CS 261 Notes: Bitcoin

Scribe: Michael Dong

10 Sept. 2018

1 Introduction

Bitcoin is a cryptocurrency created in 2009 by Satoshi Nakamoto.[1] A cryptocurrency uses rules that are enforced by cryptography instead of a trusted party such as a bank. By not trusting institutions, it provides the users with pseudo-anonymity and avoids fees from the institution.

The main goals of a cryptocurrency are:

- Provide identity management
- Allow for transactions
- Prevent double spending

To accomplish these goals, Bitcoin uses a ledger protocol called the blockchain which stores every transaction that has ever occurred. Each participant will store a copy of the blockchain locally, and in order to prevent double spending, every participant must agree on the current state of the blockchain. If a transaction only exists in the blockchain for some people, then the sender of that transaction could potentially double spend with users that do not have that transaction in the blockchain. In order to achieve consensus about the state of the blockchain, Bitcoin uses a proof of work model through the mining process.

2 Transactions

Transactions are stored in a ledger called the blockchain which is essentially a publicly visible, append only, immutable log. Each user will have a cryptographic identity by creating a (private key, public key) pair and each user is referred to by their public key.

Each transaction is made by the sender broadcasting a message containing the recipient's public key and amount they want to send and this message is signed by the sender's private key. Therefore, this transaction can be publicly verified by the sender's public key.

In order to prevent double spending, the sender also has to include a list of transactions they received as proof that they own enough Bitcoin to send the amount they want to send. To verify a transaction, the ledger owner will first check the signature of the transaction with the sender's public key and then they have to scan the ledger to make sure that the transactions the sender provided are valid and have not been spent anywhere else.

$$Tx = (PK_{sender} \rightarrow PK_{receiver},\ \text{Amount, List of transactions})_{signed_{SK_{sender}}}$$

3 Sending a Payment

To send a payment from one user to another, the sender must first create a transaction containing the sender's and receiver's public keys, the amount the sender wants to send, and a list of transactions showing where the sender's money came from. To prove that this transaction is actually created by the sender, the sender will sign the transaction with their private key.

The transaction is then sent to miners that verify the transaction and then decide whether or not to include the transaction in the block they are mining. Each new block will contain the new transactions, the hash of the previous block, and a nonce. Once a block is mined, it is appended onto the blockchain. If the block is part of the longest chain, then it is considered a valid block, and the payment is considered sent.

4 Mining

In order to add a block to the blockchain, miners will have to solve a computational puzzle by calculating a hash that is less than a certain value determined by the protocol. (i.e. a hash that starts with 33 zeros). The only way to find a valid hash is by trial and error. Miners calculate the hash of the block and if it does not meet the criteria, the miner will increment the nonce and try again.

Once the requirement of $hash(block) < target\_value$ is met, then the block is considered mined and can be added to the end of the blockchain. The mined block will then be broadcast to everyone in the network and each node will verify the newly mined block.

The proof of work criteria can be adjusted based on the rate of blocks being mined and the total amount of compute power. The target is to mine one block around every 15 minutes. As the amount of compute power increases, and blocks are being mined more frequently, the difficulty of the computational puzzle will increase in order to decrease the frequency that a block is mined.

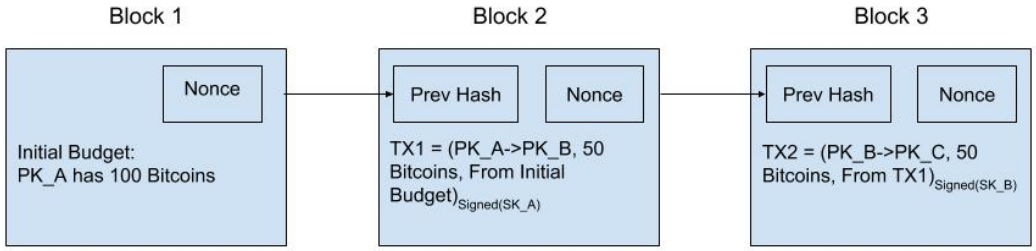

Figure 1: Blockchain

5 Verification

A block is verified by first checking that the hash of the block meets the criteria set by the protocol and then every transaction in the block must be verified to be valid. If a block was mined by a malicious node containing invalid transactions, then that block will be ignored by all the honest nodes in the network.

To check that a transaction is valid, first, the the signature of the transaction is checked with the sender's

public key. Then, every transaction in the list that the sender provided as the source of their money is checked to see that those transaction were actually sent to the sender. Finally, in order to verify that the sender actually has enough money to spend, the unspent amount of each transaction in the list is calculated by looking through the blockchain and added together. If the total unspent amount is at least the amount that the sender wants to send, then the current transaction is valid.

It is possible that two blocks are mined at the same time, causing a fork in the blockchain. In that case, blocks will continue to be mined and appended to the forks and whichever fork is the longest will be considered the valid one.

6 Incentive

In order for people to be willing to mine blocks, miners must be given an incentive to expend CPU time and electricity. In Bitcoin, the first transaction of a block is a special transaction that awards a Bitcoin to the miner of the block. This is also the way that new Bitcoins are added into circulation. Another incentive can be transaction fees paid by the senders to the miners.

7 Presentation: Bitcoin Wallets

A Bitcoin wallet has three tasks:

- Public key distribution program (As well as key generation)
- Transaction signing program
- Network program (Receiving and transmitting new transactions and downloading blockchain information)

There are three types of Bitcoin wallets:

- Full service wallets
- Signing only wallets
- Distributing only wallets

The main security concern with Bitcoin wallets is losing your private keys or having your private keys stolen.

7.1 Full Service Wallets

The tasks a full service wallet perform are:

- Generate Private Keys
- Derive Corresponding Public Keys
- Distribute Public Keys
- Monitor for outputs sent to public keys
- Create and sign transactions
- Broadcast transactions

One concern with full service wallets is that the private keys are stored on a device connected to the Internet and can therefore be attacked. (i.e. keylogger, remote access)
Encrypting wallet files will help against some attacks but private keys can still be captured from memory.
Therefore, full service wallets such as desktop wallets have become less popular recently.

7.2 Signing Only Wallet

Signing only wallets can be more secure than full service wallets since private keys are generated and stored on devices that are not connected to the Internet. Signing only wallets are used with networked wallets, such as full service wallets or distribution only wallets, to interact with the Bitcoin network. Common types of signing only wallets are offline wallets and hardware wallets.

7.2.1 Offline Wallets

- Stored on an offline computer
- Distribute public keys to receive payment
- Transactions are generated and copied over to offline wallet for signing
- Signed transactions are copied back to networked wallet for distribution

7.2.2 Hardware Wallet

- Private keys are stored on an external physical device (i.e. Trezor, Ledger)
- Device prompts user to physically confirm before signing transaction

7.3 Privacy and Security

Bitcoin is not completely anonymous since if two transactions have the same public key for the sender, then it is known that both transactions were sent by the same person. If any of these transactions end up on a website that knows your identity, then all of your transactions can be linked to you. In order to avoid this, a different public key should be used for every transaction. By using hierarchical deterministic key creation, it is possible to generate multiple, seemingly unrelated, public keys from one private key.

Even if your private keys are digitally secure, your funds may still not be safe. Physical extortion and scams have been known to occur to owners of cryptocurrency.

References

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008