Echo Sidechains Whitepaper

Contents

Echo Sidechains

Intro to Sidechains

A sidechain is a mechanism that allows users to transfer cryptocurrencies to other blockchains and enables the ability to return their cryptocurrencies back to the main network at any time. The technology extends cryptocurrencies existing functionality and provides its users with access to new and innovative uses cases.

By using coins in other blockchains, users can obtain access to a wider range of features and opportunities while still retaining full ownership.

The core concept behind this technology is as follows: when users want to transfer cryptocurrencies from the main chain to the secondary chain (sidechain), users "freeze" their crypto coins on the main chain by sending them to a predefined address. By doing so, users "unfreeze" an equivalent sum of sidechain coins, allowing them to use the same amount of the related coins on the other chain. The reverse process is similar: users freeze the required amount of sidechain coins on the secondary chain and "unfreeze" an equivalent amount of coins in the main chain.

Motivation and Key Benefits

A sidechain implementation allows developers to experiment with and access various features and technologies, innovate by creating new cryptocurrency functionality, and release new features to market much faster than would have been possible on the main chain. These new innovations also promote the main chain as a reliable and accessible medium of exchange and a trustworthy store of value. In addition to the above, sidechain technology improves the interoperability between multiple blockchains and the traditional financial ecosystem.

Another great advantage of sidechain technology is the ability to reduce transaction latency and transaction fees. By using main coins on the sidechain, users have the ability to transfer funds between accounts in a much faster and cheaper way and will only be subjected to regular latency and fees when they would need to transfer the coins back to the Bitcoin network in the future.

Prior Work and Vision of Extending BTC with Sidechains

In 2014, a number of groups, including Blockstream, published a paper titled "Enabling Blockchain Innovations with Pegged Sidechains" [BCDF + 14]. The paper describes the basic idea of the technology, the benefits it could provide, as well as suggested design and architecture. The main advantage of the proposed **Pegged Sidechain** idea, according to the authors, is the ability to deliver new functionality for Bitcoin much faster by safely implementing it in an external blockchain, thus isolating the main Bitcoin network from otherwise dangerous changes.

The preferred implementation option is Efficient SPV Proofs [BCDF + 14] which requires the storage of proof of work of another blockchain on the main chain. The document contains other options for implementation, such as:

- **Federated Peg**: an implementation where the connection between two blockchains is managed by a federation of nodes;
- **Atomic Swaps**: an implementation where users can directly exchange coins without using centralized intermediaries, in a safe and guaranteed way.

The sidechain implementation using Efficient SPV Proofs seemed like a very promising solution, however, it required making changes to the Bitcoin protocol itself, which is a long, dangerous, and complicated process. In this regard, the implementation of a Federated Peg turned out to be a good alternative which didn't require making changes to the Bitcoin protocol and allowed testing the idea of a sidechain in the real world.

Unfortunately, the idea of Efficient SPV Proofs proved to be susceptible to miner attacks. As miners can conduct 51% attacks in altcoins, with Efficient SPV Proofs in place, miners could use their computational power to generate a false SPV chain, which gives them the ability to claim the coins that were transferred to the sidechain. Moreover, the more successful the project is, the more funds it will hold - thus making such attacks more profitable and appealing.

Sidechain Design Strategies

As described above, sidechain technology enables transfer of crypto coins from one blockchain to another. In other words, the secondary blockchain has to send a certain amount of related sidechain coins to users' addresses.

Triggering such an event requires some sort of bidirectional communication between both of the blockchains, which is very hard to achieve in a decentralized and trustless way. In general, our implementation should address the following problems:

- Develop a communication/mechanism between multiple blockchains.
- Making this mechanism trustless, thus applicable in adversarial environments.

The blockchain itself cannot request external information on events, so our proposed solution to the first problem is adding third parties to the process which will be responsible for information transfer between the blockchains. This role can be taken upon by the users themselves and by individual witnesses, whose task is to monitor the networks for such information.

The solution to the second problem requires a mechanism that will allow all network members to reach a consensus on the transfer event, without necessarily having access to a fully synchronized node on the secondary blockchain. This could be achieved using the SPV (Simplified Payment Verification) mechanism. An SPV is a process where a "light client" (i.e., not a full node) simply relies on miners for transaction verification, while being able to verify the heaviest and correct chain by themselves. Even though users won't be able to verify transactions in general, they could still verify specific transactions by requesting full nodes for specific blocks containing their transactions and their inclusion proofs. [Nak09]

Following such an approach, the secondary blockchain must keep the block headers of the main blockchain and information about related transfer transactions. This way it would be possible to support any mechanism which requires validation of the main blockchain by the secondary blockchain. However, utilizing SPV transfer proofs only allows the implementation of a one-way peg. Unfortunately, implementing a reverse transfer mechanism, in order to support a full two-peg sidechain, is much more

difficult because the main blockchain isn't aware of the secondary blockchain and Bitcoin does not support SPV validation at the script level.

One possible work around to this problem is a federated sidechain.

Federated Sidechains

Due to the difficulty of verifying transactions on the main chain, it was proposed to offload such a mechanism to a federation of trustworthy nodes, usually with access to a shared multisignature wallet. The federation will be responsible for validating on-chain transfer transactions and freezing/unfreezing bitcoins held by the multisignature wallet.

Liquid Liquid is an example of an implementation of a similar federated sidechain. The idea was introduced in 2015, a year after the release of a paper describing the technology [BCDF + 14]. In 2017, Liquid launched the first testnet working against the main Bitcoin network. In 2018, Liquid was launched as a production-ready mainnet and became available for use by Blockstream's partners. The main purpose of Liquid is to enable fast and private transfers, thus providing a decent alternative to Bitcoin users who require fast bitcoin and multi-asset transfers, such as traders or exchanges.

RSK Rootstock (RSK) is a Bitcoin sidechain which aims to provide the possibility of using Turing-complete smart contracts for the bitcoin ecosystem. The idea for the project was introduced in 2014. The Whitepaper was published in 2015 by Sergio Demian Lerner providing a technical description of the project. [Ler2015]

Security Model It's paramount for a federated sidechain model to be as safe and as secure as possible. This means that:

- The federation must consist of trustworthy and politically independent members.
- The size of the federation shouldn't be too small in order to minimize the likelihood of collusion, as well as the likelihood that a majority of participants may be compromised.
- On the other hand, the size of the federation shouldn't be too high, so that it could reach a consensus without grinding the sidechain's functionality to a halt.

It is worth noting that federated sidechains do not impose limits on the integration of other approaches for sidechain implementation. For example, the RSK network uses a hybrid approach and is additionally protected by mechanisms such as merge-mining, long miner rewards maturity, and signed notifications,which effectively protect coins from double-spending attacks.

Pros and Cons The disadvantages of the federated model are as follows:

- Since the coins are managed by a single multi-signature wallet(or contract), a certain level of centralization exists with regards to the fault tolerance of the system. Federation members need to always be online for continued operation. In the case where some of the members are not available, the sidechain may grind to a halt.
- It's not a fully trustless model, as some level of trust in the federation is required.

- Federation management is centralized. In many cases, federation membership management is in the hands of the federation itself.

It is worth noting that all of the above-mentioned disadvantages are compromises necessary for achieving an optimal operation of the network. With the right approach of federation membership management, the system can be fairly decentralized and fault-tolerant. Also, additional mechanisms such as the delegation of voting allow network participants, although indirectly, to effectively influence the choice of federation participants.

In turn, this approach has several advantages:

- A bit counterintuitively, but centralization can also be regarded as a feature. Given the high level of inactivity of network users, centralization helps to increase the availability and liveness of the system.
- The federated approach does not require making changes to the current Bitcoin protocol and depends only on the functionality implemented in the secondary blockchain. Risks associated with the mechanism are assumed only by those participants who opt-in to use the sidechain.
- This approach ensures that even if the main chain miners want to disable/ban the sidechain, they will not be able to do so, since the sidechain peg can be committed in an undetectable way on the main network (sidechain transfer transactions do not differ from other transactions on the network).
- A federated sidechain is agnostic to the underlying consensus technology and (almost) agnostic to the main chain it works against.

Drivechains

Quick Explainer Drivechains approach allows a subset of miners on the main chain to manage funds freezing/unfreezing via voting. The Drivechain protocol can be implemented by a soft fork, which would have to be accepted by the miners: When the network receives an unpeg transaction, the miners will initially add information about it to the coinbase transaction and vote for accepting it on the network. Only after a certain number of blocks and only in the case of a successful vote, the transfer transaction is added to the blockchain.

Security Model Drivechain security model is based on the following:

1. All money transfer operations occur with a long enforced delay, which allows for disputes.
2. Sidechain security is similar to Bitcoin security itself. Since we assume miners honest majority, frozen funds will not be double-spent or withheld, as the network won't reach a consensus on such an event. Even if such a block is added to the network, the other miners would not accept it and would fork away.

The idea is that, given a long delay interval between transfer proposal and commitment, the network of honest miners and full nodes will have the opportunity to dispute adversarial behavior (e.g., on-chain or by another soft work).

Pros and Cons The obvious advantage of this approach is the high level of trust. The popularity and reputation of Bitcoin is so high that the level of trust is comparable to the level of Bitcoin network security. This guarantees high levels of reliability and honesty.

However, it should be noted that to implement this functionality, miners (and full nodes) must accept changes to the Bitcoin protocol (even as a soft fork). This is an extremely complex and lengthy process. The disadvantages of the approach also include the long enforced duration of deposits and withdrawals. The original document states duration in weeks, which naturally can be very inconvenient for users. Moreover, given the high volatility of bitcoin, it'll be hard to freeze your savings for several weeks without any ability to recover them ahead of time.

Another disadvantage of this approach is that it will exist only as long as the Bitcoin community is interested in its existence. As soon as this implementation becomes less interesting to the Bitcoin community, the risk of uncooperating with transfer transactions or spending any frozen funds by attackers (which may include miners) may increase significantly.

Echo Sidechains Implementation

Overview

Echo's Bitcoin and Ethereum sidechains approach is based on the federated sidechain model, further enhanced by the Echo protocol. An active list of federation members (hereinafter referred to as committee members) is elected to monitor and verify cross chain transactions, thus responsible for handling the mechanism of interaction between blockchains. Main chain frozen funds are stored in a multi-signature address (in the case of Bitcoin) or a smart contract account (Ethereum) which are controlled by the committee members.

The mechanism for transferring main coins to the Echo network is as follows:

1. Users receive a personal deposit address for the main chain from the Echo network.
2. Users transfer the desired amount of main coins to the deposit address.
3. Transferring funds to this address results in freezing them on the main chain and the same amount of eBTC or eETH coins will be issued on Echo network and credited to the originator.

Echo sidechains are symmetrical, such that withdrawing main coins back to the main chain is a very similar process:

1. Users inform the Echo network of the intention to "unfreeze" a certain amount of main coins. To do this, they send withdraw operation on the Echo network, which contains information about the output amount and the recipient's address in the main chain.
2. The operation triggers the withdrawal process, as a result of which the committee members collectively unfreeze the required number of main coins. The eBTC or eETH tokens are automatically burned on the Echo side.

Echo sidechain supports similar flow to transfer Ethereum chain ERC20 tokens from/to Echo which is described in detail in the corresponding section.

A user can receive her personal deposit addresses and history of the deposits and withdrawals using the Echo DB API or Echo Wallet API. Please see the corresponding documentation for the details.

Who Is the Committee?

The committee is a group of Echo network participants, where every member is explicitly elected to participate in the committee. In addition to participating in the Echo consensus protocol, each elected member has voting rights on accepting/rejecting network events (incoming transactions from the Bitcoin/Ethereum network, transfer events, membership changes, etc.). The account, however, does not allow participants to make decisions on these events independently.

Each of the committee members must send its vote in favor of the transfer of funds to or from the main chain. Committee members are voting via special Echo operations and these votes are collected in the special objects in the Echo database.

More than 2/3 of the votes collected is treated as a proof that some event happened on the main chain and can trigger a transaction to be sent back to the main chain. Hereinafter collecting of more than the threshold amount of votes will be referred as operation approved by committee.

Each of the committee members publishes its public data (Bitcoin public key and Ethereum address) on the network which are used later when constructing transfers on the main chain.

Members of the committee should be carefully selected. Since network development depends on the actions of the committee, all committee members should be interested in the successful development of the sidechain in particular and the project in general. One of the main factors here is the need for all committee members to keep a certain amount of Echo tokens staked in the system. Accordingly, any byzantine behavior on the network may result in slashing of staked Echo tokens.

Each active committee member must maintain the Echo blockchain and the Bitcoin/Ethereum blockchains (full node) in active and synchronized state. This means that the node of each active committee member oversees the main chain network and checks blocks for transactions that are affecting the sidechain.

Committee members do not manually create and send sidechain operations, they are generated automatically upon receiving signals from Echo blockchain or transactions from the main chain. Operations that are sent by members of the committee are free and sender-validated (i.e. only members of the committee can send these operations)

How Are They Chosen?

The committee members are not only responsible for ensuring the stable operation of the sidechain mechanism, but also have to sustain an up-to-date status of the committee itself. It is the committee members themselves who decide which of the participants should be added to the committee, or who should be excluded from it using Echo blockchain special operations.

Security Model

Any sidechain mechanism implies stability against the following three critical situations:

1. double waste of funds (on the main chain side or the sidechain side)
2. loss of access to funds (on the main chain side or the sidechain side)
3. ability of any committee members to make a sole decision and corrupt the state of the chain

The security of the Echo Sidechain with respect to the first point is based on two aspects:

1. To avoid possible main chain forks all blocks should be processed with reasonable lag, 12 blocks for the Bitcoin chain and 20 blocks for the Ethereum chain. Hereinafter we will refer to the transaction as confirmed in the main chain if it has received the above mentioned number of confirmations in the chain.
2. From the Echo side, this security is guaranteed by EchoRand, which reduces the probability of network forks to an extremely low level.

The second situation is covered with the ability to manually create transactions and transfer funds out of the address/account controlled by the committee and 24 hours delay in processing the deposits/withdrawals.

In addition to that sidechain it includes decreasing after some predefined time the number of signatures required to withdraw funds and ability to cancel the deposit transaction during 24 hours for the Bitcoin sidechain. For details please refer to corresponding sections.

Voting process covers the third possible vulnerability by not allowing any of the committee members to simulate non existent transactions on the main chain or to transfer funds out of the committee controlled account/address.

Bitcoin Sidechain

Echo BTC sidechain allows Echo account owners to exchange their BTC with the corresponding asset in the Echo network (eBTC). User operations on the Echo chain and transactions on the Bitcoin chain trigger the processes inside the sidechain which result in various Echo operations and Bitcoin transactions signed and sent by the committee members.

User operations

Initially, to enter funds the user needs to receive their "personal" unique address. Transfer of funds to this address will always result in freezing of funds on the BTC side and issuing the corresponding eBTC amount to the account on Echo's side.

To create an address, the user must call the `sidechain_btc_create_address_operation`. When it gets to the block, the operation provokes the nodes to generate a new Bitcoin address for the user.

The address script allows the input to be spent if the number of signatures is more than 2/3 of all active members of the committee, or by means of the user's backup address provided in the operation.

The latter guarantees the user who contributes to the sidechain the possibility of a refund in the event of an error in protocol operation and prevents the likelihood of unilateral blocking of funds (loss of funds). The user must specify the backup address upon creating a request for address generation.

Creating a replenishment address is free for the account's first call. All subsequent calls will result in error, except for the cases when the previous address becomes outdated (this is described below).

To transfer eBTC funds back to Bitcoin, the user needs to send `sidechain_btc_withdraw_operation` operation within the Echo network providing the address in the Bitcoin network and desired amount of Bitcoins to withdraw. The transfer operation is marked as pending and will be processed in 24 hours.

Committee member operations

After a user deposit address is created, it is added to the list of observed addresses. When the Bitcoins are transferred to the deposit address they are collected eventually on the sidechain main address (or SMA) which is a multisig address of Bitcoin, management of which is given to active members of the committee.

Upon receiving the withdrawal operation, each of committee members generate corresponding transactions to withdraw the Bitcoins to the specified withdrawal address.

Deposit and withdrawal flow are described in detail below.

BTC to eBTC conversion takes place in 3 stages:

1. After the transfer to the deposit address is confirmed on the Bitcoin chain and detected by the sidechain, each of the committee members creates and sends `sidechain_btc_create_intermediate_depos` with the transaction details to the Echo network.
2. 24 hours after the deposit operation is approved by committee, each of committee members creates the unique intermediate address script, creates a transaction from the deposit to the intermediate address, sign it and send `sidechain_btc_intermediate_deposit_operation` which contains the signature. After the operation is approved by the committee, a transaction is sent to the Bitcoin network. This transaction should have RBF flag enabled so if it gets stuck in the mempool the deposit owner will be able to send a replacement transaction with a higher fee and return his BTC to the backup address. Intermediate script provides ability similar to SMA script to reduce the number of required signatures during the time.
3. After the transaction is confirmed on the Bitcoin chain and received back by sidechain, each of committee members creates `sidechain_btc_deposit_operation` with transaction details, and after the operation is approved by committee, corresponding amount of eBTC-s are issued to the user account, `sidechain_issue_operation` is applied and the deposit is stored in the Echo database.

This flow allows the locking of funds in the intermediate address and guarantees that the SMA transaction will not fail because of the users' refund transaction sent earlier.

BTC to eBTC conversion takes place in 3 stages:

1. After the withdrawal operation is sent by the user it is stored in Echo database and specified amount of eBTC-s are withdrawn from the user's account.
2. In 24 hours this withdrawal becomes active and will be aggregated by the next aggregating transaction.
3. After the committee approves the fact that the aggregating transaction has received necessary confirmations on the Bitcoin blockchain, withdrawal is treated as confirmed and `sidechain_burn_operation` is applied.

Aggregating transaction

Aggregating transaction - a transaction on the Bitcoin network, the result of which is the combination of incoming inputs and the SMA balance. This transaction is also used to transfer withdrawn funds to user addresses. Every 4 hours the sidechain checks for deposits and withdrawals ready to be processed or any change in committee that can affect SMA address, creates a corresponding Bitcoin transaction, signs

it and sends the signature to the Echo node using `sidechain_btc_aggregate_operation`. After the operation is approved by the committee, the aggregating transaction is sent into the Bitcoin network.

The amount transferred to the SMA is the sum of the previous SMA balance and all funds received minus the transferred amount and the fee for the current transaction.

Please note that the input and output SMA can be different in case of changes in the committee as SMA script includes the committee Bitcoin public keys.

After the aggregating transaction is confirmed on the Bitcoin chain, each of committee members creates `sidechain_btc_approve_aggregate_operation` with transaction details.

The SMA address script includes a mechanism for reducing the threshold after a certain period of time. In the case when three months go by and the output has not been used up, only the signatures of more than half the committee will be needed to allow spending. After 6 months, more than a third of the votes will suffice. This is necessary to allow the recovery of funds even in the case when part of the committee loses its keys.

CPFP and unconfirmed transactions chain

CPFP mechanism will be used in the case that the SMA transaction gets stuck in the mempool due to a low transaction fee. Fee for subsequent SMA transactions in the virtual chain will be increased compared to the regular SMA transaction fee to increase the probability of the whole chain to be mined. SMA transactions virtual chain length will be limited to three SMA transactions due to the limit of the overall size of transactions in the virtual chain. Second transaction fee will be three times more than the one that got stuck, and the third SMA fee will be 8 times more.

Changes in the Committee

Changes to the list of committee addresses may occur in the following cases:

1. A new committee member is added to the list (`committee_member_activate_operation`);
2. A committee member is removed from the list (`committee_member_deactivate_operation`);
3. A committee member has changed his Bictoin address (`committee_member_update_operation`).

Since the committee addresses are part of the multi-signature addresses, all 3 of these cases must initiate the change of the SMA. The process of changing the SMA is implicit. This means that when you change the SMA, the transaction is not sent only because of the need to change the address. The address changes with the next aggregate transaction.

As the deposit addresses are also multi-signature addresses containing committee member's public keys, in the case of a change in committee all previously generated deposit addresses are marked as outdated and will no longer be returned when the user tries to receive his address. The user needs to generate a new deposit address. This operation once again becomes available for a one-time call.

Since after changing (replacing, adding or deleting) a single or several committee addresses, it is still possible to use the previously generated replenishment addresses, addresses marked as outdated continue to be processed by the committee. In the case when incoming funds to such address can no longer be

spent by the committee (it is not possible to reach the threshold), the address is marked as unsupported and removed from the list of observed addresses.

Fee payment

All fees below are specified in bytes, which are calculated based on transactions virtual sizes. Fees in satoshi and approximate fees in USD are provided in the table below.

	Deposit fee	Withdrawal fee	Minimum deposit	Minimum withdrawal
Bytes	1000	1000	10000	10000
Satoshi	12000	12000	120000	120000
USD(appox)	0.98	0.98	9.8	9.8

Satoshi per byte is defined to be equal to 12 initially, which will allow the transactions to be mined in the nearest blocks. All parameters (fees, minumums and satoshi per byte) are defined in the Echo config and can be increased or decreased by commiittee members.

Fee calculations Below are the calculations of the sizes of the transactions in the case of low activity, i.e. SMA transactions include only one deposit or one withdrawal. Resulting numbers shows that in such case there will be almost no profit, even some loss in the case of 19 committee members.

Committee member count	Deposit to intermediate	Intermediate to SMA	Total size for deposit	With-drawal	Total size
5	243	460	703	294	997
10	341	657	998	393	1391
15	421	890	1311	509	1820
19	492	1032	1524	581	2105

Decrease of fees Fees can be decreased in the future in case of activity growth. Fee calculations for more active deposit/withdrawals distibution provided below for the deposit fee 750 bytes and withdrawal fee 750 bytes.

Distribution	Deposit + withdrawal count	Profit/loss
10%	1	-3025
20%	2	-1340
40%	4	16160
20%	6	17500
10%	8	13460

Overall profit after 100 SMA aggregating transactions during 17 days will be 42755 bytes. All the possible profit remaining on the SMA address will allow to use CPFP or to update SMA address in case of

committee members update.

Bitcoin scripts

Deposit address script example for 15 committee members

```
OP_DUP OP_HASH160 <Backup Public Key Hash> OP_EQUAL
OP_IF
    OP_CHECKSIG
OP_ELSE
    OP_DROP 8 <PubKey ComMember 1> ... <PubKey ComMember 15>
        <Unique Hash> 16 CHECKMULTISIG
OP_ENDIF
```

Intermediate address and SMA script example for 15 committee members

```
IF
    <now + 6 month> CHECKLOCKTIMEVERIFY DROP
    6
ELSE
    IF
        <now + 3 month> CHECKLOCKTIMEVERIFY DROP
        8
    ELSE
        11
    ENDIF
ENDIF
<PubKey ComMember 1> ... <PubKey ComMember 15> <Unique Hash> 16 CHECKMULTISIG
```

Bitcoin node

Committee members should run Bitcoin full node in order to fully validate transactions and blocks and have the most up to date state of the chain. Recomended verision is 0.18+.

Ethereum Sidechain

Echo Ethereum sidechain allows Echo accounts owners to exchange their Ether and ERC20 tokens with the corresponding eETH asset or tokens on Echo network. A special smart contract is deployed into the Ethereum network by committee members which controls the deposited funds and tokens and provides an interface to manage them. The Ethereum sidechain tracks the events emitted by this contract and performs corresponding operations on the Echo side after the block where the transaction with the emitting call is located and confirmed on the Ethereum network.

In order to transfer ERC20 tokens from and to the Echo chain, ERC20 tokens should be registered in Echo network. Registration of the Ethereum ERC20 token deploys an ERC20 smart contract in Echo network and informs the sidechain to listen to the events of the connected ERC20 token on the Ethereum

side. When a token is transferred to a deposit address on the Ethereum chain, a corresponding amount of related tokens on the Echo side will be transferred to the user's account.

User operations for Ethereum

Initially, to enter funds, the user needs to receive their "personal" address, transfer of funds to which will always mean freezing of funds on the Ethereum side and issuing the corresponding amount of eETH to the account on Echo side.

To create an address, the user can send `sidechain_eth_create_address_operation` within the Echo network. This operation will trigger sending of the transaction which invokes the corresponding method of the smart contract on the Ethereum side. This method will create a deposit sub-contract and will emit an event with address of the newly created contract. After the address is approved by committee, it can be used for deposit.

To transfer eETH back to Ethereum, the user can send `sidechain_eth_withdraw_operation` within the Echo network by providing the address in the Ethereum network and desired amount of Ether to withdraw.

User operations for ERC20

In order to provide users the ability to use ERC20 tokens in the Echo network, the owner of the token in the Ethereum network should register the token on the Echo network using `sidechain_erc20_register_token_operation`, providing the address of the token already deployed in the Ethereum network. This operation will deploy an ERC20 token on the Echo side and fund its contract pool so the subsequent calls of the token smart contract will be free for committee members.

To create the ERC20 deposit address users should use the same `sidechain_eth_create_address_operation`. Transfer of the ERC20 tokens to this address will freeze them on the Ethereum side and eventually issue the corresponding amount of tokens on the Echo side to the user account.

To release tokens on Ethereum chain, the user needs to send the `sidechain_erc20_withdraw_token_operation` operation within the Echo network providing the address in the Ethereum network, address of the token, and desired amount of tokens to release.

Committee member operations for Etherum

The Ethereum sidechain listens to the events of the smart contract deployed in the Ethereum network. When the Ethers are transferred to the created address they are automatically transferred by the deposit sub-contract further to the main contract and the event is emitted by the main contract.

Upon receiving the withdrawal operation, each of the committee members generate a corresponding transaction to invoke the method of the main smart contract which will withdraw the Ethers to the specified withdrawal address after the operation is approved by committee on the contract side.

Deposit and withdrawal flow are described in detail below.

ETH to eETH conversion takes place in 3 stages:

1. When the event of new address creation is emitted by the main smart contract, each of the committee members receives this event and sends `sidechain_eth_approve_address_operation` into the Echo network. After the address is approved by the committee it is added to the list of observed addresses.
2. When the deposit is transferred to the created address and the transfer event is emitted by the main smart contract, each of the committee members creates and sends `sidechain_eth_deposit_operation` into the Echo network with the transaction details.
3. In 24 hours each of the committee members creates and sends `sidechain_eth_send_deposit_operation` which approves the deposit.
4. After the operation is approved by committee, eETH-s are issued to the user account and `sidechain_issue_operation` is applied.

eETH to ETH conversion takes place in 4 stages:

1. Withdrawal operation is withdrawing the eETH-s from the users account and is creating pending withdrawal object in the Echo chain.
2. 24 hours after the withdrawal operation is sent by the user, each committee member is sending `sidechain_eth_send_withdraw_operation`. After the operation is approved, each committee member is sending transaction into Ethereum network by invoking the withdraw method of the main smart contract.
3. After the withdrawal is approved on the smart contract side, the Ethers are transferred to the specified account and the appropriate event is emitted.
4. Each committee member sends `sidechain_eth_approve_withdraw_operation` into the Echo network after receiving this event.
5. After the operation is approved by committee, the withdrawal is marked as processed and `sidechain_burn_operation` is applied.

Committee member operations for ERC20

After the ERC20 token is registered in the Echo network, the Ethereum sidechain starts to listen to the events of the ERC20 smart contract in the Ethereum network. When the transfer event is emitted and the destination address is one of the addresses created by the Echo node, the corresponding amount of related tokens are transferred to the account that is linked to that address.

Upon receiving the ERC20 withdrawal operation, each of the committee members generate corresponding transactions to withdraw the Ethers to the specified withdrawal address.

Deposit and withdrawal flow are described in detail below.

ERC20 token transfer to Echo takes place in 2 stages:

1. After the transfer event is emitted by the ERC20 contract, each of the committee members creates and sends `sidechain_erc20_deposit_token_operation` into the Echo network with the transaction details, token info and amount.
2. In 24 hours each of the committee members creates and sends `sidechain_erc20_send_deposit_token_oper` which approves the deposit.
3. After the operation is approved by the committee, ERC20 tokens are issued to the user account on the Echo network using `sidechain_erc20_issue_operation`.

ERC20 token transfer to Ethereum chain takes place in 4 stages:

1. When the ERC20 token withdrawal operation is received, the specified amount of tokens are withdrawn from the user's account and pending ERC20 withdrawal object is created in the Echo chain
2. 24 hours after the ERC20 withdrawal operation is sent by the user, each committee member is sending `sidechain_erc20_send_withdraw_token_operation`. After the operation is approved, each committee member is sending transaction into Ethereum network by invoking the ERC20 withdraw method of the main smart contract.
3. After the withdrawal operation is approved on the smart contract side, the tokens are transferred to the specified account and appropriate event is emitted.
4. Each of committee members sends `sidechain_erc20_approve_token_withdraw_operation` into the Echo network after receiving this event.
5. After the operation is approved by the committee, the token withdrawal is marked as processed and tokens are burned by `sidechain_erc20_burn_operation`.

Changes in the Committee

Changes to the list of committee addresses may occur in the following cases:

1. A new committee member is added to the list (`committee_member_activate_operation`);
2. A committee member is removed from the list (`committee_member_deactivate_operation`);
3. A committee member has changed his Bictoin address (`committee_member_update_operation`).

Since the committee addresses are stored in the main smart contract deployed on the Ethereum network, all 3 of these cases must initiate the update of these addresses on the contract side. The smart contract provides the interface for updating the list of addresses of the committee members. During such change each of the committee members send a transaction to the Ethereum network which invokes the update function of the smart contract. After the operation is approved on the main smart contract side, the list of committee members is updated in the contract.

Fee payment

Committee members pay all fees connected with smart contract calls on the Ethereum chain. The gas price is defined in the Echo blockchain config. Fees related to the ERC20 smart contract calls on the Echo side are covered by the fee pool of the contract.

Further Development

Further development of the Sidechain has two main vectors:

1. Quality and stability - further development of the current protocol to ensure a higher quality of implementation;
2. Security and Privacy - Expanding and Improving the Protocol to enhance Security and for the full guarantee of withdrawal of funds.

Taproot and Schnorr Signatures Integration

In addition to the functionality provided by the Echo protocol, we are also responsible for ensuring the smooth operation of the mechanism from Bitcoin's side. We understand that in the case of the high popularity of transfers between Bitcoin and Echo, the load on the Bitcoin network will also increase. This is because each aggregation transaction includes the signatures of the committee and RedeemScript, which both have their own size and will be included in the chain, therefore increasing the block size and blockchain in general.

Further development of Bitcoin Core, namely the integration of Taproot and Schnorr Signatures into the protocol, will allow us to solve this problem.

As you can see above, the current script for generating both the replenishment address and the SMA is quite complex and large in size, since at least 15 signatures must be included. Using Schnorr Signatures, this implementation will be changed. Instead of publishing all public keys of the committee, the new implementation will have only one threshold public key used (based on the public keys of the committee members).

In turn, the implementation of Taproot eliminates the need to include the full RedeemScript in each aggregate transaction, which also has a positive effect on its size.

In addition, the latter allows changing the approach to the mechanism of adding a backup address and to provide an opportunity of not disclosing the backup address each time the deposit is spent.

Refund from the Reserve Pool

ECHO tokens, transferred by the committee as a deposit when applying for the role of a committee member, form a reserve pool for refunds in case of force majeure situations. These situations are resolved by voting, where the following user roles are involved:

- ECHO-holder;
- eBTC-holder;
- Committee member.

Each of these has its voting weight depending on the role. An account can have several roles, but a vote can be cast only under one role. This role is defined by the protocol as a role with the largest voting weight for this account.

Collateralized Debt Position Addresses

Another vector of protocol development is the integration of the Collateralized Debt Position Addresses (CDPA) mechanism. The purpose of this mechanism is to provide the user with the ability to enter BTC into Echo without losing the ability to manage BTC on the Bitcoin side.

Its implementation entails the following approach:

The user blocks a certain amount of ECHO on the Echo CDPA. This amount determines the limit of the entered BTC. Entering BTC into this type of address does not lead to aggregation of funds, but freezes the funds on the Bitcoin address.

The script for this type of address, as well as other replenishment addresses, enables, in addition to spending funds through a multisignature address, the ability to spend funds using only the backup address, without the need of collecting signatures from the committee. This means that throughout the entire period of using the funds on the basis of the collateral, the user has the opportunity to transfer BTC to another address at any time without the fear of losing funds.

The user can send an ECHO funds transfer request at any time. To do this, he must have an eBTC amount on the account corresponding to the initial input, which will be burned when ECHO is released and the BTC is transferred from the CDPA to the output address previously specified by the user.

If the user utilizes their out on the BTC side and spends its funds, on the Echo side the collateral ECHO is put up for sale at a more favorable rate than the market rate (the stock of the rate is provided at the stage of calculating the deposit limit). The BTC gained from the sale of ECHO is burned, therefore stabilizing the overall Sidechain balance.

The mechanism for issuing collateral for sale will also be used in cases when the transferred from Echo amount of BTC exceeds the unsecured balance. It will also be used in case of the high volatility of the BTC or ECHO rate.