Blockchains, CryptoCurrencies and the Future of Finance

Talk by

Aditya Relangi & Zainil Momin

Blockchains, CryptoCurrencies and the Future of Finance Part 1

by

Aditya Relangi

Overview

- How it came about
- Bitcoin in detail
- Challenges
- Beyond Currency

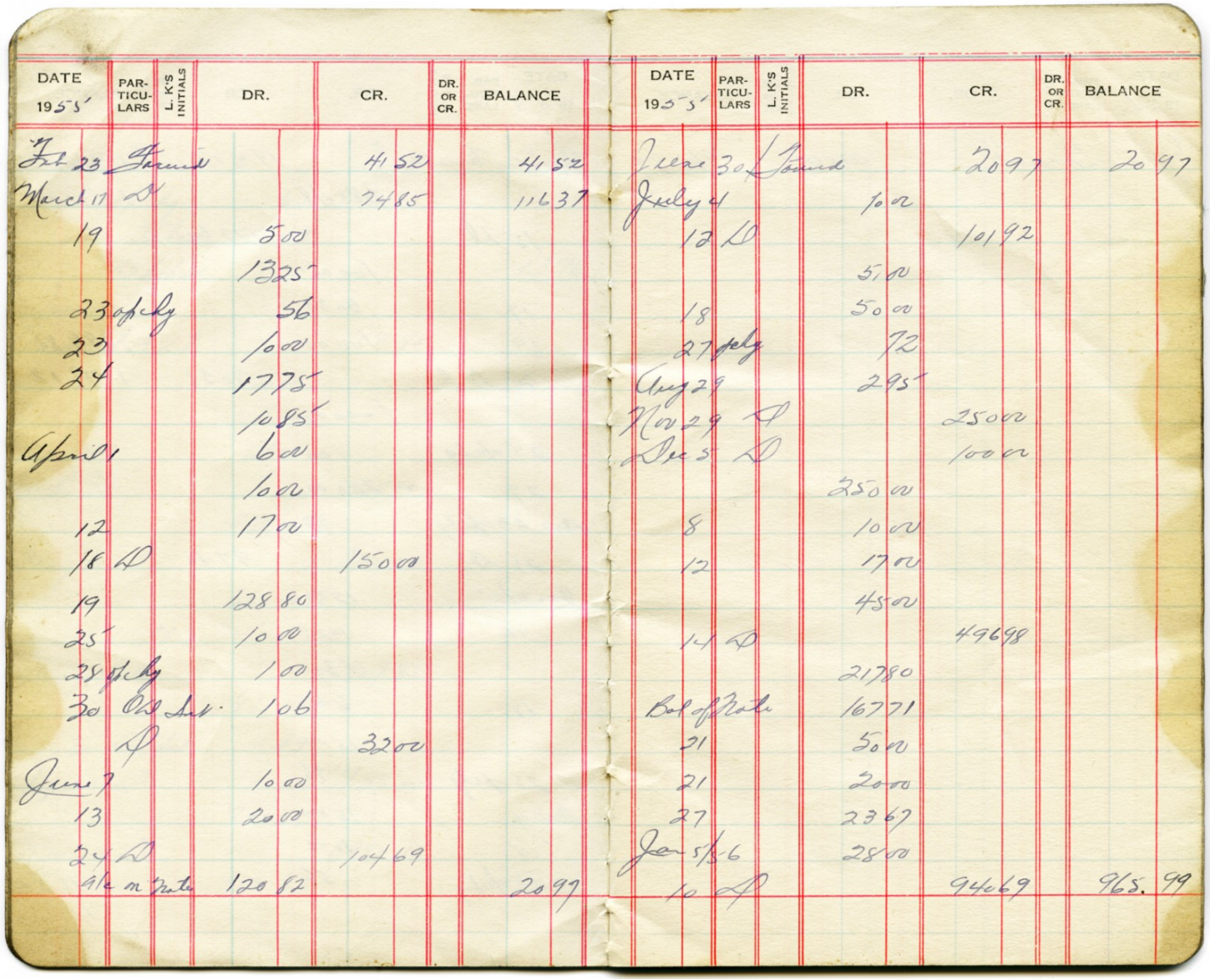
How it came about

- Satashi Nakamoto
- Blockchains/Cryptocurrencies came into prominence with Bitcoin
- White paper published in Nov, 2008
- First bitcoin was mined 3 Jan, 2009

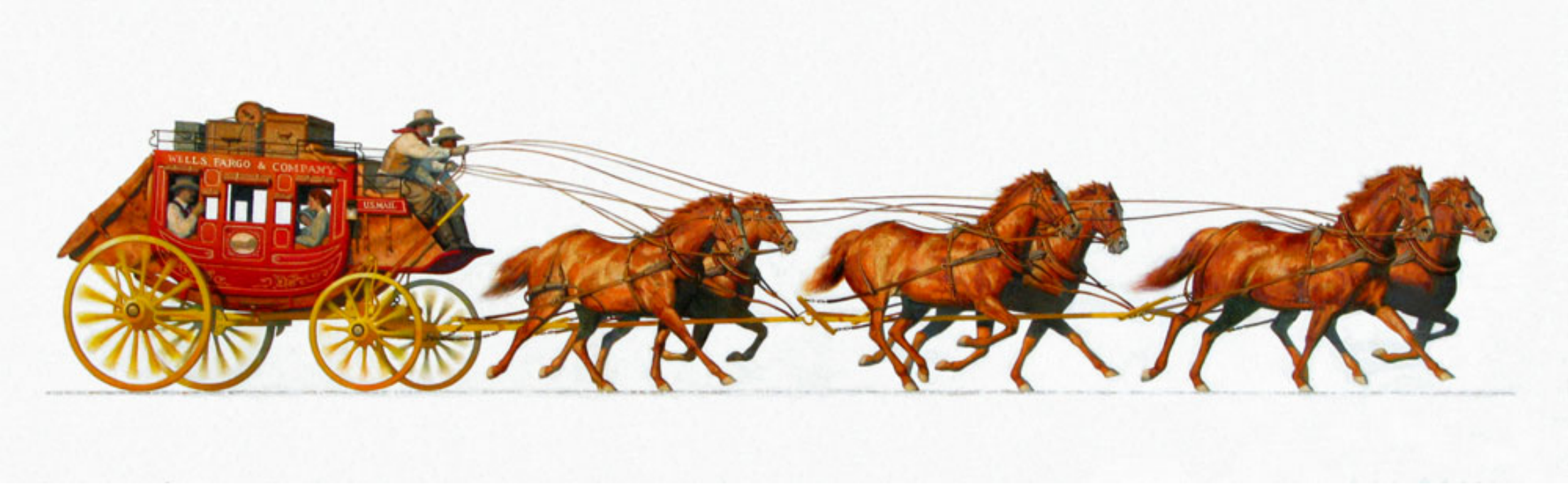
Historically how did people exchange value?

Ledgers

One true source, how true is it?



Trusted intermediary?



Daily Debtor

12 OCT 2017

Adi owes Zainil 10$

By SAMUEL L JACKSON

Well, the way they make shows is, they make one show. That show's called a pilot. Then they show that show to the people who make shows, and on the strength of that one show they decide if they're going to make more shows. Some pilots get picked and become television programs. Some don't, become nothing. She starred in one of the ones that became nothing.

Normally, both your asses would be dead as fucking fried chicken, but you happen to pull this shit while I'm in a transitional period so I don't wanna kill you, I wanna help you

thee.

International Moose Count Underway

By BOB O'BOBSTON

The UN-sponsored International Moose Census got off to a flying start today with hopes for an increase in the worldwide moose population compared to last year's disapointing figures. Among the traditional early reporters were Egypt, returning figures of six moose, a twenty percent increase on 2011's figures of five, and Uruguay whose moose population remains stable at eleven.

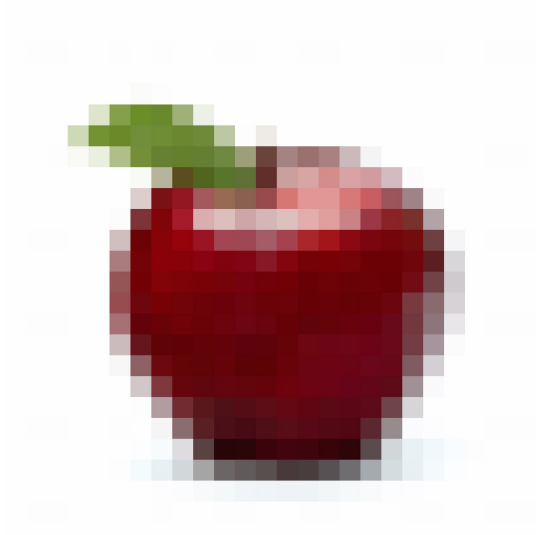
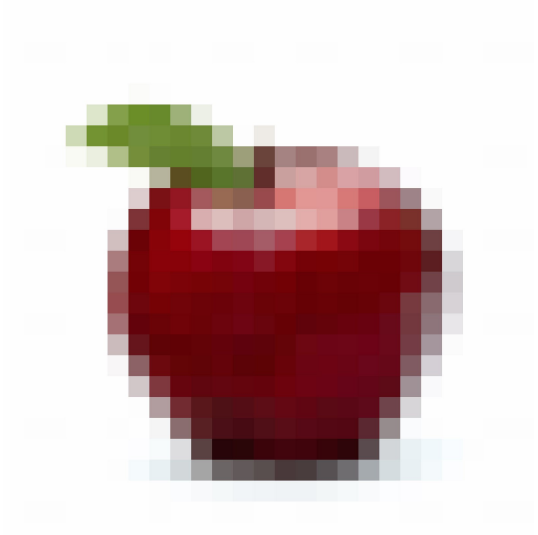
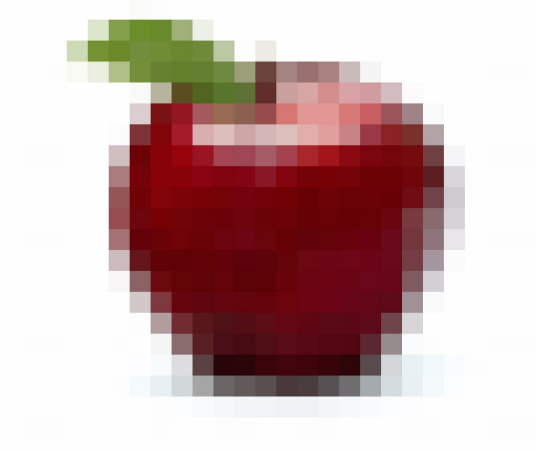
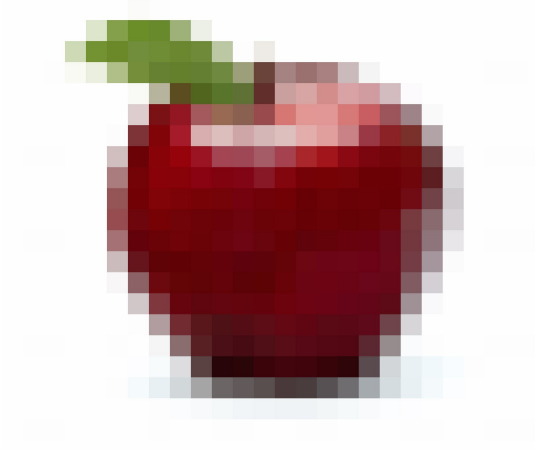
According to Robbie McRobson

markets has been Singapore but the tiny island nation is set to report a net loss, expecting a decrease of more than five percent on last year's 50,000 moose counted. The head of Singapore's Agency for Agriculture, Jing-Feng Lau, explained to an incredulous Singaporean parliament yesterday that bad weather had contributed to this season's poor showing, most notably when a cargo of 150 moose were swept out into the Indian ocean in a monsoon.

Yet again the global demand for moose will be met largely by the US and Canada. The recession-hit States is taking comfort in its moose growth figures with gross production expected to break 700,000 and net exports to grow by 2%. The worldwide dominance of Canada shows no signs of abating though with this year's moose population expected to match

How about a public ledger?

Transfer of digital assets is not the same as transfer of physical assets

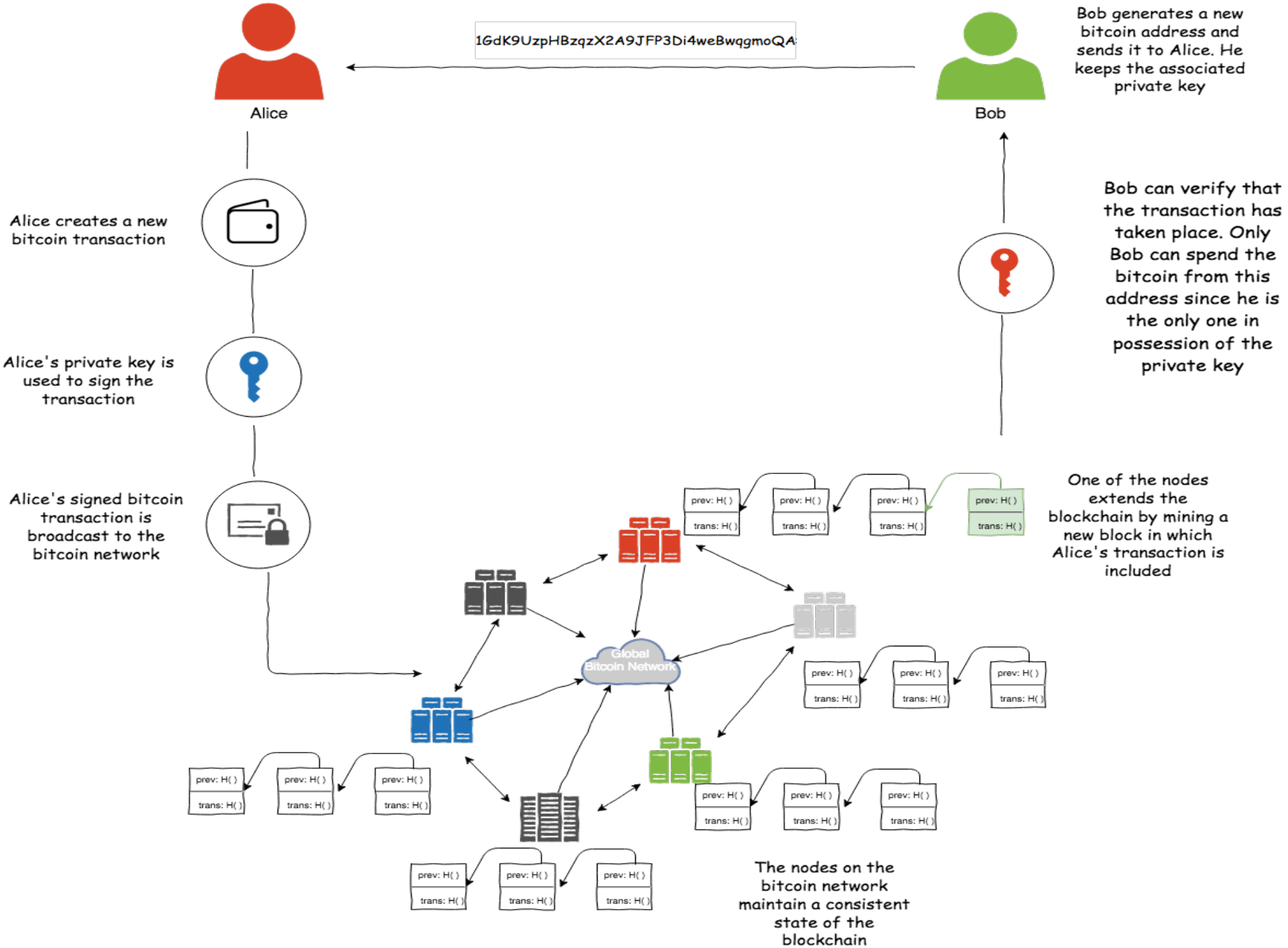
How can we build a secure, incorruptible system in a trustless environment?

Decentralized peer-to-peer network

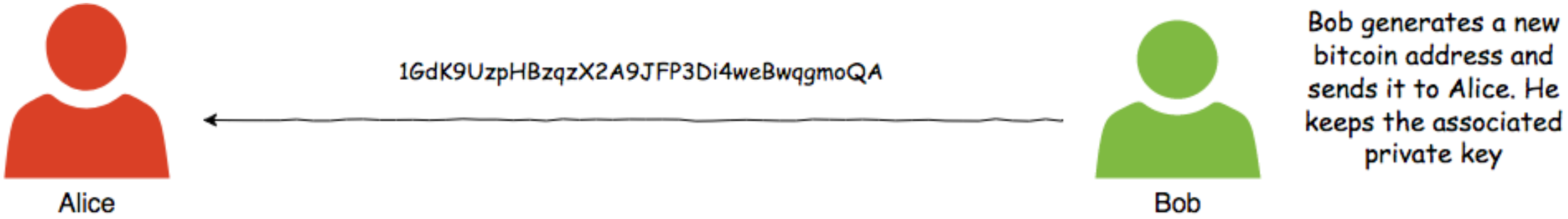
Public transaction ledger

Strong mathematical proof

Bitcoin: High-level Overview



Identities

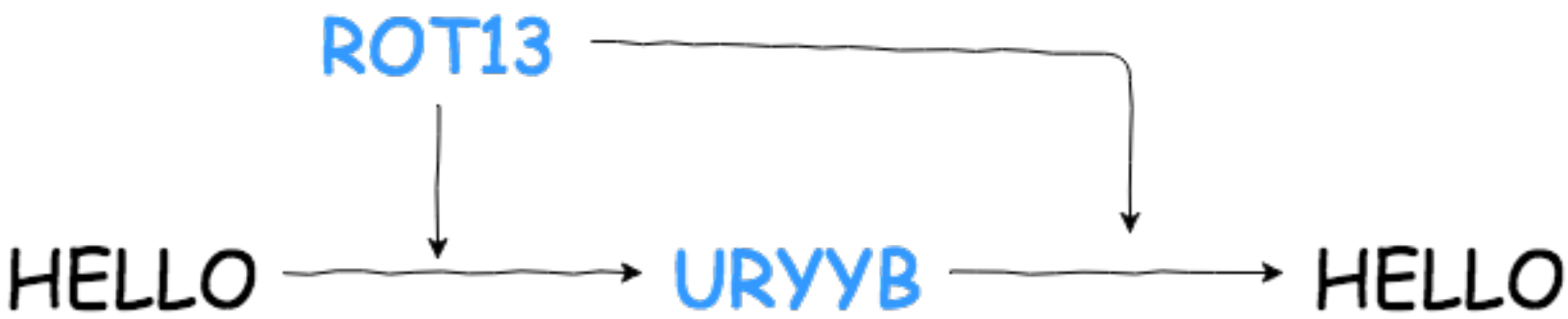

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
Alice
Bob
Bob generates a new bitcoin address and sends it to Alice. He keeps the associated private key

Cryptography

Classical Era

Modern Era

Symmetric Cryptography



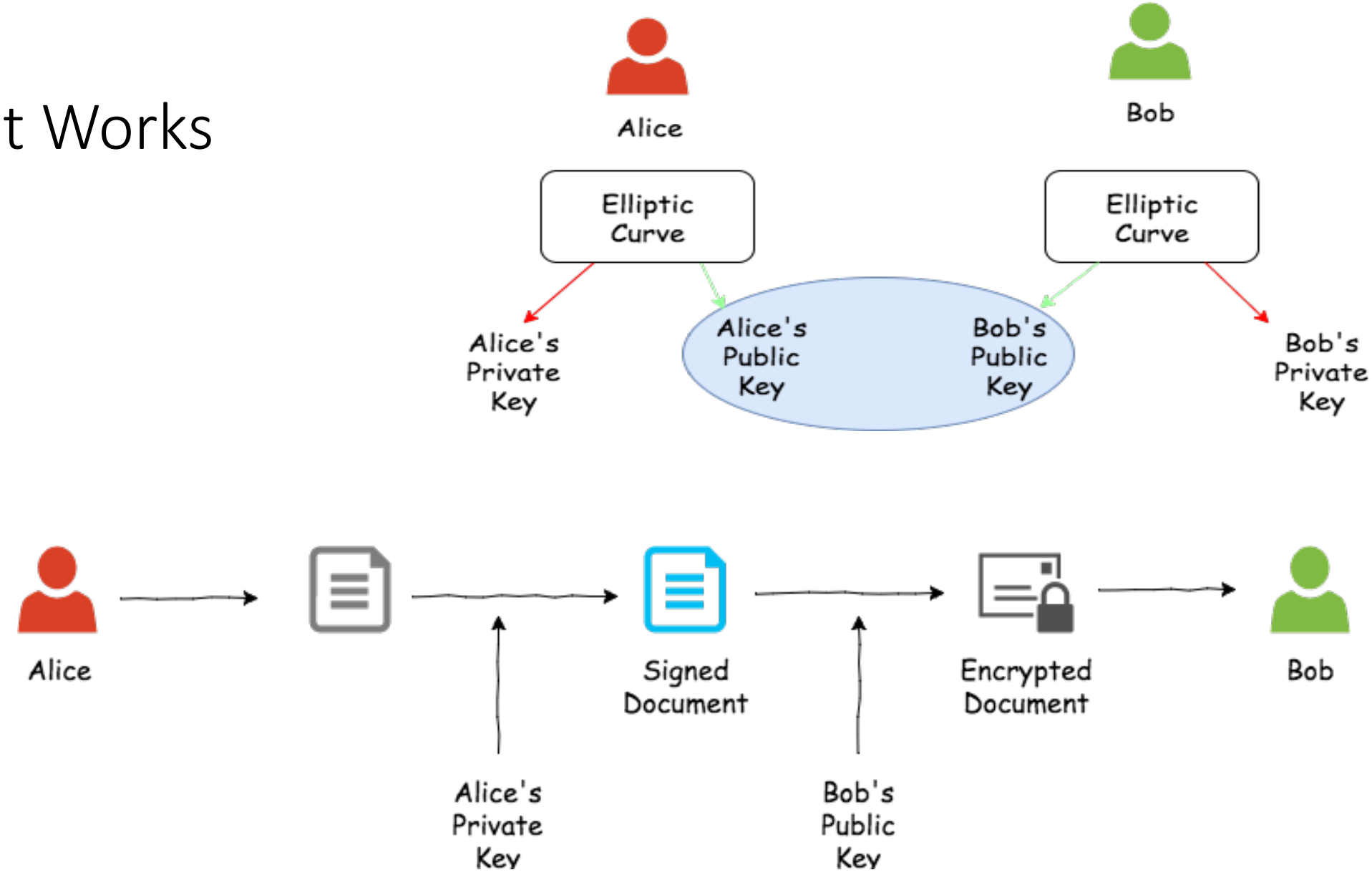
One Key

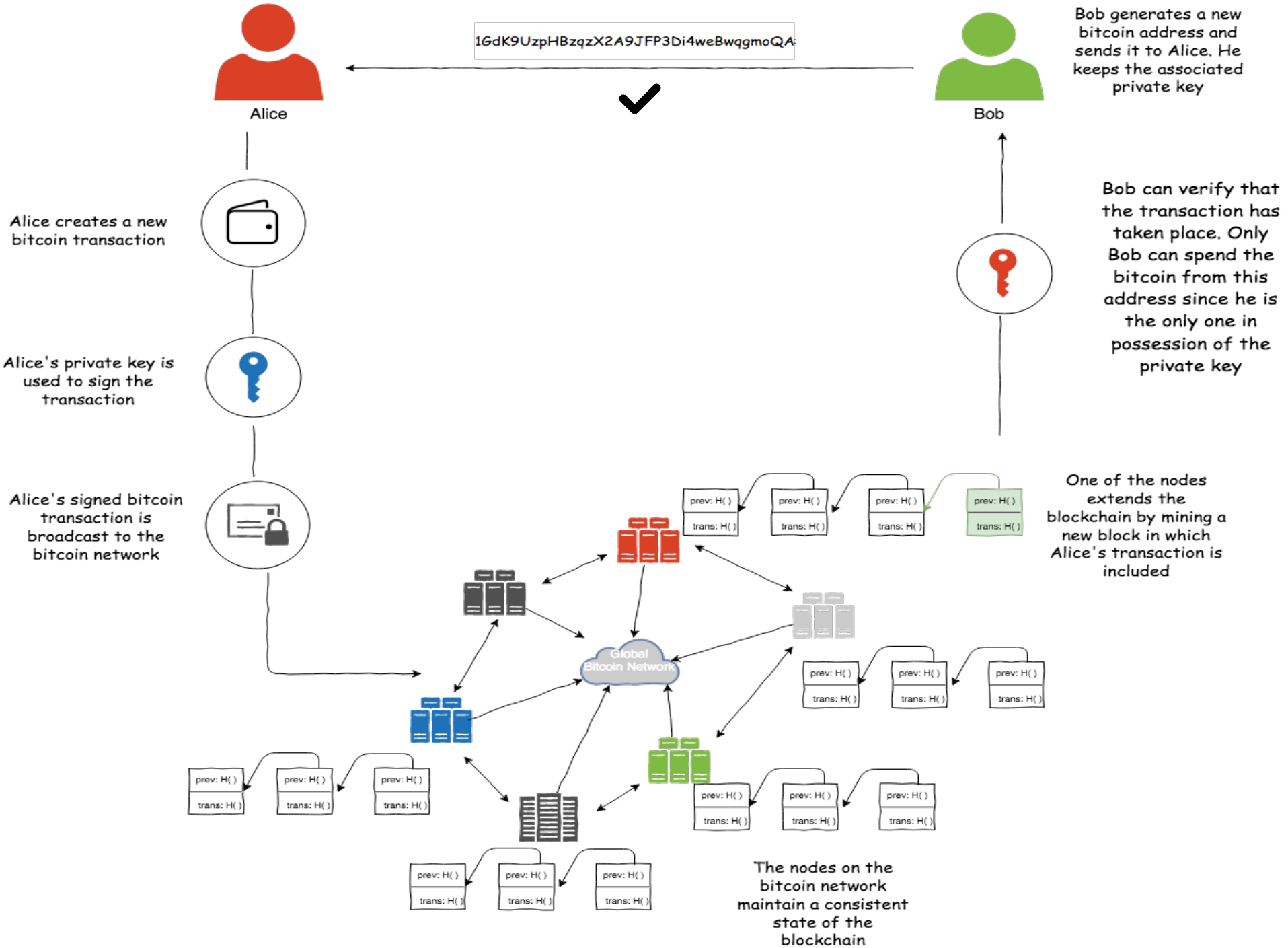
Anyone with the key can access it

Transferring keys is a hassle

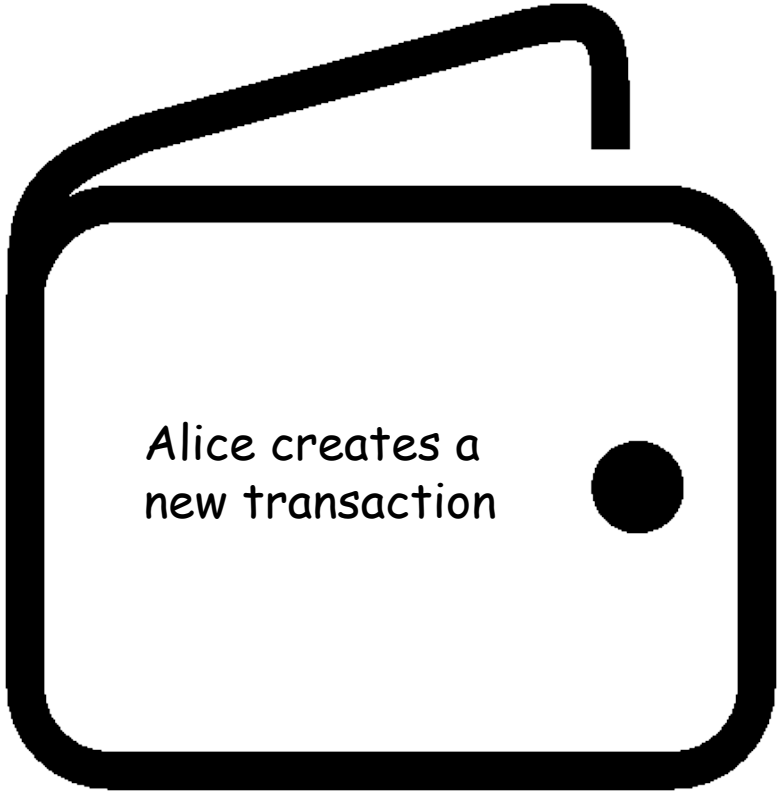
Asymmetric Cryptography

How it Works


Alice
Bob
Elliptic Curve
Elliptic Curve
Alice's Private Key
Alice's Public Key
Bob's Public Key
Bob's Private Key
Alice
Signed Document
Encrypted Document
Bob
Alice's Private Key
Bob's Public Key


1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
Alice
Bob
Bob generates a new bitcoin address and sends it to Alice. He keeps the associated private key
Alice creates a new bitcoin transaction
Alice's private key is used to sign the transaction
Alice's signed bitcoin transaction is broadcast to the bitcoin network
Bob can verify that the transaction has taken place. Only Bob can spend the bitcoin from this address since he is the only one in possession of the private key
One of the nodes extends the blockchain by mining a new block in which Alice's transaction is included
Global Bitcoin Network
prev: H( )
trans: H( )
The nodes on the bitcoin network maintain a consistent state of the blockchain

Wallet



The wallet software uses the unspent output from pervious transactions to create this transaction

The wallet can create a transaction with multiple inputsand outputs.

Immutability

Structure of a Transaction

metadata

input(s)

output(s)


```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "in":[
   {
    "prev_out":{
     "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
     "n":0
    },
     "scriptSig":"30440..."
   },
   {
    "prev_out":{
     "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
     "n":0
    },
    "scriptSig":"3f3a4ce81...."
   }
  ],
  "out":[
   {
    "value":"10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```

Signed Transaction

The signed transaction ensures that it is coming from Alice

Alice's private key is used to sign the transaction

Alice's signed bitcoin transaction is broadcast to the bitcoin network

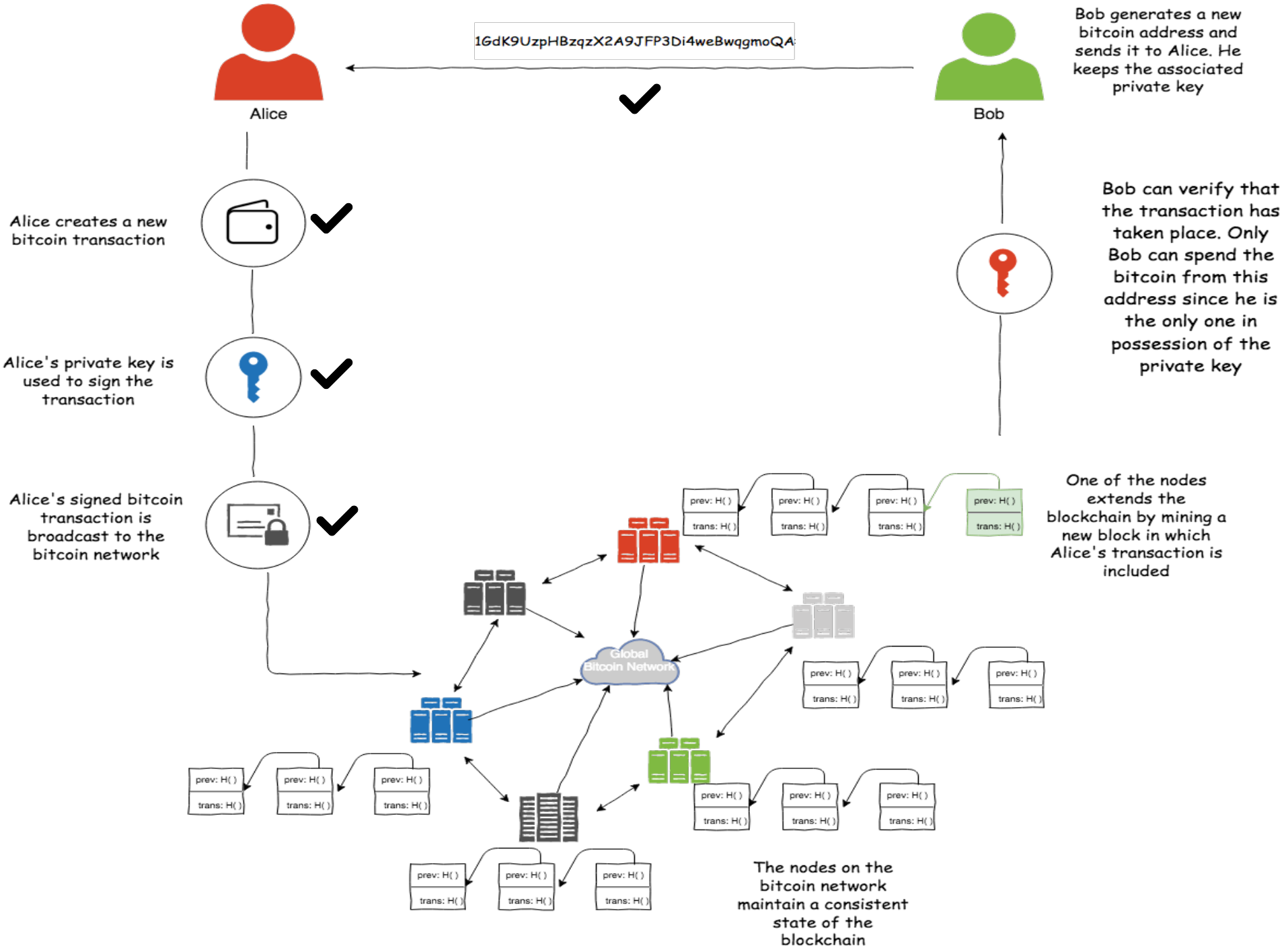
Structure of a Transaction

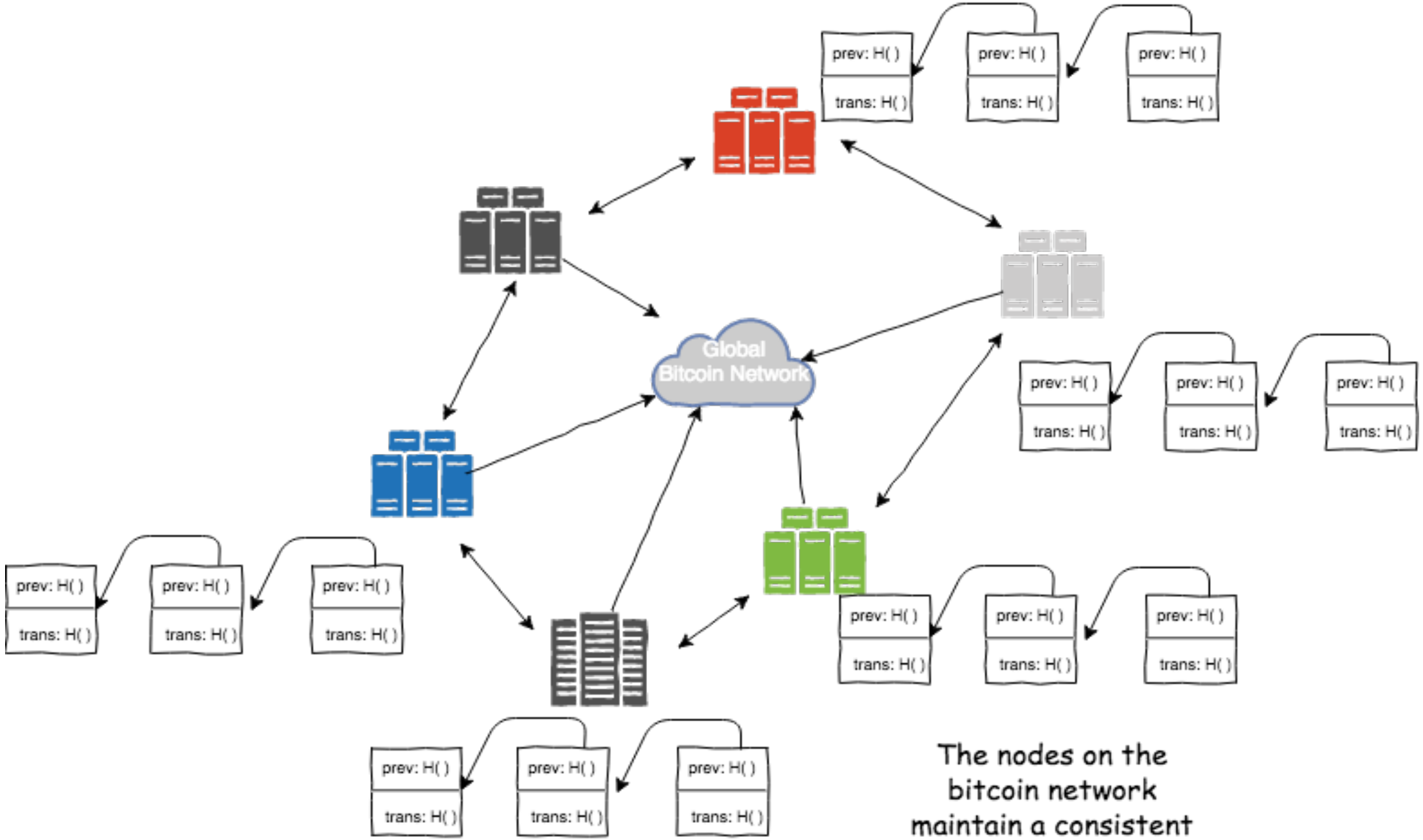
metadata

input(s)

output(s)


```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "in":[
   {
    "prev_out":{
     "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
     "n":0
    },
     "scriptSig":"30440..."
   },
   {
    "prev_out":{
     "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
     "n":0
    },
    "scriptSig":"3f3a4ce81...."
   }
  ],
  "out":[
   {
    "value":"10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```


1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
Alice
Bob
Bob generates a new bitcoin address and sends it to Alice. He keeps the associated private key
Alice creates a new bitcoin transaction
Alice's private key is used to sign the transaction
Alice's signed bitcoin transaction is broadcast to the bitcoin network
Bob can verify that the transaction has taken place. Only Bob can spend the bitcoin from this address since he is the only one in possession of the private key
One of the nodes extends the blockchain by mining a new block in which Alice's transaction is included
Global Bitcoin Network
prev: H( )
trans: H( )
The nodes on the bitcoin network maintain a consistent state of the blockchain



The nodes on the bitcoin network maintain a consistent state of the blockchain


DETOUR

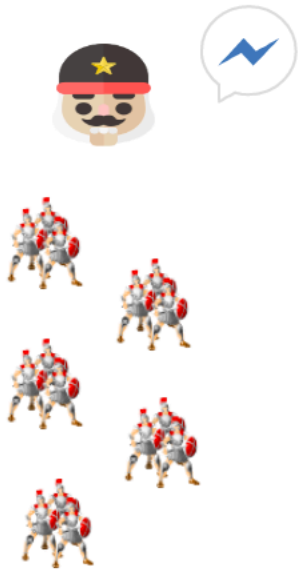
Cryptographic Hash Functions

A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size which is designed to also be a one-way function.

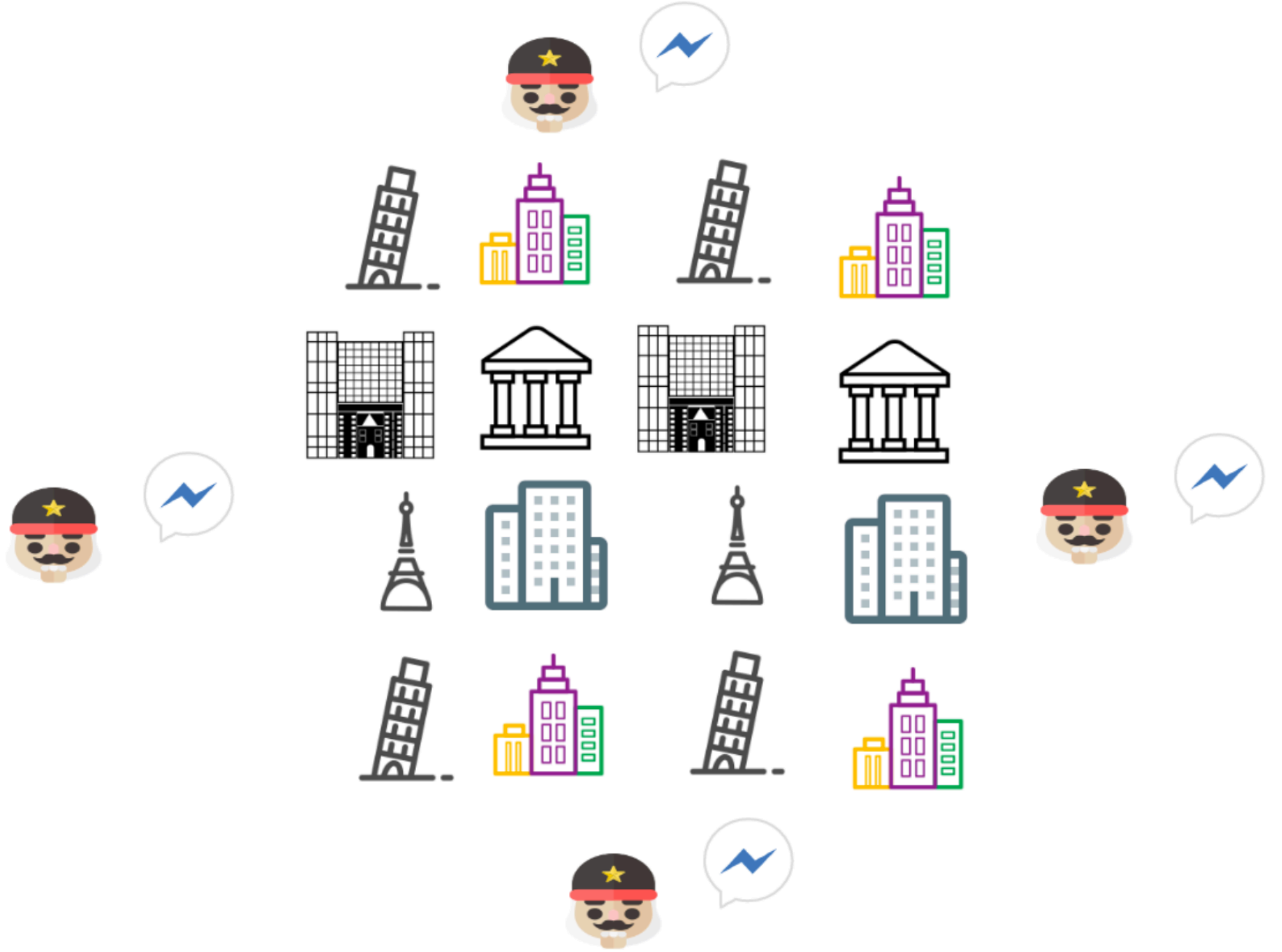
Sha256('HELLO8') = d8ae00e2046dcd2b1e46565a84967e343b81e07eee16895c9146b0cc8cbed47c

Message	Hash
HELLO0	332840f1770b255cfa575247c43bbdad2dda2e083b4f10e9e906bb19b7ebf6b1
HELLO1	de0908f14ca7100599d7abca6d532d13094379827faa2a1f7daa4c90b8d7283c
HELLO2	1421c4691b03d0cd3b0d14cd0dd254487d58e486009c2a97141760080bd654ae
HELLO3	66b769237270c887138e1cc6dfc4785e325e45a20d73499f8a4980db2f28c43b
HELLO4	b85b73224c1b104744d8ae9f0b29b0017387f54c69732d7ef6ff49f335564ec3
HELLO5	a5e8efe56be3923e89d55fac8dff05f50e7cf3cd7e66c1f2a1745ffe7972d498
HELLO6	49c565c90a5248f4ebe2d551ca6901c581093d836b8a0acd562f33808007c5a5
HELLO7	23bcdfedac1a51c295805e67f18e41bd8b152921d3dfe8f962698b1b182bf245
HELLO8	d8ae00e2046dcd2b1e46565a84967e343b81e07eee16895c9146b0cc8cbed47c

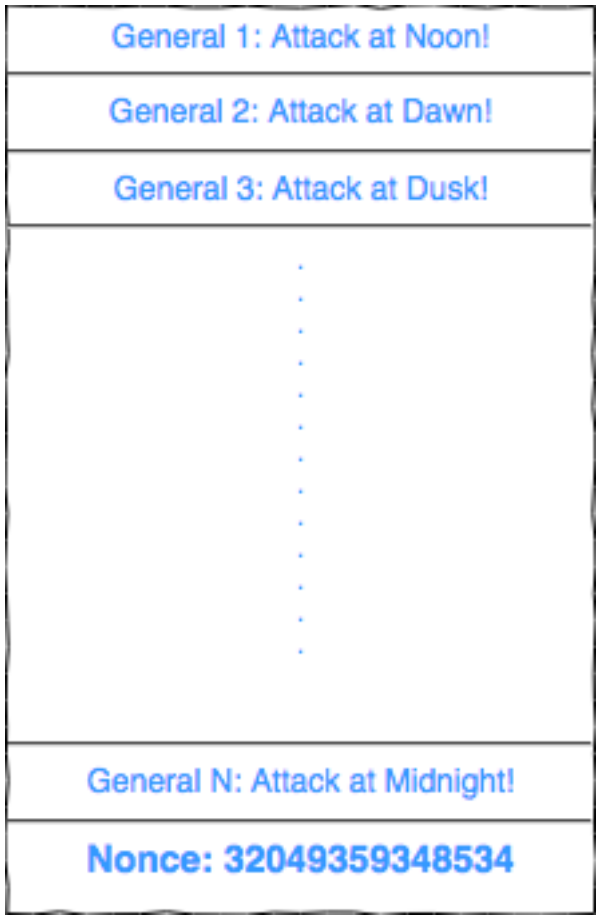
Byzantine Generals Problem



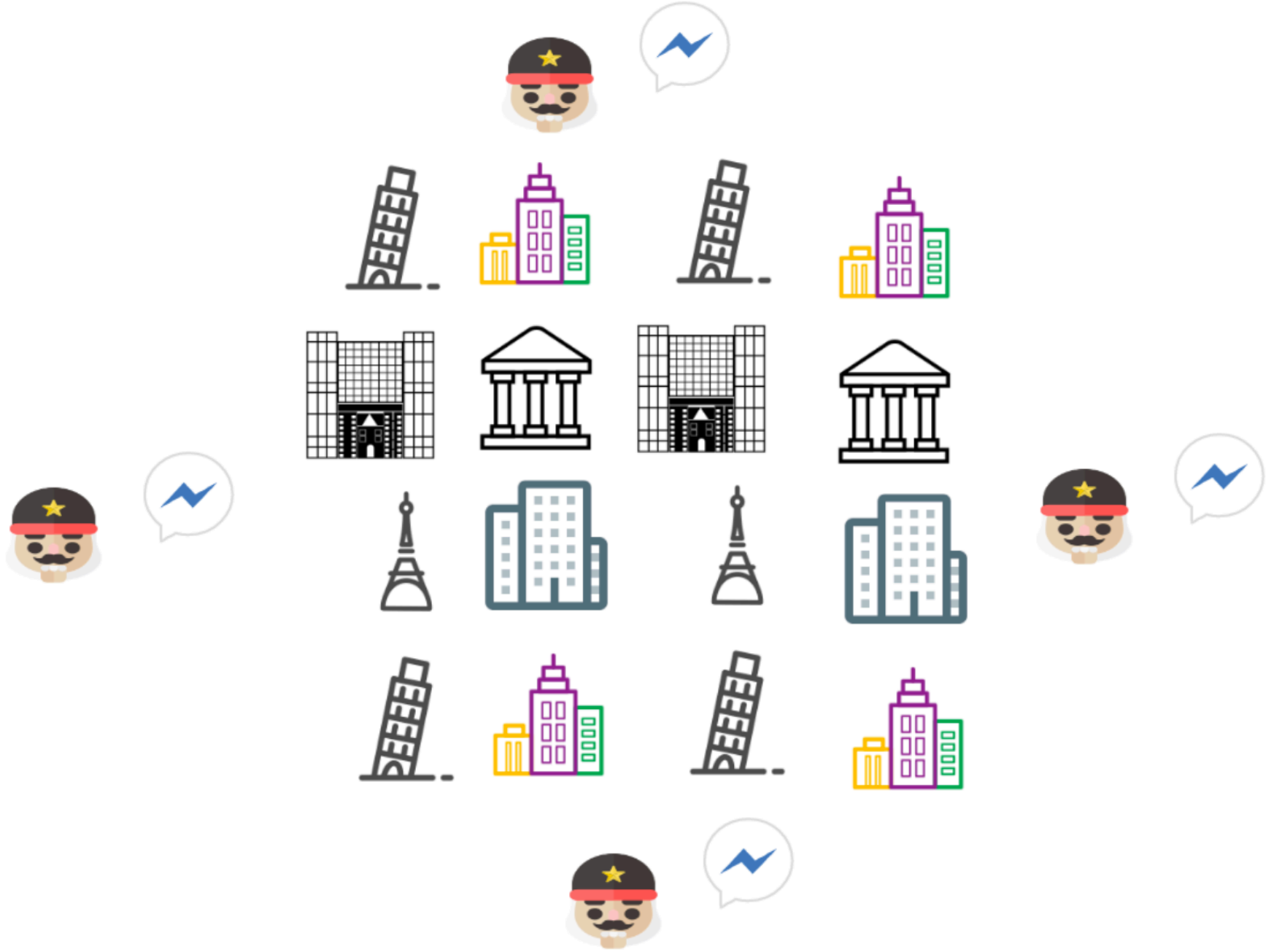

Attack!



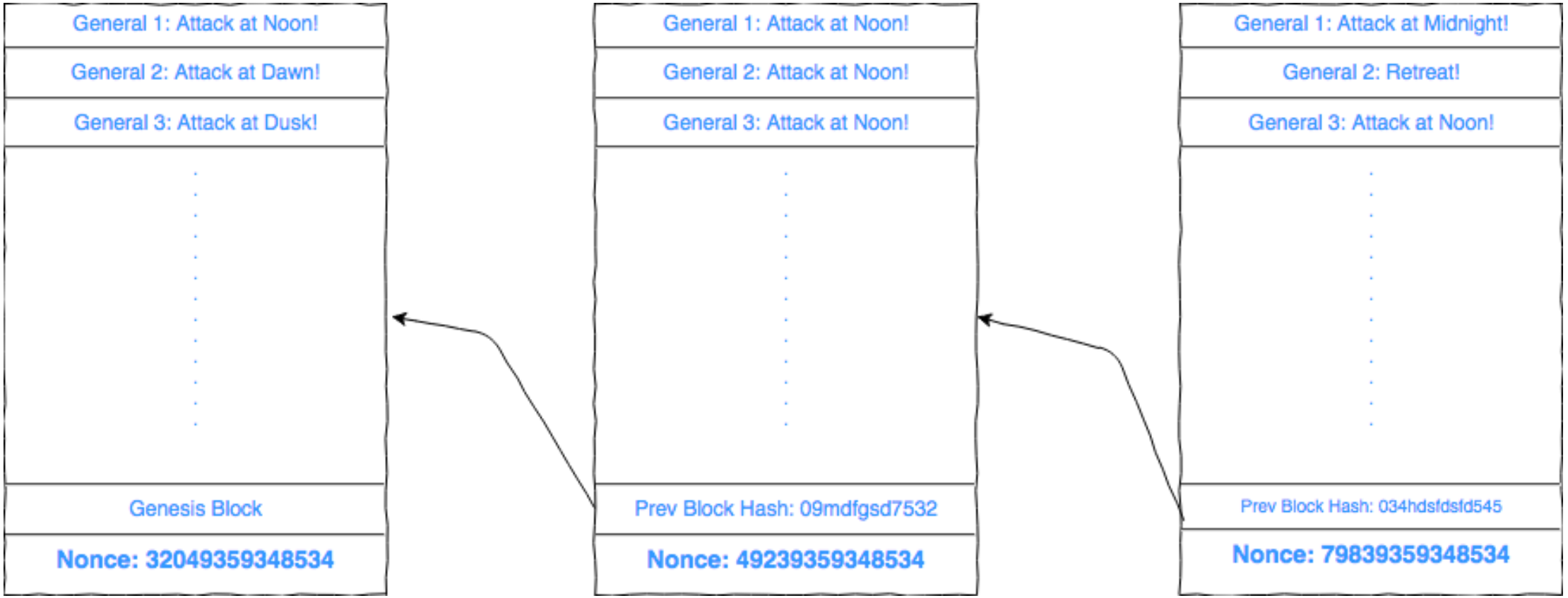
A Block



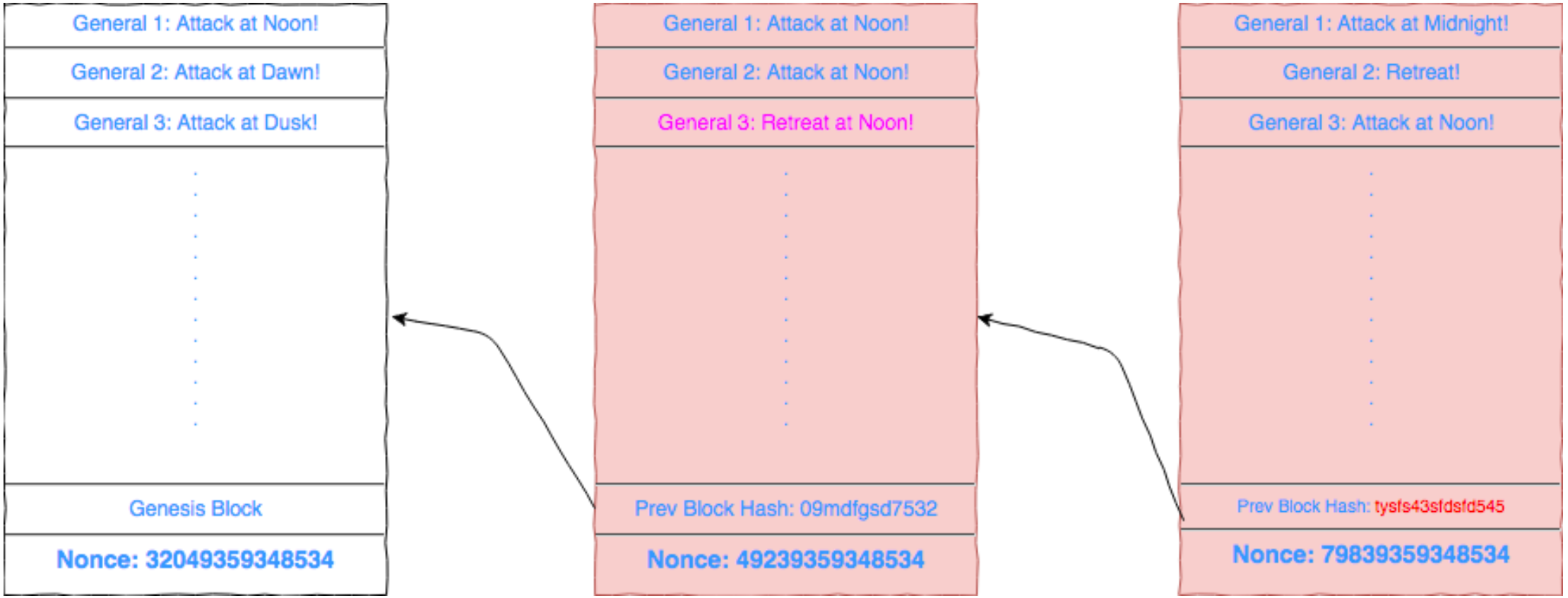
Hash: 00000000000000000c679b8cac54f95c2a5733d36bbb80956101ece2cec6e37



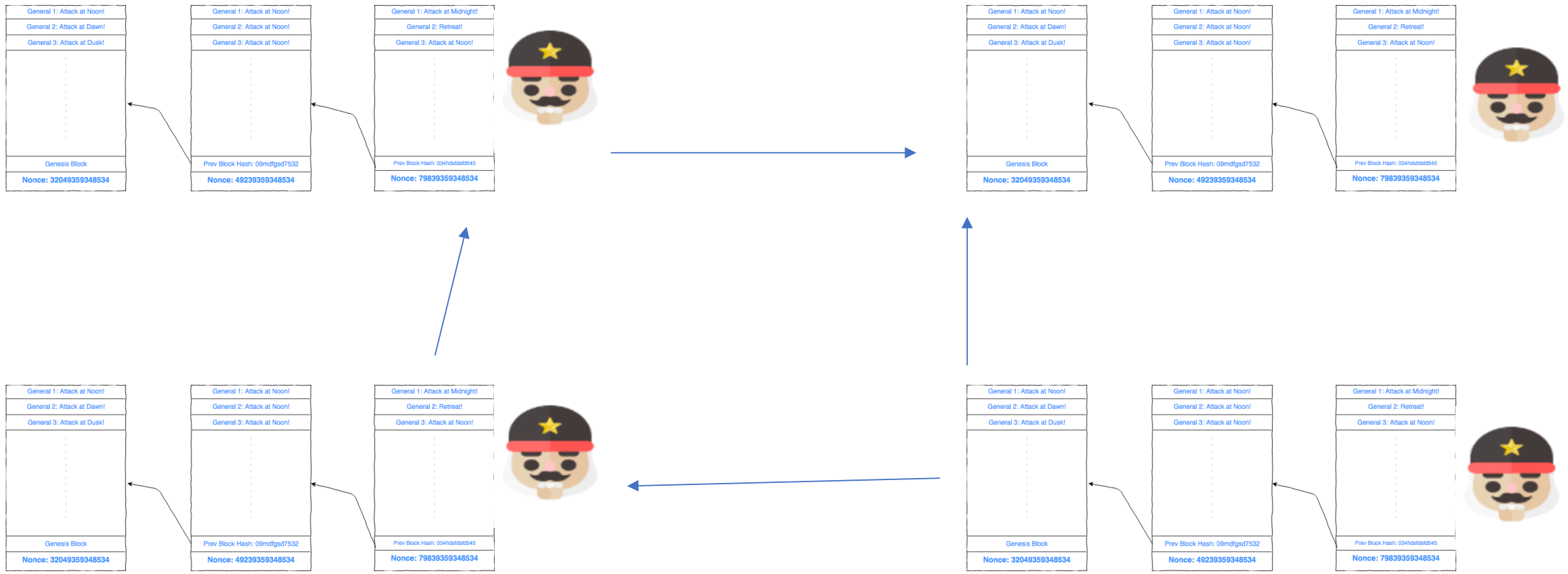
A Block Chain

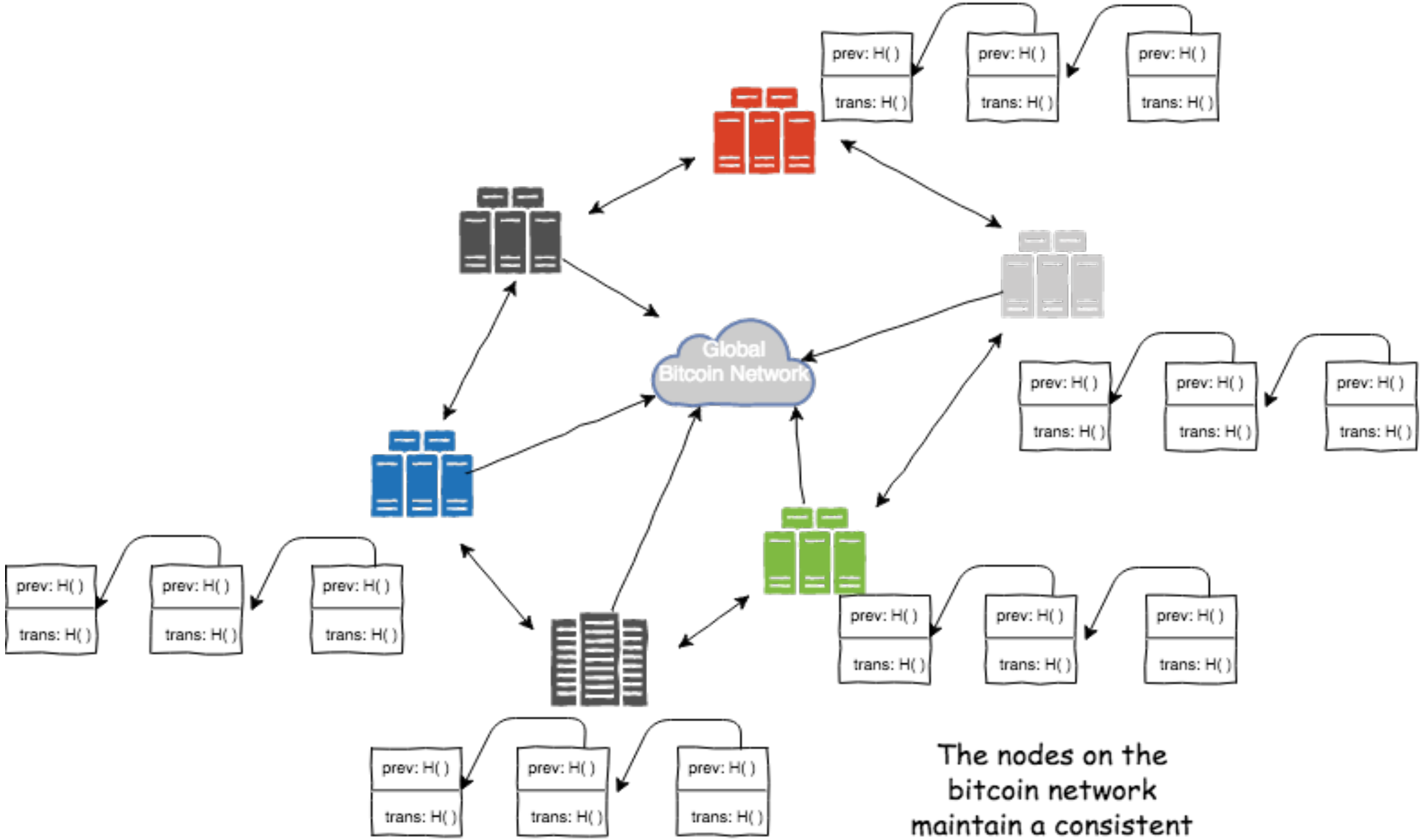


Any forgery is easily detected

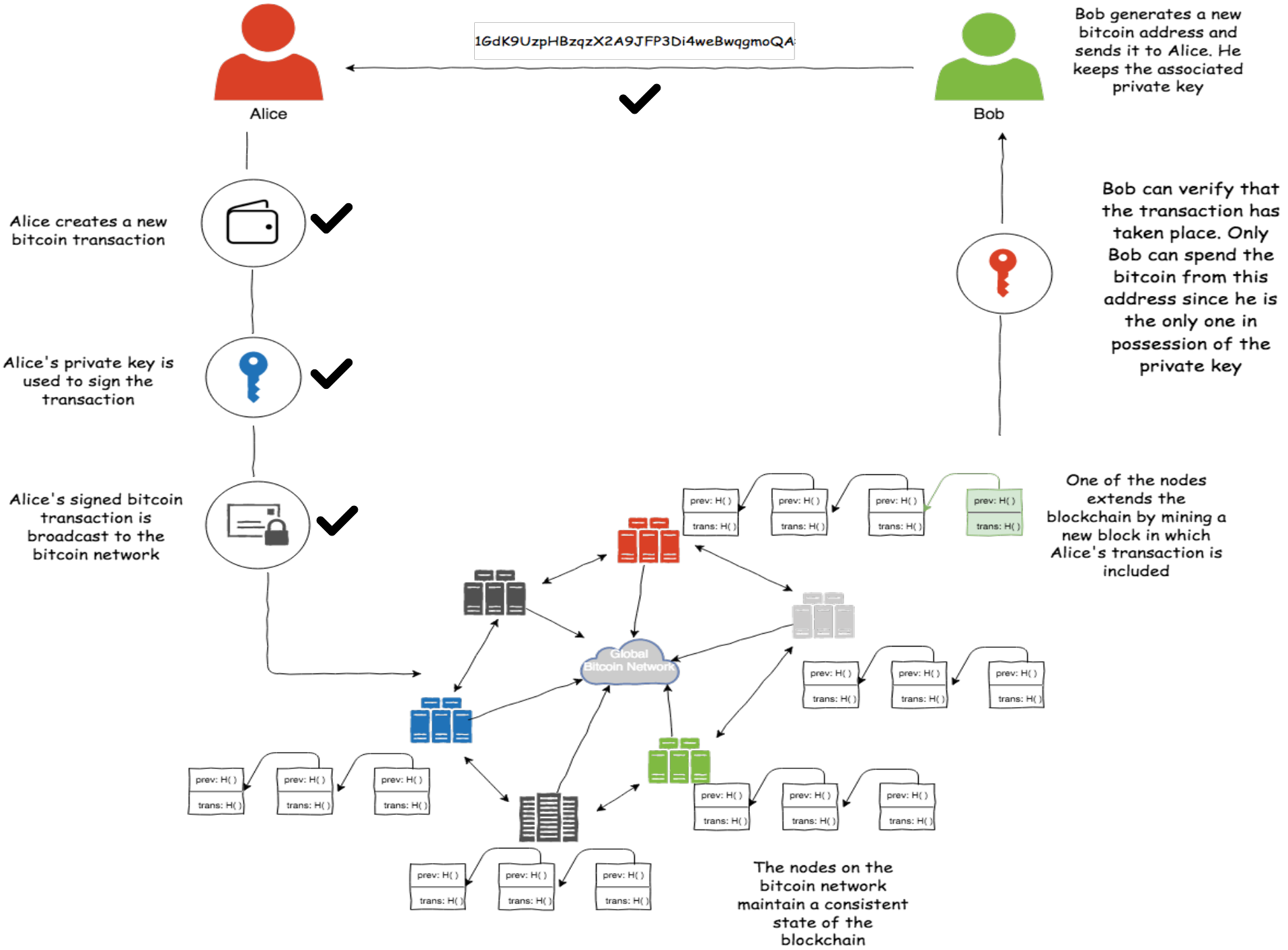


Distributed Block Chain





The nodes on the bitcoin network maintain a consistent state of the blockchain


1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
Alice
Bob
Bob generates a new bitcoin address and sends it to Alice. He keeps the associated private key
Alice creates a new bitcoin transaction
Alice's private key is used to sign the transaction
Alice's signed bitcoin transaction is broadcast to the bitcoin network
Bob can verify that the transaction has taken place. Only Bob can spend the bitcoin from this address since he is the only one in possession of the private key
One of the nodes extends the blockchain by mining a new block in which Alice's transaction is included
Global Bitcoin Network
prev: H( )
trans: H( )
The nodes on the bitcoin network maintain a consistent state of the blockchain

A Transaction’s Journey

The nodes check the validity of the transactions

The nodes in network place groups transactions into a block

Structure of a Block

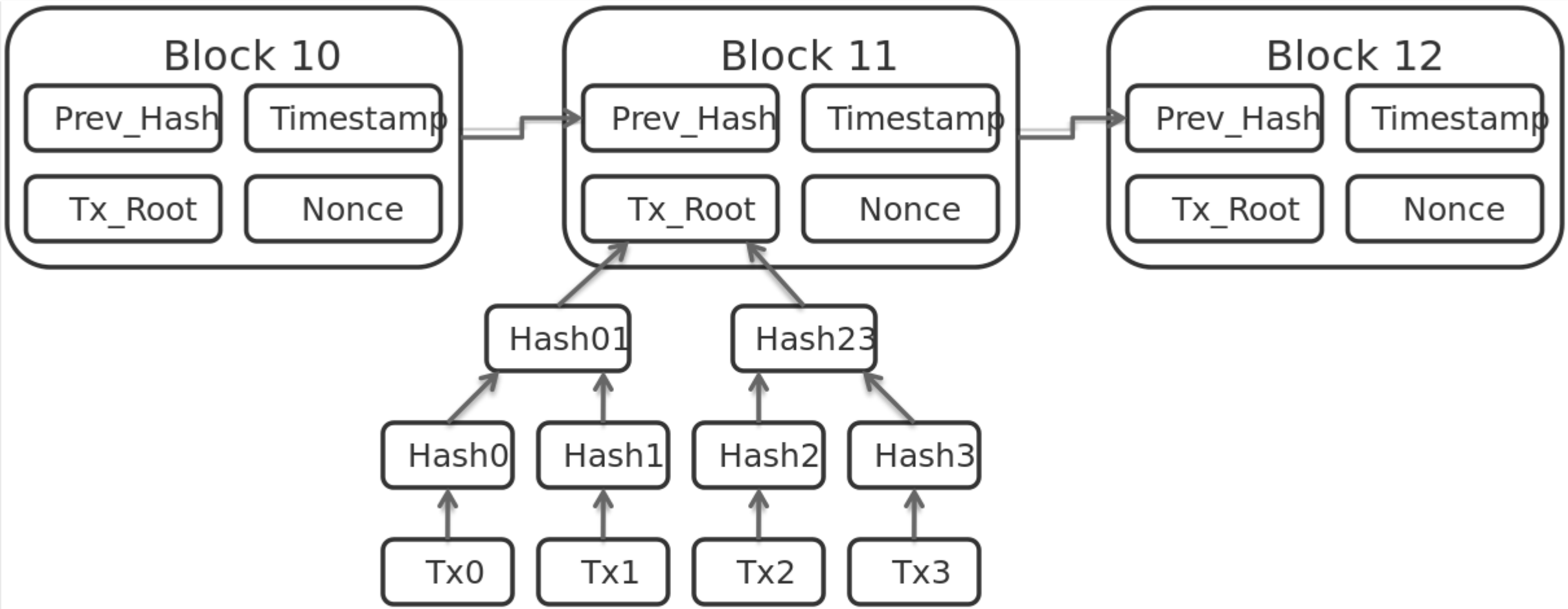

```
{
    "size" : 43560,
    "version" : 2,
    "previousblockhash" :
        "000000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249",
    "merkleroot" :
        "5e049f4030e0ab2debb92378f53c0a6e09548aea083f3ab25e1d94ea1155e29d",
    "time" : 1388185038,
    "difficulty" : 1180923195.25802612,
    "nonce" : 4215469401,
    "tx" : [
        "257e7497fb8bc68421eb2c7b699dbab234831600e7352f0d9e6522c7cf3f6c77",

 #[... many more transactions omitted ...]

        "05cfd38f6ae6aa83674cc99e4d75a1458c165b7ab84725eda41d018a09176634"
    ]
}
```

These blocks are mined to meet certain conditions that ensure the proof-of-work

Mined blocks are propagated across the network

Other nodes in the network extend the chain

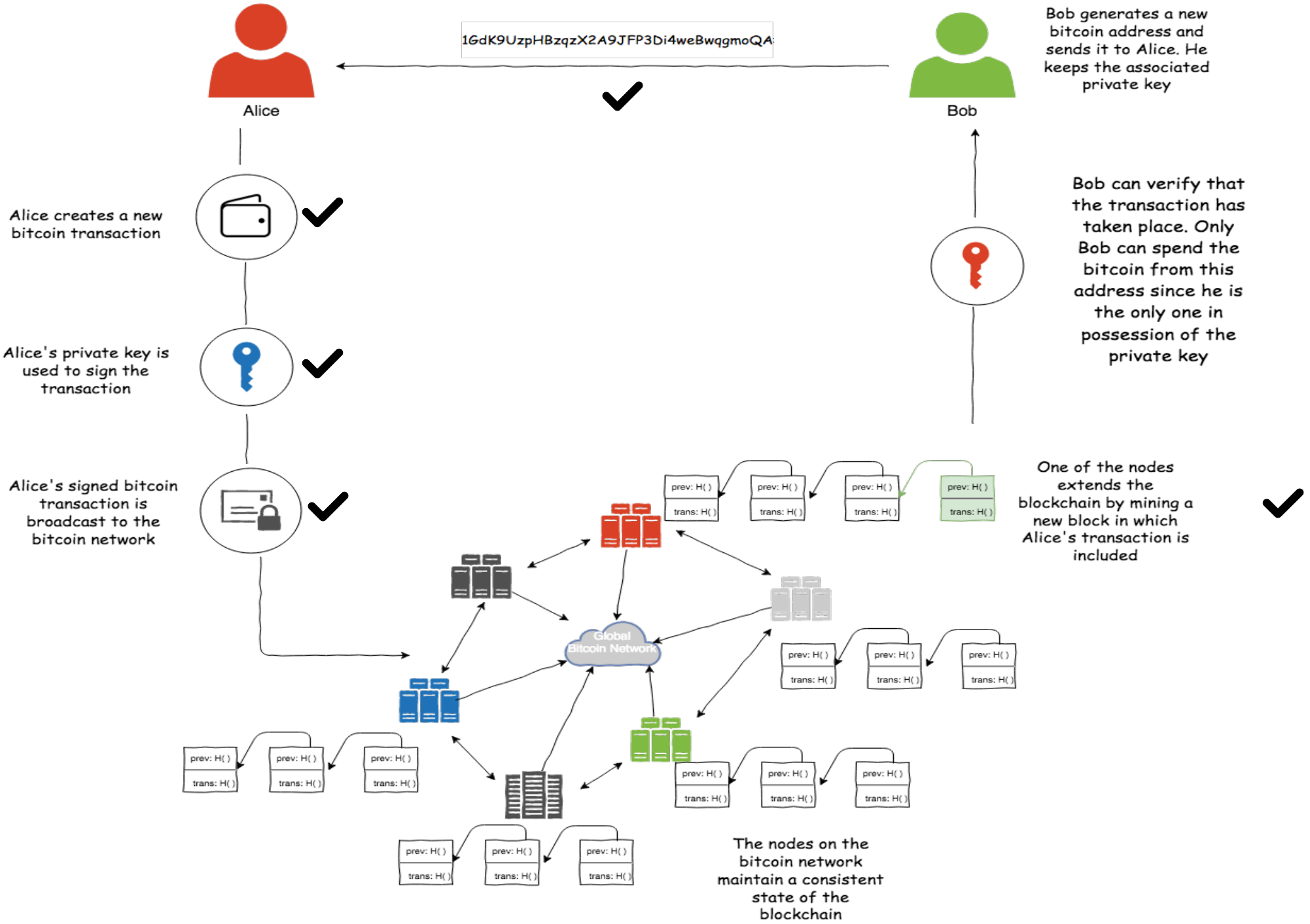
And the process continues….


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Why should miners mine?

Coinbase Transaction


```
{
    "hex" : "01000000010000000000000000000000000000000000000000000000000000000000000000ffffff
    "txid" : "d5ada064c6417ca25c4308bd158c34b77e1c0eca2a73cda16c737e7424afba2f",
    "version" : 1,
    "locktime" : 0,
    "vin" : [
        {
            "coinbase" : "03443b0403858402062f503253482f",
            "sequence" : 4294967295
        }
    ],
    "vout" : [
        {
            "value" : 25.09094928,
            "n" : 0,
            "scriptPubKey" : {
                "asm" : "02aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b210
                "hex" : "2102aa970c592640d19de03ff6f329d6fd2eecb023263b9ba5d1b81c29b523da8b2
                "reqSigs" : 1,
                "type" : "pubkey",
                "addresses" : [
                    "1MxTkeEP2PmHSMze5tUZ1hAV3YTKu2Gh1N"
                ]
            }
        }
    ],
    "blockhash" : "000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
    "confirmations" : 35566,
    "time" : 1388185914,
    "blocktime" : 1388185914
}
```


1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA
Alice
Bob
Bob generates a new bitcoin address and sends it to Alice. He keeps the associated private key
Alice creates a new bitcoin transaction
Alice's private key is used to sign the transaction
Alice's signed bitcoin transaction is broadcast to the bitcoin network
Bob can verify that the transaction has taken place. Only Bob can spend the bitcoin from this address since he is the only one in possession of the private key
One of the nodes extends the blockchain by mining a new block in which Alice's transaction is included
Global Bitcoin Network
prev: H( )
trans: H( )
The nodes on the bitcoin network maintain a consistent state of the blockchain

Vulnerabilities

- Double Spending Attack
- 51% Attack

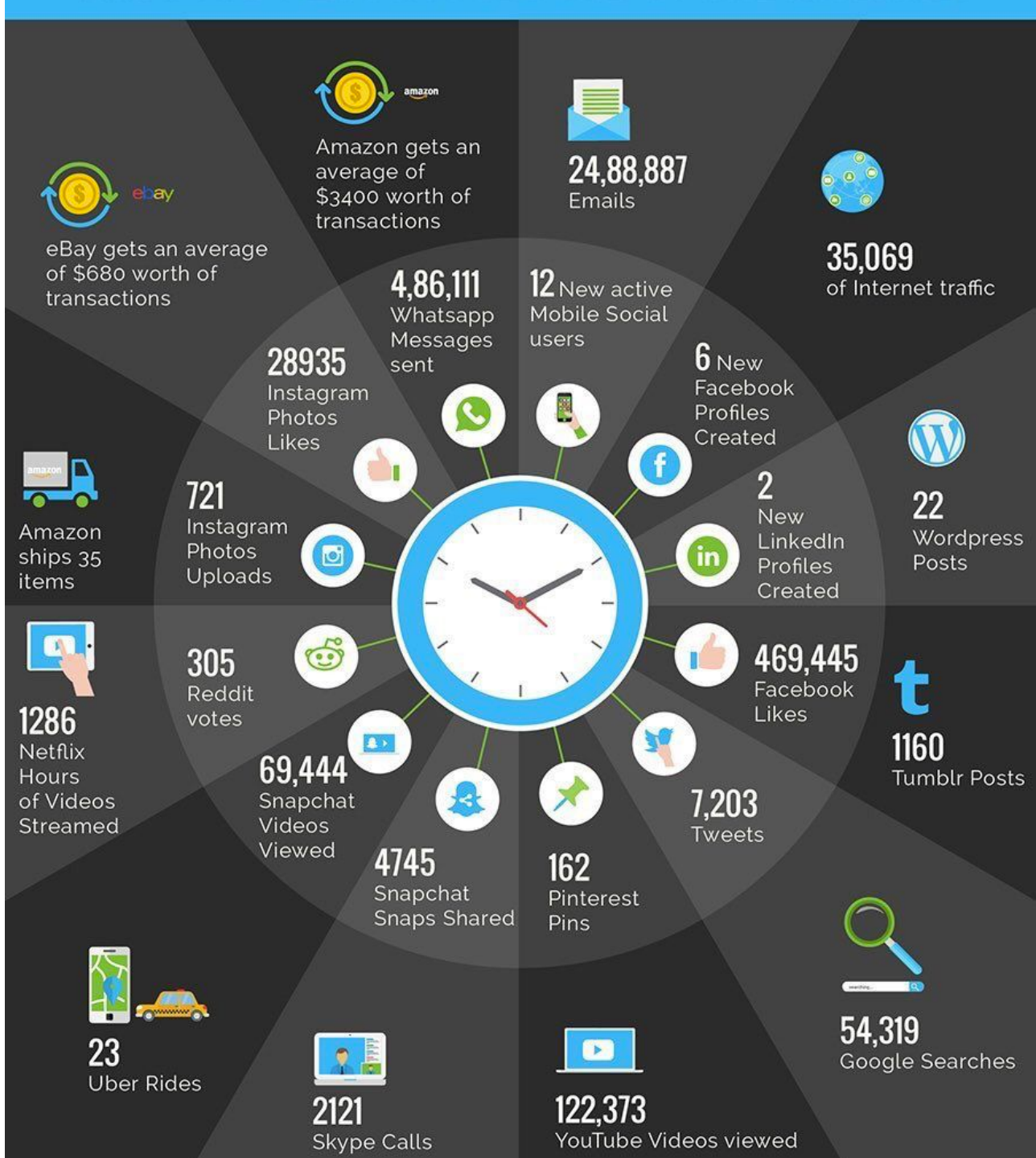
Mining

Things to note

- Limited Supply
- Deflationary Currency
- 10 minutes to create a block
- About 5 transactions a second
- Exponential growth in mining hardware
- Green Transactions

Scalability

- Visa does 25,000 transaction per second
- Paypal about 2,000 per second
- Bitcoin is at 7 transactions per second



Alt Coins

- Namecoin – Alternative DNS
- Litecoin – Scrypt proof of work, 2.5 minute blocks
- Zcash – Privacy on the blockchain
- Ethereum

Beyond Currency: The Blockchain

Validating Transactions

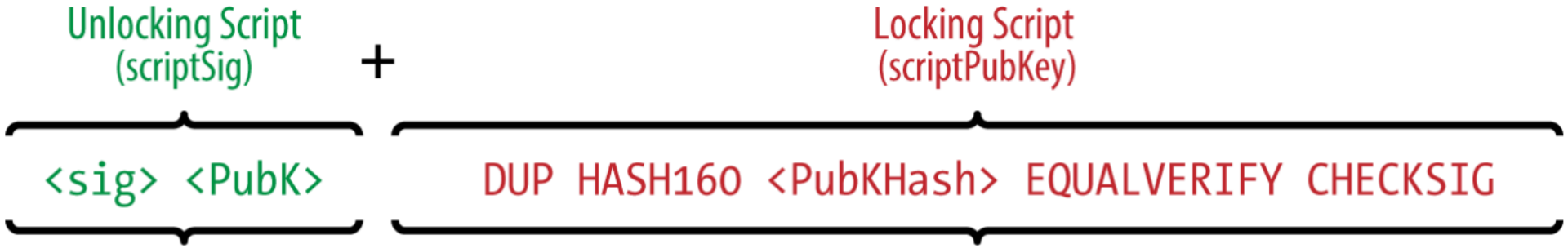
metadata

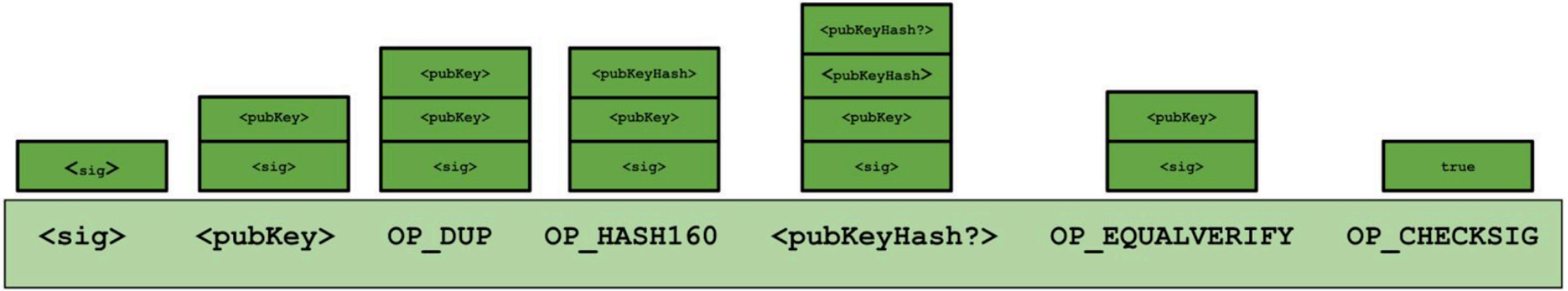
input(s)

output(s)


```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "in":[
   {
    "prev_out":{
     "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
     "n":0
    },
     "scriptSig":"30440..."
   },
   {
    "prev_out":{
     "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
     "n":0
    },
    "scriptSig":"3f3a4ce81...."
   }
  ],
  "out":[
   {
    "value":"10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```

Bitcoin Script





Questions?