ICT in Financial Management

Topic: Blockchain Technology Bitcoin and Beyond

Presentation by:

Festus Kitui
Kituif@gmail.com
+254-722-53-69-84

21st April 2017

Blockchain Technology

Bitcoin and Beyond

Presentation by:

Festus Kitui

21st April 2017

- What is a Blockchain
- What is Bitcoin
- How does a Blockchain get built
- How does a Blockchain get verified
- Value - BTC

Simply defined a Blockchain is little more than a:

- Distributed
- **Secure**
- Logfile – (Ledger)

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

- People use the term ‘blockchain technology’ to mean different things, and it can be confusing. Sometimes they are talking
- about The Bitcoin Blockchain, sometimes it’s other virtual currencies, sometimes it’s smart contracts. Most of the time though,
- they are talking about distributed ledgers, i.e. a list of transactions that is shared among a number of computers, rather than
- being stored on a central server.

The common themes seem to be a data store which:

- Usually contains **financial transactions.**
- • Is replicated across **a number of systems in almost real-time.**
- • Usually exists over a **peer-to-peer network.**
- • Uses **cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights.**
- • Can be **written by certain participants.**
- • Can be **read by certain participants, a wider audience.**

- Has mechanisms to make it **hard to change historical records, or at least make it easy to detect when someone is trying** to do so.

[redacted]

- There is a big difference in what technologies you need, depending on whether you allow *anyone to write to your blockchain,* or known, vetted participants. Bitcoin allows *anyone to write to its ledger.*

[redacted]

Public blockchains.

Ledgers can be 'public' in two senses:

1. Anyone, without permission granted by another authority, can write data

2. Anyone, without permission granted by another authority, can read data

Usually, when people talk about public blockchains, they mean anyone-can-write.

Private blockchains.

Conversely, a 'private' blockchain network is where the participants are known and trusted: for example, an industry group, or a group of companies owned by an umbrella company.

Many of the mechanisms aren't needed – or rather they are replaced with legal contracts.

This changes the technical decisions as to which bricks are used to build the solution.

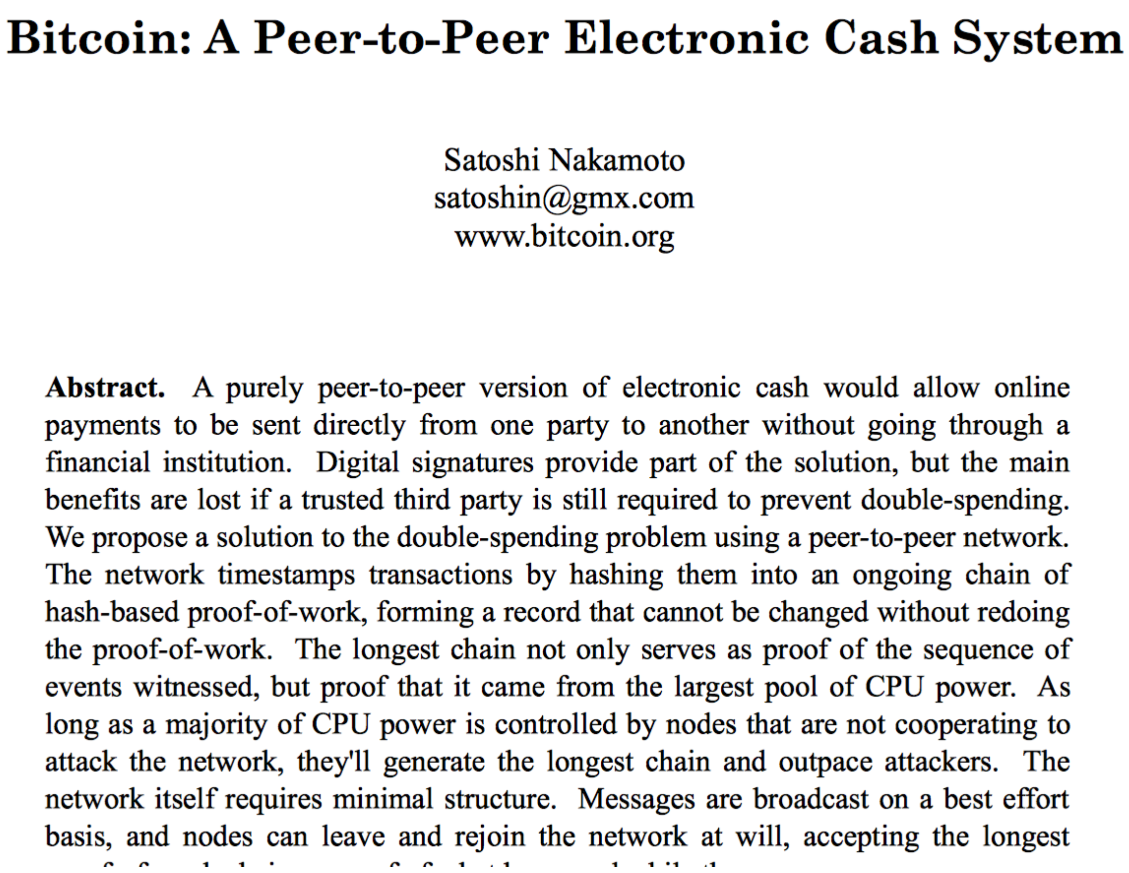
- A **protocol** that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency*

- 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 "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* [redacted] 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

- 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

- “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

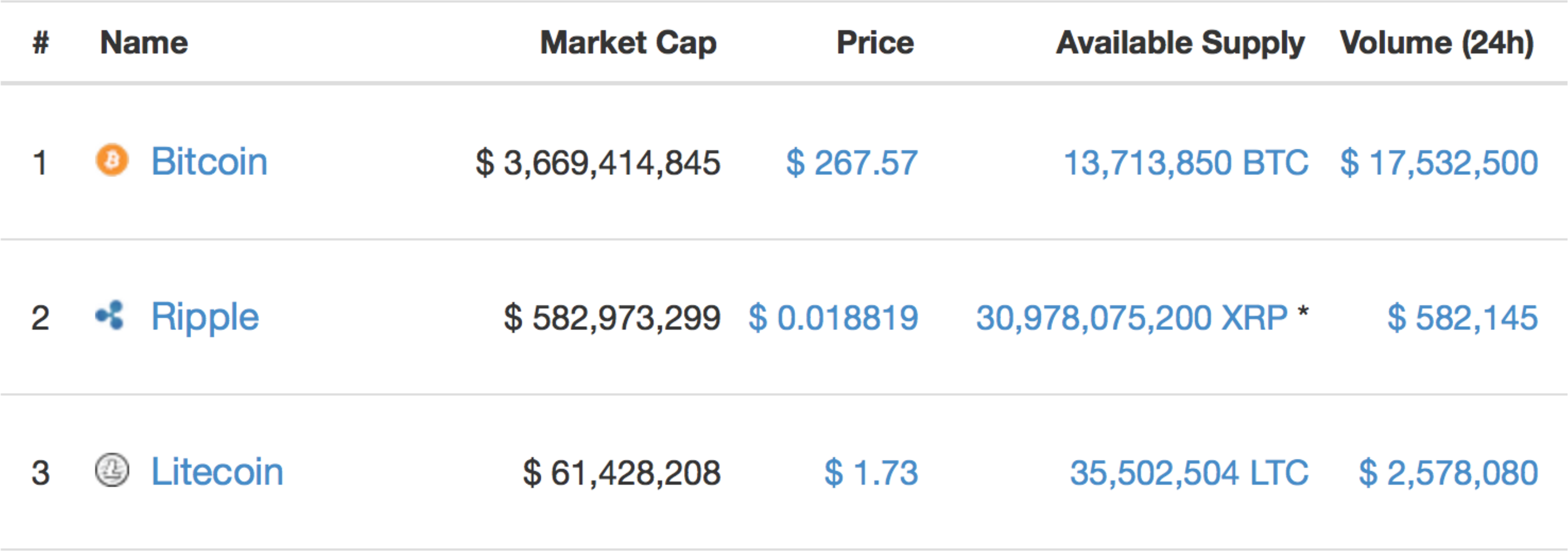
[redacted]

The worth of a thing

is the price it will bring.

[redacted]

3.6 Billion Dollar Market Cap!



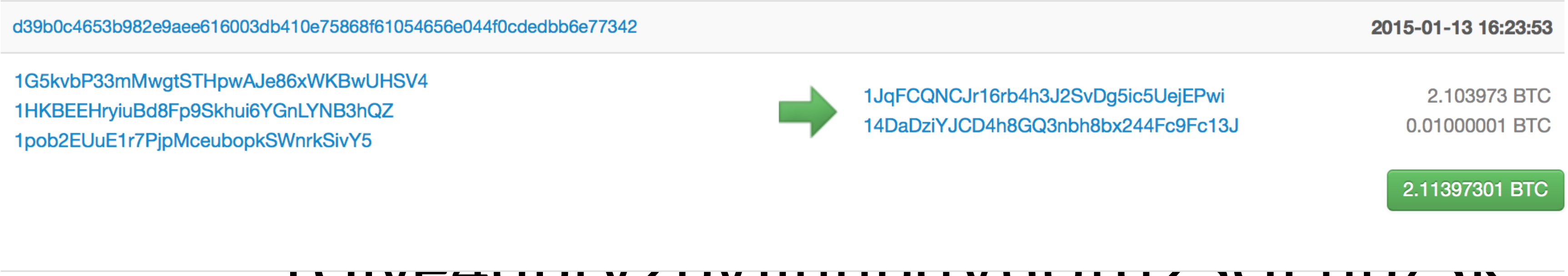
#	Name	Market Cap	Price	Available Supply	Volume (24h)
1	Bitcoin	$ 3,669,414,845	$ 267.57	13,713,850 BTC	$ 17,532,500
2	Ripple	$ 582,973,299	$ 0.018819	30,978,075,200 XRP *	$ 582,145
3	Litecoin	$ 61,428,208	$ 1.73	35,502,504 LTC	$ 2,578,080

- 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 http://en.wikipedia.org/wiki/Gossip_protocol

[redacted]

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

- Transactions are sent to public key



d39b0c4653b982e9aee616003db410e75868f61054656e044f0cdedbb6e77342 2015-01-13 16:23:53

1G5kvbP33mMwgtSTHpwAJe86xWKBwUHSV4
1HKBEEHryiuBd8Fp9Skhui6YGnLYNB3hQZ
1pob2EUuE1r7PjpMceubopkSWnrkSivY5

→

1JqFCQNCJr16rb4h3J2SvDg5ic5UejEPwi 2.103973 BTC
14DaDziYJCD4h8GQ3nbh8bx244Fc9Fc13J 0.01000001 BTC

2.11397301 BTC

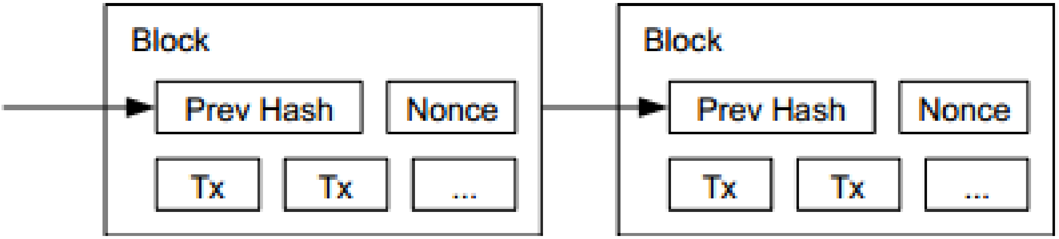
[redacted]unts

- 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

- Every *viable* transaction is stored in a public ledger
- Transactions are placed in blocks, which are linked by SHA256 hashes.
- https://blockchain.info



[redacted] – Video

- http://www.bitcoinmining.com

What is Bitcoin Mining?

- “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!

[redacted] coins

In addition to mining bitcoins, they can be acquired from a

bitpay

coinbase

BTC e

BITTREX

[redacted]

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

TRUSTED BY OVER 44,000 BUSINESSES AND ORGANIZATIONS

[redacted]

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

- 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/

?