Bitcoin and Cryptocurrencies

- Lecture 1: Bitcoin networks
- Professor Radjabov Mukhammad

Online Transactions

- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation

- Can't be used online directly

➢ Electronic credit or debit transactions

  ◆ Bank sees all transactions

  ◆ Merchants can track/profile customers

E-Cash

- Secure
  - Single use
  - Reliable
- Low inflation
- Privacy-preserving

E-Cash Crypto Protocols

- Chaum82: blind signatures for e-cash
- Chaum88: retroactive double spender identification
- Brandis95: restricted blind signatures
- Camenisch05: compact offline e-cash

- Various practical issues:
  - Need for trusted central party
  - Computationally expensive
  - Etc.

Bitcoin

- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log

Size of the BitCoin Economy

- Number of BitCoins in circulation 11.8 million (December 2013)
- Total number of BitCoins generated cannot exceed 21 million
- Average price of a Bitcoin: around $300
  - Price has been unstable.
- Total balances held in BTC 1B$ compared with 1,200B$ circulating in USD.
- 30 Transactions per min. (Visa transaction 200,000 per minute.)

BitCoin: Challenges

- Creation of a virtual coin/note
  - How is it created in the first place?
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
  - Is the coin legit? (proof-of-work)
  - How do you prevent a coin from double-spending?
- Buyer and Seller protection in online transactions
  - Buyer pays, but the seller doesn't deliver
  - Seller delivers, buyer pays, but the buyer makes a claim.
- Trust on third-parties
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank or clearing house

Security in Bitcoin

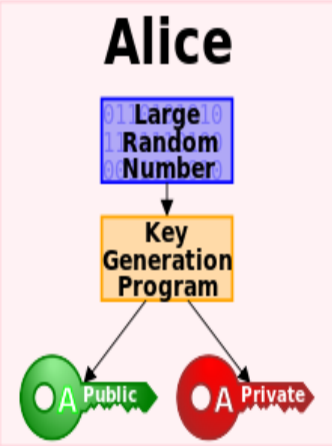
- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

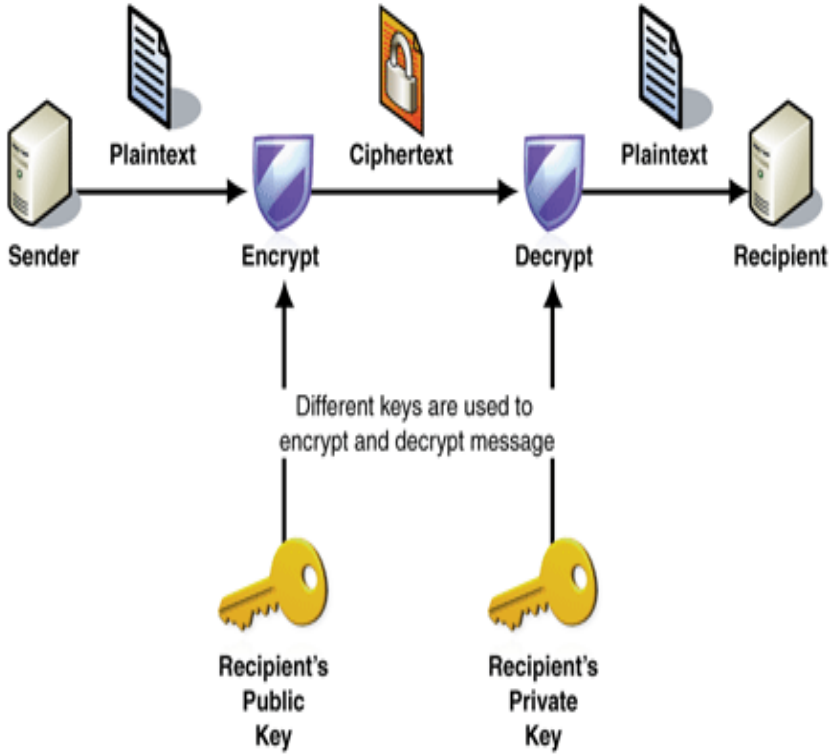
Security in Bitcoin

- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

Public Key Crypto: Encryption

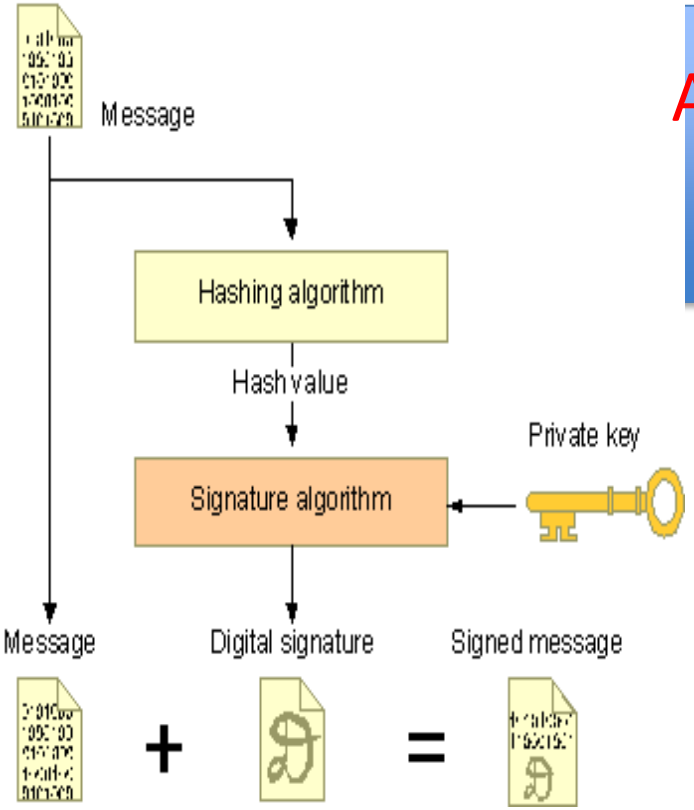
- Key pair: public key and private key





Public Key Crypto: Digital Signature

- First, create a message digest using a cryptographic hash
- Then, encrypt the message digest with your private key



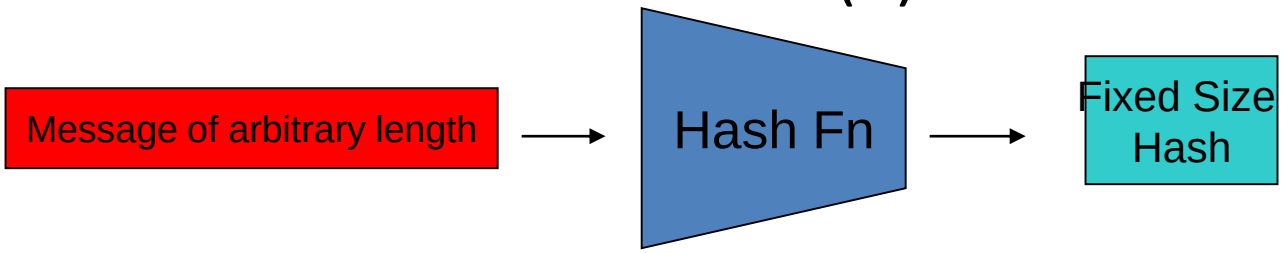
Authentication

Integrity

Non-repudiation

Cryptographic Hash Functions

- **Consistent:** hash(X) always yields same result
- **One-way:** given Y, hard to find X s.t. hash(X) = Y
- **Collision resistant:** given hash(W) = Z, hard to find X such that hash(X) = Z



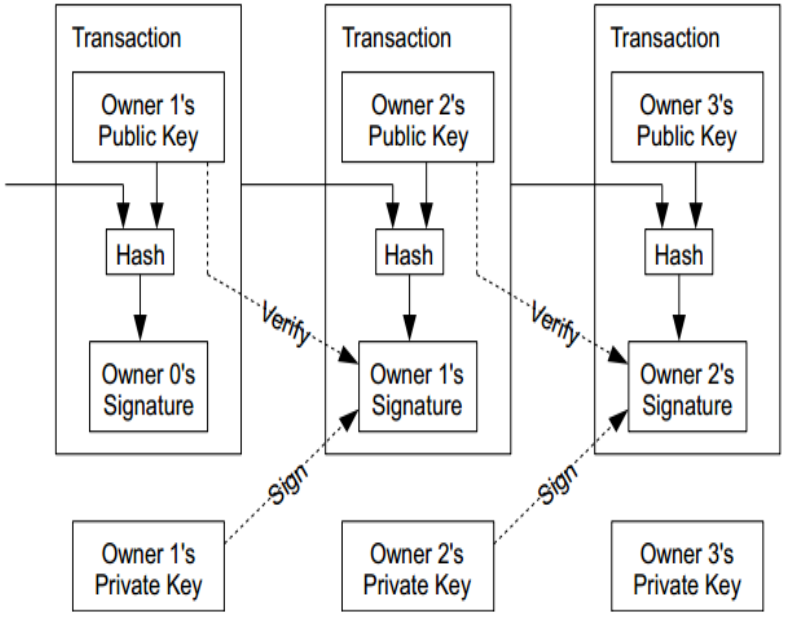
Back to BitCoin

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins

Bitcoin

- Electronic coin == chain of digital signatures
- BitCoin transfer: Sign(Previous transaction + New owner's public key)
- Anyone can verify (n-1)th owner transferred this to the nth owner.
- Anyone can follow the history

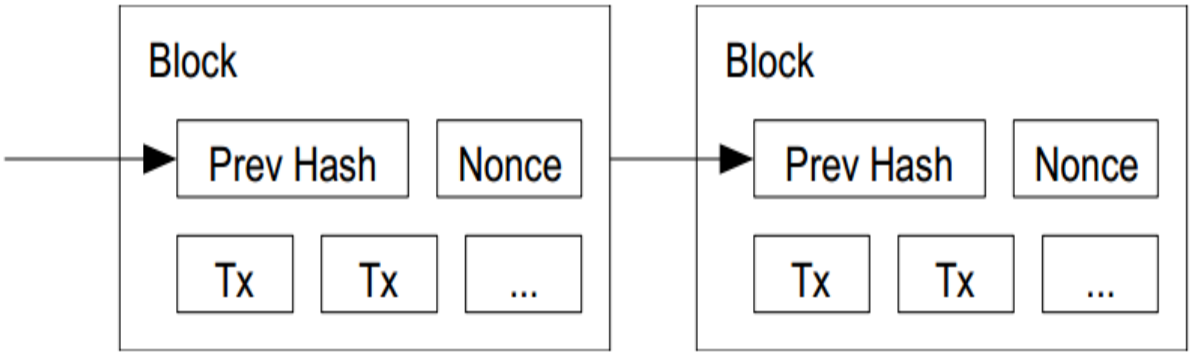
Given a BitCoin



Bitcoin Transactions

Use of Cryptographic Hashes

- Proof-of-work
  - Block contains transactions to be validated and previous hash value.
  - Pick a nouce such that **H(prev hash, nounce, Tx) < E**. E is a variable that the system specifies. Basically, this amounts to finding a hash value who's leading bits are zero. The work required is exponential in the number of zero bits required.
  - Verification is easy. But proof-of-work is hard.



Preventing Double-spending

- The only way is to be aware of all transactions.
- Each node (miner) verifies that this is the first spending of the Bitcoin by the payer.
- Only when it is verified it generates the proof-of-work and attach it to the current chain.

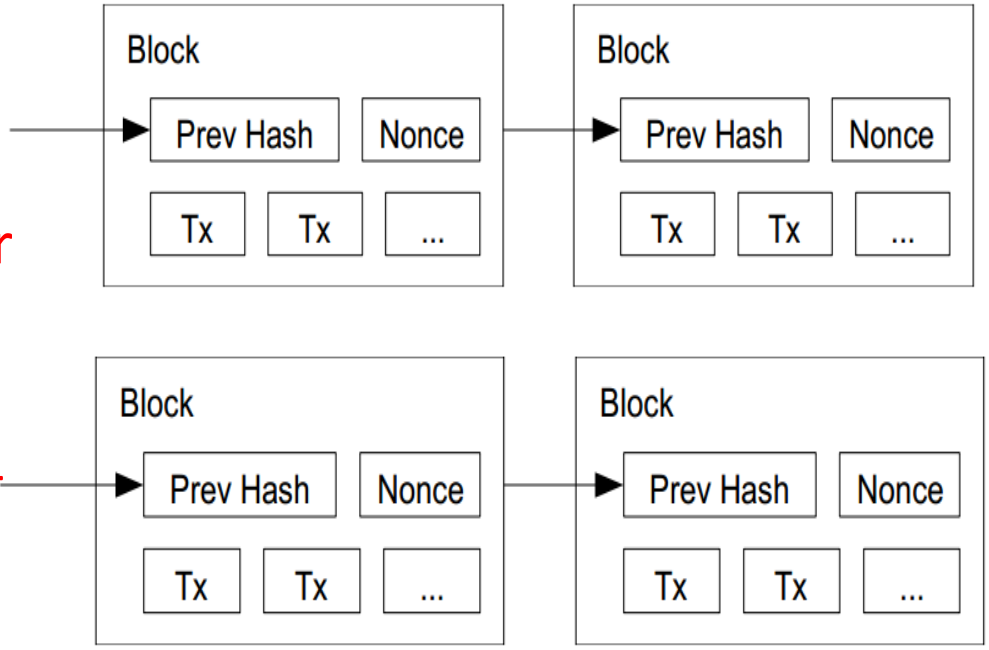
Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Tie breaking

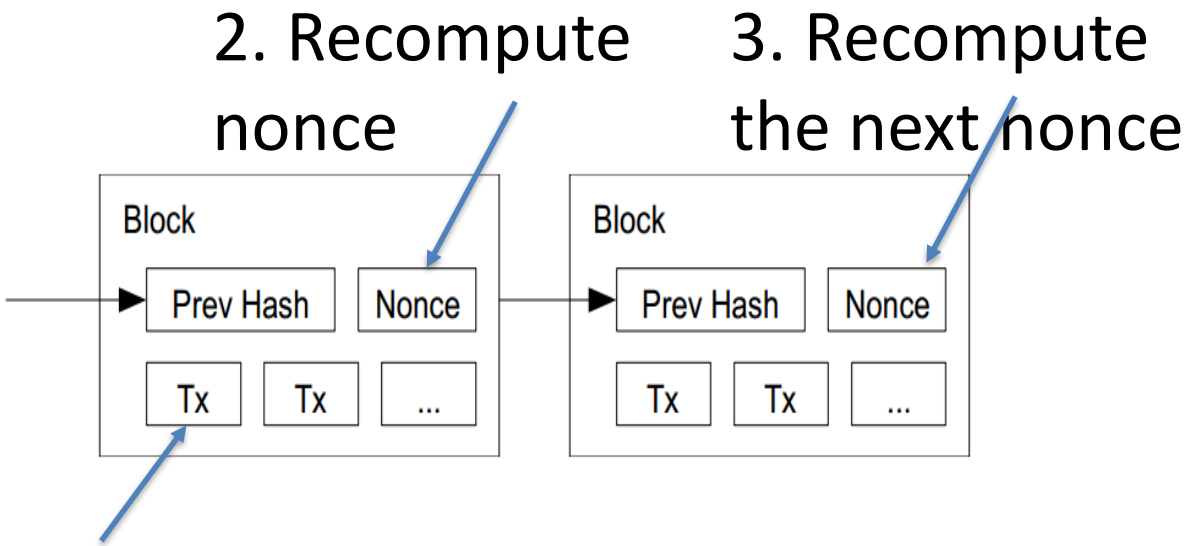
- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

Two different block chains (or blocks) may satisfy the required proof-of-work.



Reverting is Hard

- Reverting gets exponentially hard as the chain grows.

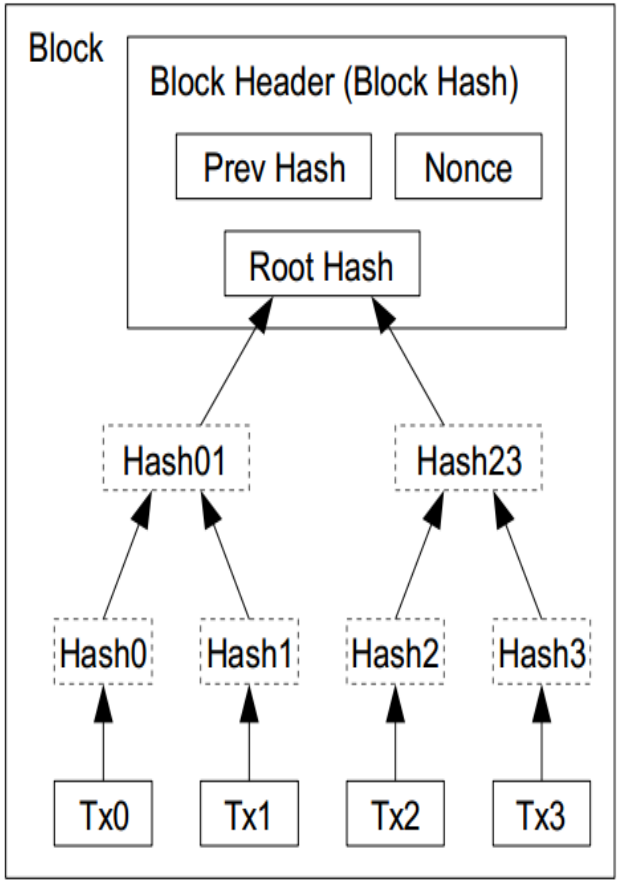


Practical Limitation

- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer. Because if you wait longer it becomes more secure. For large $$$, you wait for six blocks (1 hour).

Optimizations

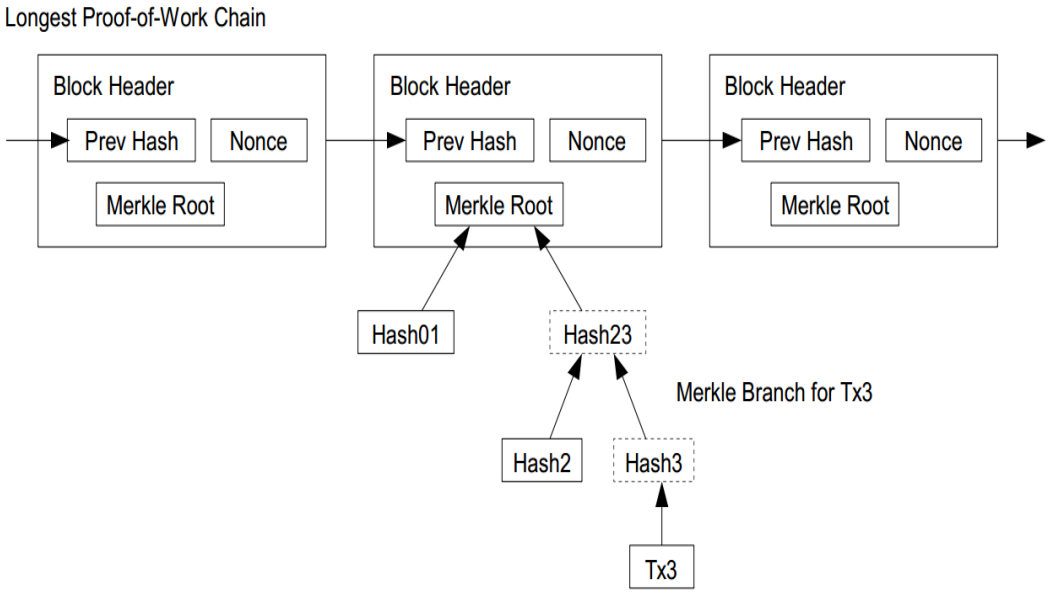
- Merkle Tree
  - Only keep the root hash
    - Delete the interior hash values to save disk
    - Block header only contains the root hash
    - Block header is about 80 bytes
    - 80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year
  - Why keep use a Merkle tree?



Transactions Hashed in a Merkle Tree

Simplified payment verification

- Any user can verify a transaction easily by asking a node.
- First, get the longest proof-of-work chain
- Query the block that the transaction to be verified (tx3) is in.
- Only need Hash01 and Hash2 to verify; not the entire Tx's.



BitCoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the "network's capacity"
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new Bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25.
  - Halved every 210,000 blocks (every four years)
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)

Privacy Implications

- No anonymity, only pseudonymity
- All transactions remain on the block chain– indefinitely!
- Retroactive data mining
  - Target used data mining on customer purchases to identify pregnant women and target ads at them (NYT 2012), ended up informing a woman's father that his teenage daughter was pregnant
  - Imagine what credit card companies could do with the data

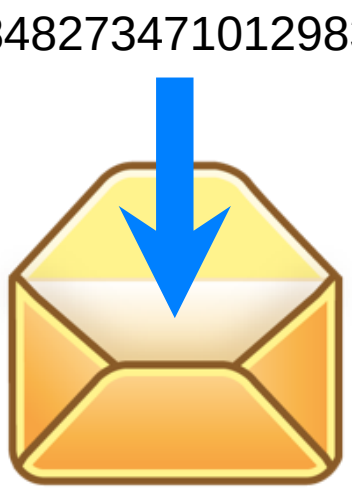
Zerocoin

- A distributed approach to private electronic cash
- Extends Bitcoin by adding an anonymous currency on top of it
- Zerocoins are exchangeable for bitcoins

What is a zerocoin?

A zerocoin is:

- Economically: a promissory note redeemable for a bitcoin
- Cryptographically: an opaque envelope containing a serial number used to prevent double spending

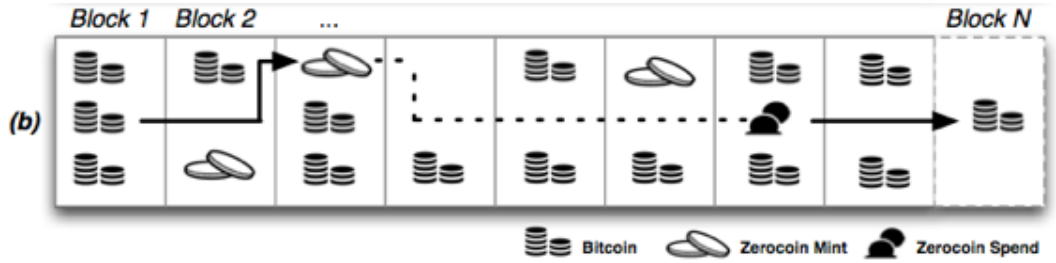


Commitments

- Allow you to commit to and later reveal a value
- Binding: value cannot be tampered with
- Blinding: value cannot be read until revealed

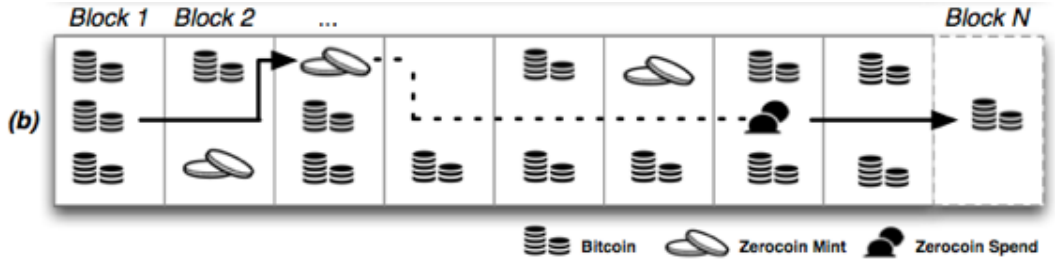
Zerocoins: where do they come from?

- Anyone can make one
- Choose a random serial number and commit to it
- Mint a zerocoin by putting a mint transaction in the block chain which “spends” a bitcoin and includes the commitment
- Spending a zerocoin gives the recipient a bitcoin



Zerocoins: ...and where do they go?

- The “spent” bitcoins end up escrowed
- To spend a zerocoin
  - You reveal the serial number
  - Prove it is from some zerocoin in the block chain
  - Put the spent serial number in the block chain



Zero-knowledge proofs

- Zero-knowledge [Goldwasser, Micali 1980s, and beyond]
- Prove knowledge of a witness satisfying a statement
- Specific variant: non-interactive proof of knowledge
- Here we prove we know:
  1. The serial number of a zerocoin
  2. That the coin is in the block chain

Zero-knowledge proof

- Inefficient approach
  - Identify all valid zerocoins in the block chain (call them $C_1 \ldots C_N$)
  - Prove that S is the serial number of a coin C and $C = C_1 \vee C = C_2 \vee \ldots C_N$
  - This "OR" proof is O(N)
- Zerocoin uses cryptographic accumulators
  - Sublinear

Zerocoin protocol

Generate a commitment to a random serial number *S*:

(Store serial number *S* and randomness *r*)

Accumulate all valid coins, compute witness w_i

Reveal *S* and prove knowledge of witness to commitment accumulation and its randomness *r*

Discussion

- The future of Bitcoin?
- Attacks on Zerocoin?
- Should we tradeoff privacy for usability? Is privacy a main principle?

Reference

- The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous
- The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)
- Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial
- Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent
- Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)