Matt Parker
almost
understands
Bitcoin

crypto-currency

crypto-currency
crypto-commodity?

crypto-currency

crypto-currency

public
peer-to-peer
ledger

PUBLIC ADDRESS:

1EMb7znZa9qyMXH5gdb81v7QUFvnJsXfUm

PUBLIC ADDRESS:

1EMb7znZa9qyMXH5gdb81v7QUFvnJsXfUm

PRIVATE KEY:

5HzvVzLLsjCVVXxsC3UWuSJc56
rUW2njfoCYjpKYxiYp79FAVPj

input number

```
01001101011000010111010001110100001000000101000001100001011100100110101101100101110010
```

input number

```
0100110101100001011101000111010000100000010100000110000101111001001101011011001010111001
```

```
0000000000000000000000000000000000000000000000000000000000001011000
```

size (64 bits)

input number

0100110101100001011101000110100000100000010100000110001010111001001101011011001010111001

bonus one

0000000000000000000000000000000000000000000000000000000000001011000

size (64 bits)

input number

01001101011000010111010001101000010000010100000110000101110011010110110010101100101

bonus one

00000000000000000000000000000000000000000000000000000000000000000000000000001011000

size (64 bits)

input number

01001101011000010111010001101000010000010100000110000101110011010110110010111100101

bonus one

00000000000000000000000000000000000000000.......0000000000000000000000000000000000

000000000

00000000000000000000000000000000000000000000000000000000000000000000000000001011000

size (64 bits)

input number

010011010110000101110100011
101000010000001010000011000
010111001001101011011001010
11100101 bonus one

000000000000000000000000000
00000000000.........0000000
000000000000000000000000000

0000000000
000000000000000000000000000
000000000000000000001011000

multiple 512 bits

size (64 bits)

```
4d617474 20506172 6b657280 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000058
```

```
4d617474 20506172 6b657280 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000058
```

$$Ch(x, y, z) = (x + y) \wedge (\sim x + z)$$

$$Maj(x, y, z) = (x + y) \wedge (x + z) \wedge (y + z)$$

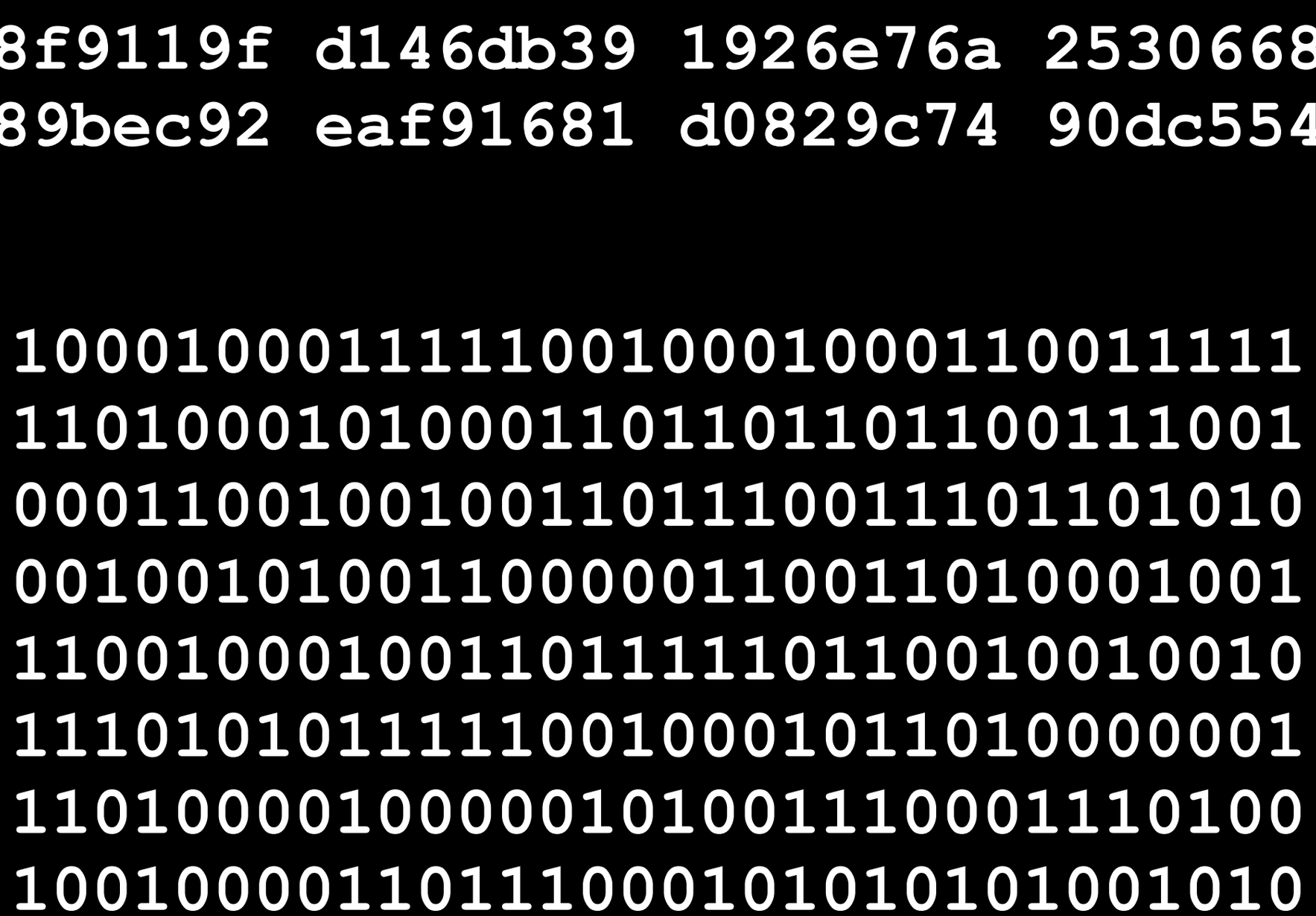
```
4d617474 20506172 6b657280 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000058
```

$$Ch(x, y, z) = (x + y) \wedge (\sim x + z)$$

$$Maj(x, y, z) = (x + y) \wedge (x + z) \wedge (y + z)$$

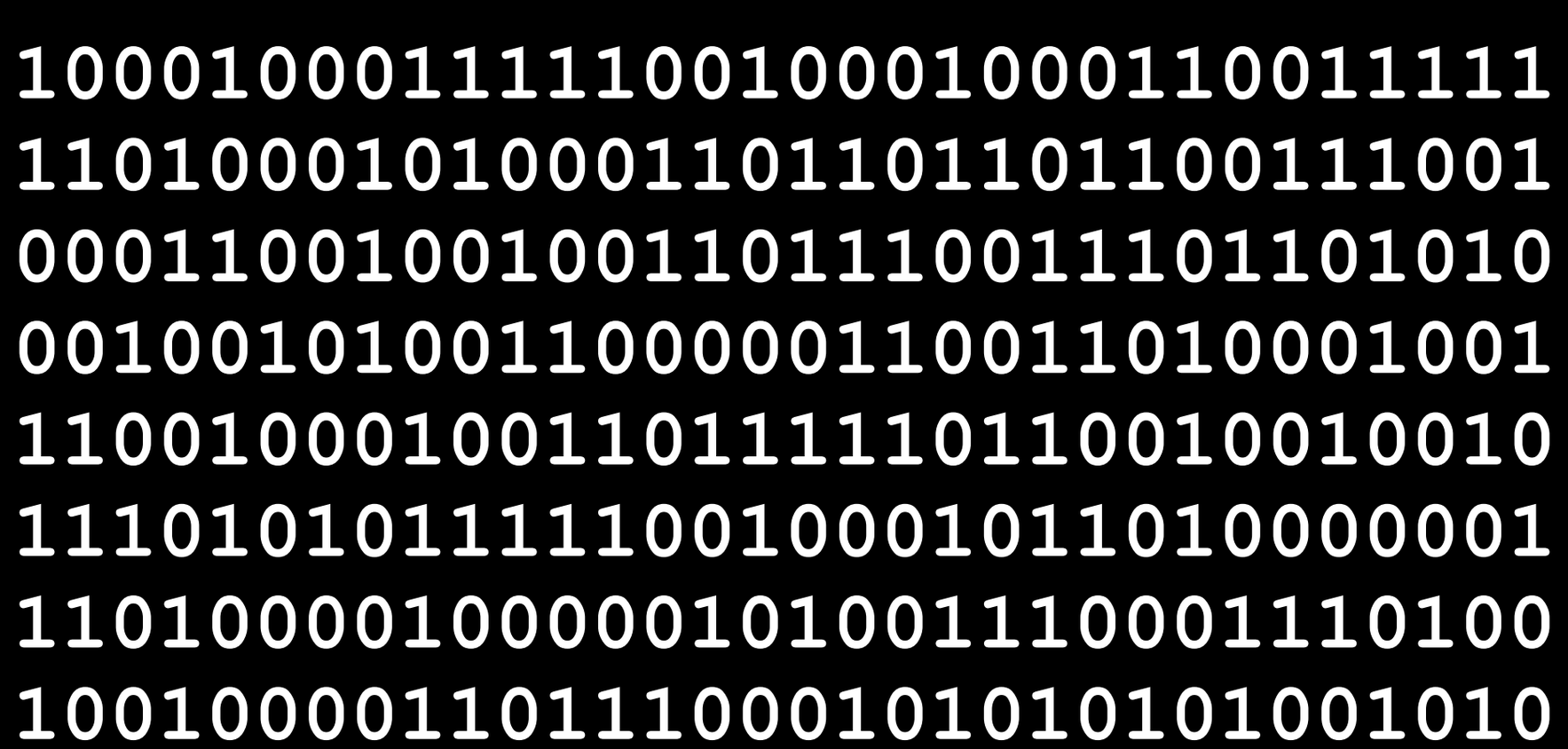
```
6a09e667 bb67ae85 3c6ef372 a54ff53a
510e527f 9b05688c 1f83d9ab 5be0cd19
```

```
88f9119f d146db39 1926e76a 25306689
c89bec92 eaf91681 d0829c74 90dc554a
```



“Matt Parker”

```
88f9119f d146db39 1926e76a 25306689
c89bec92 eaf91681 d0829c74 90dc554a
```



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 the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

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 the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Matt Parker
almost
understands
Bitcoin