What is Bitcoin?

“Consensus technology has the power to do for economics what the internet did for information” - Dan Larimer

Ross Rydman – 2014

For Academic Use Only

The 30 second description…

Bitcoin is the currency of the Internet: a distributed, worldwide, decentralized digital money.

Unlike traditional currencies such as dollars, bitcoins are issued and managed without any central authority: there is no government, company, or bank in charge of Bitcoin. There is no one you need to trust.

As such, it is more resistant to wild inflation and corrupt banks. With Bitcoin, you can be your own bank.

The word Bitcoin means many things…

- Bitcoin the Protocol
  - The invention of bitcoin – a solution to Double spending/Byzantine Generals Problem
  - Analogous to HTTP or TCP/IP – A foundation/protocol to build applications on top of

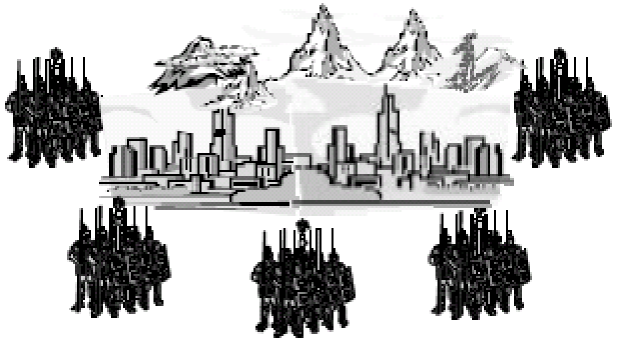
- Bitcoin the Currency
  - The first application of the bitcoin protocol
  - Analogous to Email or SMS

- Bitcoin the Monetary Unit
  - A unit of measure for the Bitcoin Currency
  - Analogous to “one dollar” or “one euro”

This distinction is important…

- No question that Email has changed the way people communicate
- However email’s impact on communication is miniscule compared to the impact of the underlying technology: The Internet
- When the Internet was gaining traction in the early 90’s it faced many critics
    - Ex: “It will never be more then a fancy computerized library”
- Very few saw the potential in what the Internet would become
    - Facebook, Skype, Email, Videogames, News, Youtube, Netflix, Music, etc.
    - The applications built upon the technology are endless
    - The Internet has revolutionized communication, media, work, trade, leisure, etc.
- Now the Bitcoin protocol stands to do the same for “property”

Bitcoin the Protocol



- Decentralized
  - Solution to Byzantine Generals Problem
  - No central point of failure or control
  - Protocol changes must be adopted by majority of mining nodes
- Mesh network of Nodes
  - Broadcast and verify transactions
  - May function as miners or not – if miners they add transactions to blocks
- Blockchain
  - Public ledger of all transactions
  - Rolled into “blocks” and added to chain approx. every 10mins
- Proof of Work/Mining
  - Proof that a certain amount of work (hashing) was done
  - Guarantees through probability that next block found will be from a random node
- Public/Private Key Cryptology used for Addresses
  - Practically infinite number of addresses can be “generated” at any time by anyone
  - Public key becomes your “address” to receive bitcoin to
  - Private key is needed to unlock access to bitcoins sent to the public key – Private key verifies that you hold the permission to transact with those bitcoins – Transactions are signed with private key
  - A “Bitcoin Wallet” is just a database of Public Key/Private Key pairs you possess

The word Bitcoin means many things…

- Bitcoin the Protocol
    - The invention of bitcoin – a solution to Double pending/Byzantine Generals Problem
    - Analogous to HTTP or TCP/IP – A foundation to build applications on top of
- Bitcoin the Currency
    - The first application of the bitcoin protocol
    - Analogous to Email or SMS
- Bitcoin the Monetary Unit
    - A unit of measure for the Bitcoin Currency
    - Analogous to “one dollar” or “one euro”

Bitcoin the Currency

- Fulfills all the traditional requirements to be a currency/money
  - Divisible – One bitcoin = 100,000,000 satoshi
  - Fungible – Each bitcoin is exactly the same as each other bitcoin
  - Store of Value – Limited and finite supply
  - Medium of Exchange – Accepted as barter medium between sellers
  - Unit of Account – Countable and Verifiable
- First truly global currency ever created
  - No single entity claims rights over it nor controls it
  - Can transact across borders with zero restrictions
- Will always exist
  - Like any other mesh network, bitcoin only needs two nodes to function
  - As long as two or more people use bitcoin it will still exist
  - Critical mass is needed for adoption to be widespread but not for it to be consider successful or useful – even if only two people used bitcoin, they could find it useful

The word Bitcoin means many things…

- Bitcoin the Protocol
  - The invention of bitcoin – a solution to Double pending/Byzantine Generals Problem
  - Analogous to HTTP or TCP/IP – A foundation to build applications on top of

- Bitcoin the Currency
  - The first application of the bitcoin protocol
  - Analogous to Email or SMS

- Bitcoin the Monetary Unit
  - A unit of measure for the Bitcoin Currency
  - Analogous to “one dollar” or “one euro”

Bitcoin the Monetary Unit

- Bitcoin network represents bitcoin units as integers (whole numbers)
  - Therefore, “one bitcoin” is actually 100,000,000 units (aka Satoshis)
  - “one bitcoin” is then for practical purposes infinitely divisible
  - Decimal place is added to the user interface as a convenience but under the hood all transactions happen as integers
- 2012 World GDP: $72 trillion USD
  - 1/300th of total “satoshi” supply in Bitcoin
  - More then enough “units” to be used as only denominated currency Globally

Common Concerns with Bitcoin

- Privacy Concerns
  - Data mining treasure trove as it is used today
    - Sol: Coin mixing/Zerocoin
  - Node originating transaction has publically known IP Address
    - Sol: Tor/I2P
  - Traditional entry/exit points link addresses to people
    - Sol: Zero-knowledge proof systems to validate user identity
- Network Security and Robustness Concerns
  - 51% Attack -> Centralization of mining
    - Sol: Commodity mining hardware widely distributed
  - Node computing requirements grow rapidly with scale -> Centralization of nodes
    - Sol: Blockchain pruning, storage compression, SPR nodes
- User Security Concerns
  - Tons of examples of lost coins, stolen coins, hacked exchanges, etc.
    - Sol: user education of importance of “holding the keys” and using trust-less services
    - Multi-sig and Hardware wallets may hold key to user-friendly security

What’s the near future look like?

Bitcoin-like implementations can be created to solve many currently centralized systems

Problem	Timeframe/Solution
DNS (Domain Naming System)	Today: Namecoin
Stock Markets/Futures Markets/Forex Markets/etc.	Today: Bitshares X/Nxt/Mastercoin
Betting/Gaming	Months: Bitshares LKS
Decentralized Marketplace	Now: OpenBazaar
Multi-party Fulfillment Contracts (Smart Contracts)	Months: Bitcoin/Bitshares/Ethereum
Escrowed Transactions	Today: Bitcoin with m-of-n signatures transactions
Collateralized loans	Months: Bitshares/Nxt/Mastercoin
Micropayments/Tipping	Today: Bitcoin/Dogecoin/etc
Political voting	Months: Could verify identify via zero-knowledge proof
Web-of-Trust style Identity Service	Months: Keyhotee

What’s possible in the distant future?

Many manufactured things become Autonomous Agents (Cars, Roads, Lights, UAVs, etc)

- Each Agent has its own balance sheet
- Can operate or provide service to people or other agents for a profit
- Can pay for utilities or consumables from profits
- Can pay dividends to original creators from profits
- Can create child replicas from profit in order to scale with demand

- Ex: Autonomous Taxi Cab Service

Recommended Resources

- General Bitcoin Info – www.bitcoin.org
- Bitcoin News – www.coindesk.com
- Bitshares/Keyhotee information – www.invictus.io
- Bitcoin Price Charts – www.bitcoinwisdom.com
- Easiest way to buy Bitcoin in US – www.coinbase.com
- Sub-reddit - www.reddit.com/r/bitcoin

References

Some ideas, explanations, and graphics we're borrowed from the following:

- http://preshing.com/20140127/what-is-a-bitcoin-really/
- http://expectedpayoff.com/blog/2013/03/22/bitcoin-and-the-byzantine-generals-problem/
- http://en.wikipedia.org/wiki/Bitcoin