Exploring Cryptocurrencies

Anthony Tam & Michael O'Connell

Distributed Ledger

Distributed Ledger

- A ledger is a collection of transactions within the network
- A transaction is the transfer of funds from a sender to a recipient
- A copy of the ledger is maintained by every node in the network, so that no one node can decide what transactions are included in the ledger
- Additionally, all transactions added must be verified by the sender

Digital Signatures

Digital Signatures

- Digital signatures are used, in verifying transactions, in the exact same manner which they are used in verifying SSL certificates as we learned in CSC347
- The sender of a transaction simply signs the transaction with their private key, which is then easily verifiable using their public key, so everyone on the network can know that the sender really did mean to transfer funds

Proof of Work

Proof of Work

- In order to solidify a segment of the ledger into the record, you have to form a block
- A block is a list of transactions which have occured on the network
- In order to create a block, a member of the network must find a string which, when hashed with the list of transactions, contains a particular prefix; this string is called the “Proof of Work”

Proof of Work

- This “Proof of Work” is then verified by the other nodes in the network, at which point they then add it to their copies of the ledger
- As an additional security measure, the block also begins with the hash of the previous block, which ensures that no blocks have been maliciously inserted, removed, or altered by any other nodes on the network

MONERO

What Makes Cryptonote Based Coins Different

Dashcoin

Stealth Addresses

Stealth Addresses

- Protects the privacy of the receiver
- The sender can use the public view key and the public spend key of the receivers wallet to create a 1-time public spend key
- This key is publicly available but due to the cryptographic nature of creating the key, it cannot be traced to a specific wallet

Stealth Addresses

- The receiver can then use their wallet’s private view key to find this 1-time spend key
- When the public 1-time spend key is found, the receiver can create a corresponding private 1-time spend key
- This now gives the receiver access to spend the funds

Ring Signatures

Ring Signatures

- Protects the privacy of the sender
- Made up of the sender's signature and an arbitrary number of signers (selected by the sender)
- These “fake” signers are past transaction outputs which are chosen randomly from the blockchain
- This makes all the inputs of the transaction appear to be valid, however there is only 1 valid transaction

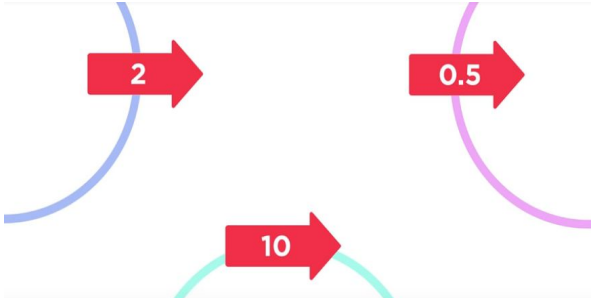
Ring Signatures

- Each output on the blockchain has a corresponding key image, this image cannot be linked back to a specific transaction and is stored in the blockchain once spent
- This allows miners to know which transaction is valid and add it to the blockchain
- The recipient of a transaction is now no longer able to identify the sender, but can use the key image added to the blockchain from this transaction to know the transaction is valid

Ring Confidential Transactions

Ring CT

- Protects the privacy of both parties by hiding transaction amounts
- Previously a transaction was broken into multiple outputs, broken down by 10^n
- This means signers in the ring must be of the same denomination



Ring CT

- Ring CT hides this information from the public, meaning denominations are no longer required and the total amount is no longer visible by the public
- Any output from the blockchain can now be used in any new inputs, increasing security

Ring CT

- Ring CT hides this information from the public, meaning denominations are no longer required and the total amount is no longer visible by the public
- Any output from the blockchain can now be used in any new inputs, increasing security

Ring CT

- When transactions are sent, the sender is required to commit to the transactions using a specific formula

$$rct = xG = aH(G)$$

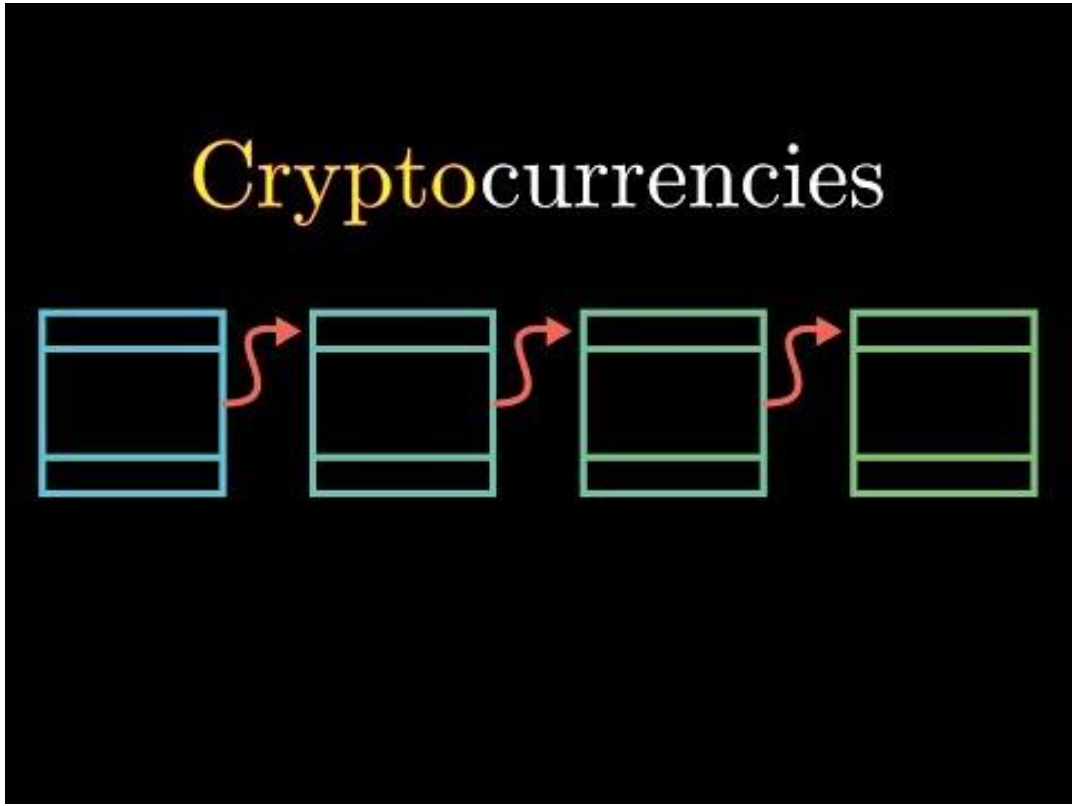
- This zero knowledge proof allows miners to ensure the transaction contains only positive values and the sender has a high enough balance for the transaction

51% Attack

51% Attack

- With proof of work, a node will select the chain with the most work done
- Is it possible to falsify this chain?
- If a malicious user posts a false set of transactions and completes the required POW, this will form a new chain
- This user will then need to have at least equal power to the network in order to continue to grow this chain and have it be accepted

A concise explanation...



A Demo