Elastos Sidechain White Paper

Blockchain Driver Smart Web

Elastos Foundation

March 25th, 2017

Summary

This document is V0.3 of the Elastos Sidechain White Paper, which focuses on the Elastos Sidechain technology solution. In the future, we will continue to upgrade this document to reflect the latest development status of Elastos.

Copyright Notice

Table of Contents

Summary 2
Copyright Notice 2
1 Overview 4
2 Transfer between Main Chain and Sidechains 5
2.1 Transfer from Main Chain to Sidechain 5
2.2 Transfer from Sidechain to Main Chain 6
2.3 Arbitrator 7
3 POW-based Sidechain 8
4 DPOS-based Sidechain 9
5 Friend Chain 10
References 11
Contact Us 12

1. Overview

To reduce the pressure on the main chain and provide a better experience for DAPP, Elastos adopts a main chain + sidechain hierarchical structure. The main chain is only responsible for the circulation of ELA. DAPP runs on the side chain, and through the Elastos side chain transfer mechanism, the secure transfer of value between the main chain and the side chain is completed.

The Elastos main chain uses the arbitrator's joint signature and SPV (Simplified Payment Verification) mechanism to guarantee the security of the transfer with the sidechain, and the main chain token holders jointly elect a certain number of “arbitrators.” The arbitrator is responsible for signing the token withdrawals from the side chain to the main chain. Most of the arbitrator signatures can unlock on the main chain a “token withdrawal” transfer from the representative side chain’s account to the ordinary account. SPV ensures the security of recharging operations from the main chain to the side chain. Each side chain node synchronizes all of the block headers of the main chain. Along with the merkle proof path and transaction information, a decentralized consensus can be completed on the transfer transaction with the help of a data structure and algorithm.

The Elastos sidechain can use any consensus mechanism. At present, the Elastos team has already developed a POW consensus based sidechain that can connect with the main chain to complete SPV and DPOS based deposit and withdrawal operations. This POW-based sidechain can use the computing power of the main chain to protect its own security. The right to use the main chain's computing power is passed to the "arbitrator" elected by the DPOS-based consensus. Each arbitrator takes turns doing block packing for the sidechain.

Through cross-chain technology, Elastos is now able to complete mutual transfers with other blockchain systems which issue their own token. This kind of blockchain, which can transfer funds with Elastos, is called a “friend chain.”

2. Transfer between the Main Chain and Sidechains

The key to the side chain technology is being able to solve the transfer problem between the main chain and the side chain, and it is necessary to have a mechanism to ensure that the transfer between these two is safe and reliable. For this reason, Adam Back, et al. published the famous white paper on side chains, and proposed a technique called Two-Way Peg to solve the problem of asset transfer between two chains. The basic principle is to use SPV-based mutual verification to confirm the transaction exists on the other chain, but there is a premise, which is that all of the other party's block header information must be saved. There is a one-to-many relationship between the Elastos main chain and side chain. Using symmetric bidirectional anchoring, it is not a problem if the side chain saves just one copy of the main chain's entire block header information. However, the main chain may not save all of the side chain's block header information, so it is not possible to use symmetrical SPV-based bidirectional anchoring on the mainchain-sidechain architecture of Elastos.

Elastos adopts different mechanisms to ensure the transfer of funds in both directions between the main chain and the side chain.

2.1 Transfer from Main Chain to Sidechain

Elastos main chain to side chain transfers are implemented based on SPV. The SPV module of the main chain needs to be integrated on the side chain. This module is used to synchronize the main chain block and the transfers from the main chain to the side chain at any time. The transfer process is as follows:

1. The user transfers n ELAs from the main chain address U to the representative side chain on the main chain address S through the wallet and attaches his own address u in the side chain to the transaction and sends it to the main chain. This transaction is marked as tx1.
2. The main chain's miner node packages tx1 and successfully generates a block.
3. After waiting for sufficient confirmations, the node of the arbitrator-on-duty A obtains the main chain transfer transaction through its SPV module. From the transaction tx1, it obtains the transfer address u, and constructs the send token transaction tx2 whose receiver address is u. The number of tokens sent is equal to that of the tx1 U to S transfer number. tx2 carries both the SPV proof path and tx1.
4. The node of the arbitrator-on-duty A sends tx2 to the side chain node.
5. The side chain packages tx2 and generates a block.
6. After waiting for sufficient confirmations, the user will see in his wallet that his own side chain address u has accepted n STokens into his account.

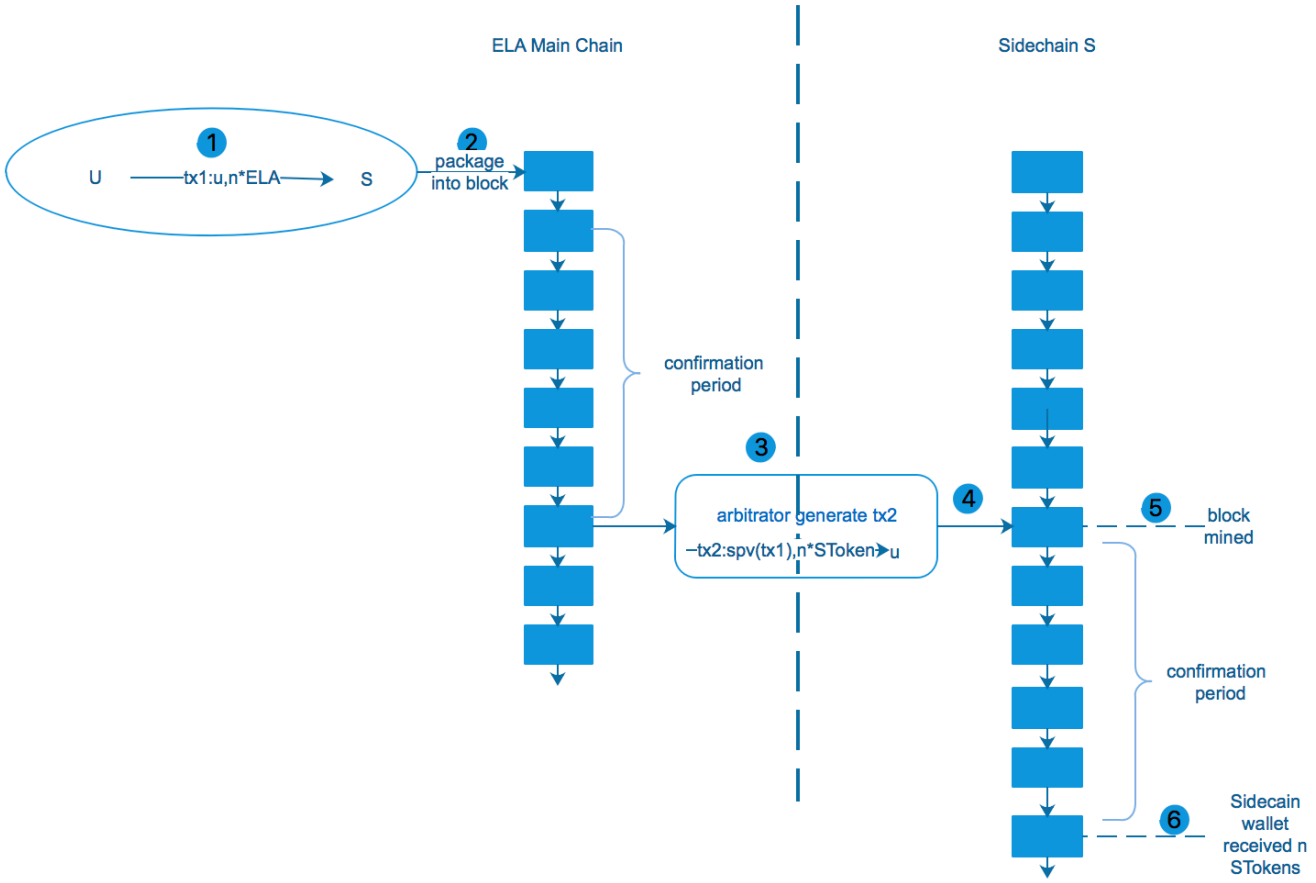

Figure 1: Transfer from Main Chain to Sidechain

2.2 Transfer from Sidechain to Main Chain

The security of an Elastos side chain to main chain transfer is guaranteed by the main chain's arbitrator mechanism. The transfer process is as follows:

1. The user sends a request from his wallet on the side chain from address u to withdraw m SToken, and on the transaction attaches his address U on the main chain, then sends it to the side chain. This transaction is marked as tx3.
2. The side chain miner node packages the transaction that includes tx3 and generates the block.
3. After waiting for sufficient confirmations, the node of the arbitrator-on-duty A gets tx3 from its own side chain node.
4. The node of arbitrator-on-duty A constructs a main chain tx4 transaction based on tx3. Tx4 transfers m ELA from S to U. After that A broadcasts this transaction to all arbitrator nodes for signature.
5. Once the node of arbitrator-on-duty A receives over two-thirds of the arbitrator signatures, it submits tx4 to the main chain with all received signatures.
6. Miners generates a block which includes tx4.`

7. After waiting for sufficient confirmations, the user will see in his wallet that his own main chain address U has accepted m ELAs in his account.

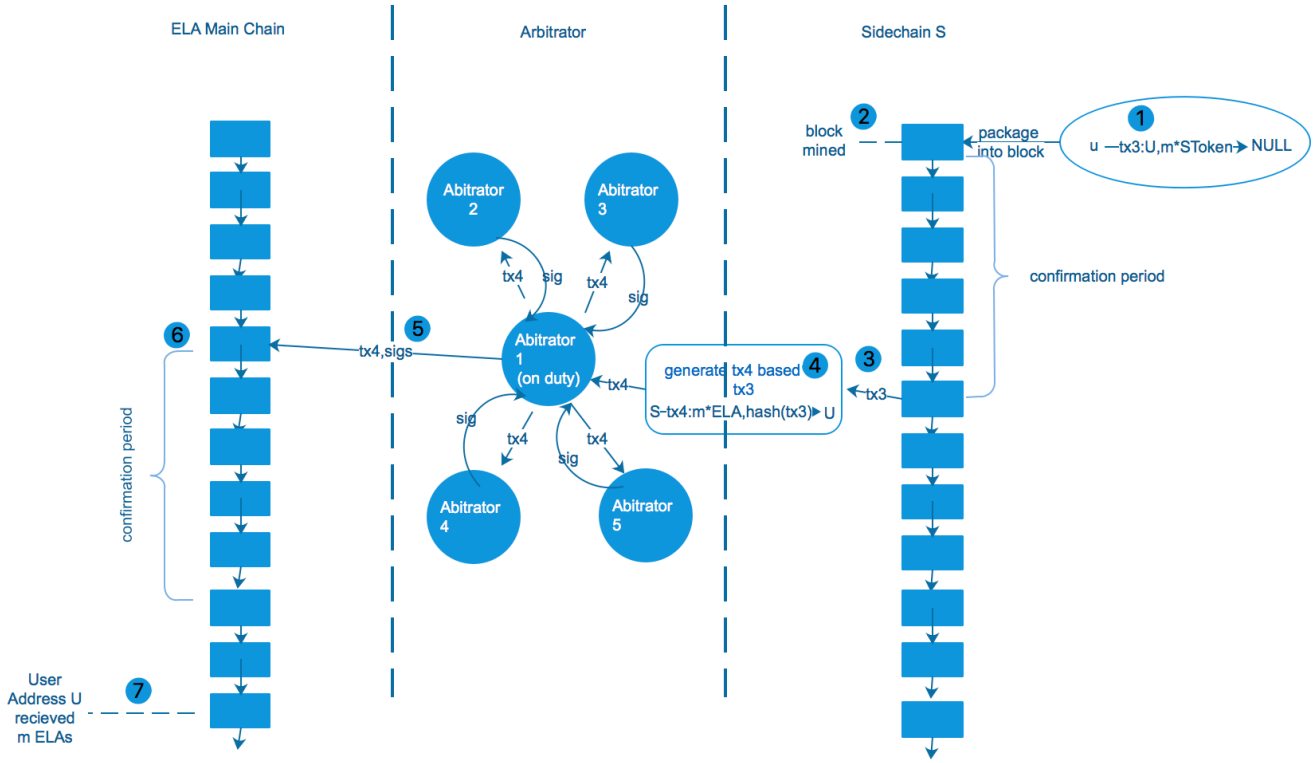

Figure 2: Transfer from Sidechain to Main Chain

2.3 Arbitrator

The above transfer process involves the arbitrator. During the main chain to the side chain transfer process, the role of the arbitrator is to generate and transfer the transaction to the side chain without participating in the signature; during the side chain to main chain transfer process, the arbitrator must not only generate and transfer the transaction, but also sign the transaction, which allows the "withdrawal transactions" on the main chain, transfer from the account representing the side chain to the ordinary account, to be verified by each main chain node.

The arbitrators are elected by voting on the main chain and rotate regularly. Each arbitrator needs to provide enough computing and network resources to be able to run at least one main chain node and N nodes corresponding to N side chains. The arbitrator's revenue comes from the transaction fees obtained for packing blocks for the side chains.

3. POW-Based Sidechain

Elastos provides POW-based sidechain implementation. Using this implementation, you can easily build a sidechain to develop DAPP applications.

This POW-based side chain uses the merged mining method with the Elastos main chain to obtain computing power. The main chain's current arbitrator-on-duty acts as the miner to package the transaction of the side chain and generate the mining transaction on the main chain. Then through the merged mining method with Bitcoin, according to the principle of merged mining, the Proof of Power is then also transmitted to the side chain, and any of the side chain's full nodes can verify the validity of the block in accordance with the Proof of Power.

All the main chain arbitrators, in an arbitrator election cycle, will perform corresponding duties in turn as "arbitrators-on-duty of generating side-chain blocks" in rotating order. This includes the responsibility of generating blocks for the side chain. A rotation switch is triggered by generating a block on a side chain. Each arbitrator generates a block on one side chain in turn, and the rotation sequence is determined by the result of the previous round of voting. The block generation behavior is ultimately reflected in the mining transaction posted to the main chain. Each main chain node will do a consensus process about whether the mining transaction is legal. One of the main verifications is whether the signer who issued the mining transaction had the right as an arbitrator to generate a block.

The proceeds from the side chain (only transaction fee, no token generating) are still allocated to the miners and the foundation. The miners here are the arbitrators who are currently generating "mining transactions" on the main chain. Of course, this mining transaction that is placed on the main chain must also pay a miner's fee. This miner's fee is paid to the Bitcoin miners who are providing real computing power.

In the above-mentioned model of side chain merged mining, the safety of side chains is guaranteed by both the election trust of the main chain, and the computing power provided by the merged mining, which completes the transfer of trust from the main chain to the side chain. The POW consensus strategy used in the side chain is simple and reliable. The transaction history will not be tampered with on the side chain due to some evil parties. Side chains can also be mined not through the main chain, but the miners must compete with the main chain's merged mining computing power. Therefore, when the POW rules are followed, the main chain will provide sufficient security for the side chains.

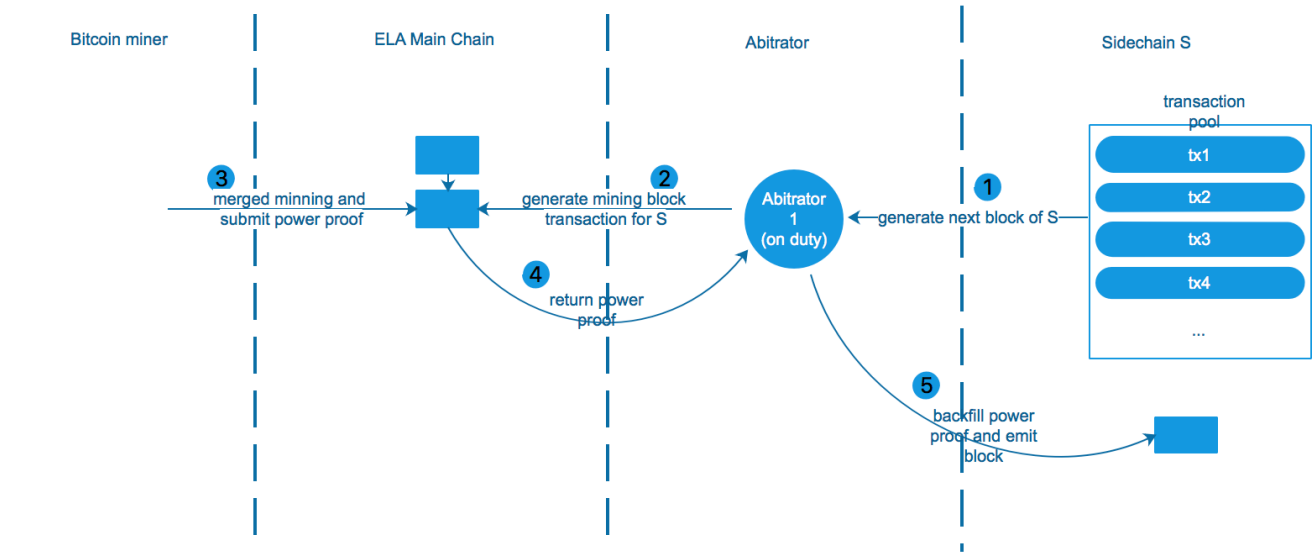

Figure 3: Process of ELA Sidechain merged mining

4. DPOS-Based Sidechain

Elastos is also planning to develop a DPOS consensus-based side chain. The arbitrator of the main chain represents the agent role of DPOS consensus on the side chain. This is still equivalent to guaranteeing the security of the side chain through the main chain, but it reduces the mining process, and allows for faster block generation speed. Each node on the side chain can obtain the main chain's voting information through the attached main chain SPV module, thus allowing for consensus on the legality of the arbitrator.

5. Friend Chain

The concept of sidechain comes from Bitcoin. In this scenario, the side chain does not have its own token. A chain with its own token has an independent economic system. The transfer between Elastos and this own token chain needs to be based on the current two token's market exchange rate to go forward. This chain with its own token is called a "friend chain".

Elastos support for friendchain is separated into a two-stage process: the first stage supports the cross-chain atomic transaction between the friend chain and the Elastos main chain. This type of transaction is peer-to-peer. It requires the parties to negotiate exchange rates and create mutual, constrained atomic exchange transactions; the second phase will be based on decentralized exchanges, supporting the free exchange of the main chain and friend chain tokens. Users will no longer need to create exchange transactions from user to user.

The first phase of atomic trading will be achieved by means of a hash lock. A specific example is used to describe the exchange process below.

Assume there is a friend chain F, with its own token FToken. Alice and Bob need to exchange ELA and FToken between the Elastos public chain (here represented by E) and chain F. Alice has addresses EA and FA on chain E and chain F, respectively. Bob has addresses EB and FB on chain E and chain F, respectively. Assuming a market exchange rate of 1:10 currently (1 ELA exchanges 10 FTokens), Alice wants to exchange 10 ELA for 100 FTokens with Bob.

1. Alice initiates a special transfer transaction tx1 from EA to FA on chain E. The transfer amount is 10 ELAs. The unlock condition of this transaction is the signature generated by EB's private key, along with an additional hash lock. Alice generates a random number x, which gets a hash(x) for x, and is placed in this transaction. Bob needs to submit x to unlock the hash lock.
2. Bob sees tx1 on chain E, constructs another special transaction tx2 on chain F, transfers 100 FTokens from FB to FA. The conditions to unlock this transaction is the signature generated by FA's private key, along with a hash lock, which is also hash(x). It is also required to provide x as an unlock condition.
3. Alice provides the tx2 signature on chain F, along with x to unlock tx2, transferring 100 FTokens to his own separate address on chain F.
4. Bob sees tx2 is unlocked and gets x. Then Bob signs tx1 with EB's private key and provides x, unlocks tx1, and transfers 10 ELAs to his own separate address on chain E.

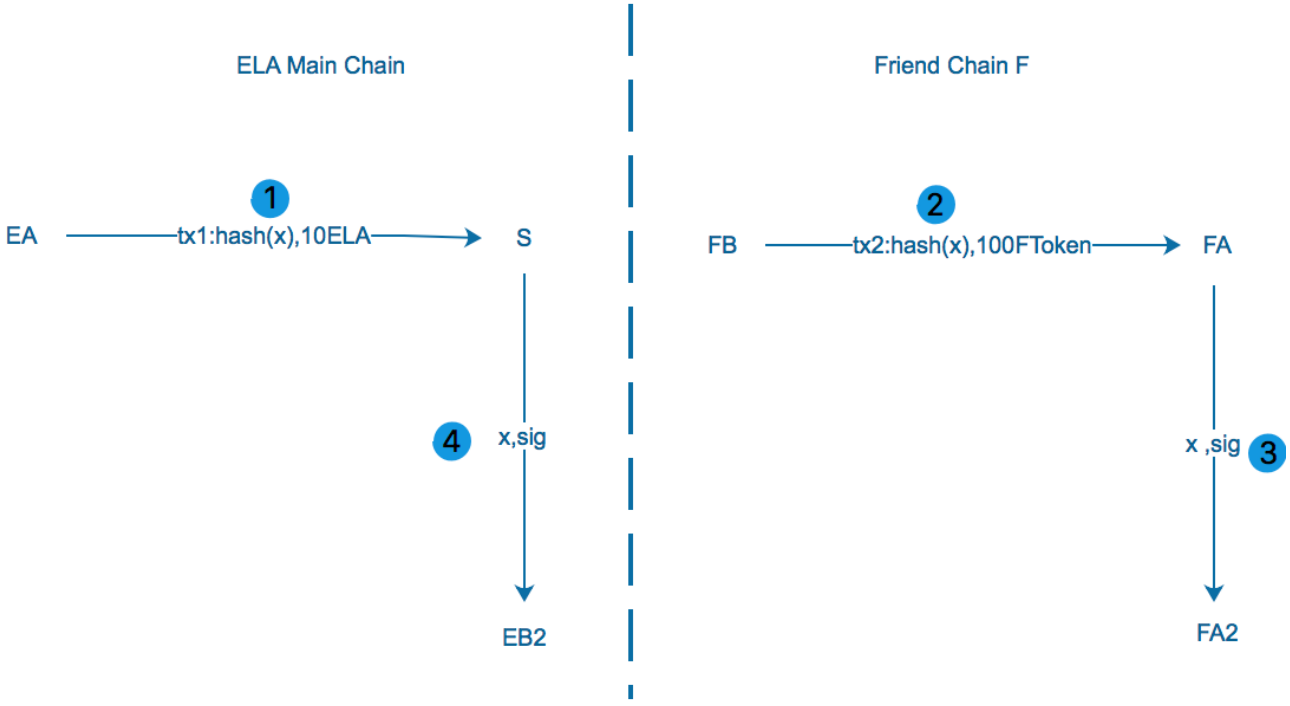

Figure 4: Exchange process between ELA Main Chain and Friend Chain

References

[1] Adam Back. Enabling Blockchain Innovations with Pegged Sidechains .https://blockstream.com/technology/sidechains.pdf， 2014-10-22

[2] Andreas M. Antonopoulos.《精通比特币（第二版）》 http://book.8btc.com/masterbitcoin2cn

[3] 周邺飞. 区块链核心技术演进之路－挖矿演进. http://www.8btc.com/blockchain-tech-mining， 2016-11-08

[4] Joseph Poon. The Bitcoin Lightning Network:Scalable O -Chain Instant Payments.https://lightning.network/lightning-network-paper.pdf， 2016-01-14

[5] bitcoin wiki. Merged mining specification. https://en.bitcoin.it/wiki/Merged_mining_specification, 2015-08-08.

Contact Us

Elastos (Shanghai):

Shanghai, Hongkou District, Tang

11th Floor Huahong International Building, 463 Tanggu Road, Hongkou District, Shanghai

Zip Code: 200080

Elastos (Beijing):

Plug & Play, Block G, Zhongguancun Zhizhi Street, 45 Chengfu Road, Haidian District, Beijing

Zip Code: 100084

Email:

Whitepaper Group: whitepaper@elastos.org

Global Community: global-community@elastos.org

Elastos Fund: elastos-fund@elastos.org

PR: pr@elastos.org

Investor Relations: ir@elastos.org

Elastos Council: elastos-council@elastos.org

Other Contact: contact@elastos.org

Elastos Website: http://www.elastos.org