EZ-Pay - Full Node vs. SPV Wallets

Author	josh
Date	2018-12-16 13:44:28

Overview

When discussing digital currencies, the question is often asked "where is the 'money' actually stored?" In the world of fiat currency (US dollars, Euros, etc.), cash stored in your physical wallet is the money. You give a $20 bill to a cashier, and they now have $20. With cryptocurrencies like Bitcoin, the actual currency is stored on a completely public, open ledger called the blockchain. The blockchain stores a *complete* record of every transfer between individuals in the history of Bitcoin's existence, so a Bitcoin wallet can easily verify that you own some amount of currency and can send it to another person.

However, there's a bit of a problem with this. The Bitcoin blockchain contains a record of every single transaction ever recorded, now over ten years of history. The blockchain is HUGE in terms of storage space - nearly 200 gigabytes these days. What if we don't have that kind of space on our computer? What if we want to have a digital currency wallet on our phone or another capacity-limited device? Fortunately, there's a type of wallet called an SPV wallet that fixes this problem. Let's discuss the difference between full node and SPV technology.

Full Node vs. SPV

The Full (Node) Experience

The most full wallet experience is using what is called a *full node*. The strategy use by a full node wallet is very simple: the entire blockchain containing all transactions is downloaded to the machine running the wallet software.

Because the full blockchain is available to the wallet, verifying ownership of the user's funds is simple. The wallet software looks at the blockchain ledger and traces the ownership of the currency back to the very beginning of Bitcoin. The blockchain is well secured by cryptography and proof of work, making it near impossible to forge any of these transfers. So, by storing the full blockchain, the wallet software can verify that all the previous transfers of Bitcoin leading up to the transfer to the current owner are valid and considered indisputable history. If your wallet can independently verify the blockchains transactions, it knows for sure that your Bitcoin is truly yours.

Wallets on a diet - Simplified Payment Verification or SPV

As we discussed, however, it can be problematic to download and store the entire blockchain for a wallet in many cases. What if a user with a small laptop, a mobile phone, or other limited-capacity device wants to participate on the Bitcoin network? A user may have limited storage capacity, or may also have limited bandwith for downloading the very large blockchain. But if we can't download the blockchain, how can we independently verify that the Bitcoin in our wallet is actually ours?

Satoshi Nakamoto, the inventor of Bitcoin, brilliantly solved this problem by developing a technology called Simplified Payment Verification, or SPV. These wallets use some neat cryptographic tricks to avoid downloading the whole blockchain, at the expense of a minimal amount of trust required to verify currency ownership.

So how do SPV wallets work? When an SPV node needs to verify ownership of a user's funds (in order to create a new transaction where they send money to someone else), the node makes special requests to full nodes it can find on the network. Instead of asking for the whole blockchain, it only asks for specific bits of information it needs to cryptographically verify that the wallet user owns their money.

SPV wallet only downloads what are called the *block headers*. These headers store important metadata about the transactions included in that block, including a sort of cryptographic summary of transactions called a *Merkle tree*. Next, the SPV wallet will ask other nodes on the network for transaction data that is relevant specifically to the user's wallet, like previous transactions that send money to the user's Bitcoin addresses.

By getting the basic transaction data from other nodes and the block headers, the SPV wallet can use cryptography that verifies that the transaction does indeed belong in a particular block (by verifying it belongs in the *Merkle tree* in the block header). The SPV node can then verify that the blockchain is valid by checking that all the block headers are valid and have sufficient "proof of work". It turns out that if the transaction the wallet needs to verify is several blocks "deep" (that is, behind the latest block proved and added to the chain), the wallet can generally trust that the funds do indeed belong to the user without having to verify the whole blockchain!

It is important to note that in order to prevent being scammed by one rogue node on the network, SPV wallets connect to many full nodes to request transaction data. It is far less likely that all the peers an SPV node connects to a trying to scam that node with falsified transaction data, so it is generally considered secure to use SPV nodes for everyday transfers. If a user wants the *most* secure wallet experience, a full node is a bit better since it verifies the whole blockchain and doesn't have to trust other parties on the network.

SPV - Wallets, simplified!

Thanks to the interesting cryptography of Merkle trees, proof of work, and block chaining, SPV wallets do not need to download the entire blockchain to securely check if a user owns their Bitcoin. By asking for specific transaction data, an SPV wallet can check that transactions sent to a user's address belong to a block using a Merkle tree. And by verifying block chaining and proof of work, the node can trust that said transaction has been accepted as part of the Bitcoin history and is therefore owned by the user. Since SPV nodes communicate with multiple full nodes, it is generally true that SPV wallets are secure despite the fact that they do not download and validate the entire blockchain. So never fear - if you're using a mobile phone wallet or a wallet on your netbook, you can participate in Bitcoin in a way that is secure!