Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

Presented by Xumiao Zhang
Agenda

● Motivation
● Transaction
● Blockchain
● Proof-of-Work
● Network
● Incentive
● Optimizations
● Conclusion
● Discussion
Motivation

- Digital payment systems without a trusted third party
- Properties
  - Decentralized
  - No double spending
  - Non-reversible transactions
  - No counterfeiting
Transacting without a trusted third party?

● Ledger
  ○ From: Manos To: Haojun Amount: $20
  ○ From: Manos To: Xumiao Amount: $10
  ○ From: Haojun To: Xumiao Amount: $20
What if …

● Anyone can add a line?
● Ledger
  ○ From: Manos  To: Haojun  Amount: $20
  ○ From: Manos  To: Xumiao  Amount: $10
  ○ From: Manos  To: Xumiao  Amount: $10
  ○ From: Manos  To: Xumiao  Amount: $10
  ○ From: Haojun  To: Xumiao  Amount: $20
Digital Signatures

- **Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

- **Proof from the sender**
Digital Signatures

- **Ledger**
  - From: Manos  To: Haojun  Amount: $20  
  - From: Manos  To: Xumiao  Amount: $10  
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

- **Proof from the sender**
- **Infeasible to forge**
Asymmetric cryptography

- Public key (pk) / Private key (sk)
- Signing / Verifying

Source: wikimedia
Digital Signatures (sign)

- $\text{sign}(\text{message, sk}) = \text{signature}$

- Ledger
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

Manos’ Private key

```
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEA6Te5SLd93XMVa6lhLaAdolyvMYJOHxqkJtjCB5TYzy/rgaoAhtZSvWA7CeSRxzSeD59LFidPujOVVShtkzuMxqQIDAQBABkA0/oCP0Y18S+ZWLr0lkq7kzxBxcRYICTRgve0GVKaq4W2SepdmBW3QvARk7FT9ZSXtadmx5p0vqcqchUZ8X3IFxAlEA/p32ShGPFBYwiRmG6vubJb9wox651r0Q9+JEFl6nPWMClQdQfAGoAfNbs7z7J253HR06qJ0aUINKQ55pHyClvFvwGwlgNvxT+NDr7jGQj7sEiPCII9LAA2kmRvqTIlS3oYf5WwMCIFHCKUWuYG8yDYu45QBtS1q/nt+mgtoF6npq4thueDPAiEApp3ifeabgjL2wA8wuD0+py3TvAx/5WYbNCXFbEiPBVo=
```

Signature

```
LdAc0H6qOqvVLUS5RPg2zLtPlii198tolTyNm6gp5kQf8jxlvnJ+tU4RFXLMrIQzc1NanR2oQ0lsTPt+IDTk6Vg==
```
Digital Signatures (verify)

- verify(message, signature, pk) = True/False
- Ledger
  - From: Manos     To: Haojun     Amount: $20
  - From: Manos     To: Xumiao     Amount: $10
  - From: Haojun    To: Xumiao     Amount: $20

Signature

LdAc0H6qOqVLuS5RPg2zLttPlLi198toITyNm6gp5kQf8jxIvnJ+tU4RFXLMrlQzc1NanR2oQOIsTPt+IDTk6Vg==

Manos’ Public key

MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAOk3uUi3fd1zFWupYSwHaCMrzGCTh8apPybYwgeU2M8v64GqAlbWUr1gOwnekcc0ng+fSI\nIVUoZM7jMaECAwEAAQ==
Digital Signatures (verify)

- `verify(message, signature, pk) = True/False`
- Ledger
  - From: Manos  To: Haojun  Amount: $20
  - From: **Manos**  To: Xumiao  **Amount: $100**
  - From: Haojun  To: Xumiao  Amount: $20

Signature

LdAc0H6qOqVLuS5RPg2zLtPlIi198toITyNm6gp5kJf8jxIvnJ+U4RFXLMrlQzc1NanR2oQOlsTPt+IDTk6Vg==

Manos’ Public key

MFwwDQYJKoZIhvcNAQEBSsQADSwAwSAJBAOk3uUI3fd1zFWupYSwHaCMrzGCTh8apPybYwgeU2M8v64GqAlbWUr1gOwnkkcc0ng+fSWIVUoZ7jMaECAwEAAQ==
Who hosts the ledger?
Let’s decentralize!

- **Manos’ Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

- **Haojun’s Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

- **Xumiao’s Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20
What if ...

- **Manos’ Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20

- **Haojun’s Ledger**
  - From: Haojun  To: Xumiao  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Manos  To: Haojun  Amount: $20

- **Xumiao’s Ledger**
  - From: Manos  To: Haojun  Amount: $20
  - From: Manos  To: Xumiao  Amount: $10
  - From: Haojun  To: Xumiao  Amount: $20
  - From: Haojun  To: Xumiao  Amount: $20
Cryptographic hash function

- SHA256 Hash
  - Arbitrary length of message → fixed length value
  - 256 bits
- One-directional function
  \[ \text{Hash}(\text{message}) = m \]
- Collision resistance
  - Infeasible to find \( x, y \) s.t. \( \text{Hash}(x) == \text{Hash}(y) \)
Cryptographic hash function

Message:

I love EECS 591!

SHA256:

8a95097abcea8333f18cec1aa5baed25dbc9edc2e08d54d7e463b7f0bea391e5
Cryptographic hash function

Message:

I love EECS 591?

SHA256:

fabebba5866a396770369ea7d37128cc4de1377075f0060bad7ee9819f976498
Cryptographic hash function

Ledger:

- From: Manos  To: Haojun  Amount: $20
- From: Manos  To: Xumiao  Amount: $10
- From: Haojun  To: Xumiao  Amount: $20

SHA256:

2c1a38dfd49e308d65bd629eb2acc24e54f7e9d6643a12bafaaea12853a044e
Cryptographic hash function

Ledger:

- From: Haojun  To: Xumiao  Amount: $20
- From: Manos  To: Xumiao  Amount: $10
- From: Manos  To: Haojun  Amount: $20

SHA256:

- 90a761629bc06e61feac922b7e7f54054d1956f3273e3fdc8984efd7e578e9f4
- ≠ 2c1a38dfd49e308d65bd629eb2acc24e54f7e9d6643a12bafaaaee12853a044e
Cryptographic hash function

Ledger:

From: Manos   To: Haojun   Amount: $20
From: Manos   To: Xumiao   Amount: $10
From: Haojun  To: Xumiao   Amount: $20
From: Haojun  To: Xumiao   Amount: $20

SHA256:

34d79cf7b6bd210d5c7f646936c2f569ed84fb6458a45a0cba079510c155752e
≠ 2c1a38dfd49e308d65bd629eb2acc24e54f7e9d6643a12bafaaeea12853a044e
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manos</td>
<td>Haojun</td>
<td>$20</td>
</tr>
<tr>
<td>Manos</td>
<td>Xumiao</td>
<td>$10</td>
</tr>
<tr>
<td>Haojun</td>
<td>Xumiao</td>
<td>$20</td>
</tr>
<tr>
<td>Lorenzo</td>
<td>Manos</td>
<td>$50</td>
</tr>
<tr>
<td>Manos</td>
<td>Xumiao</td>
<td>$10</td>
</tr>
<tr>
<td>Xumiao</td>
<td>Haojun</td>
<td>$20</td>
</tr>
</tbody>
</table>

Hash: 2c1a38dfd49e308d65bd629eb2acc24e54f7e9d6643a12bafaaee12853a044e

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Amount</th>
</tr>
</thead>
</table>

Hash: 8b1c83bd4b2a80299c821d3040b730199b24177eadae2e9f92dd50bec3ea03b0
Blockchain

Prev. Hash: 04835a87b2d3841d8540ee405b2b3d31e64c8f668049987e0f3a0d64b66cb
From: Manos  To: Haojun  Amount: $20
From: Manos  To: Xumiao  Amount: $10
From: Haojun  To: Xumiao  Amount: $20
...
Hash: 218fe14200236d8bd80acfe3d8dd0feb4e9ec7ea12417c4f90dc90765024306

Prev. Hash: 218fe14200236d8bd80acfe3d8dd0feb4e9ec7ea12417c4f90dc90765024306
From: Lorenzo  To: Manos  Amount: $50
From: Manos  To: Xumiao  Amount: $10
From: Xumiao  To: Haojun  Amount: $20
...
Hash: a172ac854450194e1a54f9a7125ec358db0da78cf6aa39361c8fd277f64be6bf
Blockchain

<table>
<thead>
<tr>
<th>Prev. Hash</th>
<th>From: Manos</th>
<th>To: Haojun</th>
<th>Amount: $20</th>
</tr>
</thead>
<tbody>
<tr>
<td>04835a87bdd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb</td>
<td>From: Manos</td>
<td>To: Xumiao</td>
<td>Amount: $100</td>
</tr>
<tr>
<td>04835a87bdd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb</td>
<td>From: Haojun</td>
<td>To: Xumiao</td>
<td>Amount: $20</td>
</tr>
</tbody>
</table>

...  

| Hash | ccfe40ec02d0e3fe2b1a1b215465da1d5de5ba87eb6564c5f2260530645c63 |

<table>
<thead>
<tr>
<th>Prev. Hash</th>
<th>From: Lorenzo</th>
<th>To: Manos</th>
<th>Amount: $50</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccfe40ec02d0e3fe2b1a1b215465da1d5de5ba87eb6564c5f2260530645c63</td>
<td>From: Manos</td>
<td>To: Xumiao</td>
<td>Amount: $10</td>
</tr>
<tr>
<td>ccfe40ec02d0e3fe2b1a1b215465da1d5de5ba87eb6564c5f2260530645c63</td>
<td>From: Xumiao</td>
<td>To: Haojun</td>
<td>Amount: $20</td>
</tr>
</tbody>
</table>

...  

| Hash | 562aa9eb468cfe51e96cc5fab232e87c7940c27a78f72055e370e85b58ac190d |
Cryptography in Blockchain

- **Transaction-level**
  - Asymmetric cryptography
  - Sign and verify with private/public key pairs
  - Prevent fraudulent transactions

- **Block-level**
  - Cryptographic hash function
  - Wrap a list of transactions
  - Blocks are chained
Which blockchain to trust?
Proof-of-Work

- Prove your computational power
- Find a special hash value for each block
Proof-of-Work

- Find a hash value starting with some ZEROs

Prev. Hash: 04835a87bddd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
From: Manos  To: Haojun  Amount: $20
From: Manos  To: Xumiao  Amount: $10
From: Haojun  To: Xumiao  Amount: $20
...
Hash: 218fe14200236d8bd80acfe3d88dd0feb4e9ec7ea12417c4f90dc90765024306
Proof-of-Work

- Find a hash value starting with some ZEROs by adding a nonce

Prev. Hash: 04835a87bdd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
From: Manos   To: Haojun   Amount: $20
From: Manos   To: Xumiao  Amount: $10
From: Haojun  To: Xumiao  Amount: $20
...
0
Hash: 15c7d3911ac2c2730548197ab940c206a319344b79f8b448dbb7896363bf98ae
Proof-of-Work

- Find a hash value starting with some ZEROs by adding a nonce

Prev. Hash: 04835a87bdd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
From: Manos   To: Haojun   Amount: $20
From: Manos   To: Xumiao  Amount: $10
From: Haojun  To: Xumiao  Amount: $20
...
1
Hash: b2c3ab174a6090d2718414f217b90c2217ea649454c5375114219270be804637
Proof-of-Work

- Find a hash value starting with some ZEROs by adding a nonce

Prev. Hash: 04835a87bddd39841d8540ee405b2bf3d31e64cbf66b049987e0fb3a0d64b66cb
From: Manos  To: Haojun  Amount: $20
From: Manos  To: Xumiao  Amount: $10
From: Haojun  To: Xumiao  Amount: $20
...
591
Hash: 0fc96f5f0991e8bf3b443939ae269c6472416a86e5fa92a1bb23637f5eebcda9
2000 YEARS
LATER
Proof-of-work

- Find a hash value starting with some ZEROs by adding a nonce

Prev. Hash: 04835a87bdd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
From: Manos To: Haojun Amount: $20
From: Manos To: Xumiao Amount: $10
From: Haojun To: Xumiao Amount: $20
...
1824168900
Hash: ddfdb3507ee66a69abb3df64ae205afb1d66934d656d6bd0c4964b32564e32de
Proof-of-work

- Find a hash value starting with some ZEROs by adding a nonce

 Prev. Hash: 04835a87bddd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
 From: Manos     To: Haojun     Amount: $20
 From: Manos     To: Xumiao     Amount: $10
 From: Haojun    To: Xumiao     Amount: $20
 ...
 1824168901
 Hash: 0000000000000000000000003939ae269c6472416a86e5fa92a1bb23637f5eebcda9
Proof-of-work

- Hard to find: $1/2^n$, $n$: number of zeros
- Easy to verify: Just run Hash and count ZEROs

→ Being an attacker is hard, too
Proof-of-work

- Being an attacker is hard, too

Prev. Hash: 04835a87bddd39841d8540ee405b2bf3d31e64cbf668049987e0fb3a0d64b66cb
From: Manos  To: Haojun  Amount: $20
From: Manos  To: Xumiao  Amount: $100
From: Haojun  To: Xumiao  Amount: $20
...
1824168901
Hash: 0000000000091e8bf3b443939ae269e6472416a86e5fa92a1bb23637f5ebe7da98001bc077de2d75013ada427f8684c77daca3b5d07ac7782f15b802e3bd968e1
Network

1. Broadcast transactions
2. Collect new transactions into a block
3. Work on finding a proof-of-work
4. Broadcast the block after finding the nonce
5. Accept the block with valid transactions and not spent
6. Express the acceptance by working on creating next
Conflict

- Two versions of the same block broadcast
Conflict

- Two versions of the same block broadcast
- Wait until hearing additional blocks making one longer
Incentive

- Reward the creator for finishing proof-of-work
  - Reward the first, the most powerful one
- A special transaction (coin) added to the block
  - No sender
  - No signature

- Block creators add coins → Gold miners add gold to circulation
Incentive

- New coins
- Transaction fees

- Want to attack? Why not stay honest?
Optimizations

● Reclaiming disk space
● Simplified payment verification
● Combining and splitting value
Reclaiming Disk Space

- **Merkle Tree**: only the root included in the hash
- Block header ≈ 80B, Block generated every 10min
  - $80 \times 6 \times 24 \times 365 = 4.2\text{MB per year}$
Simplified Payment Verification

- Only keep a copy of the block headers of the longest proof-of-work chain
Combining and Splitting Value

- Unnecessary to separate transaction for every cent
- Multiple inputs and outputs
  - Input
    - Single input from a larger previous transaction OR
    - Multiple inputs combining smaller amounts
  - Output (only two)
    - One for the payment
    - One returning the charge
Privacy

Traditional Privacy Model

Identities → Transactions → Trusted Third Party → Counterparty → Public

New Privacy Model

Identities | Transactions → Public
Conclusion

● A electronic cash system not relying on trust central authorities
  ○ Decentralized, no double spending, no forgery, transaction non-reversible

● A peer-to-peer network using proof-of-work to record history of transactions
  ○ Nodes can leave and rejoin at will
  ○ Vote with CPU power
  ○ Accept/reject blocks by extending/discard them

● Safe if honest nodes control a majority of CPU power
Discussion

- Other applications
  - Ethereum
  - Lite Coin
  - Ripple
- Majority attack
- Refund