Bitcoin and Cryptocurrencies

- Lecture 9: Record Keeping
- Professor Radjabov Mukhammad

The Initial Problem

- **The Question:** How Can we Send Money (Value) over the Internet without the need for Central Intermediaries (e.g Banks, Western Money Union, etc)
- The **Double Spend Problem:** The double spending problem is about a user being able to simultaneously spend or transfer the same money(digital token) to two or more different accounts.
- In a **centralized system**, a trusted third party/ authority sorts out this issue (Banks, Credit Card Providers etc).
- The central authority (3rd Party) has a global view of all transactions happening between the two parties and can therefore prevent a user from spending the same money to multiple accounts.

The Solution - Bitcoin

- In **a decentralized system**, this problem is much harder to solve

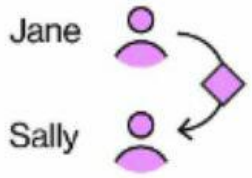
- Satoshi (Bitcoin) creator, created a technical system that simulates and replaces Trusted 3rd Parties – Blockchain

- Blockchain is the underlying technology supporting the (bitcoin) crypto-currency:
  - It is a distributed database that is practically immutable and is maintained by a decentralized Peer to Peer network
  - It uses a consensus mechanism, cryptography and back-referencing blocks to order and validate transactions

How Blockchain Works for Bitcoin

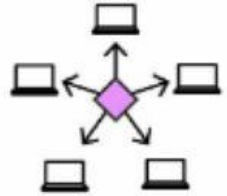
When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.

Transaction



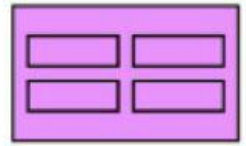
Jane uses bitcoin to buy a cup of coffee at Sally's internet café, using her private key to transfer ownership of the currency.

Mining network



Word of the transaction is sent through the bitcoin network to "miners" with powerful computers.

Block

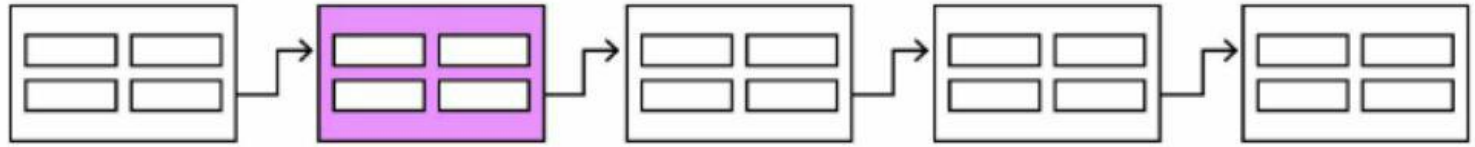


Miners use trial-and-error computations to solve a puzzle created by combining data about recent transactions. The first to find the unique number that unlocks the puzzle earns the right to bundle the transactions into a confirmed batch known as a block.

Verification

The winning miner is rewarded with newly minted bitcoin — but only after other miners confirm that the block's transactions don't contain any attempts to spend the same funds twice.

The Chain



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

Data: Bloomberg; graphic by Bloomberg QuickTake

Blockchain vs Bitcoin

- Bitcoin is a crypto-currency and is the first successful application that ran on an underlying Blockchain Technology.
- Blockchain powers the record-keeping system for crypto-currency being exchanged between users without the need for a central authority (banks)
- The reliability and efficiency of this model can be exported to other industries/use cases.

What exactly is Blockchain?

- Blockchain and DLT systems are new accounting tools that enable shared distributed recordkeeping
  -without the need to rely on a single controlling party
- Records are added into database (ledger) using consensus mechanisms or protocols.
- Video
- https://www.cigionline.org/multimedia/what-blockchain

Characteristics of a Blockchain

- The main thing distinguishing a blockchain from a normal database is that there are specific rules about how to put data into the database.
- That is, it cannot conflict with some other data that's already in the database (consistent),
- it's append-only (immutable), and the data itself is locked to an owner (ownable),
- it's replicable, distributed and highly available.
- Finally, each node agrees on what the state of the things in the database are) without a central party (decentralized).

Types of Blockchains

- **Public Blockchains**
- Public blockchains allow all/any nodes to read blockchain data and propose new transactions.

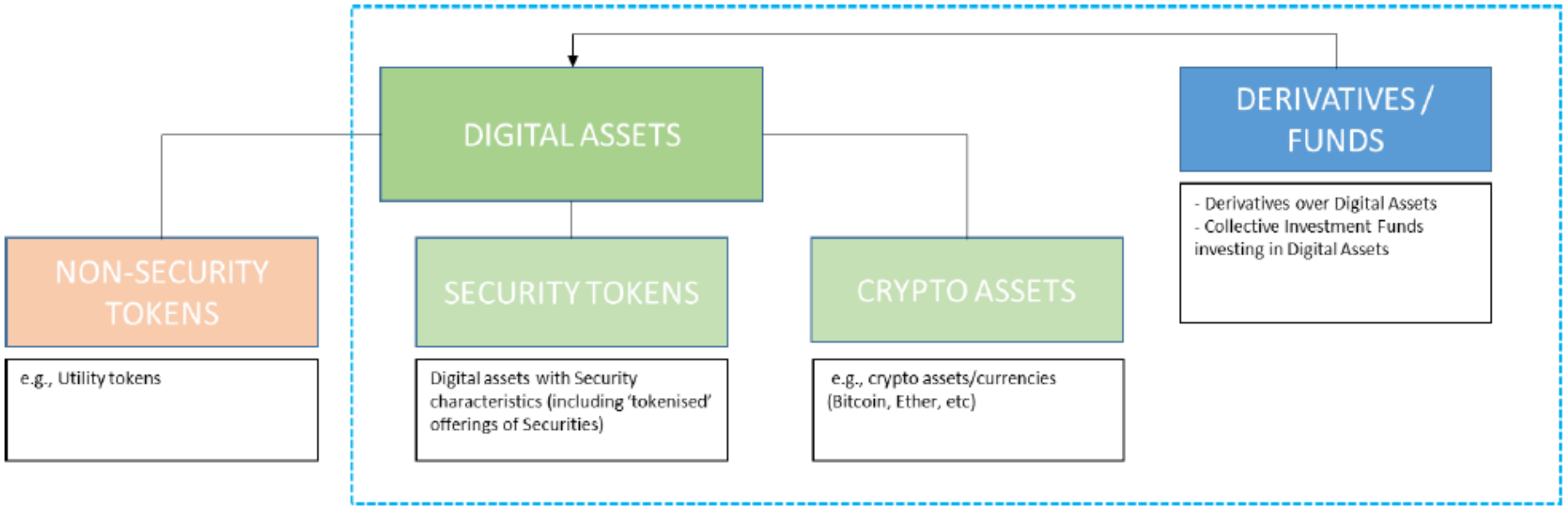
- **Private Blockchains**
- Private Blockchains allow only nodes that are preregistered by a central authority to read blockchain data and submit new transactions

Traditional Currency

- “Fiat Currency” means government issued currency that is designated as legal tender in its country of issuance through government decree, regulation or law.

- “E-money” means a digital representation of Fiat Currency used to electronically transfer value denominated in Fiat Currency.

Taxonomy of Digital Assets



Crypto-Asset/Currency/Token*

- *“Crypto Asset/Currency/ Token” means a digital representation of value that can be digitally traded and functions as*
  - *(1) a medium of exchange; and/or*
  - *(2) a unit of account; and/or*
  - *(3) a store of value, but does not have legal tender status in any jurisdiction.*
- *A Crypto Asset/Token is -*
- *(a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Crypto Asset; and (b) distinguished from Fiat Currency and E-money.”*

- *Defn: from Abu Dhabi Global Market (ADGM)*

Crypto-Token /currency

- Within the Bitcoin blockchain network, bitcoins are spent to pay for monetary transmission and pay miners or block creators for maintaining the network
- Within the Ethereum blockchain network, Ether (ETH) pays for decentralized computing power and pay miners/block creators for maintaining the network.
- One needs Crypto-exchanges & Crytpo Wallets to ‘cash’ crypto assets (convert to fiat)
- There are over 1000 crypto-currencies available and the list keeps growing

Securitized Tokens

- “Securitized Tokens” are Virtual tokens that have the features and characteristics of *a Security* under the traditional capital market regulations).
- They are a digital representation of a traditional asset (Land title, Shares, Stock, Units in a Collective Investment Fund, etc)
- They are also known as Asset-backed Tokens and are cryptocurrency versions of a traditional asset.

Non-Securitized Tokens

- Also Known as “Utility Tokens” or “Non-Security Tokens”
- These are Virtual tokens that do not exhibit the features and characteristics of a regulated investment (traditional assets).
- Could be comparable to Bonga-points, Supermarket Loyalty Points, Hotel Lunch Voucher or Frequent Flyer Miles.
- They give user access to specific benefits within a particular business network.

The Token economy

ROLE	PURPOSE	FEATURES
RIGHT	Bootstrapping engagement	Product usage, Voting, Governance, Product Access, Contribution, Ownership
VALUE EXCHANGE	Economy creation	Work rewards, Selling something, Buying, Active/Passive work, Spending, Creating a product
TOLL	Skin in the game	Running smart contracts, Security deposit, Usage fees
FUNCTION	Enriching user experience	Joining a network, Connecting with users, Incentive for usage
CURRENCY	Frictionless transactions	Payment unit, Transaction unit
EARNINGS	Distributing benefits	Profit sharing, Benefits sharing, Inflation benefits

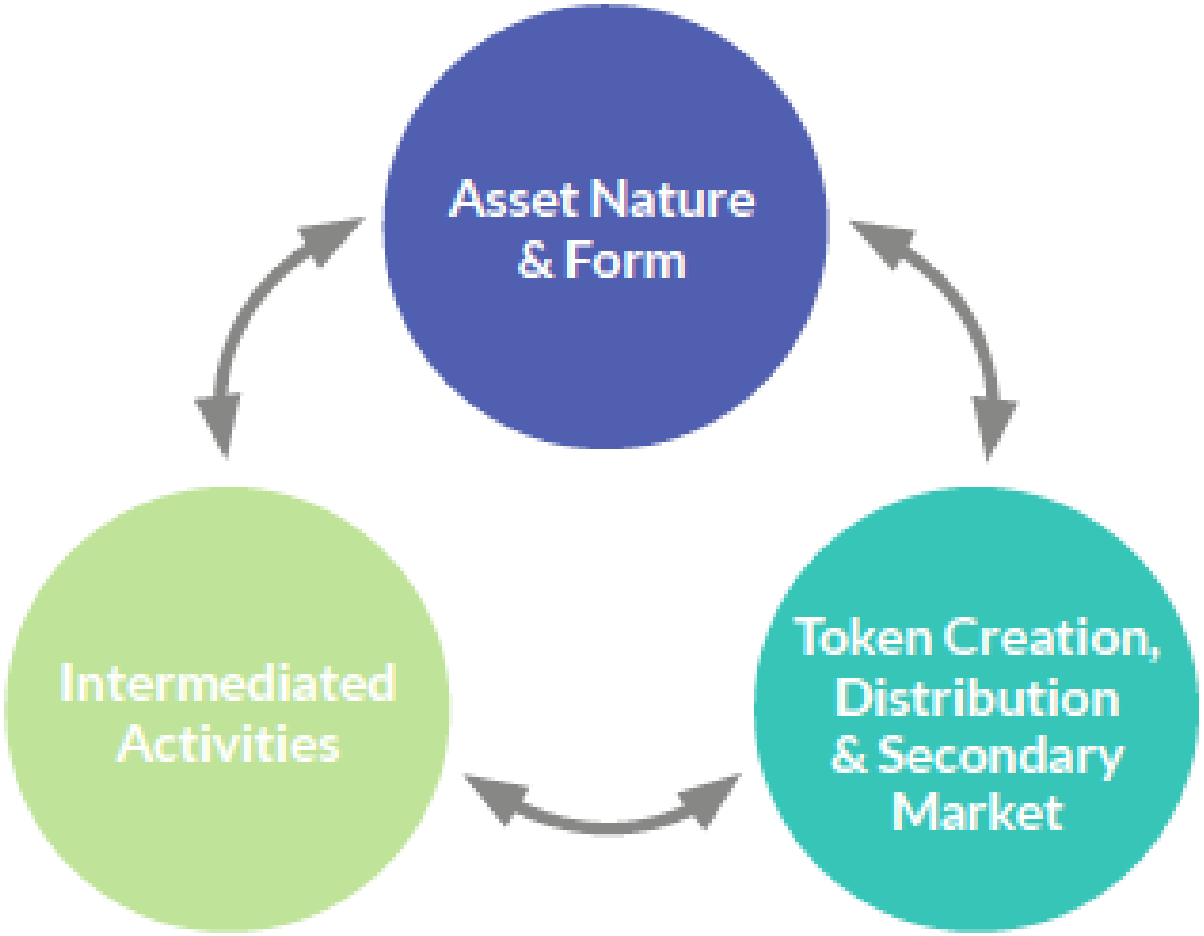
Token Opportunities

- Internet of Value: New Models for local and international payments and remittances.
- Mining: Earning rewards for maintaining Blockchain networks
- Central Banks: Using Blockchain based Funds Transfers (Cryptos pegged on Fiat Currency eg. Ripple Blockchain)
- Token-economy: Using token to incentivize behavior e.g instead of sending cash to senior citizens, send redeemable tokens to service providers (food, health, etc)
- ICOs- Initial Coin Offerings: new model for raising funds for projects
- Smart Contracts:-new models for executing legal contracts and settling payments without third parties

The Risks/Realities

- Money Laundering/Terrorists can and do use the anonymity attributes.
- Fake Crypto Assets/Currencies, Cyrpto-Exchanges & Cyrpto Projects/ICOs created and gullible citizens conned
- Blockchain Projects demand a huge paradigm shift (centralized vis decentralized) and governance frameworks
- Blockchain based solution requires and puts more responsibility on Users for the safety of their crypto-assets (Wallet Pins and Passwords)
- 51% attacks on Blockchain based systems that assume majority of the participants(nodes) are honest (mining pools are growing)

Regulatory Frameworks

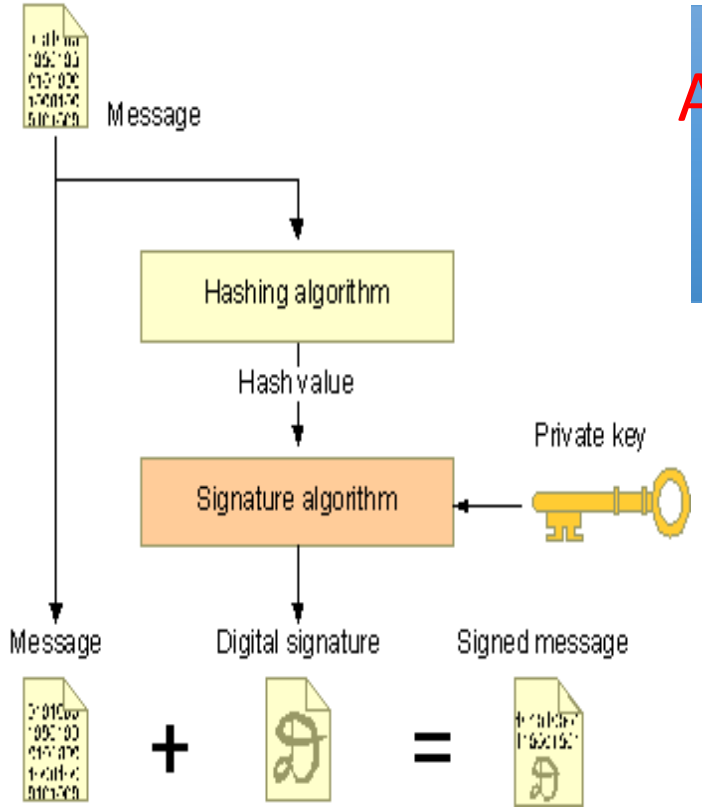


Conclusions

- Tokens/Crypto currencies are here to stay
- Progressive Governments are engaging positively to understand the ecosystem
- Best approach is to have ‘Sandbox’ Regulation to host emerging technologies in a controlled environment
- A delicate balance between embracing new technologies and their benefits while safeguarding or protecting consumer interests is required.

Public Key Crypto: Digital Signature

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



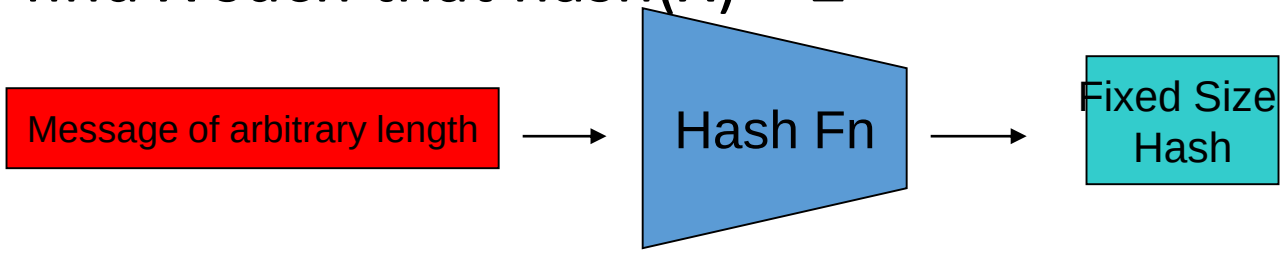
Authentication

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



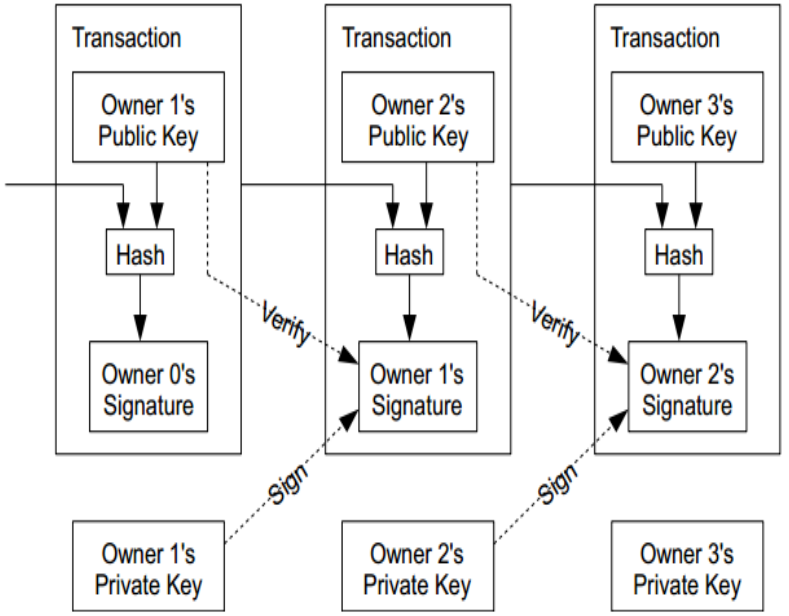
Back to BitCoin

- 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

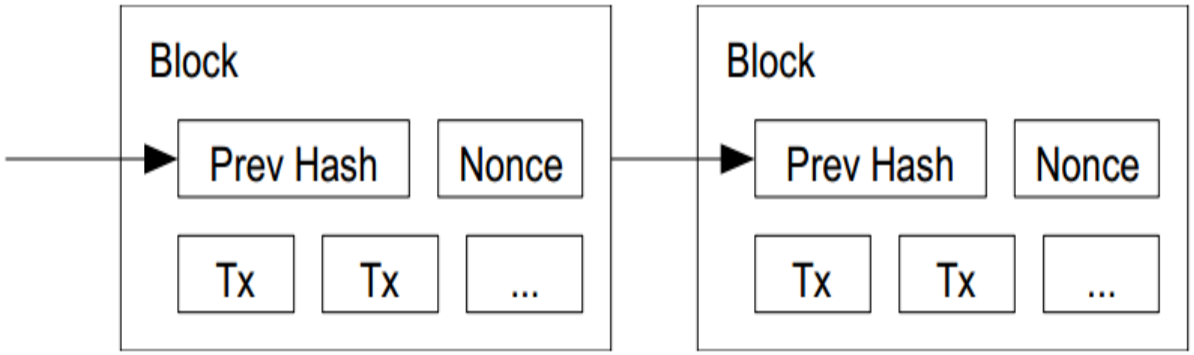
Given a BitCoin



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.

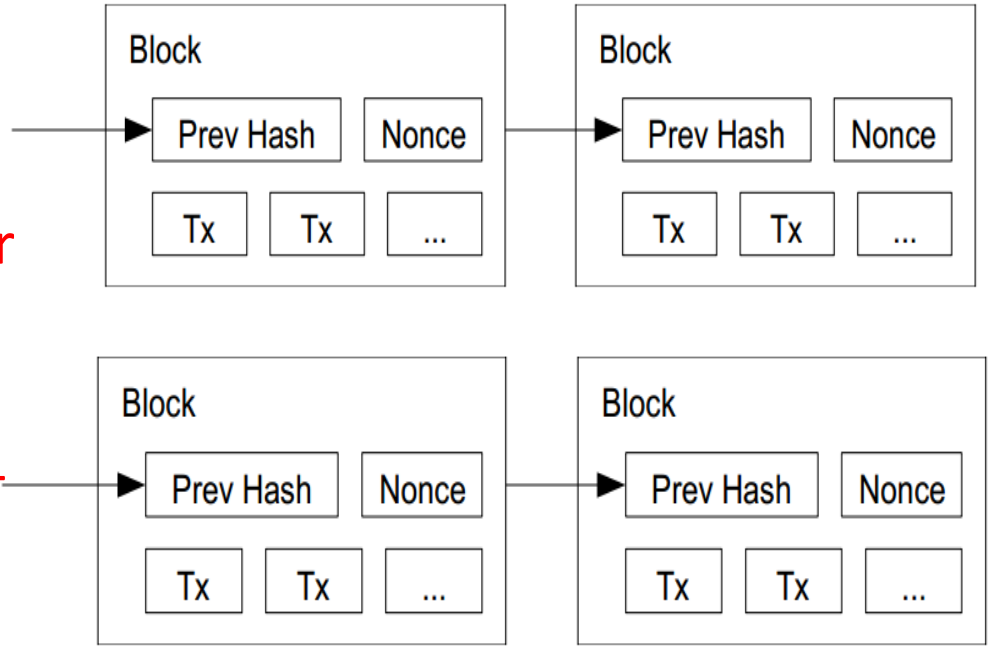
Bitcoin Network

- 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

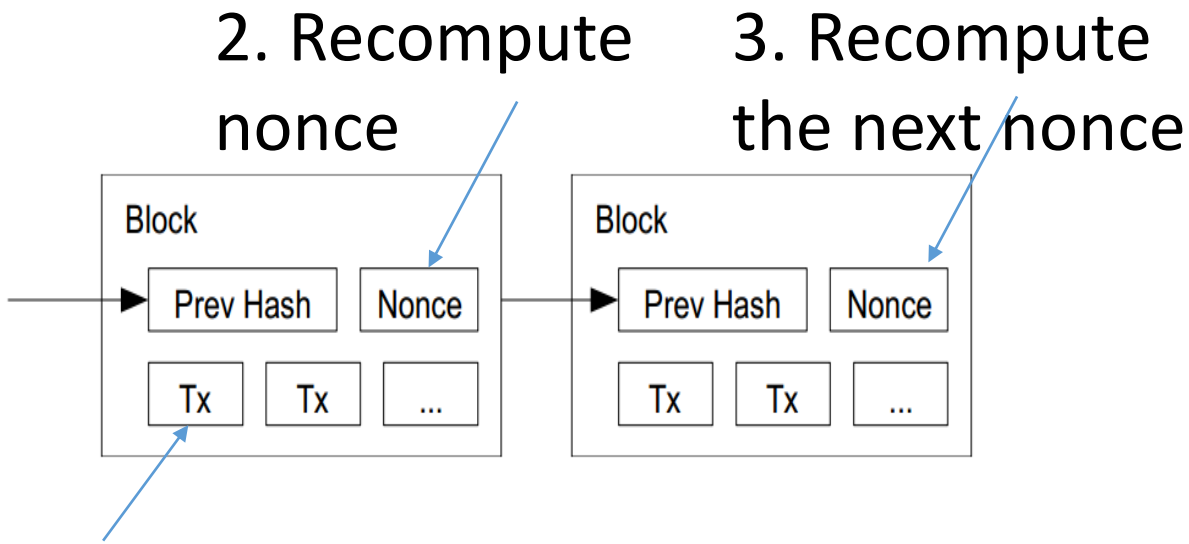
- Two nodes may find a correct block simultaneously.
  - Keep both and work on the first one
  - If one grows longer than the other, take the longer one

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



Reverting is Hard

- Reverting gets exponentially hard as the chain grows.

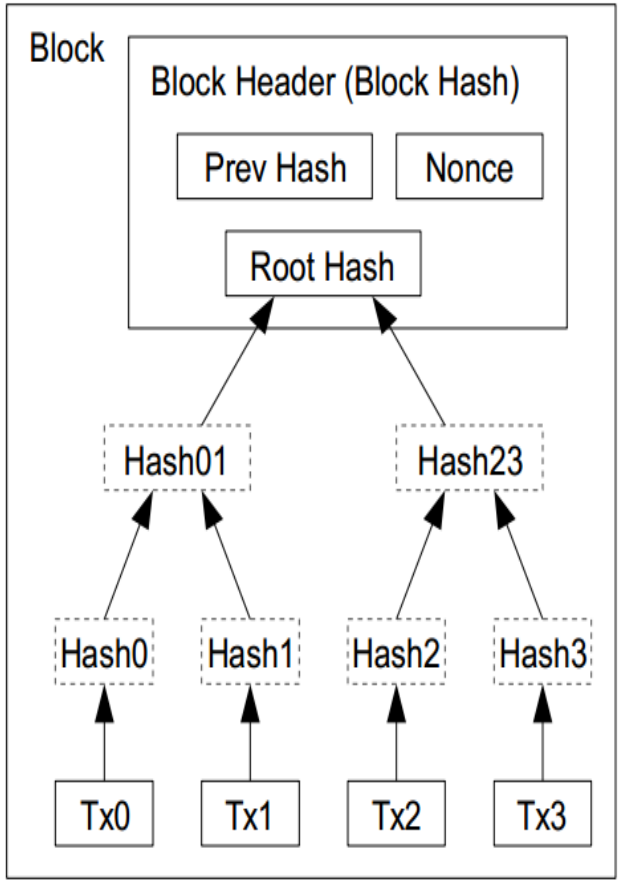


Practical Limitation

- 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

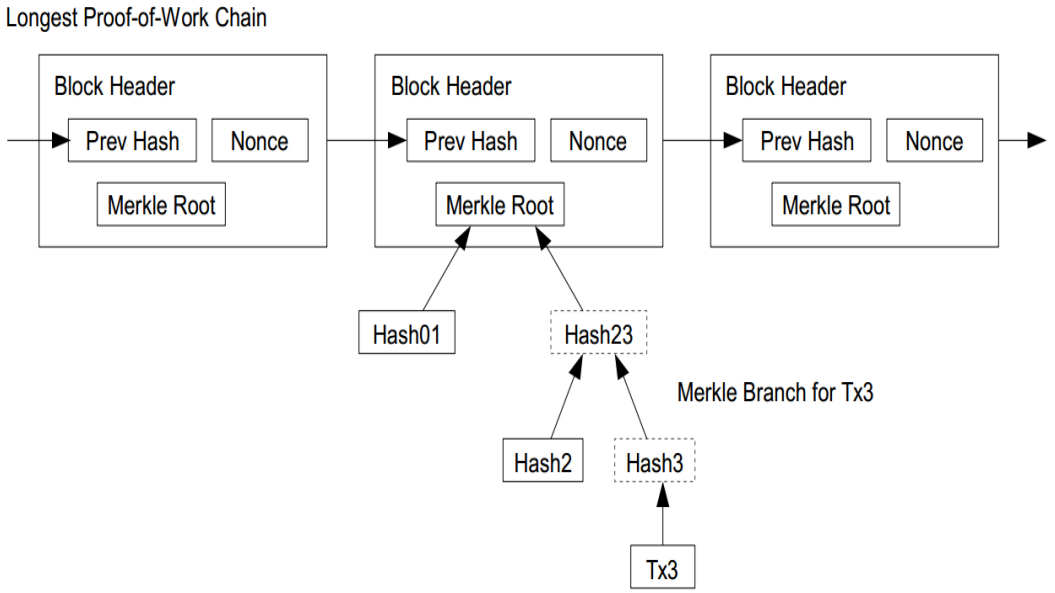
- Merkle Tree
  - Only keep the root hash
    - Delete the interior hash values to save disk
    - Block header only contains the root hash
    - Block header is about 80 bytes
    - 80 bytes * 6 per/hr * 24 hrs * 365 = 4.2 MB/year
  - Why keep use a Merkle tree?



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

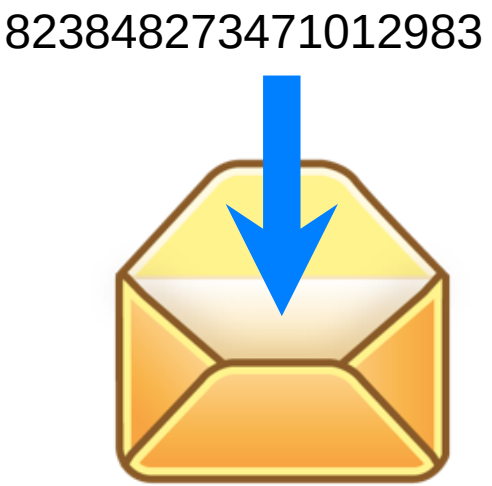
Zerocoin

- 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

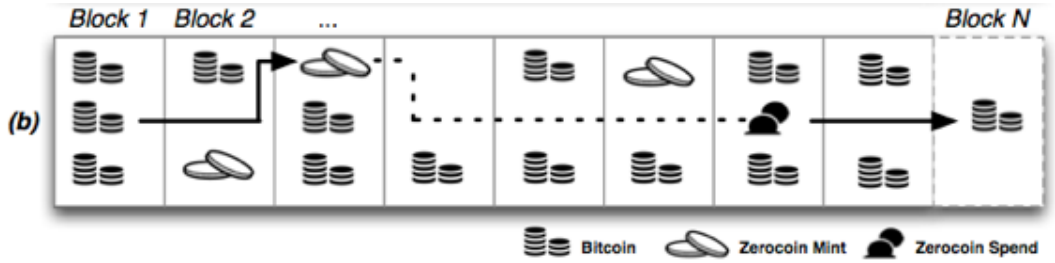


Commitments

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

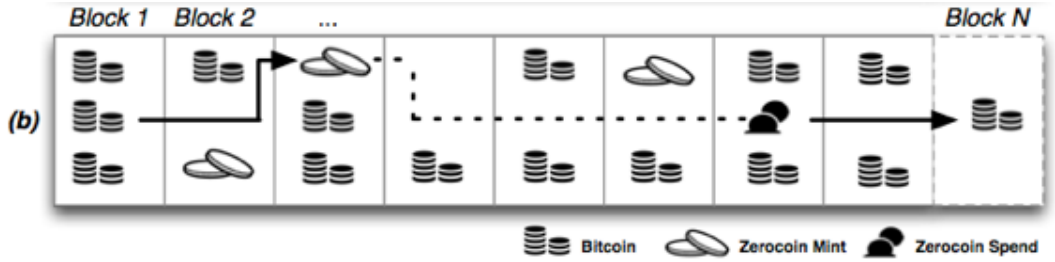
Zerocoins: where do they come from?

- 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*:

$$C = g^s h^r \bmod q \qquad \text{where } C \text{ prime}$$

(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*