Blockchain Technology
Bitcoin and Beyond

David V Duccini, MSc, MBA, CISSP, IFR Private Pilot, Rescue Diver
aka The Little Duke

http://linkedin.com/in/dvduccini

Agenda

• What is a Blockchain
• What is Bitcoin
• Where did Bitcoin come from?
• How does a Blockchain get built
• How does a Blockchain get verified
• Weaknesses of Blockchain technology
• Value
• Current applications of Blockchain technology
• Future applications of Blockchain technology
• Q & A
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 publicly 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 “scare 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
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
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?

3.6 Billion Dollar Market Cap!

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Available Supply</th>
<th>Volume (24h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$3,669,414,845</td>
<td>$267.57</td>
<td>13,713,850 BTC</td>
<td>$17,532,500</td>
</tr>
<tr>
<td>2</td>
<td>Ripple</td>
<td>$582,973,299</td>
<td>$0.018819</td>
<td>30,978,075,200 XRP</td>
<td>$582,145</td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$61,428,208</td>
<td>$1.73</td>
<td>35,502,504 LTC</td>
<td>$2,578,080</td>
</tr>
</tbody>
</table>

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
  - 338,540 blocks at time of slide prep
  - Just over 20 GB
- Using a “gossip protocol” the wallets share all transaction information with their peers
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
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.

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](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.
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
- 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”

\[
\begin{align*}
\mathcal{C} & \leftarrow \text{CHAL}(s, w) \quad \text{server challenge function} \\
\mathcal{T} & \leftarrow \text{MINT}(\mathcal{C}) \quad \text{mint token based on challenge} \\
\mathcal{V} & \leftarrow \text{VALUE}(\mathcal{T}) \quad \text{token evaluation function}
\end{align*}
\]
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
```
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
• 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

Why 51% Matters

- “When does 1 + 1 = 3 ?” *

- 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

* When everyone says it does!
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"

BÉLÉN MARTY  OCTOBER 7, 2014 AT 12:22 PM

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.

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 ($N$, 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 was Namecoin
- Early attempts to “re-level the playing field” were made by changing the hashing function from SHA256 to SCRYPT
- SCRYPT is a “memory intensive” function that was thought to be resistant to customized hardware (false)
- Changes to the blockemit time target were also changed from Bitcoins 10 minutes to 2.5 minutes to increase the velocity
- Newer ALTS incorporate every 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 500 “alternate” coins to Bitcoin
- 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:** $4,540,315,390 (Bitcoin is 3.6B of that)
  - 12/7/15: $5,936,541,651 of $6,505,398,832
- [http://coinmarketcap.com](http://coinmarketcap.com)
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

• Notable Implementations
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
  • Ross Ulbricht’s trial starts this week
• Bitinstant
  • Charlie Shrem plead guilty to aiding money laundering
• MT-GOX
  • aka “Magic The Gathering Online eXchange”
  • 700,000 coins “missing”
• Neo & Bee
• Bitstamp
Part II: Mining & Consensus

Checkpointing

How decentralized is Bitcoin?
Mining difficulty

Difficulty adjustment
Mining rewards

Total network capacity

- $2^{64}$ hashes per block (every 10 minutes!)
- $2^{75}$ hashes in 2013
  - In exchange for ~US$250M
- Consuming > 100 MW
Bitcoin mining hardware

TerraMiner™ IV - 2TH/s
Networked ASIC Miner

$5,999
Shipping June 2014

300 GH Bitcoin Mining Card
The Monarch BPU 300 C
$1,497.00

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

Mining pools

Mint(25, K_{POOL})

0x00000000000000003f89...
0x000000000000490c6b00...
0x0000000000001e8709ce...
0x00000000000007313490c6
0x00000000000045a16f89...
0x000000000000a877911f...
0x000000000000000000000000003f89...
0x000000000000490c6b00...
0x0000000000001e8709ce...
0x00000000000007313490c6
0x00000000000045a16f89...
0x000000000000a877911f...
Mining pools

Part III: Bitcoin as a currency
Why does Bitcoin have value?

*Consensus*

- Consensus in state (blockchain)
- Consensus in payment
- Consensus in rules

The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries
Joshua Kroll, Ian Davey, Ed Felten. WEIS 2013
Black Markets

Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace
Nicolas Christin, WWW 2013

Capital controls

As Inflation Rages In Iran, Bitcoin Software Not Available

BTC China CEO Attempts To Calm The Bitcoin Market After RMB Deposit Shutdown

Posted Dec 20, 2013 by John Biggs (@johnbiggs)
Purchase / Exchange Bitcoins

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

Beware the middleman: Empirical analysis of Bitcoin-exchange risk
Tyler Moore and Nicolas Christin, Financial Crypto 2013
Who Accepts Bitcoins?

E-commerce
Merchants Accepting Bitcoin

- Overstock.com
- Newegg.com
- Microsoft XBOX Network
- Tesla Motors
- Time Inc (publisher)
- Virgin Galactic
- Wordpress
- BitPay claims 44,000 merchants!

Part IV: Anonymity
Bitcoins carry a transaction history

- identification
- censorship
- recovery from theft
- economic analysis

Towards Risk Scoring of Bitcoin Transactions
Möser, Malte, Rainer Böhme, and Dominic Breuker, BITCOIN 2013
Mixes today

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.

-The Bitcoin Wiki

An inquiry into money laundering tools in the Bitcoin ecosystem
Möser, Malte, Rainer Böhme, and Dominic Breuker, ECRIME 2013