Bitcoin Fundamentals

Bob Cowles

CERN Academic Lecture Series
December 3, 2014
What is value?

What is “value”
   Effort to obtain?
   Demand?

How do you pay your taxes? Rent or mortgage?

What is the value of three sheep in two months?
Blockchain Basics

- Public transaction ledger
- All transactions available for inspection
- Pseudonymous
  - Anonymity is difficult
  - Determining identity may be difficult (skill based)
- “Mining” to prevent double-spend
Blockchain – Disruptive Technology

- History – Like archeology
- Altcoins
  - See [http://altcoins.com](http://altcoins.com) for a list of alternative digital coins
- Kickstarter alternative
- Music
  - [http://peertracks.com/](http://peertracks.com/) – funding about to end as I speak
- Replace stock exchanges – ref. Overstock.com
  - Become like a company – sell shares in yourself
- DNS – namecoin
Blockchain Characteristics

A ledger of all transactions from the “start of time”
The content of a transaction is not specified

Transactions are grouped into blocks
The first block is the “genesis block”
New blocks are added based on consensus
Each block points to the previous block forming a chain

Sometimes there is a fork in the chain
Resolved by picking the longest fork

The objective is to prevent “double-spending” by consensus

https://en.bitcoin.it/wiki/Double-spending
Bitcoin Blockchain Size and Growth

The full chain is currently about 25 GB
It has doubled in size in the last year
Bitcoin Blockchain Characteristics

Blocks are “mined” and added to the chain based upon verified “proof-of-work”

Bitcoin miners assemble a block of transactions and then attempt to solve a problem

Average time to add a new block is 10 minutes
Current parameters limit transaction rate to ~7/sec
Average actual transaction rate is ~1/sec [late 2014]

A full bitcoin network node uses significant storage (currently >25GB) and is beyond the capability of most mobile devices.
Bitcoin Daily Transactions – 7 day average
Bitcoin – Nov/Dec 2013 Price Bubble

- China discovers Bitcoin
- China restricts Bitcoin
- China further restricts Bitcoin plus Mt Gox shutdown
Proof of Work

The amount of work required changes dynamically to keep the block mine rate at approximate 1/10 minutes.

The problem: find a number (nonce) so that the cryptographic hash of the block and the nonce starts with some required number of binary zeros (currently >40).

One the problem is solved, the new block is transmitted to all others in the bitcoin network and the miners start on a new block.

The reward for being the first to solve the problem is 25 bitcoins, plus any transaction fees.
Proof of Work Issues

Rather than distributed mining, there a few large pools accounting for over 75% of the activity. See [Comparison of mining pools](https://en.bitcoin.it/wiki/Comparison_of_mining_pools).

One pool exceeded 50% at one point (GHash.IO) – very dangerous for integrity of the blockchain. See [Ghash.io](https://en.wikipedia.org/wiki/Ghash.io).

The rate (7 transactions/second) is too low to support a significant increase in use of the bitcoin blockchain.

The reward barely pays for the hardware and the energy to mine.

The increase in “value” for mining is paid out to external entities for hardware and energy.

Numerous strategies to mitigate these issues are being developed. See [live demo](https://blockchain.info/).
Wallets – Client interface to digital coin networks

**Coinbase** is popular with reasonable interface; cross platform and mobile; includes multisig capability. Currently in 19 countries.
https://www.coinbase.com/

**Multibit** is a well regarded cross platform desktop wallet
https://multibit.org/

**Armory** is considered most secure cross platform software wallet
https://bitcoinarmory.com/

Hardware wallets are available, one is **Trezor**
https://www.bitcointrezor.com/

For information about exchanges in your country see:
http://howtobuybitcoins.info/
Wallet Setup

Connect to bank account – verification takes several days

Buy bitcoin – from bank takes several days; or use credit card for immediate gratification

Configure a wallet for small amounts and quick access
Configure a vault for delayed access plus multisig

Configure backup
Wallet – Multisig

Most common is 2 of 3

Allows sharing one key

Maintains owner control

Wallet addresses start with 3

Not supported by all software

https://support.coinbase.com/customer/portal/articles/1743782-what-is-the-multisig-vault-
Wallet – Best Practices Summary

Distribute holdings between various wallets
Use a variety – desktop, mobile, offline
Prefer multisig wallets where possible
Make regular backups
Use wallet encryption
Use good passphrases
Keep software up-to-date (security fixes)

Wallet – Transactions – in person

Like cash

Easy to send or receive small amounts

No recharge

Payment Flow

https://www.coinbase.com/docs/merchant_tools/point_of_sale
Wallet – Transactions – other

Flexible – can also use email and SMS

Useful for micropayments – e.g. 10 cents for listening to a song or viewing a video or reading a blog

Simple plug-ins to add Contribute or Donate buttons to web pages

All funds sent are received (possibly minus a small fee to the miner)

Wallets consolidate small amounts and include “change back”
Wallets – Addresses

Wallet address is public for receiving payments – identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3.

The public address is not tied directly to your identity, only to your wallet.

Different address used for each transaction

Sample address: 1J98t1WpEZ73CNnQviecrnyiWrmqRhWNLY

Not anonymous – can tie back to IP address

http://www.theregister.co.uk/2014/11/27/bitcoin_laid_bare_boffinsBeat_anonymity/
Alternatives

Proof of …

Work, Burn, Ownership, Stake, …

Sidechains – allow sending Bitcoins to other blockchains
https://gendal.wordpress.com/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/

Ethereum – extend scripting language to be turing complete
https://github.com/ethereum/wiki/wiki/White-Paper

Altcoins (referenced earlier)
Proof of Stake

Difficulty of producing a block proportional to ownership

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

Many variations

- Peercoin – hybrid – mining difficulty proportional to stake
  Takes an hour to be secure
- Nxt – shareholder to produce block determined by stake
  10 blocks for security but level of security not clear
- TaPoS – every transaction has hash of previous block
  No clear way to decide who generates next block
Delegated Proof of Stake

Shareholders delegate voting power

- Every transaction transfers votes from one delegate to another.
- Votes can be *for* or *against*
- No delegate is allowed more than 2% of the votes

Top n delegates take turns generating a block

- All delegates receive equal share of avg transaction fee
- Since order of delegates is known, direct network connections can reduce network latency issues

Consensus algorithm like Ripple, but delegates are voted in/out and incentivized for good behavior
BitShares

“Decentralized Autonomous Company” (DAC)

Distributed, self-organizing, self-enforcing “company”
Re-imagine Bitcoins as “shares” in the Bitcoin company

BitShares toolkit simplifies creation of a DAC

Open source software
Sell shares in an idea …. Or even yourself
Buy stock in songs, or musicians
No need for a stock exchange

As of Nov 5, 2014, “BitShares is a manned community supporting an unmanned company that produces innovative currencies.” (BTS)
BitAssets

Derivative on an asset (USD, EUR, CHF, Gold, Bitcoin, etc.)
  E. g. BitUSD, BitBTC, BitAPPL
  http://wiki.bitshares.org/index.php/BitShares/bitAssets

BitShares necessary to participate
  Give up BitShares to go long
  Pledge 2x BitShares as collateral to short

Pay dividends – important for “savers”
  Portion of transaction fees
  Shorts give up interest – redistributed to longs
  Dividends on short squeeze

Track real world asset – important for “speculators”

More about how it works – “Bookie Bob”
  http://bitshares.org/bookie-bobs-solution-to-bitcoin-volatility/
Some Charts From Friday, Nov. 28, 2014 – bter.com

**Bitcoin BTC / USD**

**BitUSD BITUSD / USD**
And Finally …

Many online references – and many flavors of digital currencies and DACs or DAOs – use your favorite search engine

This is a disruptive technology – there are many powerful institutions threatened by the possibilities not only of digital currencies but of direct, consensus-based transfer of value

Expect intense lobbying efforts to have governments cripple various capabilities

Explore … but explore carefully!