The Yorkshire BrassBitCoin

Adam Pridmore

- Average Developer
- Below average BitCoin ~~expert~~ person

What is a BitCoin?

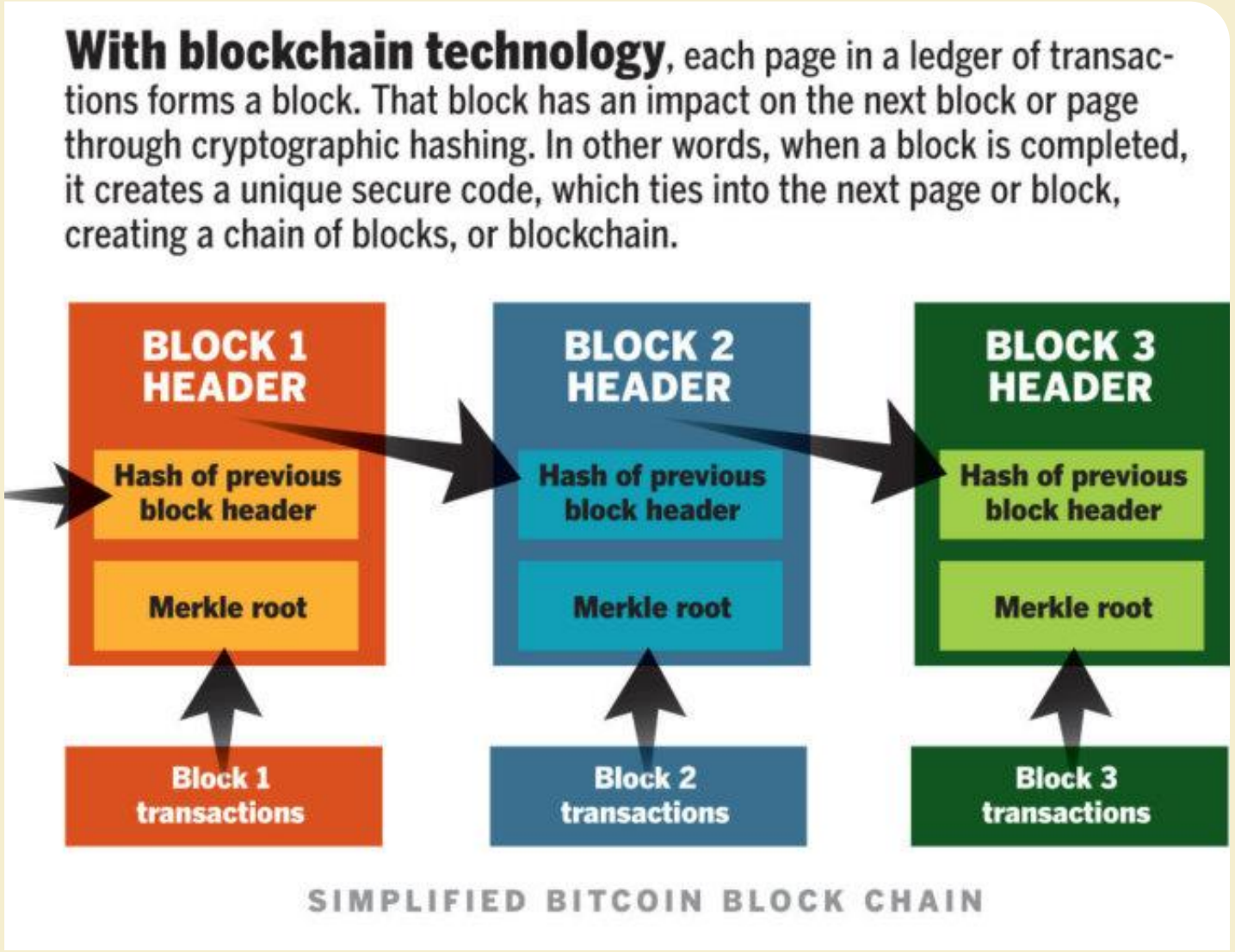
“It’s a cryptocurrency or a specific implementation of a block chain”

“Money”

What is a Block Chain?

“a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.”

“A public ledger. An immutable record which cannot be changed, even by the authors of the transactions”



Each block has

- Transactions
- Hash of previous block
- Its own hash
- Other meta data

I’ve heard about this thing called ‘mining’?

- Bitcoin mining
  - Is creating a new valid block
  - Hash of a bunch of transactions and the previous hash
  - The hash has some (hard) criteria
    - Starts with 18 zeros
    - ~2.7 Million billion hashes tried to find one
    - Real Example: 000000000000000000058dd9b08732c8f376188bd85a46e93167b772ee51c34d6

- Why do it?
  - You get some bitcoins (12.5)
  - And you get all the transaction fees in the block => more $$$

~1 coin is mined every 10 minutes
The network self adjusts this to be true every two weeks.

Block #511375

Summary	
Number Of Transactions	1045
Output Total	4,027.6304458 BTC
Estimated Transaction Volume	509.01588666 BTC
Transaction Fees	0.43300822 BTC
Height	511375 (Main Chain)
Timestamp	2018-02-28 21:27:14
Received Time	2018-02-28 21:27:14
Relayed By	BTC.com
Difficulty	3,007,383,866,429.73
Bits	392009692
Size	1022.776 kB
Weight	3992.917 kWU
Version	0x20000000
Nonce	3799536405
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000058dd9b08732c8f376188bd85a46e93167b772ee51c34d6
Previous Block	00000000000000000058c7fbeddd13770e11f51c0f3dc76eb8ab5471ee2e9b3d
Next Block(s)	
Merkle Root	9f8791f44a62d3aecb9a5f7b0ad1cdf0a3943f470a7bdab30f6826c13738cbe7

https://blockchain.info/block/00000000000000000058dd9b08732c8f376188bd85a46e93167b772ee51c34d6

The Yorkshire BrassBitCoin

The Yorkshire BrassBitCoin

Each BrassBitCoin block is made up of

index	Integer
minedBy	String
data	String
previousHash	String
nonce*	Integer
Hash	string

* A **nonce word** (also called an **occasionalism**) is a lexeme created for a single occasion to solve an immediate problem of communication - wikipedia

Hash is calculated by

The hash value is the SHA-256 hash of all the fields concatenated in order (excluding the hash) with a single space between as an upper case hex string. e.g

index	index
minedBy	Adam
data	4
previousHash	0000CA2C984CDF70E0326930902697 9A18FA25EBBAB16BD90C88F92985992609
nonce	22889

5 Adam 4 0000CA2C984CDF70E0326930902697 9A18FA25EBBAB16BD90C88F92985992609 22889
Makes this hash

hash	0000cbfe51be34fad0de5720d6253dd23556b909b2d9f1d412cf552cdb76eb91

http://www.xorbin.com/tools/sha256-hash-calculator

More details on the Block in the notes

- Genesis block - the special first block
- What all the fields are
- What a valid hash is (it starts with four 0’s)

Transactions

- See the notes

The Yorkshire BrassBitCoin Server

https://yorkshire-brassbitcoin.azurewebsites.net/

void*

- **Let's Build the Tiniest Blockchain -** (In Less Than 50 Lines of Python) https://medium.com/crypto-currently/lets-build-the-tiniest-blockchain-e70965a248b
- https://yorkshire-brassbitcoin.azurewebsites.net/
- https://blockchain.info/
- https://passwordsgenerator.net/sha256-hash-generator/