Overview/1

- What is a Blockchain
- What is Bitcoin
- Where did Bitcoin come from?
- How does a Blockchain get built
- How does a Blockchain get verified

Overview/2

- Weaknesses of Blockchain technology
- Value
- Current applications of Blockchain technology
- Future applications of Blockchain technology
- Q & A

Who am I?

- Serial entrepreneur since age 16 - first computer was an Apple][+
- Coding since 1980 in every major language (and a lot of minor ones)
- Wrote a BBS from scratch – forced to learn assembly language ;-)
- MSc Software Engineering, UST & MBA Carlson School of Management

Some of my hobbies

Blockchain Defined

Simply defined a Blockchain is little more than a:

- Distributed
- Secure
- Logfile

A digital currency was in a lot of ways the first demonstrable use

What is Bitcoin ?

- A **protocol** that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency*

- A **public**ly disclosed linked **ledger** of transactions stored in a blockchain

- A **reward** driven system for achieving **consensus** (mining) based on "Proofs of Work" for helping to secure the network

- A "scarce token" economy with an eventual cap of about 21M bitcoins

I would argue it behaves more like a security like a Stock or Bond than a currency, a crypto-equity

Bitcoin Whitepaper – 2008.10.31*

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

* Halloween

Features of Bitcoin

- Essentially it's "deflationary" – the reward is cut in half every four years, and tokens can be irrevocably destroyed
- Nearly infinitely divisible currency units supporting eight decimal places 0.00000001 (known as a Satoshi or Noncent*)
- Nominal transaction fee's paid to the network
  - Same cost to send $.01 as $1,000,000
- Consensus driven – no central authority
- Counterfeit resilient
  - Cannot add coins arbitrarily
  - Cannot be double-spent
- Non-repudiation – aka "gone baby gone" – no recourse and no one to appeal to return sent tokens

http://www.urbandictionary.com/define.php?term=Noncents

When did it start?

- "Satoshi Nakamoto" created the reference implementation that began with a Genesis Block of 50 coins

- **2008**
  - **August 18**   Domain name "bitcoin.org" registered[1].
  - **October 31**   Bitcoin design paper published
  - **November 09** Bitcoin project registered at SourceForge.net
- **2009**
  - **January 3**   Genesis block established at 18:15:05 GMT
  - **January 9**   Bitcoin v0.1 released and announced on the cryptography mailing list
  - **January 12**   First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

https://en.bitcoin.it/wiki/History

> **Why does it have value?**

The worth of a thing
is the price it will bring.

Why does it matter?

9.8 Billion Dollar Market Cap!

| ▲ #	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	$9,822,140,284	$617.20	15,913,980 BTC	$35,983,700
2	Ethereum	$1,023,247,057	$12.07	84,804,165 ETH	$7,292,870
3	Ripple	$267,292,076	$0.007534	35,475,802,044 XRP *	$3,362,080
4	Litecoin	$183,232,434	$3.82	47,915,554 LTC	$1,171,010

Decentralized

- The "digital wallet" operates in a peer to peer mode
- When it starts it bootstraps to find other wallets
  - Originally it used the Internet Relay Chat (IRC) network
  - Now based on DNS and "seed nodes"
- The wallet will synchronize with the network by downloading ALL of the transactions starting from the GENESIS block if necessary
  - 433,679 blocks at time of slide prep
  - Just over 90 GB
- Using a "gossip protocol" the wallets share all transaction information with their peers
- http://en.wikipedia.org/wiki/Gossip_protocol

Coins flow from Inputs to Outputs

A coin owner transfers coins by digitally signing (via ECDSA) a hash digest of the previous transaction and the public key of the next owner. This signature is then appended to the end of the coin.
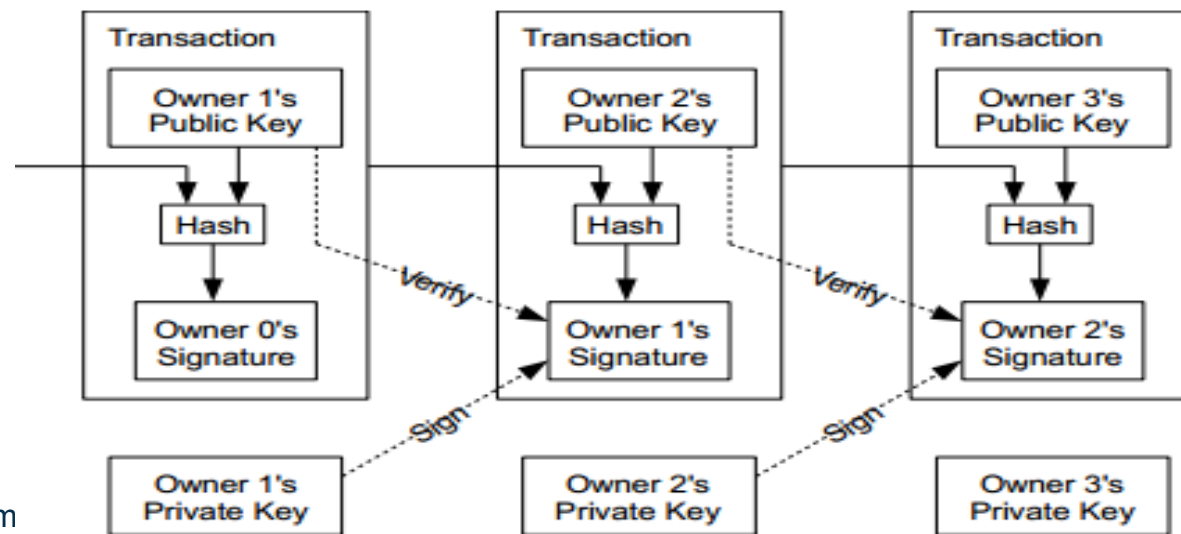
Pseudo Anonymous

- Using public key cryptography, specifically Elliptic Curve Cryptography due to its key strength and shorter keys

- Transactions are sent to public key "addresses"

  1AjYPi8qryPCJu6xgdJuQzVnWFXLmxq9s3

  1Give4dbry2pyJihnpqV6Urq2SGEhpz3K

d39b0c4653b982e9aee616003db410e75868f61054656e044f0cdedbb6e77342		2015-01-13 16:23:53
1G5kvbP33mMwgtSTHpwAJe86xWKBwUHSV4 1HKBEEHryiuBd8Fp9Skhui6YGnLYNB3hQZ 1pob2EUuE1r7PjpMceubopkSWnrkSivY5	→ 1JqFCQNCJr16rb4h3J2SvDg5ic5UejEPwi 14DaDziYJCD4h8GQ3nbh8bx244Fc9Fc13J	2.103973 BTC 0.01000001 BTC
		2.11397301 BTC

Addresses are like Accounts

- The wallet listens for transactions addressed to any of its public keys and in theory is the only node that is able to decrypt and accept the transfer

- "Coins" are "sent" by broadcasting the transaction to the network which are verified to be viable and then added to a block

- Keys can represent a MULTI-SIG address that requires a N of M private keys in order to decrypt the message

The Public Ledger

- Every *viable* transaction is stored in a public ledger

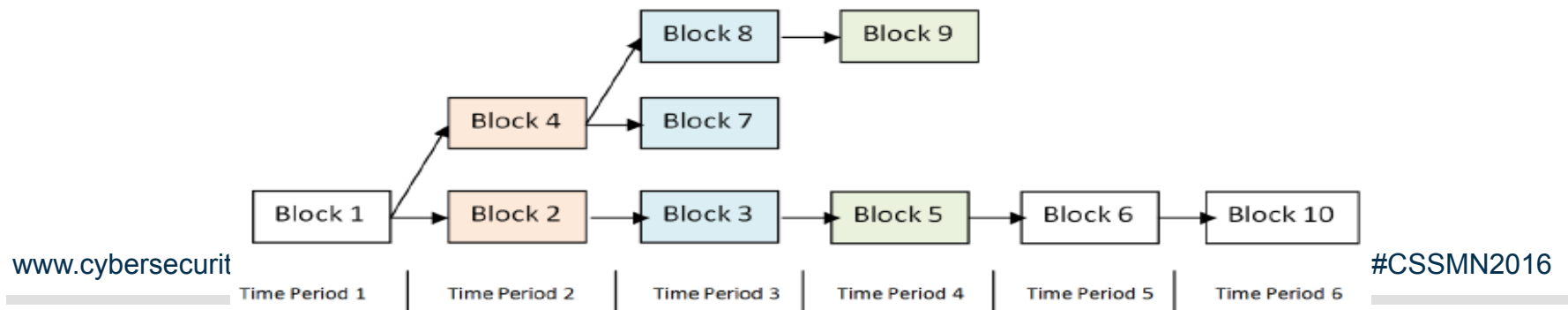- Transactions are placed in blocks, which are linked by SHA256 hashes.

- https://blockchain.info
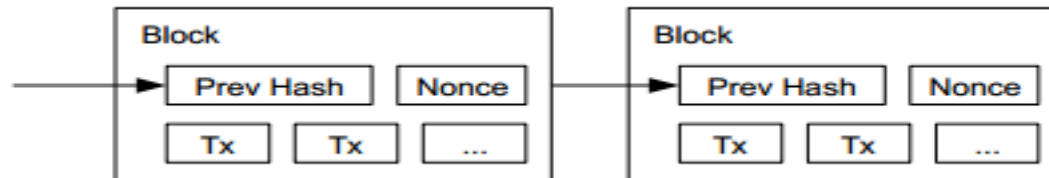
> ## "What is Bitcoin" – Video

- http://weusecoins.com

Arriving at Consensus

- Although the accepted chain can be considered a list, the block chain is best represented with a tree.

- The longest path represents the accepted chain.

- A participant choosing to extend an existing path in the block chain indicates a vote towards consensus on that path. The longer the path, the more computation was expended building it.

| Block 8 | → | Block 9 |

| Block 4 | → | Block 7 |

| Block 1 | → | Block 2 | → | Block 3 | → | Block 5 | → | Block 6 | → | Block 10 |

Time Period 1 | Time Period 2 | Time Period 3 | Time Period 4 | Time Period 5 | Time Period 6

Consensus Process = Mining

- Originally the digital wallet could also participate in the consensus process by attempting to secure the network directly

- This process is known as "mining"

- Mining involves attempting to find a numerical value, known as a "nonce" that when combined with all open transactions can be "hashed" into a value that satisfies a certain "difficulty"

- Custom, purpose built-hardware has long since replaced the function such that its no longer productive for simple CPU based systems to compete in the mining process, and thus it was removed

Hashcash *(Or How to Pay a Byzantine Generals Salary)*

- Like many great ideas to become realized, it takes a confluence of other great ideas

- Based on the idea of HashCash, a Proof of Work concept invented by Adam Back in 1997 (http://www.hashcash.org/papers/hashcash.pdf)

- Originally proposed as an anti-spam throttling mechanism

- The core idea is that before accepting a transaction, the sender must first demonstrate a "cost" via a computationally "hard" problem that can simultaneously be easily verified.

- This generally referred to as a "Proof of Work"

$$\begin{cases} \mathcal{C} \leftarrow \textbf{CHAL}(s, w) & \text{server challenge function} \\ \mathcal{T} \leftarrow \textbf{MINT}(\mathcal{C}) & \text{mint token based on challenge} \\ \mathcal{V} \leftarrow \textbf{VALUE}(\mathcal{T}) & \text{token evaluation function} \end{cases}$$

The Role of Hashing

- A **hash function** is any **function** that can be used to map digital data of arbitrary size to digital data of fixed size, with slight differences in input data producing very big differences in output data.
- MD5, SHA1, SHA256
- For example, the MD5 hashes of 'abc' compared to 'abC'

abc
0bee89b07a248e27c83fc3d5951213c1

abC
2217c53a2f88ebadd9b3c1a79cde2638

"The Quick Brown Fox Jumped Over the Lazy Dog"
2dfd75162490ed3b4c893141f9ab37cf

Proof of "Work" (or proof of waste :-)

- A **publicly auditable** cost-function can be *efficiently* verified by any third party without access to any trapdoor or secret information.

- A **fixed cost** cost-function takes a fixed amount of resources to compute. The fastest algorithm to mint a fixed cost token is a deterministic algorithm.

- A **probabilistic cost** cost-function is one where the cost to the client of minting a token has a predictable expected time, but a random actual time as the client can most efficiently compute the cost-function by starting at a random start value. Sometimes the client will get lucky and start close to the solution.

The Hash Lottery

- Hashing is straightforward, but not challenging
- Unless the goal is to say, find me a hash value that satisfies a certain level of "difficulty"
- For example, let's say the challenge is find a hash-value that begins with a number of zeros, for a given input
- The Proof of Work comes from finding a number (known as a NONCE) that when added to the input changes the output of the hash value to satisfy the difficulty.
- In the Bitcoin world this is what "mining" is and in effect is little more than a lot of hash-power spent on guessing winning lottery numbers that satisfy the difficulty of the problem in order to obtain the reward from the network

The Payout

- The node that finds the best solution to the challenge is provisionally granted a reward
- Originally in Bitcoin it was 50 new coins, today it's 12.5
- Competing solutions are evaluated based on which node offers the higher number of transactions included in the candidate block as well as the level of over-satisfying the difficulty.
- For example, if two nodes offer a solution to the challenge and both have the same number of transactions, the reward will go to the node that found a NONCE that beat the challenge
  - E.G. Find a hash that begins with 4 zeros
  - The node that supplies a hash that has 5 zeros beats the node that only finds the minimum

Transaction Confirmation

- Having a transaction provisionally accepted into a candidate block signals that the network has verified that the inputs were viable

- Every new block accepted into the chain after the transaction was accepted is considered a **confirmation**

- Coins are not considered mature until there have been 6 confirmations (basically an hour assuming a 10 minute block cadence)

- New Coins created by the mining process are not valid until about 120 confirmations

- This is to assure that a node with more than 51% of the total hash-power does not pull off fraudulent transactions

"What is Bitcoin Mining" – Video

- http://www.bitcoinmining.com

Why 51% Matters

- **"When does 1 + 1 = 3 ?" ***

  * When everyone says it does!

- In the case of Bitcoin "consensus" goes to the chain with the highest number of blocks

- Not just in theory, but in practice several large mining pools have generated six blocks in a row

- To date the network has voluntarily shifted its mining power around or faced Distributed Denial of Service attacks

Purchase / Exchange Bitcoins

In addition to mining bitcoins, they can be acquired from an exchange!

bitpay

coinbase

BTC e

BITTREX

Who Accepts Bitcoins?

Merchants Accepting Bitcoin

- Overstock.com
- Newegg.com
- Microsoft XBOX Network
- Telsa Motors
- Time Inc (publisher)
- Virgin Galactic
- Wordpress
- BitPay claims 44,000 merchants!
- http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html

Other Uses of Blockchain Tek

- Registeries
- Authoritative Systems of Record
- Directory Services
- Timestamping Services ("Proof of Existence")
- Counter-party Exchanges

Registries

World's First Bitcoin Wedding

Newlyweds Exchange Digital Vows "Because the Blockchain is Forever"

BELÉN MARTY | **OCTOBER 7, 2014 AT 12:22 PM**

| f | 266 | | 36 | g+ | 2 | in | 4 | 46 |

A new virtual era has arrived in the United States. The first "blockchain wedding" was held on Sunday, August 5, during a bitcoin conference at Disney World in Orlando, Florida. The marriage was performed and registered without the involvement of any government or religious organization, and instead submitted to an online public registry: the bitcoin blockchain.

Español

The blockchain is a decentralized, secure database that allows transactions to be seen by other users. This technology allows users to send digital currency like bitcoin, or specific documents and messages that are incorporated into the

Namecoin

The first fork of Bitcoin with a purpose

- Securely record and transfer arbitrary names (keys).
- Attach a value (data) to the names
- (up to 520 bytes, more in the future).
- Transact namecoins, the digital currency (NMC).
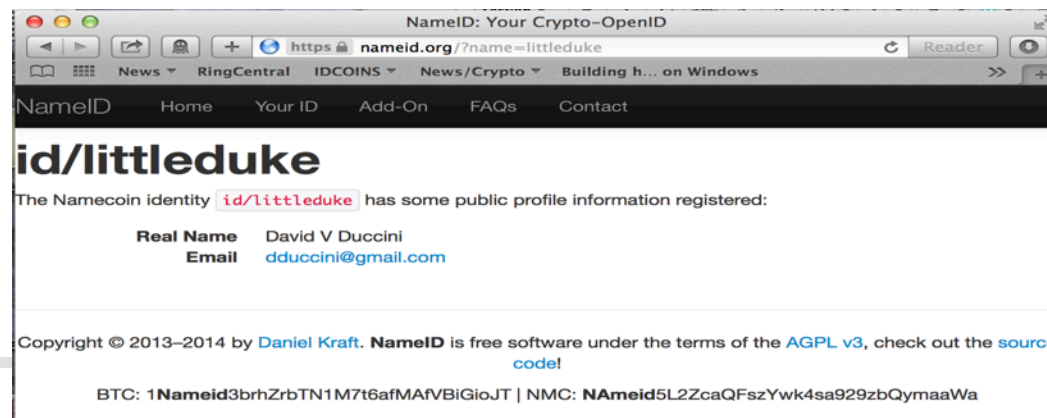
Namecoin as a fault-tolerant Domain Name System

Can act as a decentralized Domain Name Service that is resilient to censorship

http://bit.namecoin.info

Alternates to Bitcoin aka Altcoins

- "Good artists copy. Great artists steal."
- The first alternate blockchain as mentioned was **Namecoin**
- Early attempts to "re-level the playing field" were made by changing the hashing function from SHA256 to SCRYPT or sets of hash functions (X11)
- SCRYPT is a "memory intensive" function that was thought to be resistant to customized hardware (false)
- Changes to the block emit time target were also changed from Bitcoins 10 minutes to 2.5 minutes to increase the velocity
- Newer ALTS incorporate ever escalating hash functions, chained together in novel ways to resist giving purpose built hardware an advantage over CPU based mining

A Babel of Altcoins

- Now well over 640 "alternate" coins to Bitcoin (and 67 "assets), comprising ~2,300 markets!

- 99.999% of them are simply brands / clones

- Most tinker with:
  - the total coin supply
  - the hashing functions (SHA256, SCRYPT, X11 et al)
  - block emit time targets
  - Proof of Something (Proof of Work, Proof of Stake)

- Notable Alts: Ripple, Litecoin, Dogecoin

- **Total Market Cap: $ 12B** (Bitcoin is 9.8B of that)

- http://coinmarketcap.com

It's Better 2GIVE!

- https://2Give.Info

Bitcoin 1.5

COUNTERPARTY.ORG

Counterparty works by storing extra data in regular Bitcoin transactions, which makes every Counterparty transaction a Bitcoin transaction, albeit a very small one.

MASTERCOIN.ORG

- The Master Protocol facilitates the creation and trading of smart properties and user currencies as well as other types of smart contracts.
- Mastercoins serve as the binding between bitcoins (BTC), smart properties and smart contracts created on top of the Mastercoin Protocol.

NXT.ORG

Asset creation and exchange on its own blockchain

Bitcoin 2.0

- Smart Contracts
  - Escrow-free exchange
  - Insurance
- Voting
- Distributed Autonomous Organizations
- Identity & Reputation Systems
  - http://bit.ly/idcoins

Ethereum.org

Turing complete contracts on a blockchain.

- Contracts are the main building blocks of Ethereum.

- A contract is a computer program that lives inside the distributed Ethereum network and has its own ether balance, memory and code.

- Every time you send a transaction to a contract, it executes its code, which can store data, send transactions and interact with other contracts.

- Contracts are maintained by the network, without any central ownership or control.

- Contracts are written in languages instantly familiar to any programmer and powered by Ether, Ethereum's cryptofuel.
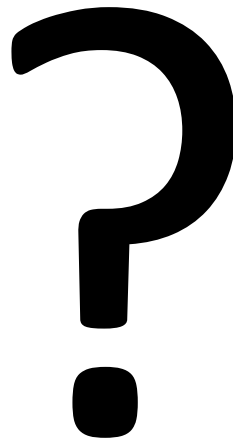
Bad Uses for Good Technology
"Guns Don't Kill People. People Kill People"

- Bitcoin has had its fair share of "bad press"

- Silk Road
  - An online anonymous marketplace for "censorship-free" commerce

- Bitinstant
  - Charlie Shrem plead guilty to aiding money laundering

- MT-GOX
  - aka "Magic The Gathering Online eXchange"
  - 700,000 coins "missing"

- Bitstamp

Resources

- Bitcoin: A Peer-to-Peer Electronic Cash System
  https://bitcoin.org/bitcoin.pdf

- http://coinmarketcap.com

- Hashcash.org

- IDCoins: A Web of Trust Blockchain for Identity and Reputation,
  David V Duccini, http://bit.ly/idcoins

- "Mastering Bitcoin", Andreas M.Antonopoulos , O'Reilly Media

- http://www.bitcoinsecurity.org/2012/07/22/what-is-bitcoin/

- https://www.weusecoins.com

Q&A

?

Contact Info

- Twitter: @TheLittleDuke

- Skype: The_Little_Duke

- LinkedIN: http://linkedin.com/in/dvduccini