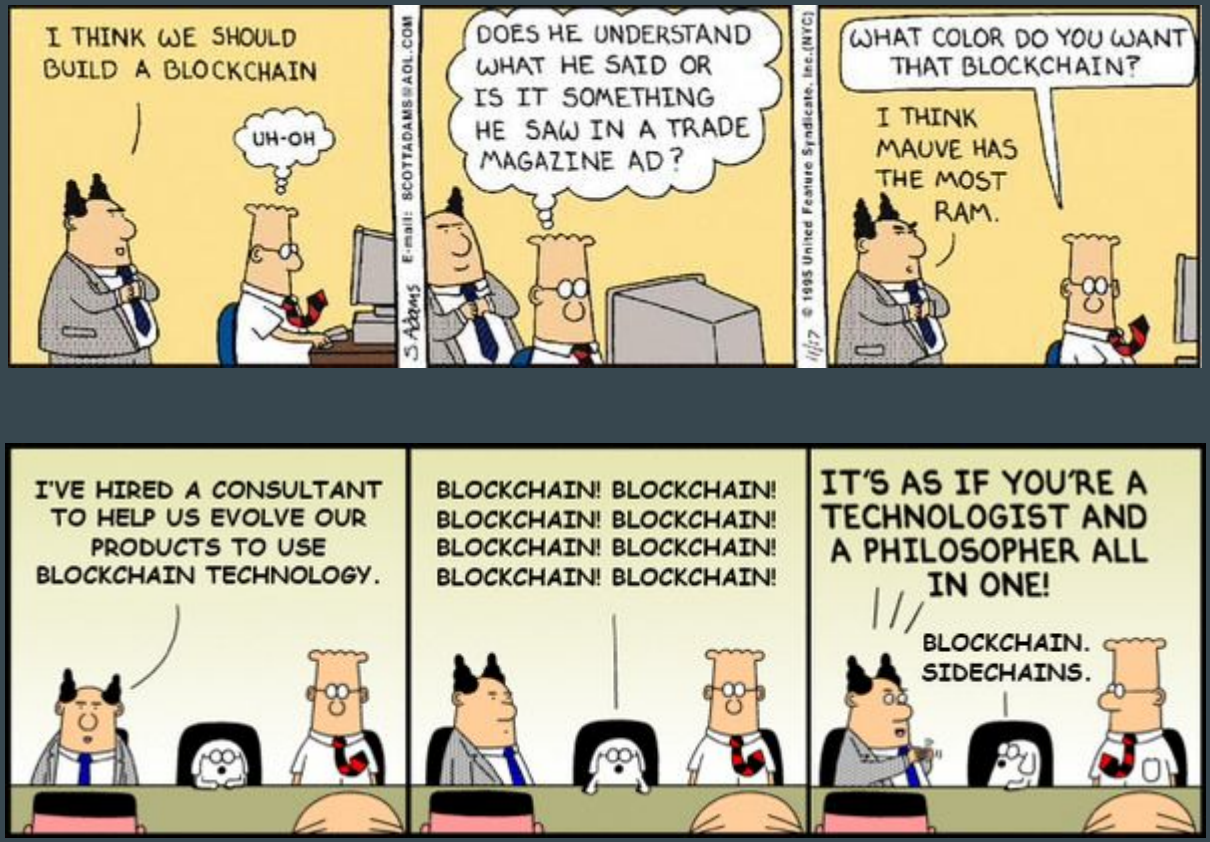
Blockchain 101

...


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

The Siege of King's Landing


KING'S
LANDING

Valyrian Voting

Message

Seal

Shalanta toma byre

Valyrian Voting: Message Contents

History of all messages received	**Vote (A: Attack / R: Retreat)**
Wax Seal of Sender	
Valyrian Inscription	

Valyrian Voting

1				
Sent	<table><tr><td>-</td><td>A</td></tr><tr><td colspan="2">W_D</td></tr><tr><td colspan="2">V_1</td></tr></table>			

Valyrian Voting

2				
Votes	AV_1	AV_1	AV_1	AV_1
Sent			<table><tr><td>AV_1</td><td>A</td></tr><tr><td colspan="2">W_T</td></tr><tr><td colspan="2">V_2</td></tr></table>	

Valyrian Voting

3				
Votes	AV_1 AV_2	AV_1 AV_2	AV_1 AV_2	AV_1 AV_2
Sent				AV_1 AV_2 **R** W_P V_3

Valyrian Voting

4				
Votes	AV_1 AV_2 RV_3	AV_1 AV_2 RV_3	AV_1 AV_2 RV_3	AV_1 AV_2 RV_3
Sent		AV_1 AV_2 RV_3 **A** W_J V_4		

Valyrian Voting

5				
Votes	AV_1 AV_2 RV_3 AV_4	AV_1 AV_2 RV_3 AV_4	AV_1 AV_2 RV_3 AV_4	AV_1 AV_2 RV_3 AV_4

Byzantine Consensus

A group of generals, each commanding a portion of the Byzantine army, encircle a city. These generals wish to formulate a plan for attacking the city. In its simplest form, the generals must only decide whether to attack or retreat. Some generals may prefer to attack, while others prefer to retreat. The important thing is that every general agrees on a common decision, for a half-hearted attack by a few generals would become a rout and be worse than a coordinated attack or a coordinated retreat.

The problem is complicated by the presence of traitorous generals.

A blockchain can achieve Byzantine Consensus under certain constraints.

The Blockchain

- Peer-to-peer, distributed database
- Ever-growing, **linked-list** of **immutable** data
- Synced across all nodes
- Solves the problem of decentralized consensus
- Was first proposed in the original Bitcoin paper. It is the underlying technology behind Bitcoin

The Cryptographic Hash

- A digital fingerprint of data

$$f(\text{data}) \rightarrow h$$

- It is practically irreversible by design
- A Blockchain implementation may use any hash algorithm: Bitcoin uses SHA256

A minimalistic Block

The hash serves two purposes - immutability and linking

A Visual Blockchain Demo

- www.desdevpro.com/blockchain-demo
- https://goo.gl/vhWl2p

Let’s talk Crypto-Currency

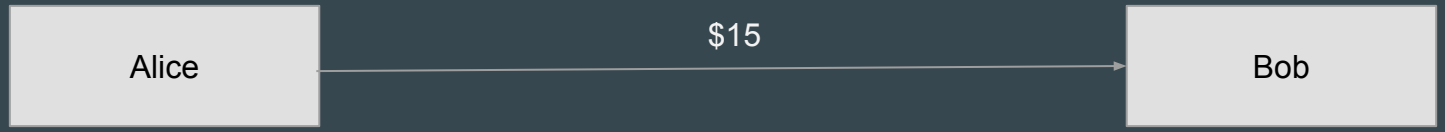
- October 2008: **Satoshi Nakamoto** published a paper describing the bitcoin digital currency
- January 2009: the bitcoin network was launched and the first units of the bitcoin cryptocurrency were issued.
- Bitcoin is a digital payment system built using the concepts of Blockchain and asymmetric key cryptography
- Decentralised, peer-to-peer network

Asymmetric Cryptography

- Also called Public Key Cryptography
- Different keys are used for encrypting and decrypting
- The public key can be mathematically derived from the private key; the other way round is not possible
- The public key can be publicized without compromising security

Conventional Payment

Direct, P2P Payment



How is this even possible?

- How do we know Alice has enough money to pay Bob?
- If Bitcoin is just digital money - a string of 0s and 1s - what stops Alice from sending the same ‘money’ to several people?
- Can someone else spend copies of Alice’s digital money?
- Can the money get lost or stolen in transit?

Designing a crypto-currency: NuCoin

- Let us try to design a basic, distributed, crypto-currency, which we will call NuCoin.
- As we go along, we will add more rules to NuCoin.
- To start, say, Alice wants to send 1 nucoin to Bob. She initiates the transaction by sending this message on the network (everyone on the network can read the message):

> I, Alice, am giving Bob 1 nucoin

NuCoin v0.1

The transaction message must be signed using the sender's private key and should contain the receiver's public key

I, Alice, am giving Bob 1 nucoin
Alice's Digital Signature
Bob's public key

- It is now possible to verify the identity of the sender and receiver
- Protected from forgery
- Double-spending is still possible

NuCoin v0.2

The transaction message must contain a unique serial number

I, Alice, am giving Bob 1 nucoin **#87276**
Alice’s Digital Signature
Bob’s public key

- Who provides the serial number? A bank? But we need a decentralized system
- Who tracks the the ownership of serial numbers?
- If all nodes on the network can (honestly) keep track, then the problem of double spending is solved

NuCoin v0.3: Enter the blockchain

All nodes have a copy of a ledger which records the ownership of nucoins:

ID	Value	Owner
87276	1	Alice
74563	5	Bob
21156	0.5	Charlie

NuCoin v0.3

- When Bob receives the message, he checks his own copy of the ledger to verify that Alice does own nucoin #87276
- He broadcasts his acceptance of the transaction. Everyone updates their copy of the ledger

Before		
ID	Value	Owner
87276	1	Alice
74563	5	Bob
21156	0.5	Charlie

After		
ID	Value	Owner
87276	1	Bob
74563	5	Bob
21156	0.5	Charlie

NuCoin v0.4: Transaction Chains

If Alice wants to send 10 nucoins to Bob, she must send a list of all transactions which add up to 10 nucoins (or more) she received (and has not spent yet) in the past. eg:

Transaction History

Txn ID	Amount	From	To
T1	10	Dave	Alice
T2	5	Jake	Alice

Outgoing payment

Txn Inputs	From	To
T1	Alice	Bob

Here, T1, T2 are hashes. This solves two problems:

1. Ensuring that Alice has enough Nucoins
2. Each transaction can be traced back to the initial transaction in the system

NuCoin v0.4: Re-using transactions?

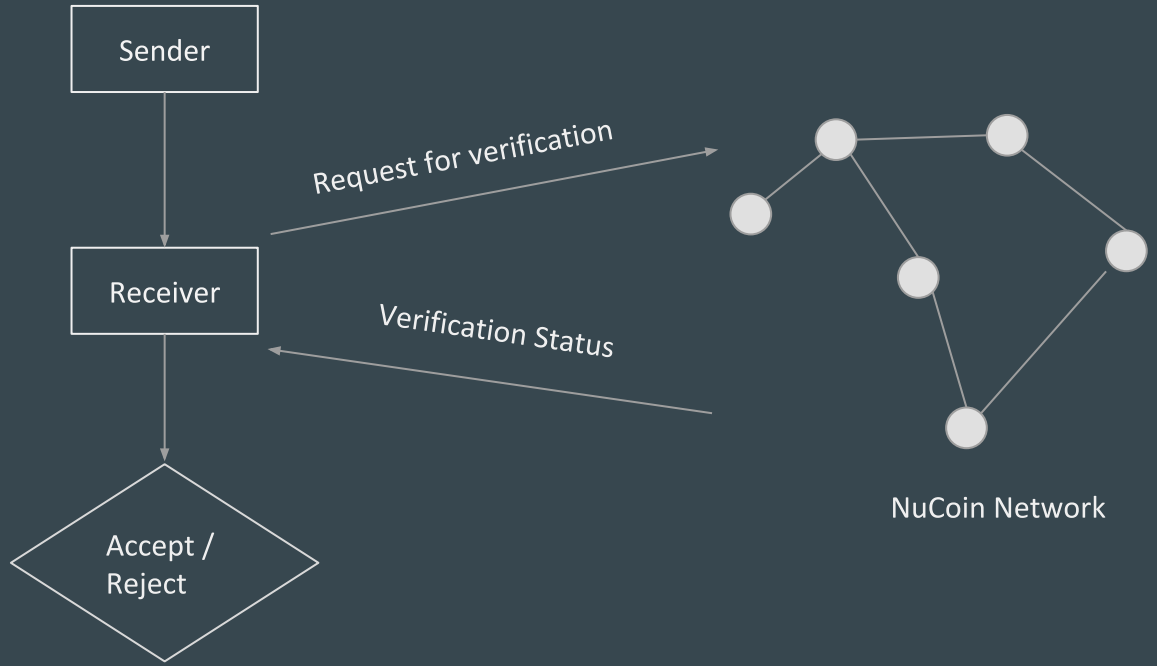
Alice can still cheat by double spending - if she sends identical messages to multiple users

Txn Inputs	From	To
T1	Alice	Bob

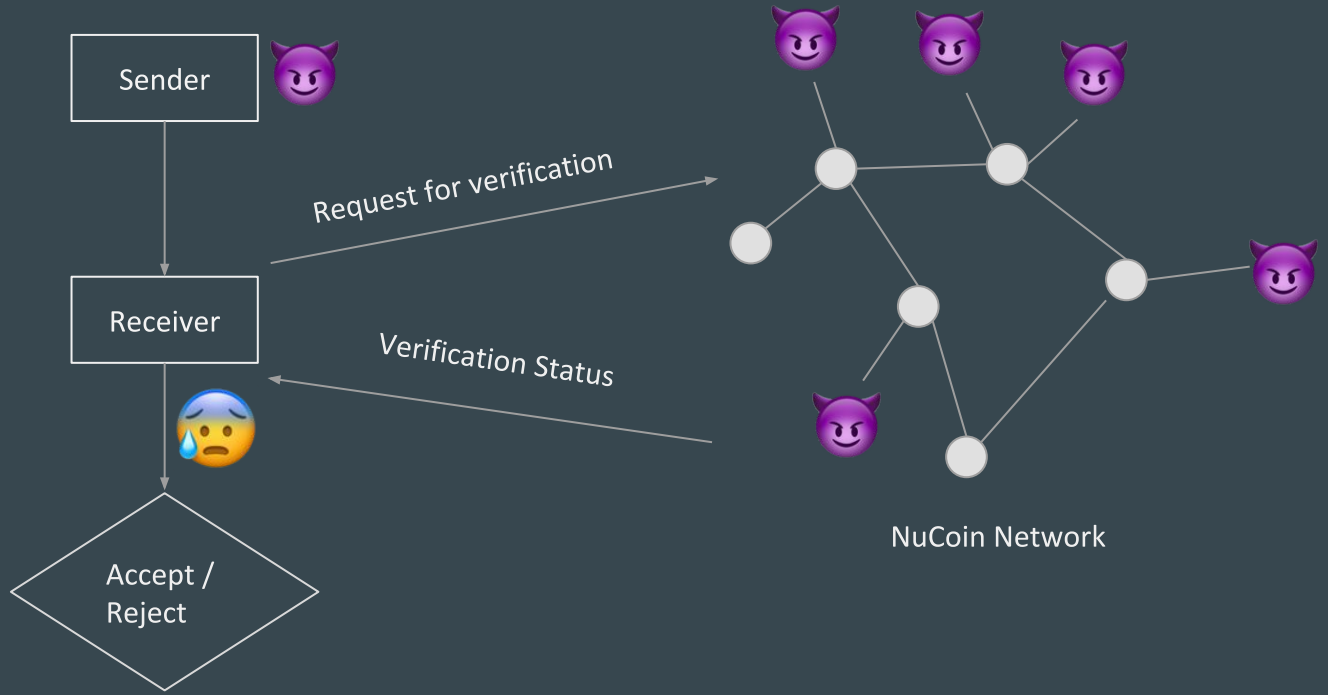
Txn Inputs	From	To
T1	Alice	Charlie

If Charlie and Bob receive this message at nearly the same time, they will both end up accepting it as valid

NuCoin v0.5: Verification by consensus



NuCoin v0.5: Verification by consensus



NuCoin v0.6: Proof of Work

PoW solves the problem of an individual or a group taking over the entire network

The computational power of the majority of the network overwhelms that of the smaller (erm.. hopefully!) portion of baddies in the network.

The idea is counterintuitive and involves a combination of two ideas:

1. to make it computationally costly for network users to validate transactions; and
2. to reward them for trying to help validate transactions

How Bitcoin works

- New transactions are placed in an unordered global pool of ‘pending’ transactions
- Transactions are picked from the pool for verification
- Transaction are verified by traversing back the transaction chain
- A node verifies several transactions and groups them together into a ‘block’
- To “suggest” a block to the network, the node must append a nonce and hash it such that the hash is less than a predefined target
- With several new block suggestions on the network, the one whose hash is solved first gets added to the global blockchain

Forks in the Blockchain

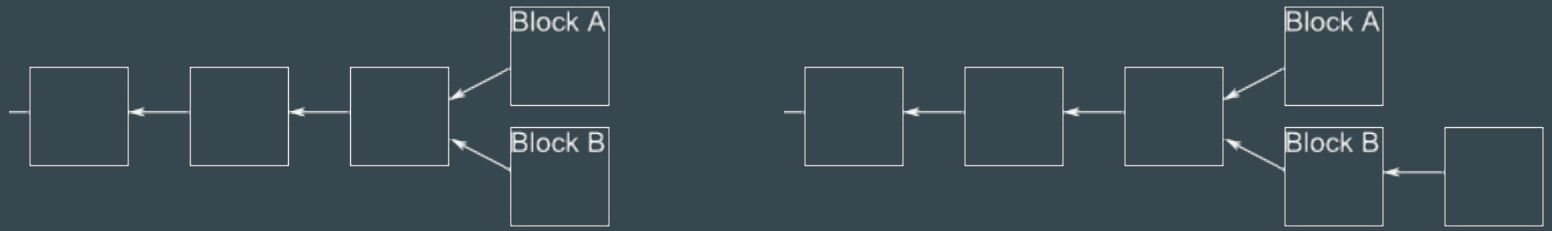
- Occasionally, a fork will appear in the block chain. This can happen, if by chance two miners happen to validate a block of transactions near-simultaneously

- Both broadcast their newly-validated block out to the network, and some people update their blockchain one way, and others update their blockchain the other way:

This is a problem – it's no longer clear in what order transactions have occurred

Resolving forks

- If a fork occurs, people on the network keep track of both forks
- Miners who receive block A first will continue mining along that fork, while the others will mine along fork B



- In the example above, the miner extended Fork B. She broadcasts it to the network
- As others receive news that this has happened, fork A will be abandoned for being shorter

Bitcoin: Mining

To “suggest” a block of newly confirmed transactions to the network, the node must append a nonce and hash it such that the hash is less than a predefined target.

Inputs for the algorithm are:

1. ID (hash) of the latest (accepted) block in the blockchain
2. all transactions within the new block
3. nonce (random token)

$$f(\text{block\#1234, txn\#10, txn\#45, …, } 23004) < \text{target}$$

This is a computationally expensive operation

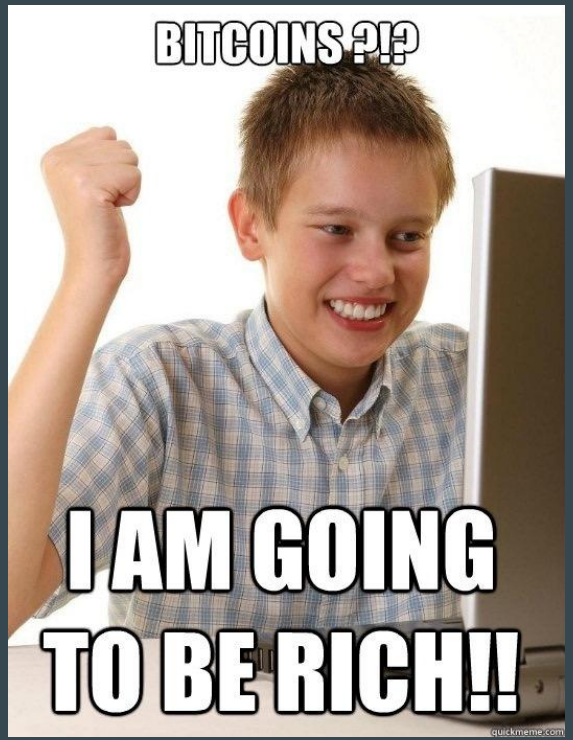
Bitcoin: Mining

- If Bob finds a nonce which satisfies the target criteria, he broadcasts its results (the block + nonce) to the network
- Unless another node ‘has won’ by broadcasting a block sooner, Bob would receive the reward (12.5 BTC as of May 2017)
- If Dave solved a block before Bob, the latter must start over again because the first parameter of his equation would need an update (also some of these transactions may already be part of the Dave’s block):

$$f(\text{block\#1234}, \text{txn\#10}, \text{txn\#45}, \ldots, 4568) < \textbf{target}$$

Bitcoin: Mining

1. Get the hardware
2. Download mining software
3. Join a pool (eg BTC Guild)
4. Set up your wallet
5. Rake in the moolah!



Bitcoin: Loose ends

- Privacy
- Legal status
- Theft
- Deflationary Nature

Blockchain is not about Bitcoin!

Blockchain is a novel solution for any use-case which requires a majority consensus among decentralized participants. People are doing awesome stuff with Blockchain!

Exhibit 6

Selected Potential Blockchain Use Cases

Financial Institutions	Corporates	Governments	Cross-industry
International payments	Supply chain management	Record management	Financial management & accounting
Capital markets	Healthcare	Identity management	Shareholders' voting
Trade finance	Real estate	Voting	Record management
Regulatory compliance & audit	Media	Taxes	Cybersecurity
Anti-money laundering & know your customer	Energy	Government & non-profit transparency	Big data
Insurance		Legislation, compliance & regulatory oversight	Data storage
Peer-to-peer transactions			Internet of Things

Source: Moody's Investors Service

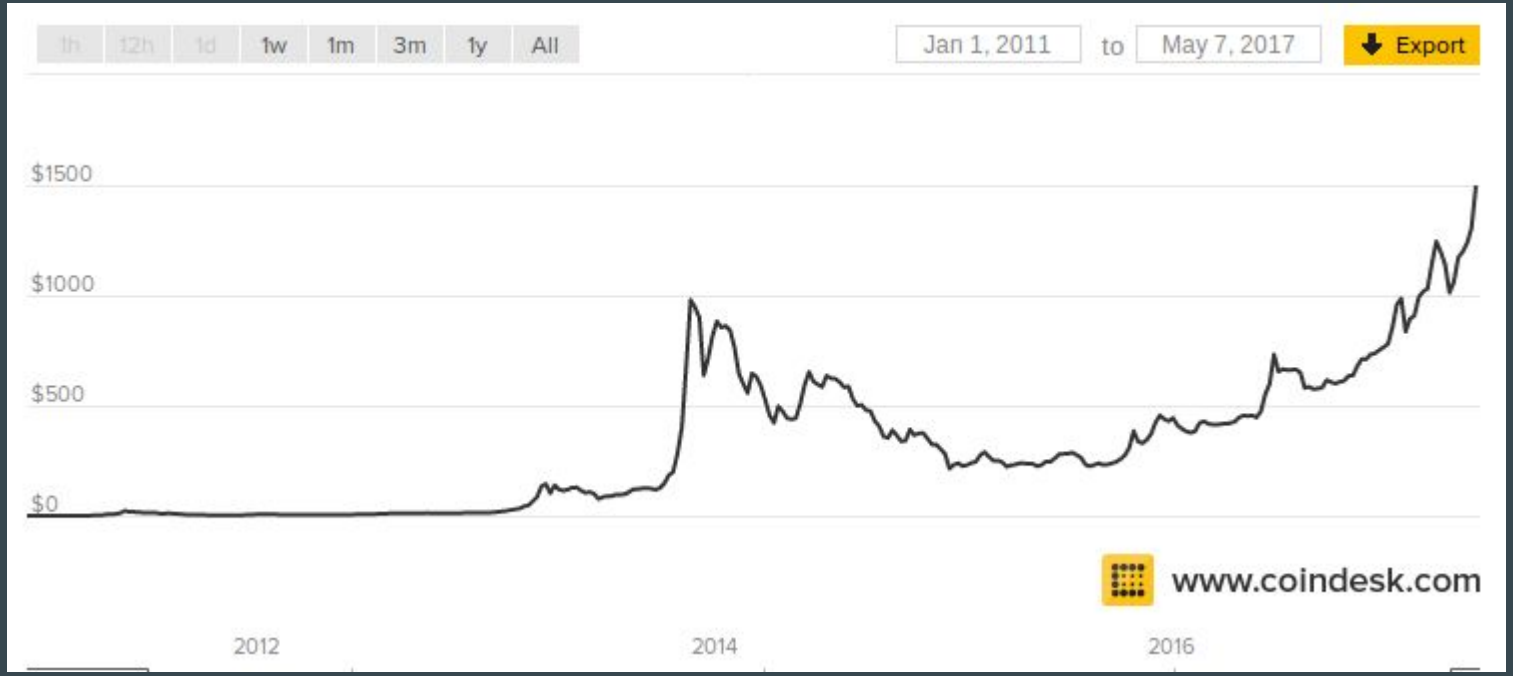
Blockchain is not about Bitcoin!

1. Distributed cloud storage. eg: https://blockstack.org/ Claims to be ‘a new internet’ - a P2P network with distributed name resolution and storage. Think: serverles websites! **Net Neutrality**
2. Copyright protection. eg: https://proofofexistence.com/about Demonstrating data ownership at a point in time without revealing actual data.
3. Verifiable data, digital identity (passports, birth certificates, lease documents)
4. Everledger diamond registration https://www.everledger.io/
5. Initial Coin Offering (ICO) and Colored Coins
6. Smart Contracts

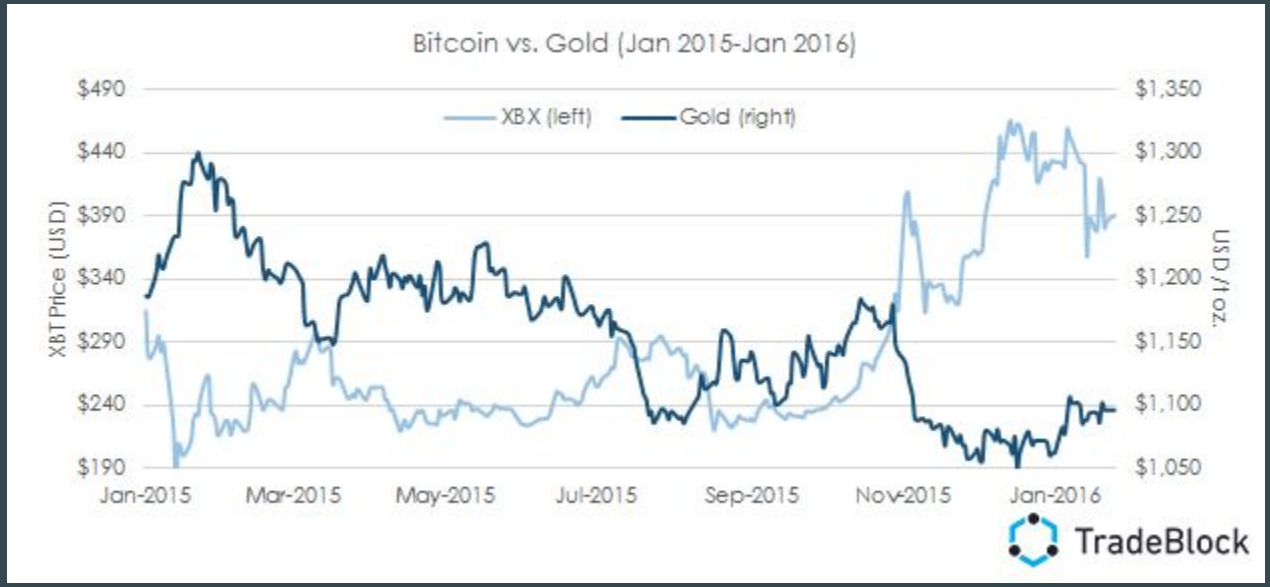
Blockchain? Really?

Grill Me!

Bitcoin: Price Index



Bitcoin: Standout Correlations



Bitcoin: Standout Correlations

Further Reading

1. http://www.reuters.com/article/us-banks-blockchain-accenture-idUSKBN1511OU
2. http://qz.com/695892/how-blockchain-technology-can-prevent-the-next-financial-crisis-disrupt-uber-and-give-us-control-of-our-data/
3. https://blockchainfutureslab.wordpress.com/2016/02/27/a-typical-day-in-a-blockchain-enabled-world/
4. https://bitcoinmagazine.com/articles/is-blockchain-powered-copyright-protection-possible-1470758430/
5. http://www.coindesk.com/math-behind-bitcoin/
6. https://blockexplorer.com/

Where it all started: https://bitcoin.org/bitcoin.pdf

Also watch out for

1. HyperLedger (https://www.hyperledger.org/)
2. Ethereum (https://www.ethereum.org/)

Subir Chowdhuri

Works a day job as a webapp developer
Builds MVPs for early-stage startups
Moonlights as a hardware hacker and 3D artist
Digs all things science. Lives to code
Is no expert on Blockchain! Once sold all his bitcoins @ US$13/BTC

www.desdevpro.com

subir@desdevpro.com

SubirChowdhuri