Bitcoin:
A Peer-to-Peer Electronic Cash System

by Satoshi Nakamoto

Jungho Bang, Shengtuo Hu

Motivation

Digital payment systems

- No counterfeiting
- No double spending
- Irreversible transaction

Motivation

Properties of **Bitcoin**

- No counterfeiting

  - NOBODY can increase money supply at will

- No double spending

  - NOBODY can spend the same value more than once

- Irreversible transaction

  - NOBODY can undo a transaction

Motivation

Properties of **Bitcoin**

- No counterfeiting

  - NOBODY can increase money supply at will

- No double spending

  - NOBODY can spend the same value more than once

- Irreversible transaction

  - NOBODY can undo a transaction

+ No central authority

  - You trust mathematics and cryptography, instead.

Building block of Bitcoin

Chain of blocks

Blockchain

- Database containing records of all transactions
- Each node in the network has a copy
- Distributed ledger
- Some nodes extend the blockchain and get a reward (miners)

Building block of a block

Signatures (Public / Private keys)

SHA256 hash

Transactions

Previous hash

Nonce

...

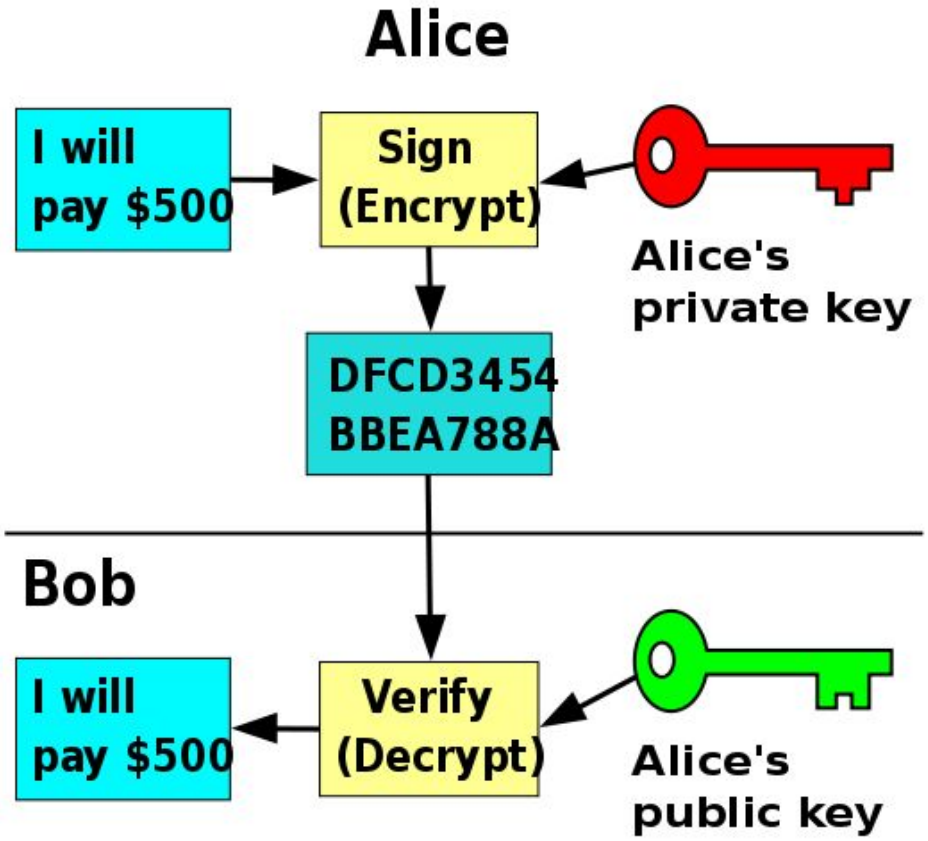
Transaction example

$10 From: Manos To: Jungho

How to prevent fake transactions?

Need to verify the sender

Asymmetrical cryptography
- Private key to sign, Public key to verify



https://commons.wikimedia.org/wiki/File:Public_key_signing.svg

Signature - signing

Transaction:
$10 From: Manos To: Jungho

Manos' private key: (Only Manos knows it)
47357636935348788769925560348779787055087122025290575751791995771298267144161

Signature:
3045022100b238de9c2a2111b6955ec13830b663adec7021c9e9e86103c251d459517e3a5202201dcbc
dc7dba48d4a9475bb4611804db8e2ea7ef28cd19cfecea8ff9164fd69cb

Signature - signed

Transaction:
$10 From: Manos To: Jungho

Signature:
3045022100b238de9c2a2111b6955ec13830b663adec7021c9e9e86103c251d459517e3a5202201dcbc
dc7dba48d4a9475bb4611804db8e2ea7ef28cd19cfecea8ff9164fd69cb

Signature - verifying

Transaction:

$10 From: Manos To: Jungho

Signature:

3045022100b238de9c2a2111b[illegible]955ec13830b663adec7021c9e9e86[illegible]03c251d459517e3a5202201dcbc
dc7dba48d4a9475bb4611804[illegible]b8e2ea7ef28cd19cfecea8ff9164fd69c

Manos' public key: (Everyone knows it)

04e00d58762e4e3f7ac61456dd8[illegible]ace7d03bd06c3703f35fc640cab[illegible]340ca4d6a0af037b29596387c9854
de367886fdd41107f49f55f1b1e922[illegible]444f4d0dc350ae

Signature - verifying

Transaction:

$100 From: Manos To: Jungho

Signature:

3045022100b238de9c2a2111b6955ec13830b[illegible]63adec7[illegible]21c9e9e86103c251d459517e3a5202201dcbc
dc7dba48d4a9475bb4611804db8e2ea7ef28cd19[illegible]a8ff9164fd69cb

Manos' public key: (Everyone knows it)

04e00d58762e4e3f7ac61456dd86ace7[illegible]03bd06c3703f35fc640[illegible]bf840ca4d6a0af037b29596387c9854
de367886fdd41107f49f55f1b1e922d444f4d0dc350ae

Signature

Verify using signature and public key

Prevent unauthorized transactions

How to store list of transactions?

SHA256 Hash

Cryptographic hash function

One way function – it cannot be decrypted back

256-bit hash value

Hash(arbitrary-length message *m*) => fixed-length hash value *h*

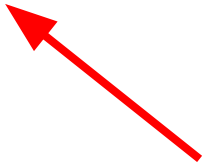
SHA256 Hash

Data:
EECS 591 is cool

Hash:
90f633c551f24e72e30586967404c8a2f2316366963cf78d626029b63c7d93a4

SHA256 Hash

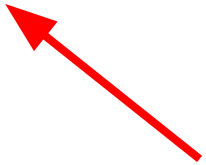
Data:
EECS 591 is cool.



Hash:
ad91ff980d1594684aa22792eb9a5234b122ed3943ba21d6f512d7d3bb27375e

SHA256 Hash

Data:
EECS 591 is cool!



Hash:
54e2d287c6c505f7d34569e02a2ae202dd04f56ca348b5e09db77c76622326d8

SHA256 Hash

As a ledger, the data has to be transactions

Record list of transactions in blocks

- sender
- receiver
- amount

SHA256 Hash

Data:
EECS 591 is cool

Hash:
90f633c551f24e72e30586967404c8a2f2316366963cf78d626029b63c7d93a4

SHA256 Hash

Data:

$100	From: UMich	To: Manos
$10	From: Manos	To: Jungho
$10	From: Manos	To: Shengtuo

Hash:

017726d548a567ce185b3d82d65ef3f2a4cebeb6180054523820fb0e25132258

SHA256 Hash

Data:

$100	From: UMich	To: Manos
$10	From: Manos	To: Jungho
$10	From: Manos	To: Jungho
$10	From: Manos	To: Jungho
$10	From: Manos	To: Shengtuo

Hash:

017726d548a567ce185b3d82d65ef3f2a4cebeb6180054523820fb0e25132258

SHA256 Hash

Data:

$100	From: UMich	To: Manos
$10	From: Manos	To: Jungho
$10	From: Manos	To: Jungho
$10	From: Manos	To: Jungho
$10	From: Manos	To: Shengtuo

Hash:

~~017726d548a567ce185b3d82d65ef3f2a4cebeb6180054523820fb0e25132258~~
351d7e1d637f6bd383635662081 59db244fdddf49f2cf76cd7b4850d422b41d3

Transactions

Why do we need names?

Let’s use public keys instead!

~~$10~~	~~From: Manos~~	~~To: Jungho~~
$10	From: 04e00d58762e4e3f7a...	To: 048cb846702ece34528...

Transactions

Data:

$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...

$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

$10 From: 04cc17dc12... To: 042222d7a…
Sig: 3045022036cfd31dbdc400993a612bf9ba....

Hash:

a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Block

Transactions:

$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367...

$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010...

$10 From: 04cc17dc12... To: 042222d7a…
Sig: 3045022036cfd31dbdc400993a6....

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3....

Block

Previous hash:
00006908f507a101e89544498...

Transactions:

$100 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...

$10 From: 04cc17dc12... To: 04997ac426...
Sig: 304502210089cbf8f4bc854fb010...

$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3....

Blockchain

Previous hash:
00006908f507a101e89544498...

Transactions:
$100 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$10 From: 04cc17dc12... To: 04997ac42...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3....

Previous hash:
a9e2a5d6100c1fa23580671cc4f3bca3...

Transactions:
$50 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
00007dcbbca72607746138920....

Previous hash:
00007dcbbca72607746138920...

Transactions:
$70 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$20 From: 04cc17dc12... To: 04997ac426...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
0000a9e2a5d6100c1fa2358067....

Blockchain

Previous hash:
00006908f507a101e89544498...

Transactions:
$100 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$90 From: 04cc17dc12... To: 04997ac42...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3....

Previous hash:
a9e2a5d6100c1fa23580671cc4f3bca3...

Transactions:
$50 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
00007dcbbca72607746138920....

Previous hash:
00007dcbbca72607746138920...

Transactions:
$70 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$20 From: 04cc17dc12... To: 04997ac426...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
0000a9e2a5d6100c1fa2358067....

Blockchain

Previous hash:
00006908f507a101e89544498...

Transactions:
$100 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$90 From: 04cc17dc12... To: 04997ac42...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
~~a9e2a5d6100c1fa23580671cc4f3bca3~~....

Previous hash:
~~a9e2a5d6100c1fa23580671cc4f3bca3~~...

Transactions:
$50 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
~~00007dcbbca72607746138920~~....

Previous hash:
~~00007dcbbca72607746138920~~...

Transactions:
$70 From: 04fe1be03... To: 04cc17dc12...
Sig: 3046022100bcfe74e2ee8972367...
$20 From: 04cc17dc12... To: 04997ac426...
Sig: 304502210089cbf8f4bc854fb010...
$10 From: 04cc17dc12... To: 042222d7a...
Sig: 3045022036cfd31dbdc400993a6....

Hash:
~~0000a9e2a5d6100c1fa2358067~~....

Cryptography in Bitcoin

For each transaction:

- Verify using signature and public key
- Prevent unauthorized transactions

For list of transactions:

- Fix the data using hash
- Small change alters all the hash values
- Irreversible transactions

Bitcoin blockchain

Who maintains Bitcoin blockchain?

What is the reward for maintaining?

How is new BTC created?

How to make **consensus** among nodes?

Mining Bitcoin

When you create a block, you can add the first transaction

Special coin-creation transaction (coinbase)

You can collect the reward, only if the block ends up on long consensus branch

Proof-of-Work

To create a block, find a special value for hash

Try to make hash below the target difficulty with Nonce

This computation proves your computing power

Prevent attacks if majority of hash power follow the protocol

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce:

Hash:
a9e2a5d6100c1fa23580671cc4f3bca3c58180d0f55e49f9e49a389f2777

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce: 0

Hash:
70c4093c8521a8cbce34e49bf8c1ed468e451ad21b7da43254c7a73746cc77ce

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce: 1

Hash:
4b8a5bce54a1ee419efa7ff0749f4352fb2750b44c65f352512b96b7740d2555

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce: 713

Hash:
a6aa43dc92c10794abb11c57aad86f63774ff93cd9492f11386137b2da9cfbc4

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce: 42757

Hash:
47adc0d03c12a047e08e7cdf430ec12ed23f2b30049d1ab894a15b5936686e3e

Proof-of-Work: Nonce

Prev Hash:
00006908f507a101e895444986908f507a101e895444986908f507a10

Coinbase:
$5 To: e8954449869...

Data:
$100 From: 04fe1be03... To: 04cc17dc12…
Sig: 3046022100bcfe74e2ee8972367dda52a8...
$10 From: 04cc17dc12... To: 04997ac426…
Sig: 304502210089cbf8f4bc854fb010c3bb774...

Nonce: 42758

Hash:
0000fb031916917b3e8a68a3d55cbf8a3a8965a5496dc68094fc0116dd38e623

Proof-of-Work

Hash and Nonce:
- Hard to find, but easy to verify

The difficulty adapts (number of prefix zeros in hash)

Proof-of-Work

So far, we build a block in one node.

How does a block propagate to the network?

Bitcoin Network

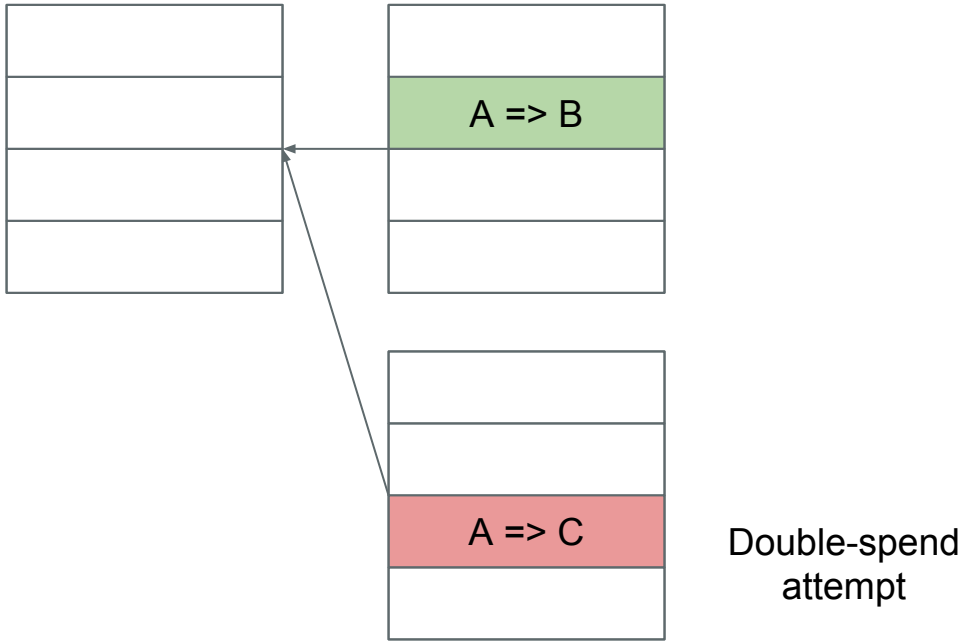
After finding the nonce, the node broadcasts the block to all nodes.

Other nodes accept the block only if all transactions in it are valid and not already spent.

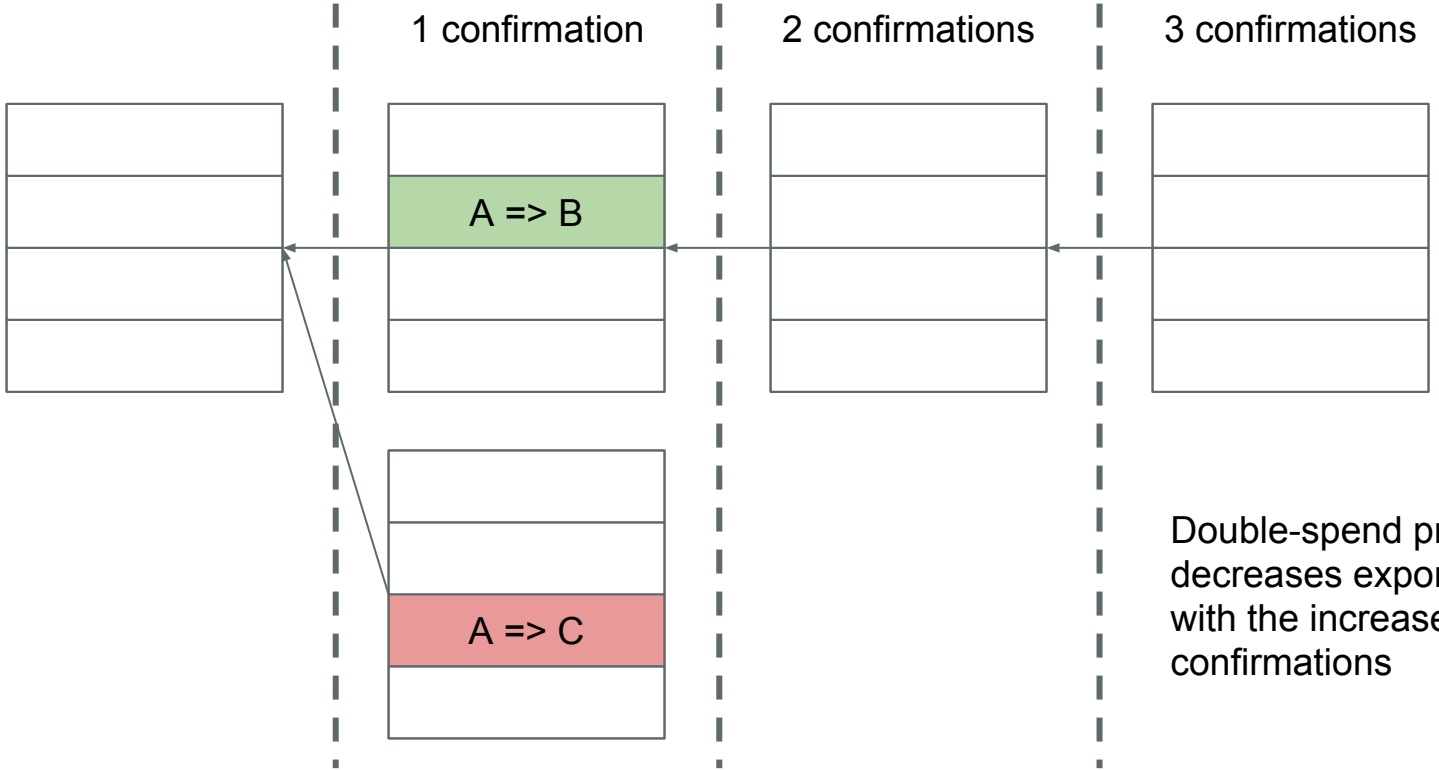
Other nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Double Spending

The same single digital coin can be spent more than once.

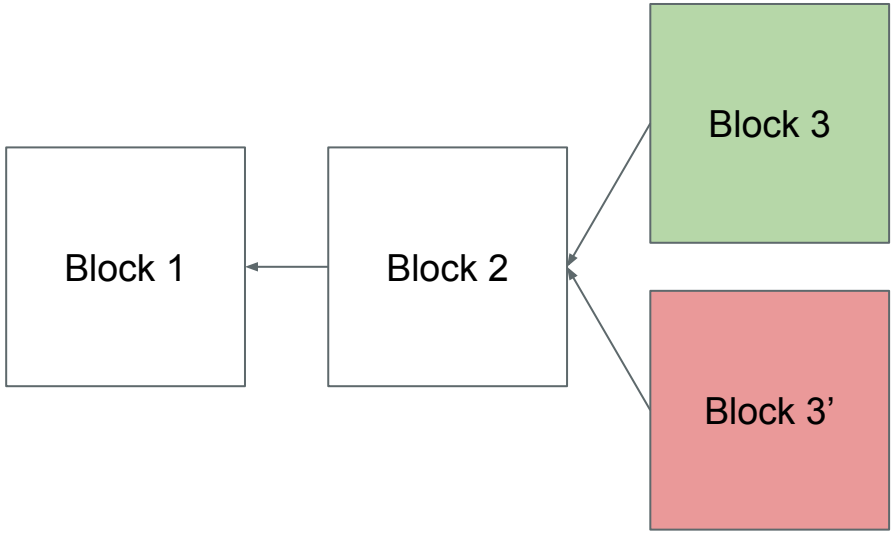


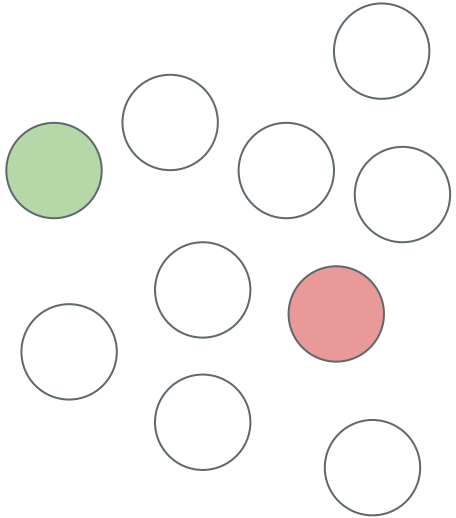
Double Spending



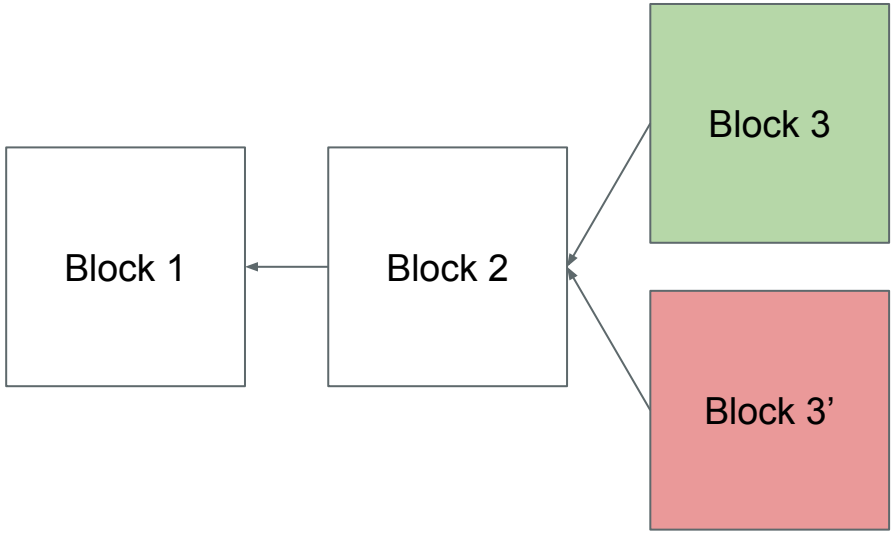
Double-spend probability decreases exponentially with the increase of # of confirmations

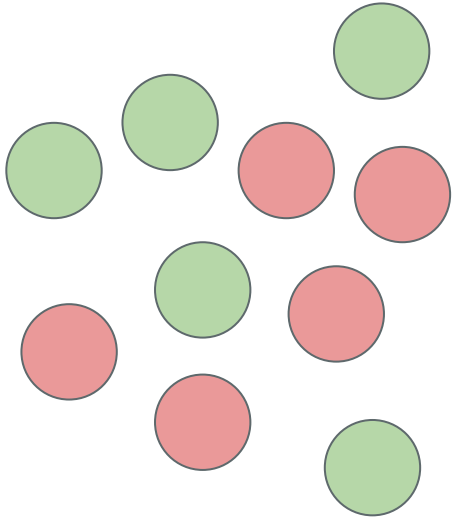
Fork



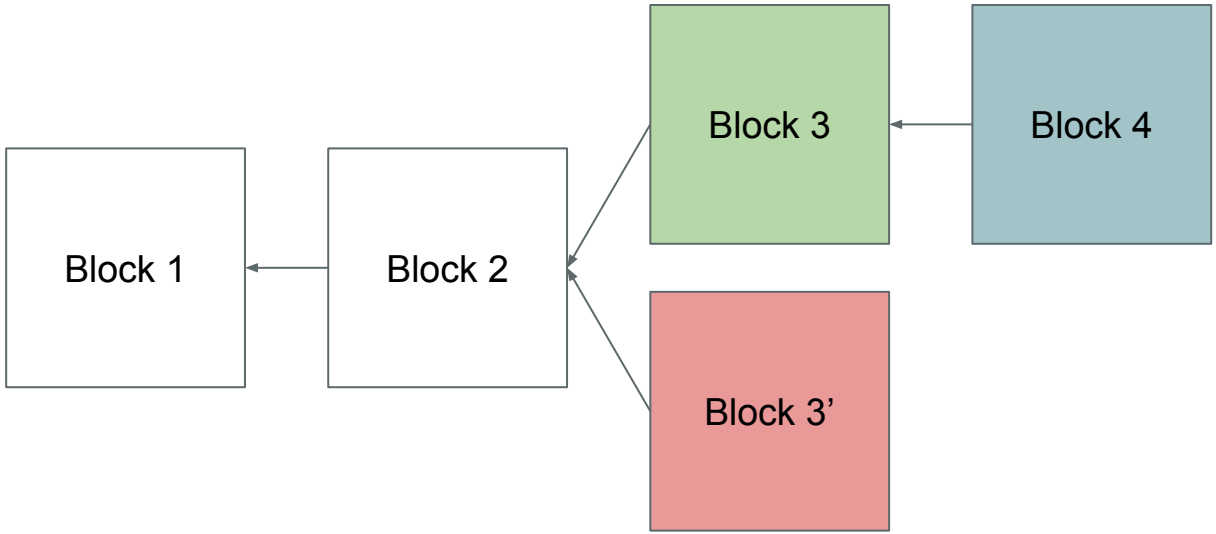


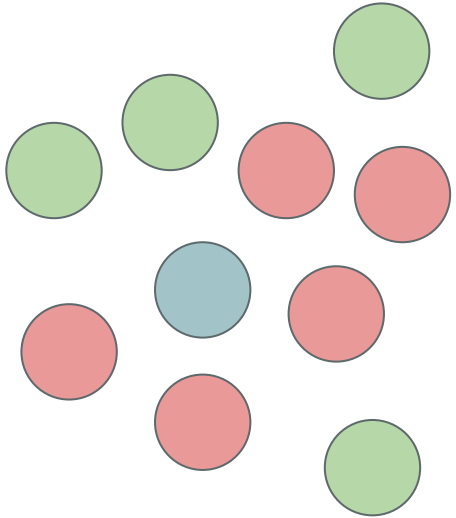
Fork



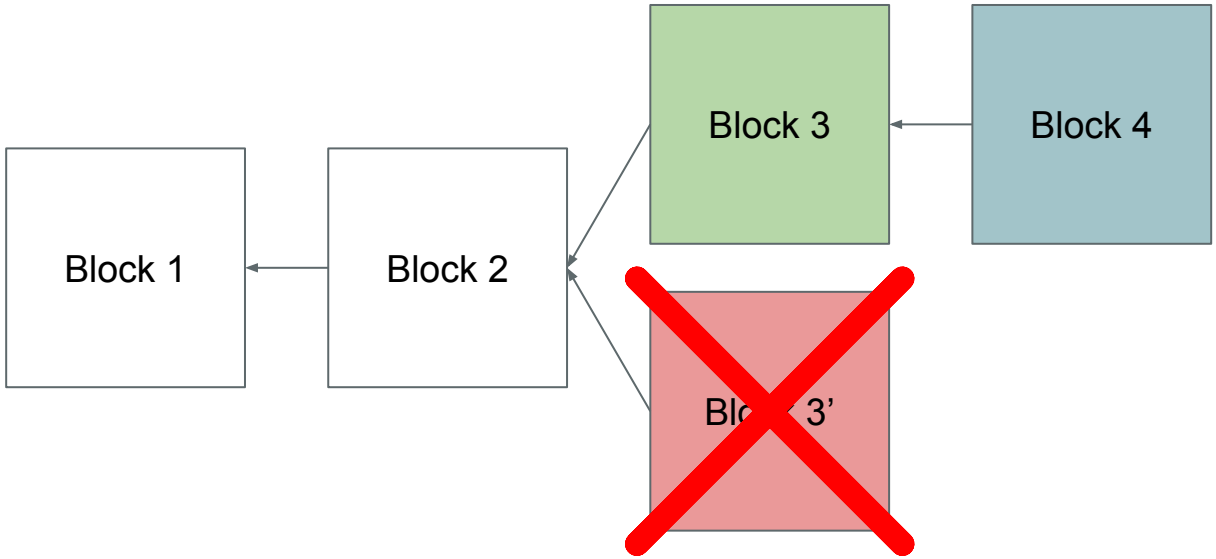


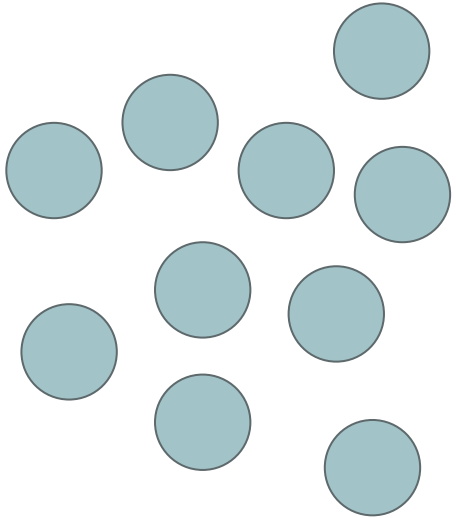
Fork





Fork





Incentive

- The first transaction in a block
  - A new coin
- Transaction fees
- Encourage nodes to stay honest

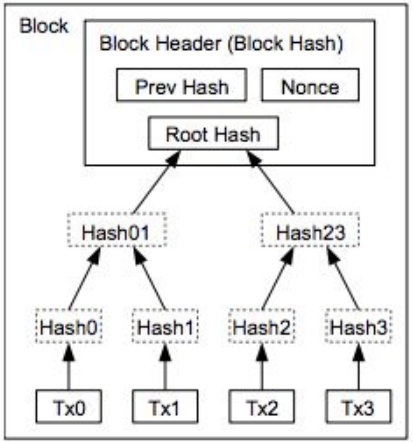
Optimizations

- Reclaiming disk space
- Simplified payment verification
- Combining and splitting value

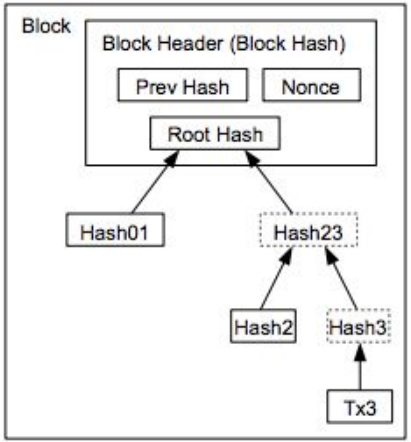
Reclaiming Disk Space

- Merkle Tree
  - Only include root hash in the block's hash

- A block header w/o transactions: ~80 Bytes
- Block generation frequency: every 10 mins
- 80 Bytes * (60 / 10) * 24 * 365 = 4.2 MB



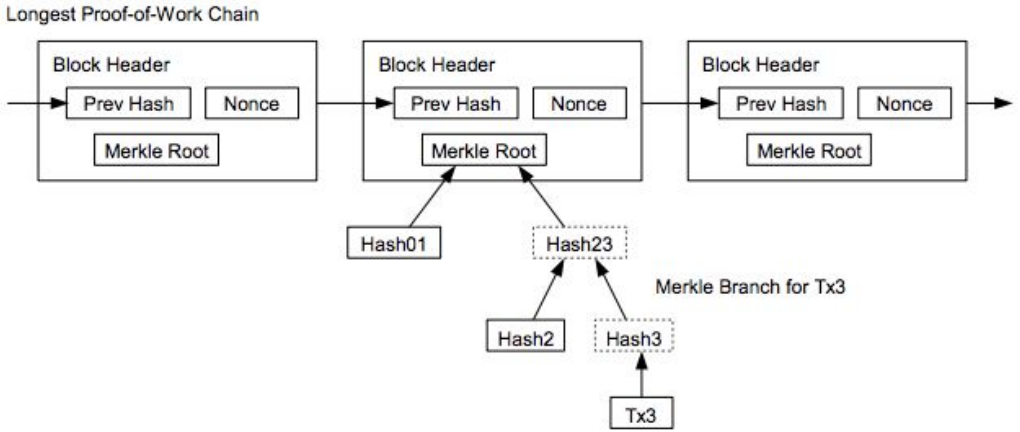
Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

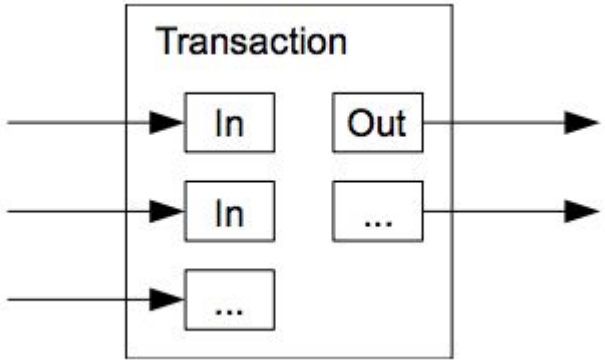
Simplified Payment Verification

- Only need to keep a copy of the block headers of the longest proof-of-work chain

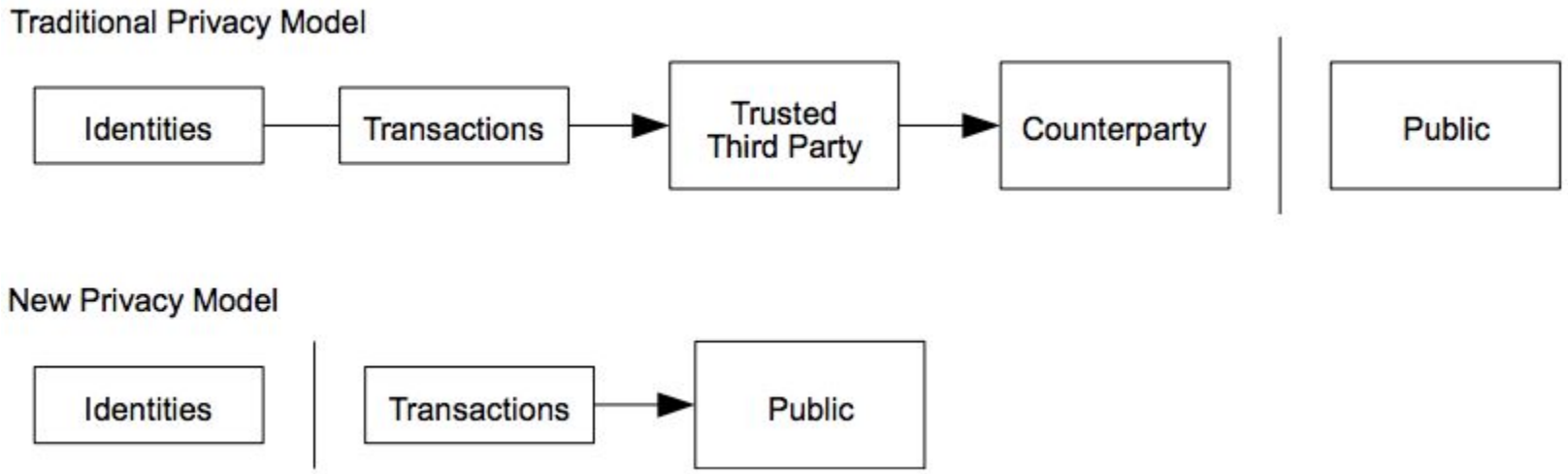


Combining and Splitting Value

- Multiple inputs and outputs
  - A single input from a larger previous transaction
  - Or multiple inputs combining smaller amounts
  - At most two outputs
    - One for the payment
    - One for returning the change



Privacy


Traditional Privacy Model
Identities
Transactions
Trusted Third Party
Counterparty
Public
New Privacy Model
Identities
Transactions
Public

Conclusion

- A system for electronic transaction without relying on trust
  - Decentralized, distributed, voluntary
- A peer-to-peer network using proof-of-work (i.e., a public ledger)
  - To record a public history of transactions
- Proof-of-work for verification

Conclusion

Pros:

- Freedom, Anonymity
- Irreversible records
- Transparent information

Conclusion

Pros:

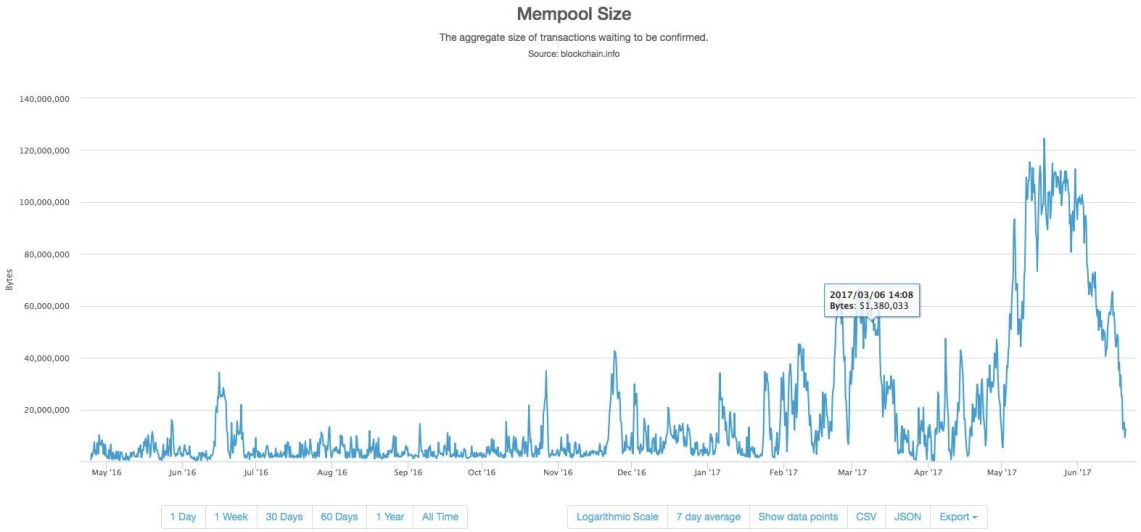
- Freedom, Anonymity
- Irreversible records
- Transparent information

Cons:

- Freedom, Anonymity
- Irreversible records
  - No chargebacks or refunds
- 51% Attack

Issues

- Throughput
  - Block size
- Scalability problem
  - Lightning Network
- Energy consumption
- Real decentralized?



Application of Blockchain

- Smart contracts (Ethereum)
- Decentralized DNS (Namecoin)
- Decentralized voting (Votecoin)
- Decentralized storage network (Filecoin)

Other Consensus Algorithms

- Proof of Stake (PoS)
- Delegated Proof of Stake (DPoS)
- ……

Thanks!

- Comments or feedbacks?