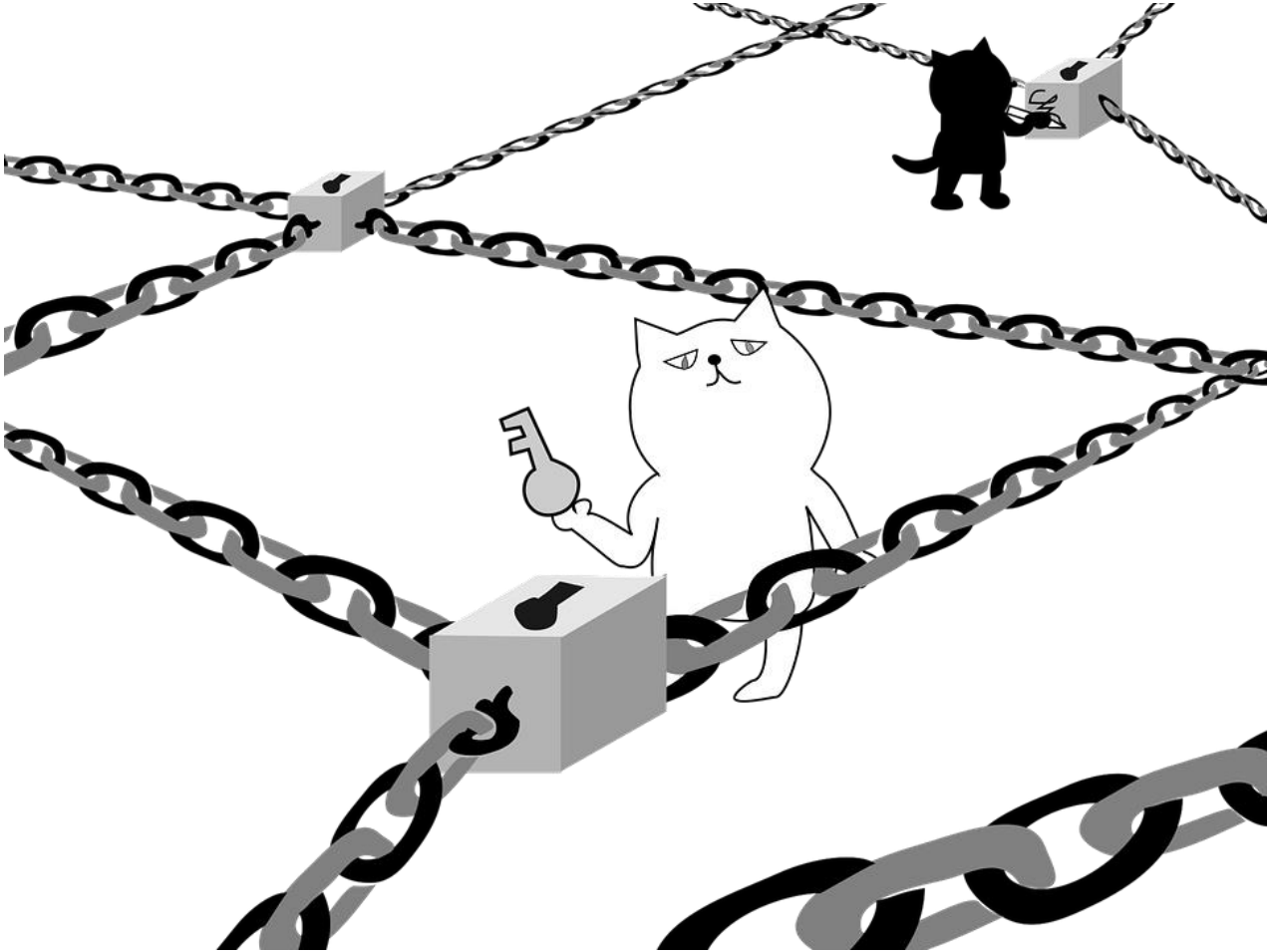
2016 Convention
23 - 24 November 2016

ACTUARIAL SOCIETY OF SOUTH AFRICA

Seductions of the Blockchain

David Kirk


bitcoin
CRYPTOCURRENCY
bitcoin
CRYPTOCURRENCY
bitcoin
CRYPTOCURRENCY



ACTUARIAL SOCIETY OF SOUTH AFRICA

A **blockchain** is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the **blockchain** in a linear, chronological order - *Investopedia*

Formal definition

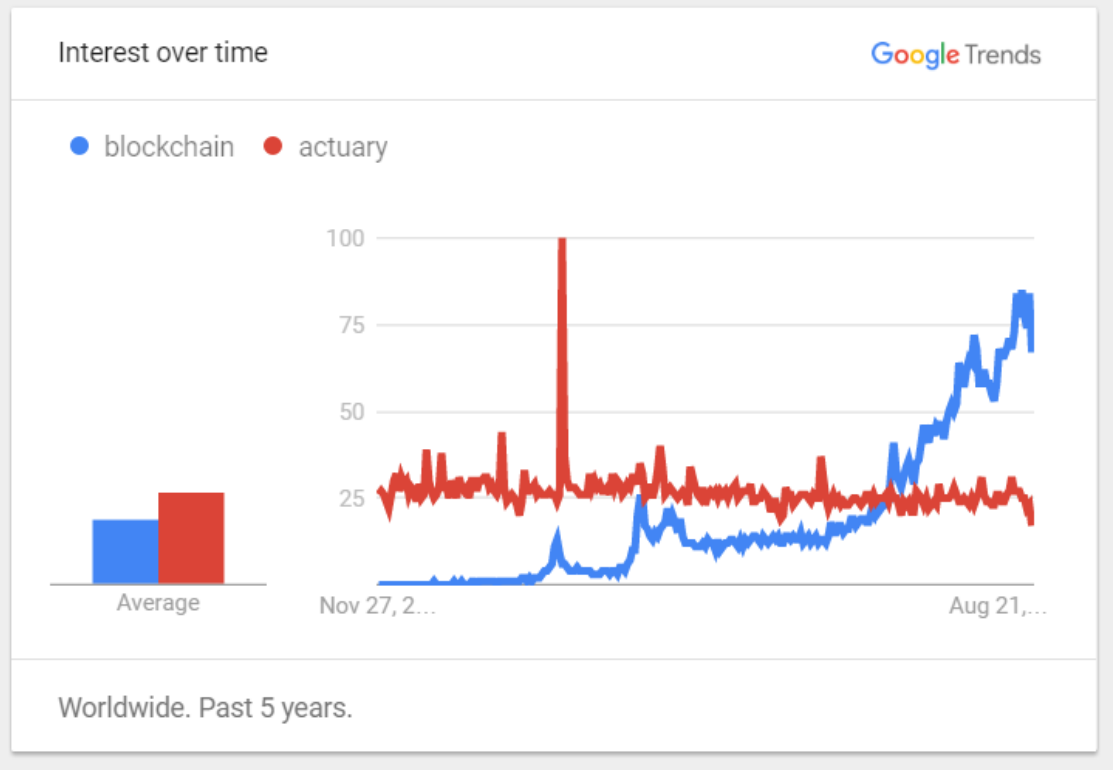
Distributed Ledger Technology

Blockchain in the news

ACTUARIAL SOCIETY OF SOUTH AFRICA

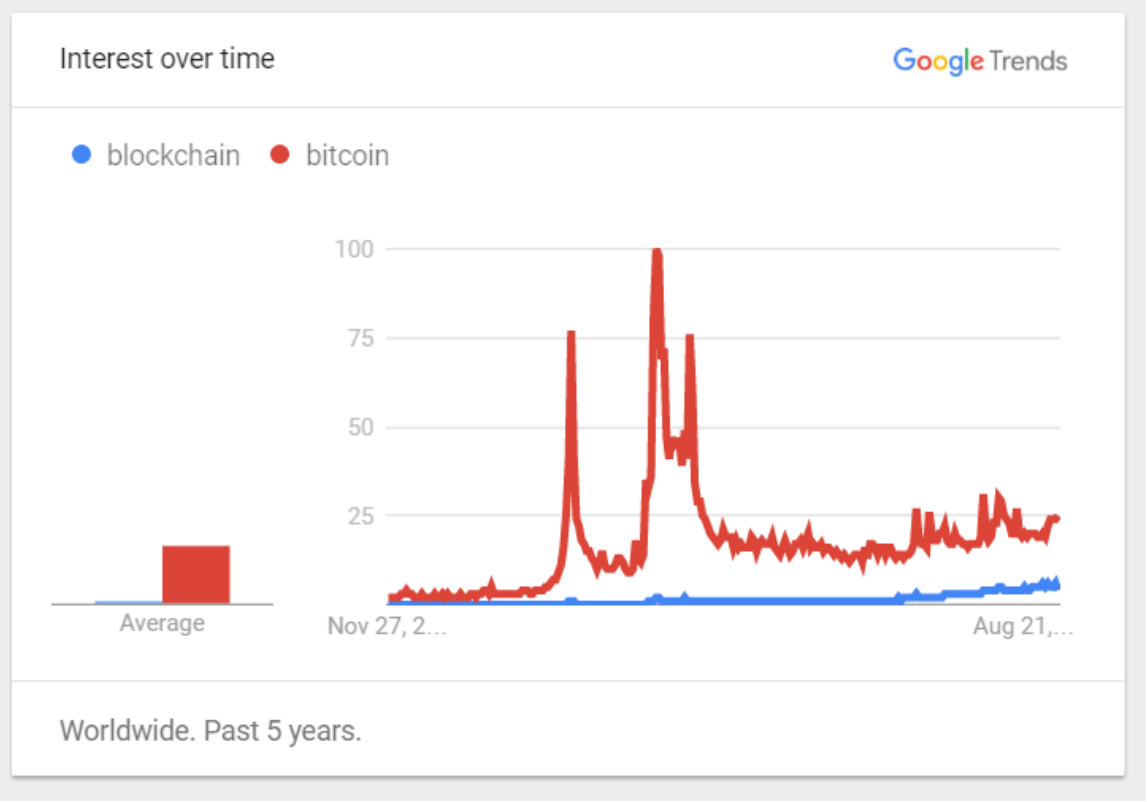
- Malta Stock Exchange Forms Blockchain Committee
- Walmart tries using blockchain to take unsafe food off shelves
- How blockchain can change the future of IoT
- Korea Exchange opens the Korea Startup Market with blockchain technology
- **Goldman Sachs Drops Out of R3 Blockchain Group**
- **Blockchain startup R3 cuts fund-raising target to $150 million: source**
- **Why Remittance Giant MoneyGram Won't Be First With Blockchain**

Why we should care



- Mathematics
- Finance
- Understanding long term
- Systems thinking and second-order impacts
- Programming
- Complex contracts
- Logic and precision

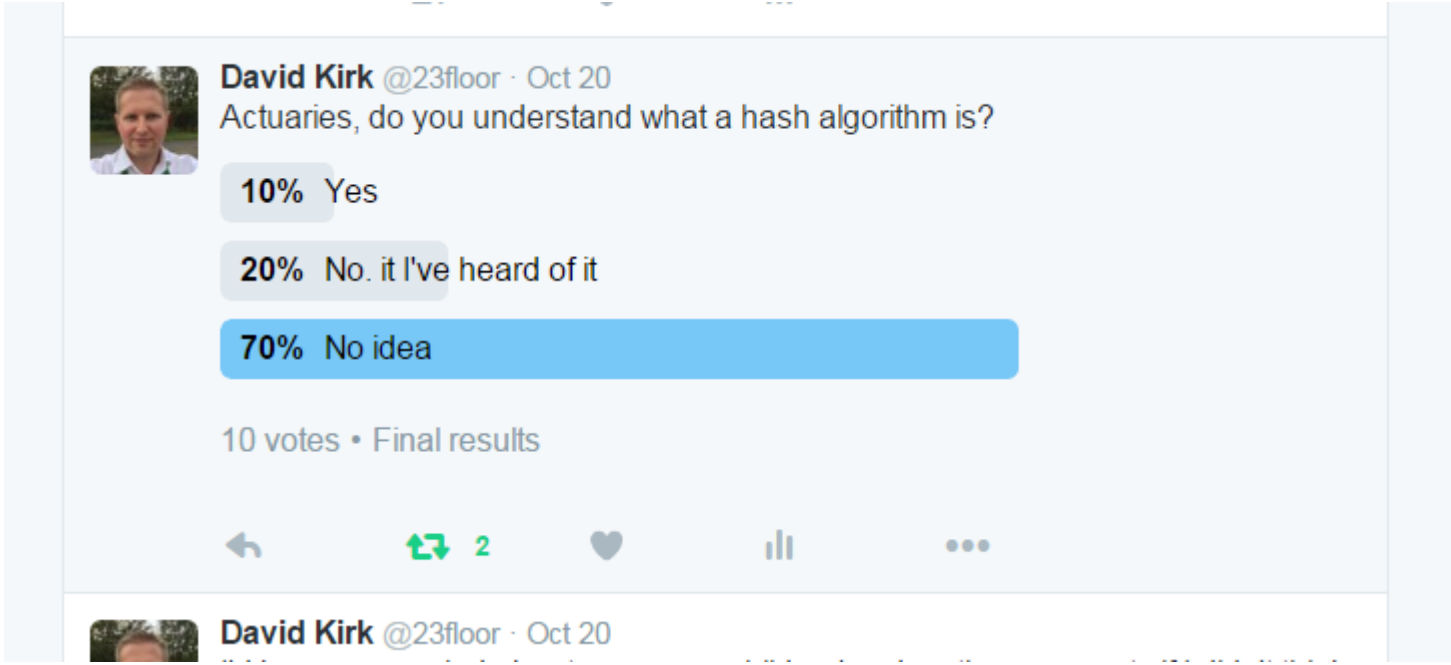
Bitcoin vs Blockchain



This is not (only) a talk on bitcoin
Blockchain goes much further

"Bitcoin the currency, I think, is going to go nowhere … the blockchain is a technology which we've been studying and yes it's real." —*Jamie Dimon on CNBC*

Hash Functions



Hash Functions

String1: “Welcome to the 2016 Actuarial Society Convention”

String2: “Welcome to the 2017 Actuarial Society Convention”

String3: entire Romeo and Juliet play (25,688 words)

MD5 Hash1: `f6cdf6b47afddfef5e48addd4e0bbd74`

MD5 Hash2: `2f5c95b044cea9d4c6137d0b915b490a`

MD5 Hash3: `f8fc4c137ee78e825b65c887c70d8751`

Hash Functions

String3: “Welcome to the 2026 Actuarial Society Convention”

String4: “Welcome to the 2202 Actuarial Society Convention”

MD5 Hash3: 0778adbb5490bedde389b855c96d3090

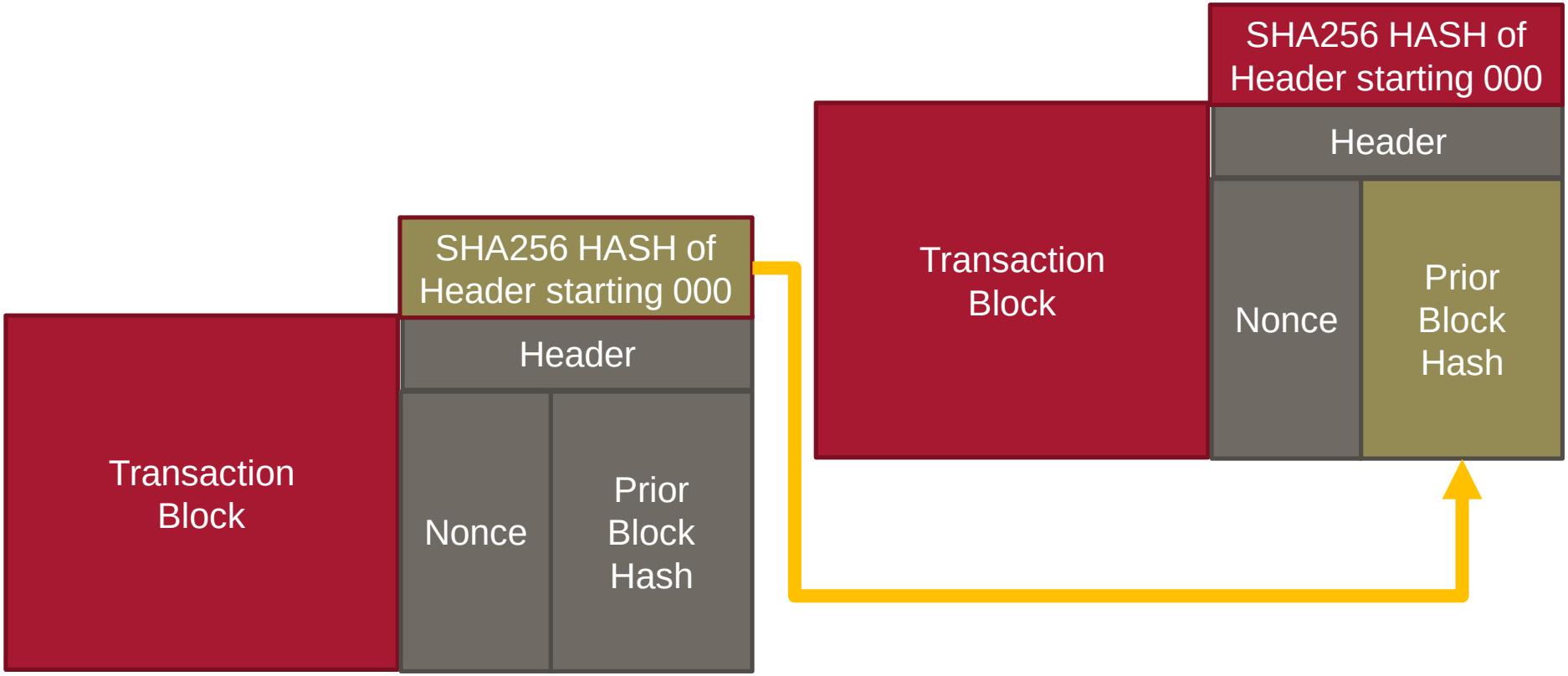
MD5 Hash4: 003614d42f2cd6c3df86afa8c8082bdb

MD5 Hash : 0000000000??????????????????????

Nonce?

Nonce-selected hash-linked chain of information blocks

ACTUARIAL SOCIETY OF SOUTH AFRICA



Bitcoin Blocks Status Search for block, transaction or address

ACTUARIAL SOCIETY OF SOUTH AFRICA

Latest Blocks

Height	Age	Transactions	Mined by	Size
440116	5 minutes ago	2030		999232
440115	19 minutes ago	1		233
440114	20 minutes ago	2349	AntMiner	998058
440113	25 minutes ago	2623	AntMiner	998067
440112	27 minutes ago	2776		998136

See all blocks

Latest Transactions

Hash	Value Out
b3987361a447232a1a8a756c9c2e2a684494baeb3bce…	0.00967 BTC
91718bc1354af9504cbba8d28d7e12bbbe12f81fa334…	9.99243502 BTC
dfaf2557671357127dfde119d2279631f3da5dfc24d56…	0.72531164 BTC
fb3a27aa2662e8b16813395255f2a733a0a7addcb58bf…	1.02803 BTC
850753a2276d95a8934ca2d67ce9d6eda74846fddb6b…	0.14024433 BTC
077613f912ee711facf0dcaafd577762be58add56dba0…	0.45341281 BTC

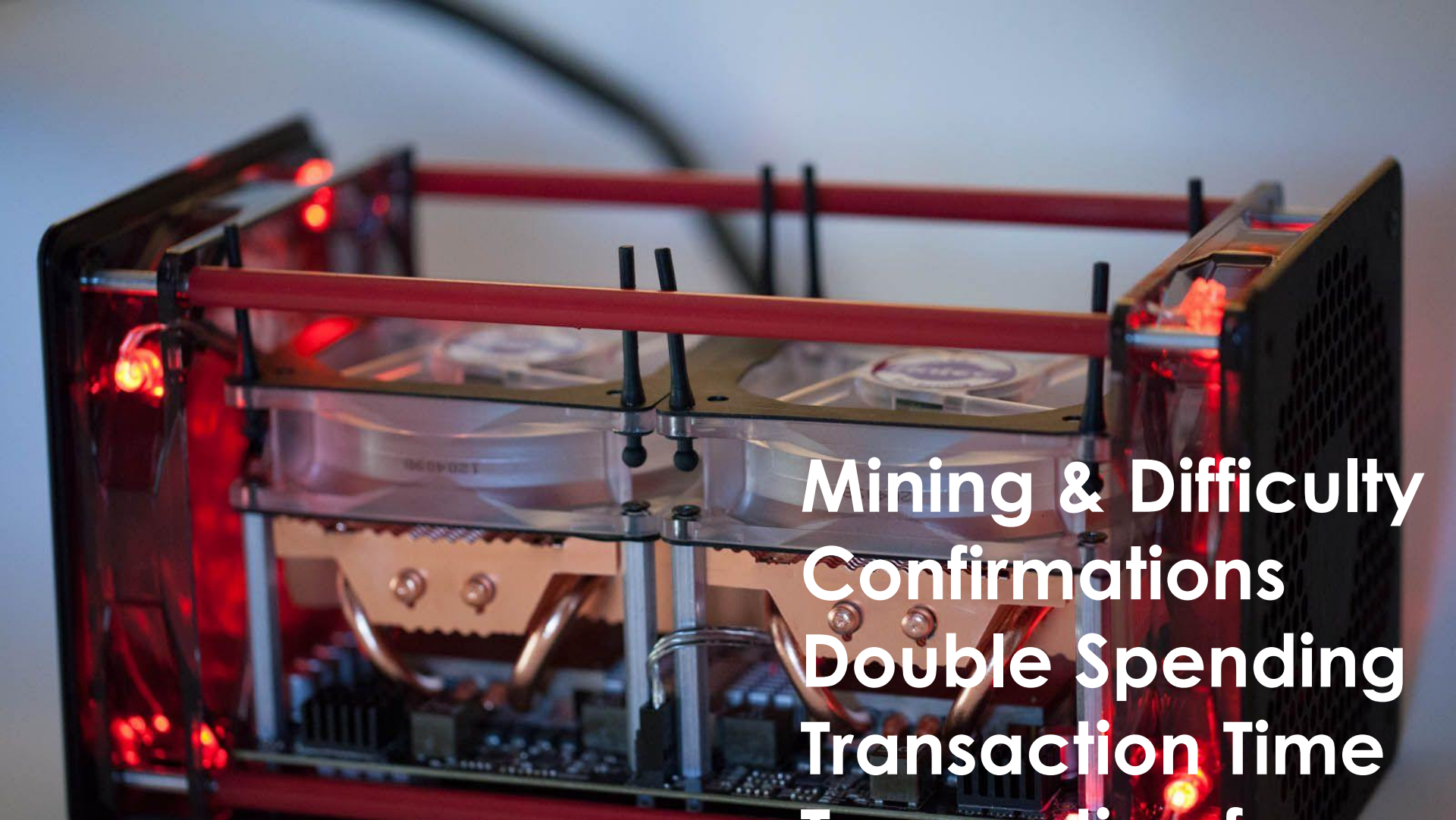
Block #440114

BlockHash 00000000000000000e69989fd815da0fe3dff021163fbd1a04a39841e8e4c96

Summary

Number Of Transactions	2349	**Difficulty**	281800917193.1958
Height	440114 (Mainchain)	**Bits**	1803e6d4
Block Reward	12.5 BTC	**Size (bytes)**	998058
Timestamp	Nov 22, 2016 11:55:26 PM	**Version**	536870912
Mined by	AntMiner	**Nonce**	3245311641
Merkle Root	c9b75f11985bb343fab9a15d57a6e...	**Next Block**	440115
Previous Block	440113		

Public Ledger
Trust without trust
No central control*
No regulator
~~No transaction costs~~
Bearer instruments
Permisionless vs permissioned blockchains


Mining & Difficulty
Confirmations
Double Spending
Transaction Time

ACTUARIAL SOCIETY OF SOUTH AFRICA

Inflation / deflation and fiat money
Anonymity
Blockchain size 65GB+

Blockchain 2.0 and Smart Contracts

ACTUARIAL SOCIETY OF SOUTH AFRICA

- *Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality. It provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM), that can execute peer-to-peer contracts using a cryptocurrency called ether. – Wikipedia*
- *DAO Decentralized Autonomous Organization*