow as a user needs to wait for confirmation and reorg periods before having access to his/her funds on either mainchain or sidechain.

Table 1 summarizes the Centralized, Federated and SPV based two-way peg designs based on their advantages and disadvantages.

Table 1
Summary of advantages and disadvantages of two-way peg designs.

Two-way peg Design	Advantages	Disadvantages
Centralized	• Asset transfer between blockchains can be fast • Simple design and implementation	• Politically centralized • Introduces single point of failure • assets can be stolen by a malicious central entity
Federated	• Better political decentralization than centralized two-way pegs • Asset transfer between blockchains can be fast • Can work well with the right number and type of entities that form the federation (Section 4)	• Not politically decentralized • Assets can be stolen if private keys of majority of entities are stolen
SPV	• Politically decentralized	• Slow transfer of assets between blockchains

3. State-of-the-art sidechain platforms

In this section we introduce and review four major state-of-the-art sidechain platforms namely, Loom (2019a), (Loom, 2019b), Proof-of-Authority (POA) Network (Arasev, 2018), (POA, 2019a), Liquid (Dilley et al., 2016), (Blockstream, 2019) and RootStock (RSK) (Lerner, 2015), (RSK, 2019) that facilitate interoperability in multi-blockchain ecosystem. For each platform, we discuss its use cases, consensus mechanisms, asset transfer protocol and limitations. We chose these platforms based on the following reasons:

- Popularity in the community and users: The popularity of a platform was determined by either one or both of the following criteria: 1) the number of users that are registered on the platform (e.g. CryptoZombies[3] a DApp on Loom has accumulated over 240,000 users since going live (Bentley, 2018)), marking its wide usage, and 2) partnership of the sidechain platform with prominent or well-known blockchain companies or organizations (e.g. bitpay[4] and BITMAIN[5]) (POA, 2019b), (RootStock, 2019), (O'KeeffeDaniel, 2018), indicating its wider adoption.
- Availability of documentations, white papers, forums and technical support (Loom, 2019a), (Dilley et al., 2016), (Lerner, 2015), (POA, 2019c), (Arasev, 2018).

3.1. Loom

Loom (2019a), (Loom, 2019b) is a platform for running Decentralized Applications (DApps) and games on sidechains connected to the Ethereum Blockchain. It utilizes the Delegated Proof-of-Stake (DPoS) protocol

[3] https://cryptozombies.io/.
[4] https://bitpay.com/.
[5] https://www.bitmain.com/.

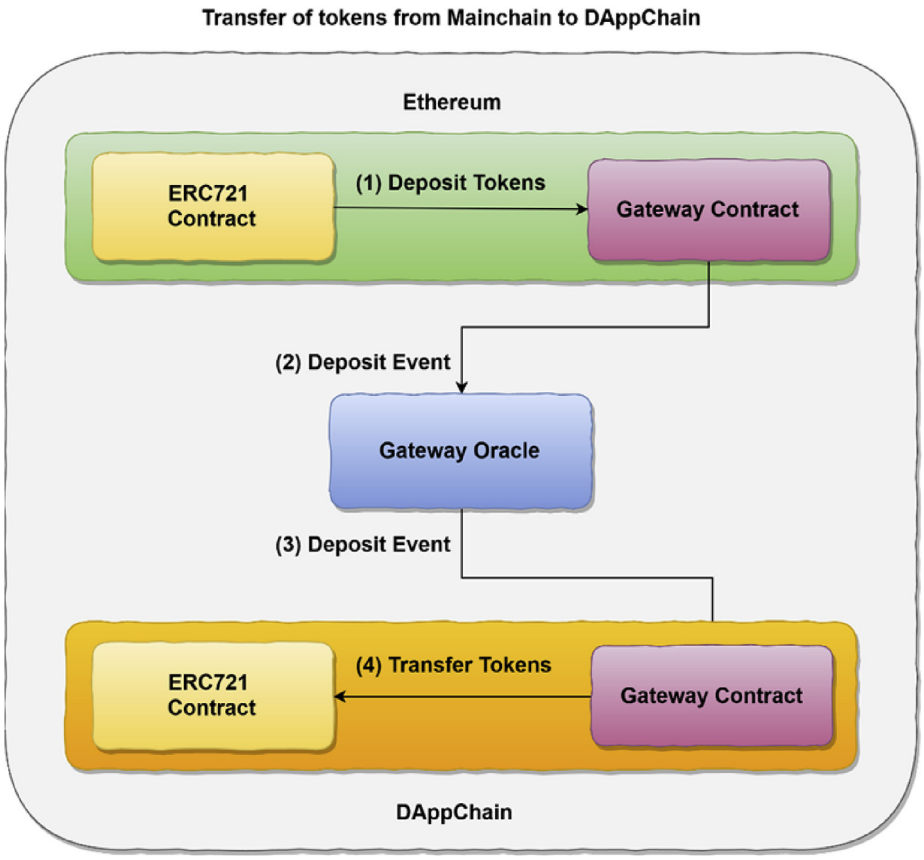

Fig. 6. Asset transfer from Ethereum to DAppChain.

to reach consensus. Each DApp runs on its own sidechain (called a DAppChain) pegged to the Ethereum main-net. This allows the users and developers to run multiple nodes for an application on the sidechain. Along with the Delegated Proof-of-Stake consensus, Loom runs on a Byzantine-fault tolerant state machine replication as a backend P2P layer called Tendermint.[6] In the Loom architecture, a transaction on the Loom network is not immediately settled on the Ethereum mainchain but instead, they are settled in bulk in order to increase scalability.

3.1.1. Use cases

The Loom network has mainly been used for the following use cases:

- **Digital Social Interaction:** The original use case of the Loom Network is DelegateCall[7] which is a forum where questions can be asked and each answer that a user provides and upvotes earns them 'Karma'. Karma can be traded on the Ethereum chain for ERC-20 tokens. ERC-20 tokens are fungible tokens, or coins, on the Ethereum Network which are not unique and can be divided into smaller portions.
- **Game development:** The second use case for the Loom Network is for running games such as games built on Unity.[8] Games require quick transaction times and the performance off the mainchain is much faster than it would be if the games were run on the Ethereum blockchain itself. The gas fees required for transaction on the Loom sidechain are much less than on the Ethereum chain making it more practical for game development. One of the most played games developed on the Loom platforms is Relentless,[9] which is a fast-paced strategic card trading game available both on mobile and desktop.

3.1.2. Consensus mechanism

Loom allows for any consensus mechanism to be implemented on a personalized DApp chain, although the Loom SDK provides support for DPoS on a shared sidechain. In Delegated Proof of Stake, witnesses are elected who propose blocks and verify transactions. These witnesses serve a fixed term before elections take place again. Each voter is required to register with the account's public address and the power of each vote is proportional to the number of tokens that account holds. Accounts are permitted in DPoS to proxy their votes to trusted third parties who votes with power proportional to proxy balance + sum (balance of principals).

3.1.3. Asset transfers

The Loom network has plans to allow for ERC721 and ERC20 tokens to be transferred from the Ethereum blockchain to the DAppChain and vice-versa using Plasma-based relays[10]. At the moment, Loom only allows for ERC721 tokens to be traded on the network. ERC721 tokens are non-fungible tokens meaning that they can be collected, and each individual token is unique and irreplaceable. Currently Loom uses a Transfer Gateway to support the transfer of these tokens. When the tokens are being deposited to the DAppChain, the tokens are sent to a gateway contract before being sent to the Gateway Oracle where the transfer is forwarded to the Gateway Contract on the DAppChain. Fig. 6 shows the asset transfer from the Ethereum blockchain to the DAppChain.

The Gateway Oracle typically runs on nodes that are serving as delegators for the Delegated Proof of Stake consensus algorithms although a

[6] https://tendermint.com/.
[7] https://delegatecall.com/.
[8] https://unity3d.com/.
[9] https://loom.games/en/.
[10] https://blog.gridplus.io/introducing-trusted-relay-networks-6c168f72a6f6.

gateway oracle can run on nodes that are standalone. If the tokens are being withdrawn from the DAppChain back to the Ethereum mainchain, the tokens are sent back to the Transfer Gateway Oracle where the user submits a Merkle proof of the user's transaction history and the withdrawal awaits a signature of approval. With this signed withdrawal record, the user may withdraw tokens back to the Ethereum mainchain. Fig. 7 shows the asset transfer from the DAppChain to the Ethereum blockchain.

The mainchain gateway contract needs to approve of the signature produced by the Gateway Oracle. When a user initially deposits tokens to the DAppChain from the mainchain, an address mapper contract creates a mapping of both the private key for Ethereum and the private key for the DAppChain. The reason that a signature is not required for depositing to the sidechain but is required for withdrawing back to the mainchain is that the signature is used to decrease the dependence on the personalized consensus algorithm being used on the sidechain when in need of transferring. The Ethereum mainchain, on the other hand, has a more trusted consensus algorithm.

3.1.4. Limitations

Some of the limitations of the Loom network are as follows:

- The entire transaction history of the sidechain is stored on the Ethereum mainchain instead of the sidechain itself decreasing the data integrity of the sidechain. The Merkle roots of the entire transaction history of the sidechain is periodically updated on the mainchain leaving open opportunities for attack in between updates of the sidechain's transaction history (Bharel, 2019).
- To further increase the reliability on the mainchain, the security guarantees of the Loom network hinge on the ability to transfer tokens back to the mainchain. If the tokens are not approved for transfer back to the mainchain, the tokens can be at risk of being compromised. Loom's security is based on the mainchain being the target of an attack and not the sidechain a game is running on. There is more incentive in putting forth the resources to take over the Ethereum mainchain then a DApp supporting a decentralized game. Loom uses Plasma to securely transfer tokens back to the mainchain without needing to trust the consensus algorithm on the sidechain. In a plasma exit, this is where a Merkle proof needs to be presented and can be challenged and the exit can fail.
- Another limitation of the Loom network is being restricted to OS X and Linux operating systems. The closest support for Windows is the Windows subsystem for Linux. Also, Loom's transfer gateway functionality can hurt the performance of the transfer of tokens between the two blockchains. The transfer gateway depends on an active presence on the Loom network and if there is not one, the transfer of tokens will be delayed.
- Loom network is based on federated two-way pegs, which introduce centralization in its blockchain-sidechain ecosystem as discussed in Section 2.2.

3.2. POA network

The POA network (Arasev, 2018), (POA, 2019a) is an open-source public Ethereum sidechain for developing smart contracts. It uses Proof of Authority (POA, 2017) as its consensus protocol. The platform provides the users and developers of smart contracts and decentralized applications with the flexibility to develop on Ethereum standards with more scalability and interoperability between other blockchain networks.

POA network supports native Solidity ("Solidity." [Online]) smart contracts, which allows effortless portability of smart contracts and decentralized applications from the Ethereum environment to the POA network. The platform charges minimal transaction fees which combined

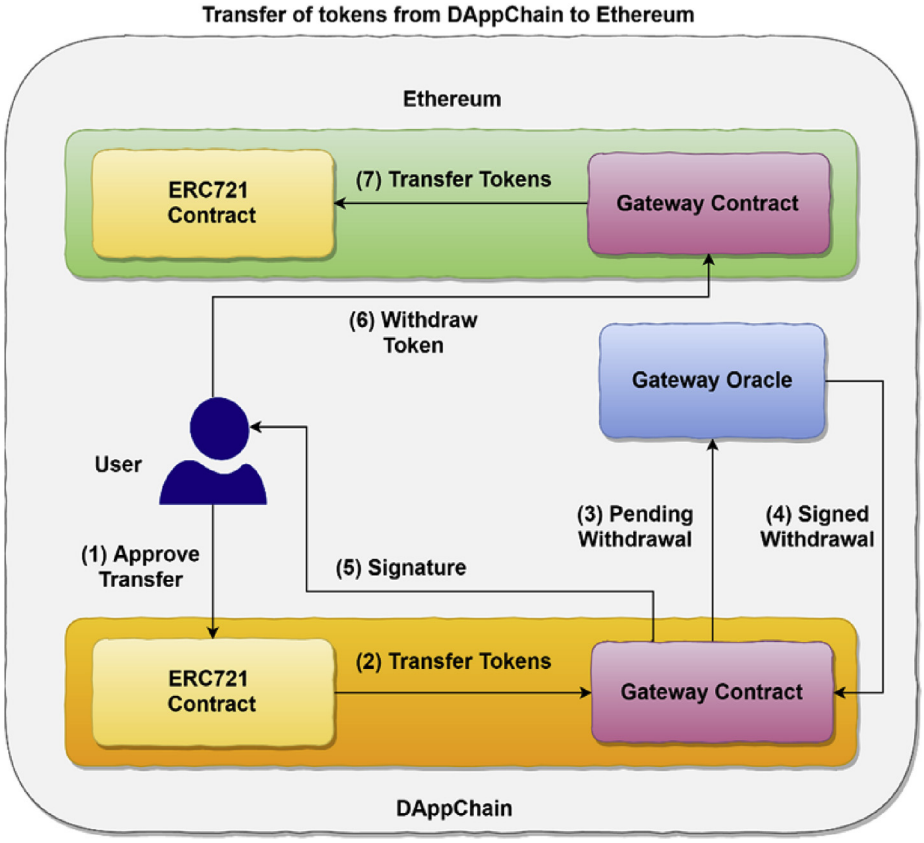

Fig. 7. Asset transfer from Ethereum to DAppChain.

with about four magnitudes in transaction speed over Ethereum encourages and promotes the development of scalable games and applications. Additionally, POA provides bridging (especially for ERC-721 tokens) capabilities which allows users to transfer their non-fungible tokens from one blockchains to another easily.

3.2.1. Use cases

The purpose of the POA network is to prove the possibility of cross-chain transfers between an Ethereum chain and a sidechain. Interoperability is a major goal of the POA Network along with an increase in scalability and the connectivity of Ethereum. POA aims to have a solution to communicating between two stand-alone blockchains. Some of the major projects that have used the POA network as of November 2018 are as follows:

- Swarm City,[11] a decentralized commerce platform, has used the ERC20 to ERC20 bridge to transfer tokens from the Ethereum chain to Kovan test-net[12]
- Sentinel Chain (Lai, 2018) is transferring ERC20 tokens from the Sentinel Chain to other EVM-based blockchains.
- Virtue Poker[13] has used the POA bridge along with their own sidechain to eliminate expensive transactions.
- Colu Network[14] has partnered with the POA network to connect their own sidechain.
- POA network is additionally working with more projects to help deal with the scalability and high gas cost of the Ethereum network.

3.2.2. Consensus mechanism

The POA network takes advantage of Proof of Authority consensus mechanism. The validators make all of the governance decisions through exclusive Distributed Applications. US public notaries serve as the validators on the network. The validators must be publicly known individuals whose participation can be easily reviewed adding a layer known as an Identity at Stake model.[15] The POA network rewards validators based on the amount staked. Currently, there are a total of 23 validators throughout the United States.

3.2.3. Asset transfers

There are three different types of transfers that can take place.

- **Native to ERC20:** In this case "Native" refers to the POA tokens. POA tokens are locked in a smart contract and POA20 tokens are then generated on the Ethereum blockchain. The POA20 tokens are the POA equivalent of the ERC20 tokens that are found on the Ethereum blockchain. These tokens are burned on the Ethereum blockchain before the smart contract is activated and the tokens are unlocked on the POA blockchain.
- **ERC20 to ERC20:** Token "X" from the first Ethereum network is locked on the first Ethereum Network. Token "Y" is generated on the second Ethereum network and then burned on the second network. The smart contract is activated, and the Token "X" is unlocked on the primary Ethereum network. The difference between this bridge and the first Native to ERC20 bridge is instead of the bridge only supporting the transfer of tokens to and from the POA network this bridge allows for the transfer of tokens between any two networks operating on the Ethereum chain.
- **ERC20 to Native:** The ERC-20 to Native bridge allows for the transfer of DAI tokens from the Ethereum Network to the xDAI chain. The DAI token is an ERC-20 token that maintains a 1:1 ratio with the United States Dollar (USD) meaning that each DAI token is always worth exactly one US dollar. The xDAI chain is an Ethereum based blockchain using the USD-stable XDAI token. DAI tokens differ from XDAI tokens by the fact that DAI tokens live on the Ethereum mainchain whereas the XDAI tokens live on a separate xDAI sidechain. It also maintains a ratio of 1:1 with the US Dollar and is backed by Ethereum collateral. XDAI tokens are minted on the xDAI chain network and burned on the xDAI chain network. The Smart Contract is activated, and the DAI tokens are unlocked on the Ethereum network. A subset of the total number of validators function as validators for each set of bridge transactions. Also, each bridge is bilateral allowing for a transfer back and forth between two blockchains. The transfers happen within one's own wallet by having representations of tokens on one network be minted on the other network.

3.2.4. Limitations

Some of the limitations of the POA network are as follows:

- POA network suffers from the problem of centralization due to the power that the 23 validators hold. The governance of the network is entirely determined by these validators. These validators reside solely in the United States and are public notaries of the United States. They are chosen by individual qualities such as public reputation, personal knowledge and experience. They also need to be diverse geographically within the United States, so validators come from different states. One of the restrictions on adding to the number of validators is finding potential validators that meet the needed qualifications.
- Since all the validators of the POA network are based in the United States, this introduces geographical centralization element in the network. This type of model is undesirable as the validators may choose to censor information from other regions or countries.
- The POA Network plans on an increase in validators but there is worry that an increase in the number of validators will impede the performance of the network as it would take longer time for block-signatures and hence, transaction confirmations.

Table 2 provides a comparison of Ethereum, Loom network and the POA network based on average block confirmation time, transaction rate, smart contract execution capability, security guarantee and if the transactions are confidential.

As it can be seen form Table 2, the similarities between the mainchain i.e. Ethereum and its sidechain are that all the platform support smart contract execution and none of them support private transactions. The table also shows that the loom network has the fastest block confirmation times and supprts high rate of transactions.

Table 2
Comparison of Ethereum, Loom and the POA network.

Features	Ethereum[a] (mainchain)	Loom[b] (sidechain)	POA network[c] (sidechain)
Average block confirmation time	~15 s	~1 s	~5 s
Transactions rate	~15 transactions/sec	≫ 1 transaction/sec	~60 transaction/sec
Turing complete Smart contract execution	Yes	Yes	Yes
Security guarantee	Staking	Validators + Voters	Validators
Confidential transactions	No	No	No

~ means approximately, ≫ means much greater than.

[a] https://etherscan.io/.
[b] https://blockexplorer.loomx.io.
[c] https://blockscout.com/poa/core/.

[11] https://swarm.city/.
[12] https://kovan-testnet.github.io/website/.
[13] https://virtue.poker/.
[14] https://cln.network/.
[15] https://blockonomi.com/proof-of-authority/.

3.3. Liquid

Liquid (Dilley et al., 2016), (Blockstream, 2019) is a commercial sidechain by Blockstream. It enables instantaneous movement of funds between exchanges, without waiting for the delay of confirmation in the Bitcoin blockchain. The transaction on the Liquid platform are completed in an average of 2 min. Liquid supports private transactions which allows traders and exchanges to trade/transact in private, preventing front-running of large orders.

Liquid also supports Issued assets where an organization or a company that serves as the custodian of assets (physical or cryptocurrency), can issue a tokenized version of the asset using the platform. Once the assets are tokenized on the Liquid platform, they can be traded freely within the network, taking advantage of Liquid's speed and private trading features. The Liquid Network consists of a '*Strong Federation*' (Dilley et al., 2016) (discussed Section 3.3 B) which consists of several financial institutions and cryptocurrency exchanges who all run high-performance computing hardware to secure the network.

3.3.1. Use cases

Since, strong federations were designed to provide solutions to problems related to transaction latency, commercial privacy, reliability and fungibility, the most prominent use case of the Liquid platform is in international exchange:

- **International Exchange:** Bitcoin can facilitate cross border payments and remittance, but it is limited by its own design choice that hampers its performance (Karame et al., 2012). It also suffers the wrath of market-dynamics like most if not all cryptocurrencies at this time. Consequently, the high latency of Bitcoin network requires Bitcoin to be tied up in multiple exchange and brokerage environments. The lack of privacy also adds to its cost of operation. Additionally, local currency trade with Bitcoin can be a subject to illiquidity due to market fragmentation because of which many organizations and commercial entities choose to operate or design their own high frequency methods of exchange (Moore and Christin, 2013). These solutions and workarounds have often introduced in centralized systems and other issues (Karame et al., 2012). Thus, with strong federations, Liquid, introduces improved security and privacy, with lower latency than the Bitcoin network (Dilley et al., 2016).

3.3.2. Consensus mechanism

Dilley et al. (2016) recognized both, the latency issues with using a Proof-of-work consensus mechanism and using a centralized system. Inspired by that, the authors decided to implement Liquid in a manner that would allow users to transfer assets between blockchains by providing explicit Proof-of-Possession (PoP) within transactions. Building up on the idea of federated two-way peg design introduced by Back et al. (Backet al., 2014), the authors have introduced the concept of Strong Federations (Dilley et al., 2016). Strong Federations are made up of two types of independent entities, namely:

- **Block-signers:** maintain the blockchain consensus and to advance the sidechain. They sign transaction blocks on the sidechain.
- **Watchmen:** are responsible transferring assets from the sidechain to the mainchain by signing transactions on the mainchain. Thus, they are only required to be online when assets are beings transferred between the blockchain.

In a Strong Federation, entities that form the federation cannot directly control a user's assets on the system other than their own. In such systems, just the knowledge of a private key is enough to practice the *right to spend* and hence, no intervention of a third party is required. Strong federations also have a mechanism that allows settlements to be transferred back to the mainchain in case of a federation failure.

Liquid replaces dynamic miner (such as in Bitcoin) with a fixed signer set for a federation to have low latency and eliminate the risk of reorganization from a given hostile minority. It implements a validation of a script (which can be static or can change subject to fixed rules) instead of a Proof-of-Work consensus protocol similar to private chains (Friedenbach and Timón, 2013). In federated two-way pegged chains, as discussed in Section2, the script implements a 'n' of 'm' multi-signature scheme which requires each block to be signed by a predetermined number of signers/entities (for instance 'n' of 'm' signers/entities). As a result, this mechanism can achieve Bitcoin like Byzantine robustness as a minority of malicious entities would not be able to affect the system. Fig. 8 depicts how the consensus is achieved on the Liquid platform.

Fig. 8 can be summarized in the following steps:

- Entities propose candidate blocks in a round-robin fashion to all other signing participants.
- Each entity signals their intent by pre-committing to sign the given candidate block.
- If threshold X is met, each entity signs the block.
- If threshold Y (which may be different from X) is met, the block is accepted and sent to the network.
- The next block is then proposed by the next entity in the round-robin.

In Bitcoin, there is a tendency for chain reorganization in the newly added blocks due to probabilistic generation of blocks (Eyal and Sirer, 2018). Since, block generation in case of strong federations are based on a fixed set of block signers instead of being probabilistic, Liquid chain never reorganizes. This allows significantly faster transaction confirmation times than Bitcoin.

3.3.3. Asset transfers

Native Assets: The Liquid network supports accounting of other assets (including traditional currencies, real-world assets and other cryptocurrencies) in addition to Bitcoin. These are known as native assets and

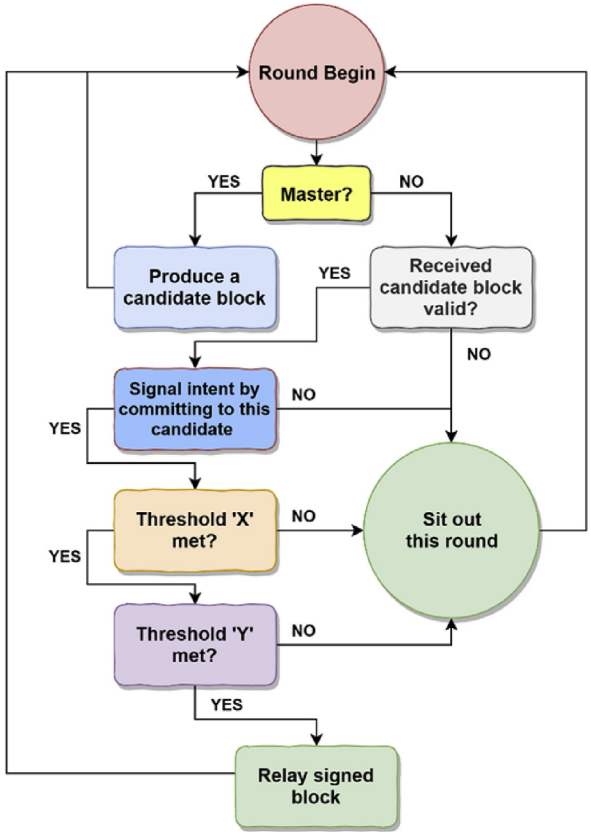

Fig. 8. Block-signing by entities on the Liquid platform.

are accounted separately from the base Bitcoin cryptocurrency. These assets can be issued by any participant by means of a special asset-generating transaction. They can also optionally set conditions by which additional issuance can take place in the future:

- A policy for an asset being generated is decided upon by the asset issuer, which includes conditions for asset redemption.
- The asset issuer creates a transaction with one or more special asset-generating inputs, whose value is the full issuance of the asset. This transaction uniquely identifies the asset.
- A member of the strong federation confirms the asset-generating transaction after which the assets become transactable.
- The asset issuer then distributes these assets to its user-base as per requirement. This is done by using standard strong federation transactions.
- When the users wish to redeem their asset tokens, they transfer their asset holdings back to the issuer in return for out-of-band goods or the provided service. The issuer then destroys these tokens.

Peg-out Authorization: When Bitcoins are frozen on the Bitcoin blockchain and pegged in to the Liquid network they become Liquid Bitcoin (L-BTC). The L-BTCs can be then utilized on the Liquid network and can be transferred back to the Bitcoin blockchain at any given time. As discussed earlier, moving assets back to the Bitcoin blockchain is foreseen and mediated by a set of watchmen, who create the transactions on the Bitcoin side. These transactions take place with the help of peg-out authorization proofs which have the following design:

- **Setup:** Each participant i chooses two public-private keypairs: (P_i, p_i) and (Q_i, q_i), where p_i is an "online key" and q_i is an "offline key". The participant then provides P_i and Q_i to the watchmen.
- **Authorization:** To authorize a key W (which will correspond to an individually-controlled Bitcoin address), a participant takes the following steps.
  - ≻ They compute $L_j = P_j + H(W + Q_j)(W + Q_j)$ for every other participant index j, where H is a random oracle hash that maps group elements to scalars.
  - ≻ The participant knows the discrete logarithm of L_i, and can therefore produce a ring signature over every L_i. They do so by signing the full list of online and offline keys as well as W.
  - ≻ The participant sends the resulting ring signature to the watchmen or embeds it in the sidechain.
- **Transfer:** When the watchmen produce a transaction to execute transfers from the sidechain to Bitcoin, they ensure that every output of the transaction either 1) is owned by them or 2) has an authorization proof associated to its address.

3.3.4. Limitations

Some the limitations of the Liquid platform are as follows:

- Currently, only members of the Liquid network can run full nodes. Although the developers plan to allow other users to run full nodes to validate the network, it is not feasible at its current state.
- Liquid nodes require more computing resources than Bitcoin as the platform requires a Bitcoin node alongside the Liquid node to be able to validate asset transfers.
- Liquid network used federated two-way pegs which introduces political centralization in the sidechain ecosystem.

3.4. RootStock (RSK)

RSK (Lerner, 2015), (RSK, 2019) is an open-source sidechain pegged to the Bitcoin main-net for the execution of smart contracts, it is an evolution of QixCoin ("Qixcoin." [Online]), a Turing-complete cryptocurrency developed in 2013. RSK implements the concept of merged mining (Lerner, 2016) which provides incentives to the miners of the Bitcoin blockchain to be actively involved by mining on RSK platform.

RSK incorporates a Turing complete, resource-accounted, and deterministic virtual machine (called the RootStock Virtual Machine or RVM) for the parallel execution of smart contracts in the Bitcoin ecosystem by several nodes. The execution of smart contracts can result in the processing of messages between multiple other smart contracts, creation of new transactions or change of a state of smart contract's persistent memory. RVM is compatible with Ethereum's Virtual Machine (EVM) at op-code level which allows the execution of Solidity ("Solidity." [Online]) smart contracts on RSK.

3.4.1. Use cases

The compatibility of RVM with EVM opens the door up for the implementation of several innovative smart contracts and use cases as it allows the developers working on the Ethereum platform to take advantage of Bitcoin's robustness. Some of the most important use cases are discussed below:

- **Retail Payment Systems:** With the implementation of RSK, Bitcoin could be adopted globally for day-to-day retail transactions. In its current state, it is not feasible to use Bitcoins in retail due to its slow confirmation time (~10 min–1 h to ensure irreversibility). RSK can allow consumers to have the security of Bitcoin with faster transaction times (~10 s). This would allow merchants to accept payments faster without having to rely on third-party gateways. Additionally, the RSK platform can handle high volume of transactions per second (~300–1000 transactions per second) which is yet another necessity for a payment processing platform to succeed in the retail industry.
- **Supply Chain Traceability:** With RSK smart contracts could be implemented to track and trace the physical location and condition of a product. Such contracts could be particularly useful in food, retail, healthcare and transportation industries. Once again, such contracts would be backed by the security and robustness of the Bitcoin protocol.
- **Digital Identity:** Developing countries struggle with the lack of documentation and identification for the poor, which can prevent them from voting, accessing healthcare and financial aid, reporting criminal activities. Hence, with RSK digital global registries could be implemented at extremely low costs, this could be a major step in the improvement of overall infrastructure of such countries.

3.4.2. Consensus mechanism

While mining on the Bitcoin blockchain, conflicting situations may arise when multiple miners solve a block at the same chain height. In such situations, it becomes hard to decide which miner's block to select and add to the network. Additionally, miners are often required to stop mid-state and restart mining on new blocks each time a new block is solved and added to the network. These situations result in poor mining efficiency, greater network latencies and mining time gaps.

To mitigate this RSK utilizes DECOR+ (Lerner, 2015) protocol, a reward sharing scheme which reduces competition while mining providing miners with the option to switch to the newest block later. With DECOR + conflicts are resolved deterministically when all nodes have the same blockchain state information, the resolution is chosen in such a way that it maximizes the revenue for all miners involved whether they were involved in the conflict or not. The protocol has the following main features:

- If a miner switches each time a new block is accepted to the RSK network, they compete for a full block reward.
- If a miner switches late i.e. they keep mining older blocks, they create uncles[16] and earn a share of the block reward.

[16] https://www.investopedia.com/terms/u/uncle-block-cryptocurrency.asp.

In neither of these situation blocks are fully orphaned,[17] as the DECOR + protocol pays a reward to uncles, which are counted as normal blocks (GHOST protocol (Sompolinsky and Zohar, 2016)). This greatly increases the efficiency of mining on RSK.

When the RSK hashing power is below 50% of the total Bitcoin hashing power, the network could be vulnerable to 51% attacks and double spending problems. To prevent such situations, RSK utilizes federated checkpoints, which are signed by federation entities and can be used by a client to decide which is the best block with the help of multi-signature majority. Moreover, if the total RSK hashing power goes below 5% of the total Bitcoin hashing power, the federation would be able to create signed blocks. Finally, the clients stop using federated checkpoints by defaults if the total RSK hashing power is over 66% of the Bitcoin hashing power and the paid fees in a block is higher than or equal to the average reward of a Bitcoin block.

3.4.3. Asset transfers

Asset transfers on RSK take place with federated two-way pegs. When Bitcoins are transferred from the Bitcoin blockchain to the RSK sidechain they are referred to as "SmartBitcoins" (SBTC) (Lerner, 2015). Hence, SmartBitcoins are Bitcoins living natively on the RSK platform, they can be transferred back to the Bitcoin blockchain at any given time for a standard RSK transaction fee.

The federation that controls the asset transfers on RSK comprises of well-known and community respected members/entities. Each entity of the federation is identified by a public key for the checkpoint signature scheme. An entity can be added or removed from the federation by means of an embedded predefined voting system. The addition/removal of an entity from the federation requires a high majority of votes.

The RSK platform aims to maximize the incentives for merged-mining. However, RSK is not completely dependent on merged-mining as it is robust to merge-mining shortages. In case of such situations, the federation automatically takes charge of the RSK network to keep it secure.

3.4.4. Limitations

Some of the limitations of the RSK platforms are as follows:

- Currently, the RSK main-net is not available to all developers. The platform currently employs a whitelisting process where a development team/company is required to have a fully functional/semi-functional project approved by RSK to gain access to the network for testing and deployment on the platform. The whitelisting process can take a minimum of 3 days for approval. The platform aims to open the network for all users once the first stage of the bounty hunting program is completed.
- The use of federated two-way pegs introduces political centralization in the sidechain ecosystem as discussed in Section 2.2

Table 3 summarizes the key differences between Bitcoin, Liquid and RSK based on average block confirmation time, transaction rate, smart contract execution capability, security guarantee and if the transactions are confidential.

It is clear from Table 3 that only RSK supports the execution of smart contracts. It also has the fastest block confirmation times and highest transaction rates compared to the Bitcoin (mainchain) blockchain or the Liquid network.

3.5. Comparison of sidechain platforms

Table 4 provides a comparative summary of Loom, the POA Network, Liquid and RSK platforms based on possible use cases, consensus mechanism, two-way peg design and limitations. The table also highlights the advantages that these platforms provide over their parent chains.

Table 3
Comparison of bitcoin, RSK and liquid.

Features	Bitcoin[a] (mainchain)	Liquid[b] (sidechain)	RSK[c] (sidechain)
Average block confirmation time	~10 min	~1 min	~30 s
Transactions rate	~7 transactions/second	≫ 1 transaction/second	300–1000 transactions/second
Turing complete Smart contract execution	No	No	Yes
Security guarantee	SHA256D miners	Strong federation	SHA256D merger miners + federation
Confidential transactions	No	Yes	Planned for future

~ means approximately, ≫ means much greater than.
[a] https://blockexplorer.com/blocks.
[b] https://blockstream.com/liquid/.
[c] https://stats.rsk.co/.

An interesting observation from Table 4 suggests that all the four platforms discussed in this section use federated two-way pegs. This is because in its current state it is not possible to implement SPV based two-way pegs in Bitcoin, due to missing opcodes from its protocol (See Section 4). Whereas, when it comes to the Ethereum based sidechain platforms, the Loom network intends to implement a more robust, secure and decentralized two-way peg design in the future and finally, the POA network's decision to implement a federated two-way peg was based on the idea of preservation of a human element in a blockchain ecosystem.

3.6. Other projects and frameworks

There are other innovative sidechain projects and frameworks that slightly fell short of our criteria for selection. The reasons why these projects were not selected were because of incomplete and/or active development, technical difficulties and lack of thorough documentation and support.

Plasma is a framework proposed by Buterin and Poon (2019), which may have the potential to provide highly scalable solutions for the blockchain-based decentralized financial industry as it incentivizes and enforces execution of smart contracts. The platform is potentially aiming to achieve more than a billion state updates per second. The smart contracts running on the platform are incentivized to continue operation autonomously with the help of network transaction fees. This process ultimately relies on the underlying blockchain (for instance, Ethereum) to enforce transactional state transitions.

The Elements project (BlockStream, 2019) was launched in June 2015. It is an open-source, blockchain platform which is also sidechain-capable. It provides features such as Issued assets and confidential transactions. Blockchains developed with the Elements platform can be configured and developed to either run as standalone blockchains or as pegged sidechains to other blockchains which allows assets to be transferred between disparate blockchains. It utilizes and extends the current Bitcoin codebase; hence, it allows developers to take advantage of the *bitcoind*[18] Application Programming Interface (API) to develop blockchains and test proof-of-concept projects. Since, Elements is built upon the Bitcoin's codebase, it can also serve as a test-net for introducing changes to the Bitcoin protocol.

In the context of the Elements platform, a sidechain is an extension to an existing blockchain. Assets are transferable between chains allowing the main chain to benefit from the enhanced features of the sidechain,

[17] https://www.investopedia.com/terms/o/orphan-block-cryptocurrency.asp.

[18] https://bitcoin.org/en/developer-reference#serialized-blocks.

Table 4
Comparison of sidechain platforms.

Platform	Use Cases	Consensus Mechanism	Two-way peg design	Advantages over mainchain	Limitations
Loom	DelegateCall, Game development, scalable DApps	Delegated Proof-of-Stake (DPoS)/any consensus mechanism	Federated two-way peg	Scalability, Efficiency needed for games	1. Limited Windows (OS) support 2. If the tokens are not approved for transfer back to the mainchain, the tokens can be at risk of being compromised 3. The Loom Network runs on the idea that it is not necessary to store every transaction on the sidechain 4. Centralization due to federated two-way peg
POA Network	Scalable smart contracts	Proof-of-Authority	Federated two-way peg	Interoperability between blockchains	1. Centralization due to federated two-way peg. 2. Geographically centralized which may introduce censorship 3. Plans for increase the number of validators which could impede performance.
Liquid	International Exchange	Proof-of-Possession	Federated two-way peg	Faster transaction rates than Bitcoin	1. Currently not open to all users 2. Running Liquid full nodes requires more resources than running Bitcoin full nodes 3. Centralization due to federated two-way peg
RSK	Retail Payment Systems, Supply Chain Traceability, Digital Identity	Proof-of-work based merged-mining with Bitcoin, DECOR+	Federated two-way peg	Ability to execute smart contracts	1. Currently not open to all users/developers 2. Centralization due to federated two-way peg

such as rapid transfer finality and confidential transactions. While a sidechain is aware of the main chain and its transaction history, the main chain has no awareness of the sidechain, and none is required for its operation. This enables sidechains to innovate without restriction or the delays associated with main chain protocol improvement proposals. Indeed, rather than trying to alter it directly, extending the main protocol with a sidechain allows the main chain itself to remain secure and specialized, underpinning the smooth operation of the sidechain.

4. Open issues and recommendations

Sidechains are still relatively new proposals and are by no means mature enough to change the blockchain world at this time, but they sure are promising for the future of the blockchain industry. In this section, we discuss our observations as a result of the examination of sidechain filed to highlight open issues and suggest future measures and recommendations for the mitigation or elimination of these issues.

4.1. Centralization in federated two-way pegs

Political decentralization is an important characteristic of a blockchain network, as discussed in Section 2.2, federated two-way pegs introduce a level of political centralization in the sidechain ecosystem. Hence, it is important to identify and select honest and trusted entities to form a federation for the security and integrity of a network. It is extremely critical that entities have their economic interests well aligned with the proper functioning of a federation. It would obviously be a mistake to rely on a random assortment of volunteers to support a commercial sidechain holding significant value. Beyond the incentive (Parizi and Dehghantanha, 2018) to attempt to extract any value contained on the sidechain, these volunteer would also have little incentive to ensure the reliability of the network. To mitigate these concerns, we propose a federation should at least have the following attributes which may potentially lead to good results:

- Federations are most secure when each entity has a similar amount of value held by the federation. Incentives can be aligned using escrow, entity allocation, or external legal constructs such as insurance policies and surety bonds
- The total number of entities that form a federation should lie in the range - (Abdellatif and Brousmiche, 2018; Backet al., 2014). This is to maintain political decentralization and still provide the users with the ability to verify the authenticity of each entity within the federation in a relatively short period of time.
- The identity and authenticity of each entity should be verifiable. Some ways to achieve this could be providing proof of identity with government issued ID's or licenses, proof of physical address etc.
- Entities should be distributed geographically to prevent down-time in case of power failure, natural disasters etc.
- Entities should be disparate from one another and should not engage in business with one another, this would eliminate conflict of interest and censorship.

4.2. Security of federated two-way pegs

To date, there has not any major malicious attack on federated two-way peg-based platforms. However, this does not mean that there are no loopholes in the design as federated two-way pegs do introduce security risks in the sidechain ecosystem. We have identified two major instances of such security threats:

- If the private keys of the majority of the entities that form a federation are compromised, then the assets locked in the lockbox (or on the sidechain) are vulnerable to theft. This is because as discussed in Section 2.2.B, a transaction in a federated two-way peg design

requires 'n' of 'm' signatures to be approved (where 'n' is the majority in a total of 'm' entities).
- On the same line, a malicious group of entities that form a majority within a federation will also introduce a security flaw in the system as the fate of the assets locked in the lock box is controlled by these malicious entities.

One way to mitigate this threat would be to migrate to SPV based two-way peg design where the lockbox is usually controlled by the miners of the network and the only way to unlock the funds from the lockbox is to provide a valid SPV proof.

4.3. SPV based two-way pegs on bitcoin

SPV proofs can provide a solution to the political centralization issue with federated two-way pegs. As discussed in Section 2.2, SPV proofs require no single entity or a group of entities (federation), for transferring assets from the mainchain to the sidechain and vice versa. Unfortunately, SPV based two-pegs cannot be implemented on a sidechain pegged to the Bitcoin blockchain at this time. This is because in its current state Bitcoin is missing a few opcodes from its protocol such as:

- **OP_WITHDRAWPROOFVERIFY:** *OP_WITHDRAWPROOFVERIFY* would unlock 'reserve' coins on a sidechain. A user would need to provide inputs to an output such that the output would evaluate to true - which would unlock the reserve coins. The user would then be credited on the sidechain with the amount of coins they locked up on the Bitcoin blockchain. The change on the sidechain would also be sent back to the federation's reserve address (Stewert, 2017).
- **OP_REORGPROOFVERIFY:** *OP_REORGPROOFVERIFY* would allow users to submit SPV proofs in the reorg-period (Section 2.2. C). This opcode would correct invalid states of two types: 1) double spends (Bala and Manoharan, 2018), (Bae and Lim, 2018) of a parent chain lock and 2) parent chain reorganizations (Elements, 2016).

We propose the addition of these opcodes to the Bitcoin protocol in the future through Bitcoin Improvement Proposals (BIP) (Bitcoin, 2011). This would allow the community to implement sidechain technology with SPV based two-way pegs instead of relying on federated two-way pegs. SPV based designs offer a higher degree of security and decentralization (discussed in Section 2.3) due to the fact that the lock box on both the mainchain and the sidechain are controlled by the miners of the network. Hence, this would mitigate the security threats discussed in Section 4.2.

4.4. Lack of research support on current sidechain platforms

The sidechain domain is still relatively new and hence, most state-of-the-art sidechain platforms are still in development or bounty hunting phases. Based on the authors' experimental experiences, registering or submitting DApps on some the platforms (e.g. Liquid and RSK) discussed in the previous section is extremely difficult and selective as the developers do not provide access to all users on their platforms at this time. To make matters worse some of these platforms are not integrated to the Bitcoin or Ethereum test-nets at this time (e.g. Liquid). This makes performing empirical studies by researchers or practitioners on these platforms extremely difficult and expensive due to the market value of Bitcoin and Ether cryptocurrencies. Empirical research is an important tool in software engineering (Malhotra, 2015) which can reveal hidden trends, patterns, anomalies and limitations of a software system (Parizi et al., 2018). Hence, we strongly advocate:

- The integration of these platforms to their parent chain's test-nets. This would allow the researchers in the community to analyze and evaluate these platforms based on several attributes such as performance, security and privacy which would help in speeding-up development process and the overall advancement of sidechain technology.
- Developers of the sidechain platforms should allow researchers to study their platforms during the bounty hunting phase. This would provide valuable insight in terms of empirical studies and benchmarking data about a platform being developed.

5. Conclusions

In the last decade, the blockchain technology has grown exponentially with seemingly new use cases being discovered almost every day. Consequently, research in the domain has picked up pace in the recent years both to discover issues and vulnerabilities in blockchains and to provide solutions to these problems and challenges. Scalability and limited functionality have shackled blockchains ever since its proposal and implementation in 2008. The sidechain technology has been proposed recently to provide a solution for such limitations, but a comprehensive study is still lacking in literature to study the impact of sidechains both theoretically and empirically. Moreover, there has been a lack of studies discussion on how and where it can effectively be integrated into blockchains to remedy current issues in a clear context.

Hence, the motivation of our study was to take the first step and provide a comprehensive review of: 1) the available design choices for building sidechain systems, and 2) state-of-the-art sidechain platforms based on their use cases, consensus mechanisms, asset transfer protocols and limitations. As part of our review, we discussed current advancements, analyzed their impact from various viewpoints, and more importantly, identified open issues and research challenges and proposed directions for the future of research and development.

Conflict of interest

The authors declare that there is no conflict of interest associated with this paper.

References

Abdellatif, T., Brousmiche, K.-L., 2018. Formal verification of smart contracts based on users and blockchain behaviors models. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security. NTMS), pp. 1–5.

Amani, S., Bégel, M., Bortin, M., Staples, M., 2018. Towards verifying Ethereum smart contract bytecode in isabelle/HOL. In: Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, pp. 66–77.

Androulaki, E., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, pp. 30:1–30:15.

Anish Dev, J., 2014. Bitcoin mining acceleration and performance quantification. In: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1–6.

Arasev, V., 2018. POA network whitepaper [Online]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper. (Accessed 30 January 2019).

Atzei, N., Bartoletti, M., Cimoli, T., 2017. A Survey of attacks on Ethereum smart contracts (SoK). In: International Conference on Principles of Security and Trust, pp. 1–24. March.

Back, A., et al., 2014. Enabling Blockchain Innovations with Pegged Sidechains [Online]. Available: http://www.blockstream.com/sidechains.pdf. (Accessed 25 January 2019).

Bae, J., Lim, H., 2018. Random mining group selection to prevent 51% attacks on bitcoin. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops. DSN-W), pp. 81–82.

Bala, R., Manoharan, R., 2018. Security enhancement in Bitcoin protocol. In: 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1–4.

Bentley, D., 2018. Loom's Popular dApps Enable Ethereum Development at Scale [Online]. Available: https://www.the-blockchain.com/2018/07/11/looms-dapps-gain-traction-as-go-to-resource-for-ethereum-development/. (Accessed 30 January 2019).

Bharel, D., 2019. "Plasma Cash Developers' Guide: Everything You Need to Know (+ How to Use Loom's Plasma CLI) [Online]. Available: https://medium.com/loom-network/plasma-cash-developers-guide-everything-you-need-to-know-how-to-use-looms-plasma-cli-6f7b7a3c78d1. (Accessed 24 January 2019).

Bhargavan, K., et al., 2016. Formal verification of smart contracts: short paper. In: Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 91–96.

Bitcoin, 2011. Bitcoin improvement proposals (BIP) [Online]. Available: https://github.com/bitcoin/bips. (Accessed 4 July 2019).
"Liquid." [Online]. Available: https://blockstream.com/liquid/. [Accessed: 30-Jan-2019].
BlockStream, "Elements." [Online]. Available: https://elementsproject.org/. [Accessed: 11-Jan-2019].
Buterin, V., 2014. A Next-Generation Smart Contract and Decentralized Application Platform. *Etherum* [Online]. Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf. (Accessed 5 March 2018).
Buterin, V., Poon, J.. Plasma: scalable autonomous smart contracts [Online]. Available: https://plasma.io/plasma.pdf. (Accessed 3 January 2019).
Chauhan, A., Malviya, O.P., Verma, M., Mor, T.S., 2018. Blockchain and scalability. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 122–128.
Deng, L., Chen, H., Zeng, J., Zhang, L.-J., 2018. Research on cross-chain technology based on sidechain and hash-locking. In: Edge Computing – EDGE 2018, pp. 144–151.
Dennis, R., Owenson, G., Aziz, B., 2016. A temporal blockchain: a formal analysis. Proc. 2016 Int. Conf. Collab. Technol. Syst. CTS 2016 430–437.
Dilley, J., Poelstra, A., Wilkins, J., Piekarska, M., Gorlick, B., Friedenbach, M., 2016. Strong federations: an interoperable blockchain solution to centralized third-party risks. arXiv Prepr. arXiv1612.05491.
Ehmke, C., Wessling, F., Friedrich, C.M., 2018. Proof-of-Property - a lightweight and scalable blockchain protocol. In: 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), pp. 48–51.
Elements, 2016. The Federated Peg in Elements Alpha [Online]. Available: https://github.com/ElementsProject/elementsproject.org/blob/master/source/_posts/the-federated-peg-in-elements-alpha.md. (Accessed 14 January 2019).
Eyal, I., Sirer, E.G., Jun. 2018. Majority is not enough: Bitcoin mining is vulnerable. Commun. ACM 61 (7), 95–102.
Fiaidhi, J., Mohammed, S., Mohammed, S., Jul. 2018. EDI with blockchain as an enabler for extreme automation. IT Prof. 20 (4), 66–72.
Friedenbach, M., Timón, J., 2013. Freimarkets: Extending Bitcoin Protocol ´with User-Specified Bearer Instruments, Peer-To-Peer Exchange, Off-Chain Accounting, Auctions, Derivatives and Transitive Transactions [Online]. Available: http://freico.in/docs/freimarkets-v0.0.1.pdf. (Accessed 14 January 2019).
Giaglis, G., et al., 2017. Under-optimized smart contracts devour your money. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN), vol. 55, pp. 1–5 no. 9.
Halpin, H., Piekarska, M., 2017. Introduction to security and privacy on the blockchain. In: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 1–3.
Henry, R., Herzberg, A., Kate, A., Jul. 2018. Blockchain access privacy: challenges and directions. IEEE Secur. Priv. 16 (4), 38–45.
Herlihy, M., 2018. Atomic cross-chain swaps. In: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, pp. 245–254.
Kan, L., Wei, Y., Hafiz Muhammad, A., Siyuan, W., Linchao, G., Kai, H., 2018. A multiple blockchains architecture on inter-blockchain communication. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 139–145.
Karame, G.O., Androulaki, E., Capkun, S., 2012. Double-spending fast payments in Bitcoin. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 906–917.
Keenan, T.P., 2017. Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), pp. 400–4002.
Kovalchuk, L., Kaidalov, D., Shevtsov, O., Nastenko, A., Rodinko, M., Oliynykov, R., 2017. Analysis of splitting attacks on Bitcoin and GHOST consensus protocols. In: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 2, pp. 978–982.
Lai, R., 2018. Sentinel Chain, pp. 1–50.
Lerner, S.D., 2015. RSK: white paper overview [Online]. Available: https://docs.rsk.co/RSK_White_Paper-Overview.pdf. (Accessed 30 January 2019).
Lerner, S., 2016. Drivechains, Sidechains and Hybrid 2-way Peg Designs [Online]. Available: https://docs.rsk.co/Drivechains_Sidechains_and_Hybrid_2-way_peg_Designs_R9.pdf. (Accessed 7 January 2019).
Loom. Loom SDK documentation [Online]. Available: https://loomx.io/developers/docs/en/basic-install-all.html. (Accessed 30 January 2019).
Loom. Loom netwrok [Online]. Available: https://loomx.io/. (Accessed 25 January 2019).
Lou, J., Zhang, Q., Qi, Z., Lei, K., 2018. A blockchain-based key management scheme for named data networking. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking. HotICN), pp. 141–146.
Malhotra, R., 2015. Empirical Research in Software Engineering: Concepts, Analysis, and Applications. Chapman & Hall/CRC.
Miller, D., May 2018. Blockchain and the internet of Things in the industrial sector. IT Prof. 20 (3), 15–18.
Moore, T., Christin, N., 2013. Beware the middleman: empirical analysis of bitcoin-exchange risk. In: Financial Cryptography and Data Security, pp. 25–33.
Mylrea, M., Gourisetti, S.N.G., 2018. Blockchain for supply chain cybersecurity, optimization and compliance. In: 2018 Resilience Week (RWS), pp. 70–76.
Nadiya, U., Mutijarsa, K., Rizqi, C.Y., 2018. Block summarization and compression in Bitcoin blockchain. In: 2018 International Symposium on Electronics and Smart Devices. ISESD), pp. 1–4.
Nakamoto, S., 2008. Bitcoin: A Peer-To-Peer Electronic Cash System [Online]. Available: https://bitcoin.org/bitcoin.pdf. (Accessed 30 January 2019). Www.Bitcoin.Org.
O`KeeffeDaniel, 2018. Bitcoin Liquid Network Launches to Complement Lightning [Online]. Available: https://cryptodisrupt.com/bitcoin-liquid-network-launches-to-complement-lightning/. (Accessed 24 January 2019).
Parizi, R.M., Dehghantanha, A., 2018. On the understanding of gamification in blockchain systems. In: 2018 6th International Conference on Future Internet of Things and Cloud Workshops. FiCloudW), pp. 214–219.
Parizi, R.M., Dehghantanha, A., Choo, K.K.R., Singh, A., 2018. Empirical vulnerability analysis of automated smart contracts security testing on blockchains. In: 28th Annual International Conference on Computer Science and Software Engineering (CASCON'18).
Parizi, R.M., Amritraj, Dehghantanha, A., 2018. Smart contract programming languages on blockchains: an empirical evaluation of usability and security. In: Blockchain – ICBC 2018, pp. 75–91.
POA, 2017. Proof of authority: consensus model with identity at Stake [Online]. Available: https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256. (Accessed 18 January 2019).
POA. POA network [Online]. Available: https://poa.network/. (Accessed 30 January 2019).
POA. POA partnerships [Online]. Available: https://medium.com/poa-network/tagged/partnerships. (Accessed 30 January 2019).
POA. POA core [Online]. Available: https://forum.poa.network/c/poa-core. (Accessed 30 January 2019).
Robinson, P., 2018. Requirements for Ethereum private sidechains. arXiv Prepr. arXiv1806.09834.
RootStock. RSK partners [Online]. Available: https://www.rsk.co/. (Accessed 30 January 2019).
RSK. RSK [Online]. Available: https://www.rsk.co/. (Accessed 15 January 2019).
Sompolinsky, Y., Zohar, A., 2016. Bitcoin's security model revisited. arXiv Prepr. arXiv1605.09193.
Stewert, C., 2017. OP_WITHDRAWPROOFVERIFY — the Op Code that Powers SPV Sidechains [Online]. Available: https://medium.com/@Chris_Stewart_5/op-withdrawproofverify-the-op-code-that-powers-spv-sidechains-cefce996a324. (Accessed 15 January 2019).
Wood, G., 2014. Ethereum: a secure decentralised generalised transaction ledger Yellow Paper. Ethereum Proj. Yellow Pap 1–32.
Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., Zhang, B., 2018. A high performance blockchain platform for intelligent devices. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking. HotICN), pp. 260–261.
Zhou, L., Wang, L., Sun, Y., Lv, P., 2018. BeeKeeper: a blockchain-based IoT system with secure storage and homomorphic computation. IEEE Access 1.
Qixcoin." [Online]. Available: %http://qixcoin.com/%0A.
Solidity." [Online]. Available: https://solidity.readthedocs.io/en/develop/. [Accessed: 01-Mar-2018].

Amritraj Singh is a research assistant in the College of Computing and Software Engineering (CCSE) at Kennesaw State University GA, USA. He received his bachelor's degree in Electrical and Electronics Engineering in 2016 from Visvesvaraya National Institute of Technology (VNIT), Nagpur, India. He is a member of IEEE blockchain community and his research interests include blockchain-based systems, decentralized applications, smart contracts programming and security, software development, and software quality engineering and assurance. He has previously published articles in conferences proceedings such as ICBC, FIE, and CASCON.

Kelly Click is a research assistant in the College of Computing and Software Engineering (CCSE) at Kennesaw State University GA, USA. His research interest include blockchain and sidechain technologies, smart contracts, and decentralized applications development.

Reza M. Parizi is a faculty in the College of Computing and Software Engineering at Kennesaw State University, GA, USA. He is a consummate technologist and blockchain researcher with an entrepreneurial spirit. He is the member of IEEE, IEEE Blockchain Community, IEEE Computer Society and ACM. Prior to joining KSU, he was an Associate Professor at New York Institute of Technology. He received a Ph.D. in Software Engineering in 2012 and M.Sc. and B.Sc. degrees in Computer Science respectively in 2008 and 2005. His research interests are R&D in blockchain, smart contracts, IoT and emerging issues in the practice of secure software-run world applications. He serves as a program committee member for IEEE- Blockchain 2019 and ICBC 2019.

Qi Zhang received the Ph.D. degree in computer science from Georgia Institute of Technology, Atlanta, USA, in 2017. He is currently a Research Staff Member in IBM Thomas J. Watson Research Center. His research interests include Blockchain systems, Cloud computing, big data processing, and distributed systems. He published research articles in referred journals and conference proceedings such as IEEE TC, IEEE TSC, ACM CSUR, VLDB, SC, HPDC, IEEE ICDCS, IEEE ICWS, IEEE CLOUD, ICBC. Dr. Zhang received the top 5 picks award in IEEE ICWS 2017. He served as a program committee member for IEEE Blockchain 2018. He is the organizing chair of ICBC 2019.

Ali Dehghantanha is the director of Cyber Science Lab in the School of Computer Science, University of Guelph (UofG), Ontario, Canada. He has served for more than a decade in a variety of industrial and academic positions with leading players in Cyber-Security and Artificial Intelligence. Prior to joining UofG, he has served as a Sr. Lecturer in the University of Sheffield, UK and as an EU Marie-Curie International Incoming Fellow at the University of Salford, UK. He has PhD in Security in Computing and a number of professional certifications including CISSP and CISM. His main research interests are malware analysis and digital forensics, IoT security and application of AI in the Cyber Security.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, Outstanding Associate Editor of 2018 for IEEE Access, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking (JWCN) Best Paper Award, Korea Information Processing Society's Journal of Information Processing Systems (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and Co-Chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.