OPINION

Op Ed: The Value of Sidechains and Leveraging Their Potential

Since Bitcoin's launch in 2009, there has been a growing interest in tapping the potential of decentralized cryptocurrencies. However, any modifications to the consensus layer, the critical part of any cryptocurrency, must be handled with caution. Compared to other internet protocols, this makes it harder for Bitcoin to adopt new features and meet new demands. This is why sidechain technology has been proposed: It allows for the transfer of digital assets, including bitcoin, across different blockchains.

by Jeason Yi

While most cryptocurrencies are incompatible, assets are not interchangeable; “fusion” lets sidechains build the financial ecosystem of cryptocurrencies. Using sidechains, we can easily create smart contract-based stocks, futures and other derivatives; there could be thousands of sidechains pegged to Bitcoin, all serving different purposes and having different features. Meanwhile, all of these sidechains benefit from the robustness, and maintain the coin scarcity, of the main chain.

So far, some of the sidechain solutions on the market include BTC Relay by ConsenSys, Rootstock by RSK, Elements by Blockstream and non-Bitcoin sidechains like Lisk.

BTC Relay

BTC Relay, born from the Ethereum Foundation and developed by ConsenSys, is believed to be the first functional sidechain project — although it’s technically perhaps better described as an “atomic swap.” The main principle of BTC Relay is that it connects the Ethereum network with the Bitcoin network in a safe and decentralized way.

BTC Relay allows users to verify Bitcoin transactions through smart contracts deployed on the Ethereum blockchain. As such, the sidechain mechanism allows user to send transactions, not only to another address or account, but also to other blockchains.

Specifically, BTC Relay uses Bitcoin’s block header to create a tiny version of the Bitcoin blockchain. Ethereum Dapp developers can then verify the Bitcoin network activity by connecting to the BTC Relay smart contract. (It does so through a dedicated API.)

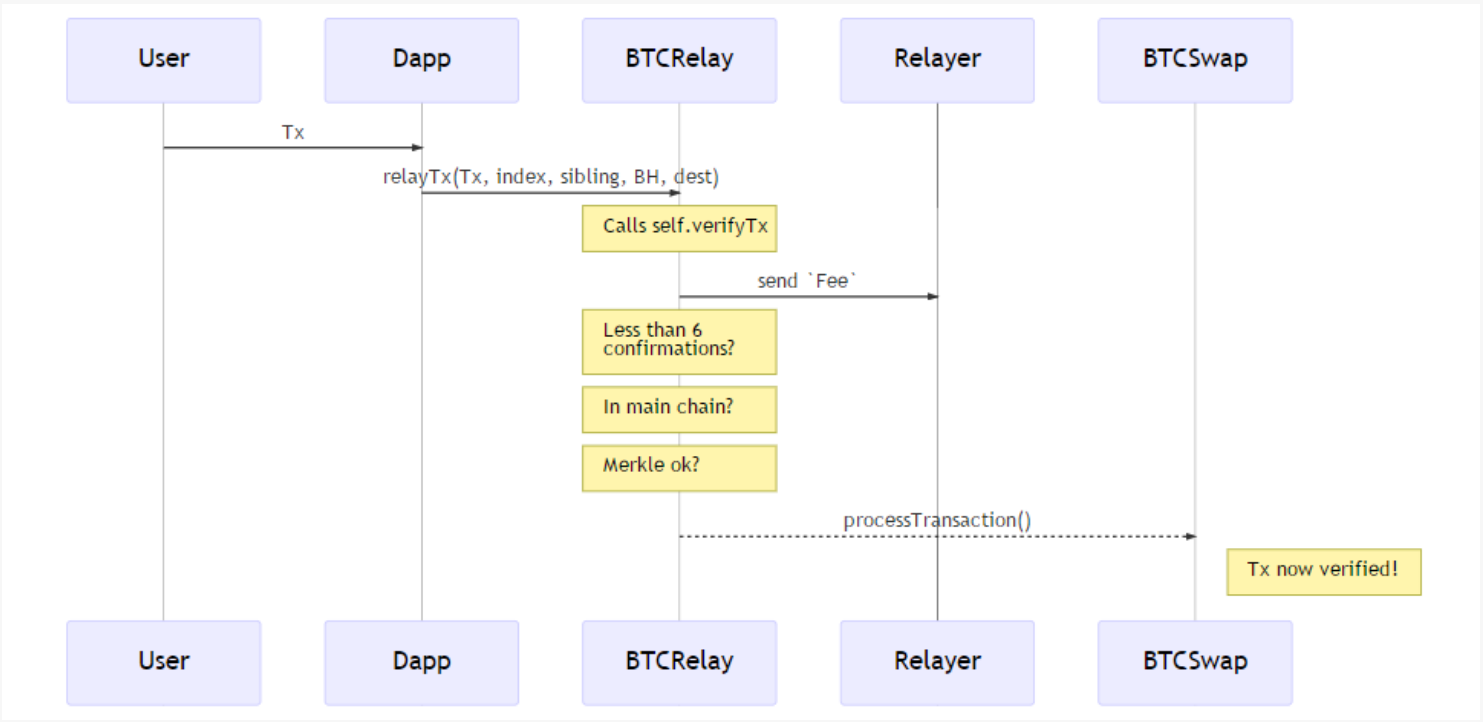
As a result, a typical use case of BTC Relay could look like this:

1. Alice and Bob agree to use the BTCSwap contract (user contract) to trade. Alice wants to buy ETH from Bob. Bob sends his ETH to the BTCSwap contract and the ETH will be locked.

2. Alice then sends BTC to Bob, and — importantly — she wants the BTCSwap contract to be informed so that the BTCSwap contract can release Bob's ETH deposit to her.

3. Alice calls the BTC Relay function using the Bitcoin transaction and the BTCSwap contract address. After the BTCRelay function has confirmed that the bitcoin transaction is valid, the BTCSwap contract will be triggered and will verify the Bitcoin transaction.

4. After the BTCSwap confirms the legitimacy of the BTC Relay address, Bob’s ETH will be released to Alice and the transaction is completed.



Rootstock

Rootstock (or RSK) is the first universal smart contract platform secured by the Bitcoin blockchain. Its goal is to implement complex smart contracts on a sidechain, adding value and functionality to the Bitcoin network.

The way this works is that when a Bitcoin user wants to use two-way anchors, he sends a transaction to a multi-signature address. The key holders of this wallet, the "federation," can (for example) consist of several well-known companies.

The RSK blockchain uses the public key associated with the funding transaction to store the smart bitcoin (SBTC). This means that the private key that controls the bitcoins in this transaction can be used to control a corresponding amount on the RSK blockchain.

Although the public key and the private keys are similar, each blockchain uses a different format to encode addresses. This means that the addresses on the two blockchains are different.

Elements

The Elements sidechain is an open-source sidechain project developed by Blockstream. Like Rootstock, the project adopts two-way pegging to Bitcoin. In addition to smart contracts, the project also introduces many other innovative features, including private transactions, Segregated Witness and new instruction code to support more functions, among others.

Lisk

Lisk is a new generation of blockchain platform that adds each application to a separate sidechain of Lisk.

Users who have experienced Bitcoin and Ethereum are probably aware that features and data are added to the main blockchain, which leads to rapid blockchain bloat. Extra large block sizes require a long time to synchronize, which is a painful experience.

Lisk's sidechain model instead provides a way to solve the problem of network congestion under high transaction volume. Users just need to download the corresponding sidechain for a specific use case when using the relevant application. This greatly reduces the sync time for downloading unnecessary data and facilitates the efficient operation of the entire Lisk network. Also, the speed of the Lisk network promises to continue to accelerate over time, which ought to give it a special advantage.

A Model of the Bytom Sidechain

Bytom is an inter-operational protocol for multiple “byte assets.”

In order to operate different on-chain assets running on Bytom, developers can create a tiny version of a sidechain. Let’s use, for example, one version called “XRelay,” which functions similar to BTC Relay. Dapp developers can then connect to the API of XRelay via a smart contract to verify the network activities of “X Chain,” the alternative blockchain XRelay connects with. In this way, cross-chain communication can complete transactional and dividend distribution contained within the contract.

Bytom will support multiple types of digital assets (for example, gold, silver, etc). Each asset will be identified by an asset ID, which will be based on the “ODIN” protocol. With various asset IDs, we can confirm the categories of that asset.

The Bytom chain sorts all assets into two categories: the Bytom token (BTM) and all other digital assets. BTM is the native currency of the Bytom blockchain, which is a

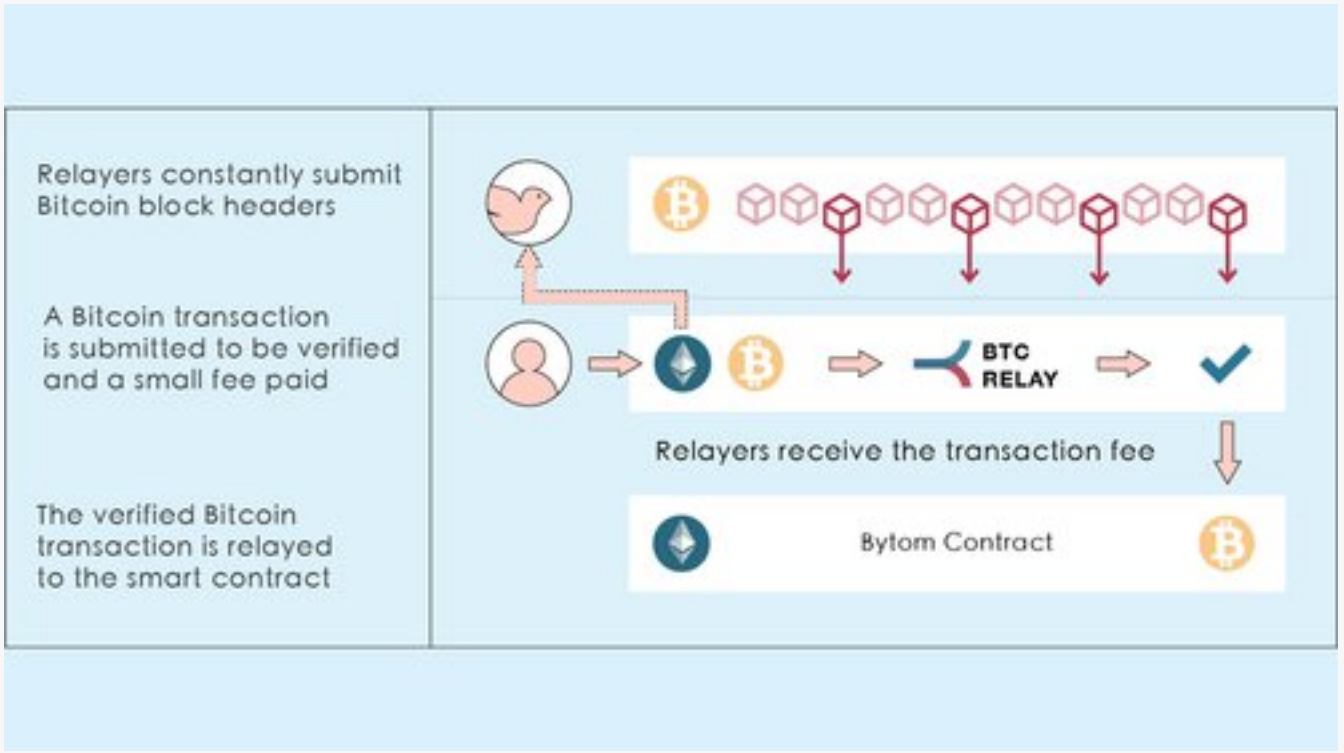
special token distributed to miners and other participants in the ecosystem. BTM is based on a Proof-of-Work mechanism to encourage miners to join in the system in a random and anonymous way.

The BTM could be used for

1. Costs of asset transactions, including the cost of running the smart contract;
2. Dividends of income assets; and
3. Deposits for asset issuance.

If the asset issuer, for example, decides to use BTC as dividends, he can lock in the corresponding amount of BTC via a sidechain and convert it into BTM at market rate. This process is executed by the type of Relay contract described through a cross-chain operation.

For example, if we want to swap BTM with Bitcoin, we can do it using a Bytom chain contract like this:



Sidechain technology is appropriate for the mission of Bytom: to build a market where “byte assets” and assets on different blockchains can interact and be exchanged freely. Bytom will facilitate the exchange, interoperation and flow of

byte information and byte assets that are stores of value.

Jeason Yi, author of this guest post, is senior engineer of Bytom.io. He has been in blockchain development since 2013. The views expressed are those of Mr. YI and do not necessarily reflect those of Bitcoin Magazine or BTC Media.

Jeason Yi

Guest Contributor

Jeason Yi is senior engineer of Bytom.io. and holds a Master's degree in Software Engineering from the University of Science and Technology of China. He has worked at the Asia-Pacific R&D Center studying Linux and joined 8btc in 2016 in the area of blockchain development. He is one of the writers of *A Guidebook for Blockchain Development*.

Jul 13, 2017 10:51 AM EST

RELATED ARTICLES:

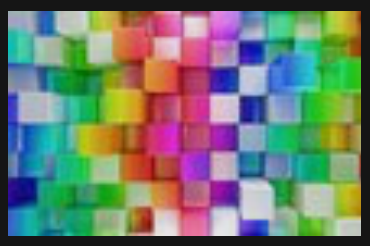
Op Ed: Why Connecting All the Blockchains Is the Final Step for Mass

by Dr. Julian Hosp

Op Ed: The Future Is

Op Ed: The Future is Bright — for 3 Out of 4 Blockchain-Based

by Jeremy Epstein



Op Ed: New Study Finds That 3 Million+ People Use Cryptocurrencies

by Kayla Matthews

Newsletter

The biggest stories in bitcoin delivered weekly
to your inbox

email

Subscribe

Store

Call for Writers

We are always looking for talented writers to join our team. If you have an article you'd like to have published to our audience please reach out to

editor@bitcoinmagazine.com


BTC