Blockchain Concepts



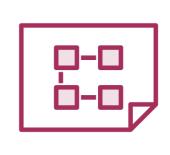
Jan-Erik Sandberg

www.jan-erik.com

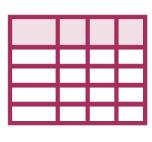


What is Blockchain?









Bitcoins = Blockchain?

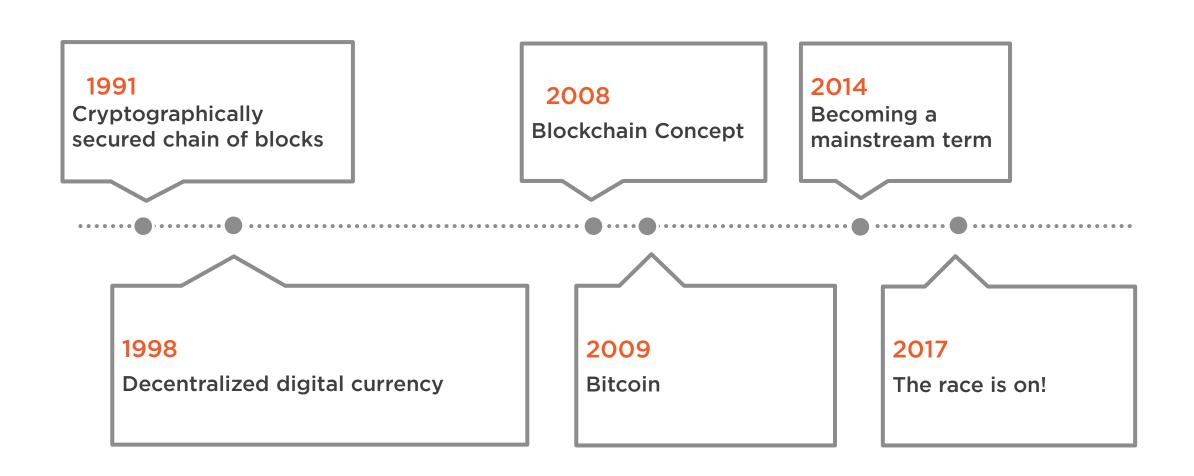








The Brief History of Blockchain



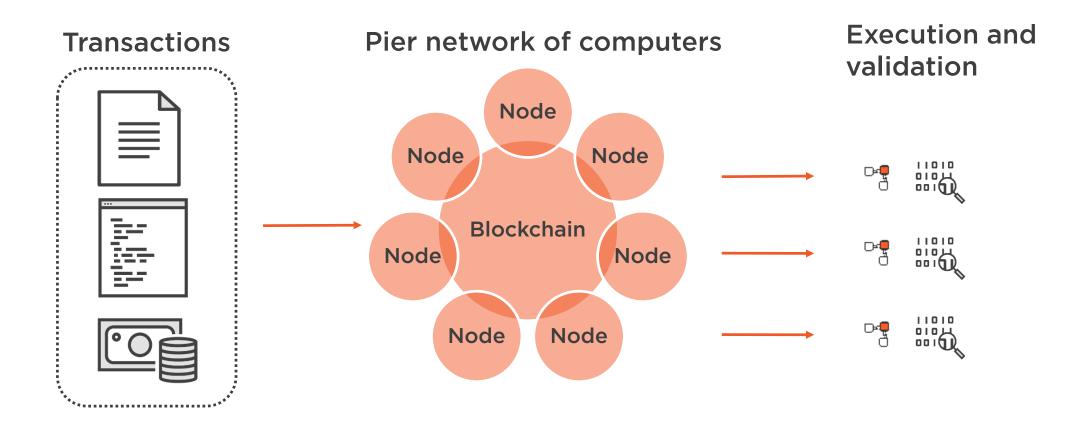


The Characteristics of Blockchain

Global Singelton Accessible Non-stoppable Verifyable



How Does It Work?





Transactions in the Blockchain

Atomic, full operation run or not at all

Inspectable

Run independently

Immortal



Hashing

Length of output always the same

Digital fingerprint

One-way



Hashing

```
{Output= (input )}
input=5 gives output=10
input=4 gives output=10
input=3 gives output=10
input=9 gives output=20
```



SHA 256

Original text

The Vikings were seafaring Scandinavians engaged in exploring, raiding and trading in waters and lands outside of Scandinavia from the eighth to eleventh centuries.

SHA-256 Result

5f21bfa66f27e8449122e4bd838ddb19a3 6a76f3daa6d326450f77f12b1cb0f7

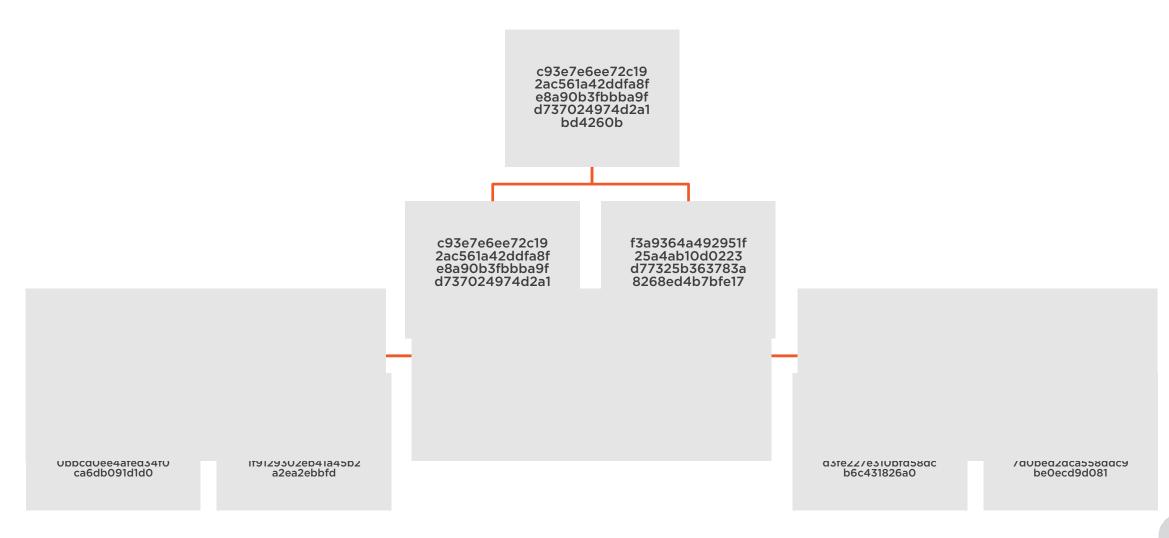


Common Uses for Hashing Algorhitmes

Storing passwords Verify consistency Security



Merkel Tree



The Block

Message:

"Peter is certified"

Hash: 00004575ae3e1d026f612 6130b38b8934623ecf13be 20d58d5b50a2b5722c4f7

Nounce:

314115



A Chain of Blocks

Number

Message: "Chris is certified"

Hash:

0000bccfaf339aff3cb5d3dea7e2f d5ed4781cc1e646cbd15540ad090 0965ceb

Nounce: 831345

Timestamp: 1489688563

Previous: 0000baa3fdb747ee8f8c19e87a20 aec1a5602d2ddd7a3d66593ef9f4 dcbb9f15 Number 10

Message: "Peter is certified"

Hash: 0004575ae3e1d026f6126130 b38b8934623ecf13be20d58 d5b50a2b5722c4f7

Nounce: 314115

Timestamp: 1489688569

Previous: 0000bccfaf339aff3cb5d3de a7e2fd5ed4781cc1e646cbd15 540ad0900965ceb

Number 11

Message: "Bob is not certified"

Hash: 00060e7eec74eb92d8463f72578 d2d4949fd6332c69ef3a1b443232 ea47c9d4

Nounce: 78152

Timestamp: 1489688573

Previous: 0004575ae3e1d026f6126130b38b 8934623ecf13be20d58d5b50a2b5 722c4f7

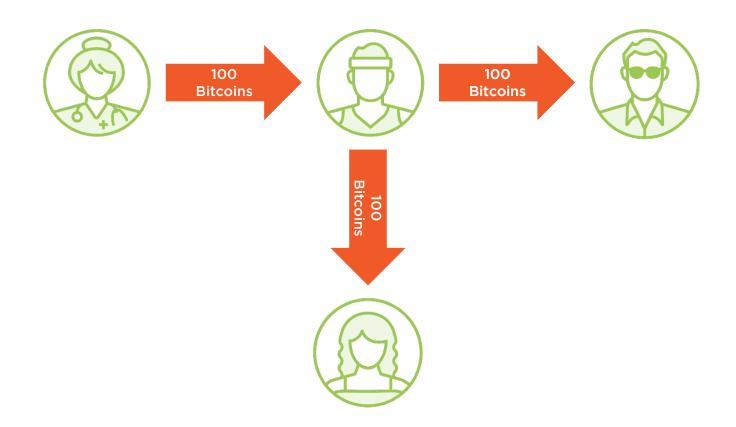


A Distributed Chain of Blocks





Forks





Securing Your Data

Obfuscation Encryption



Encrypting a Message



"Peter is certified"

Hash: 00004575ae 3e1d026f612 6130b38b893 4623ecf13be 20d58d5b50 a2b5722c4f7



AES 128 BIT

Key:

8B5EDB0C3E 21D6D0C74C D785843C73 74



Message:

"rOOZhSnznPh TXUrpBDrNff8 QZH3Ms/OHsM u7LeNrGY8="

Hash: 00004575ae3e 1d026f6126130b 38b8934623ecf 13be20d58d5b 50a2b5722c4f7



Public vs. Private

Public

Available to everyone with an internet connection

Expensive transactions and storage

No given point of attack

Rely on community

Democratic

Private

Similarities to traditional databases

Cost controlled

Known entities

Controlled storage

Transition to blockchain

Fewer points of attack



The Major Offerings









Usages for Blockchain

Digital currencies

Internet of things

Product lifecycle

Certifications

Secure information sharing

Virtual products



Summary



Basics of blockchain

Hashing

The Block

Security

Implementations and usages

