Cryptocurrency is becoming popular

**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing all that comes after it.
Properties of Digital Currency

- Say Bob pays for purchase with digital coins

- What properties must seller check about coins?
  - Valid (i.e., not forged)
  - Not already spent
  - Owned by Bob (i.e., not stolen)

- How do shopping portals check these today?
  - Rely on bank, Visa, Mastercard, …
Imagine public ledger of transactions

- Every transaction ("A paid $X to B") in ledger

Benefits:
- Any user cannot spend more money than earned

How to achieve such a public ledger?

- Paxos log?

Any user can propose transaction between any pair of users!
Encryption and Hashing

- Every user has (public key, private key) pair
- $Enc(m, pub_u)$: can decrypt only with $priv_u$
- $Sign(m, priv_u)$: can use $pub_u$ to verify signature

- Cryptographic hash function:
  - Hard to infer value given $hash(value)$
Preventing Theft

- Represent coin transfer from Alice to Bob as:
  \[ T = pub_{Bob}, \text{sign}(hash(T'), priv_{Alice}) \]
  - \( T' \) is transaction via which Alice acquired this coin

- When Bob transfers coin to Charlie later:
  \[ T'' = pub_{Charlie}, \text{sign}(hash(T), priv_{Bob}) \]
  - Anyone can use \( pub_{Bob} \) from \( T \) to verify signature

- What would it take to spend another user’s cash?
Transactions

- Note that the previous slide shows how transactions are crafted.
- The output of the transaction is the currency.
  - The precision of the output of the transaction limits the extent to which the currency can be subdivided.
    - Smallest unit is satoshi and $10^8$ satoshis is one bitcoin.
- As seen in the previous slide, each output also consists of some indicator of the public key needed to redeem the currency.
Public Ledger

- Distributed system comprising 1000s of nodes
- **Broadcast** transactions; **valid if majority report**
- No money stolen unless private key leaks

- **How to identify majority?** Majority of IP addrs?
- **What can Mallory do if she controls majority?**
  - Export different views of ledger to different users
  - Double spending!
- **Sybil attack:** Same user runs many nodes
Desired Properties of Ledger

- **Strongly consistent**
  - All users must see the same set of transactions

- **Append-only**
  - Can only add transactions
  - Cannot remove transactions
Every node **must do work to participate**

- Called mining
- Essentially relates to solving a puzzle – whoever solves it first is able to add its block after others have verified.
Structure of Bitcoin Ledger

- Each miner picks a set of transactions for new block
- Links to previous block by including its hash
- Pick nonce for header
The puzzle is: Find nonce such that

\[
\text{hash (nonce } \mid \mid \text{ prev_hash } \mid \mid \text{ block data) } < \text{ target}
\]

i.e., hash has certain number of leading 0’s

- At any time, all nodes in race to identify nonce for next block
- Target set such that new block every 10 minutes
- Incentive for any node to participate?
Coping with Forks

- “Correct” nodes accept longest chain (most difficult to break computationally)
  - Older a block, the “safer” it is from being deleted
- Common practice: Transaction 6 blocks deep “committed” (no formal grounding).
Block confirmation

- Consensus is gradual – so users must wait for transactions to be accepted.
- During a fork one of the branches will be eventually discarded after miners converge on the other.
- If the two branches include “conflicting” transactions, one may be included in the longest chain.
  - However, if the other chain later surpasses, it may have to be revoked.
  - Sometimes could result in double spending (although rare).
- If majority of miners follow default protocol, Bitcoin avoids these issues.
Randomized leader election

Each time a nonce is found:

- New leader elected for past epoch (~10 min)
- Leader decides which transactions comprise block

- Probability of a node selected as leader?
  - Proportional to node’s % of global hashing power
    - Because more likely to solve the puzzle.
    - Miners could get paid a part of the transaction fees (transactions fees also eliminates flooding of small transactions).
Scaling Bitcoin

- **Scaling limitations**
  - 1 block = 1 MB max (~ 2000 transactions)
  - 1 block every 10 mins $\Rightarrow$ 3-4 txns / sec

- **Visa peak load comparison**
  - Typically 2,000 txns / sec
  - Peak load in 2013: 47,000 txns / sec

- **Joining requires full download of ledger**

- **High energy consumption**
Impact of Bitcoin

- Idea of public ledger (called blockchain) widely applicable
  - Remove dependence on centralized trust

- Impact of using blockchain to create digital currency
  - Various new directions have emerged (but we won’t cover).