Overview of Bitcoin, Blockchain, and Cryptofinancial Technology

Ryan X. Charles Blockchain University Tokyo, Dec. 17, 2015



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

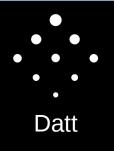


Outline

Who am I?
Bitcoin History & Technology
Altcoins & Other Blockchains
Non-Blockchains
Bitcoin Economy
Bitcoin Implementations



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



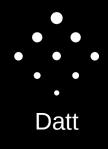
Who is Ryan X. Charles?

- Programming since age 10
- Web designer/developer, 1999 2005
- Physicist, 2005 2013
- Angry at govt/banks, 2008
- Discovered bitcoin, 2011
- Full-time bitcoin, 2013
- BitPay -> reddit -> BitGo -> Datt
- bitcore, Copay, fullnode, Datt



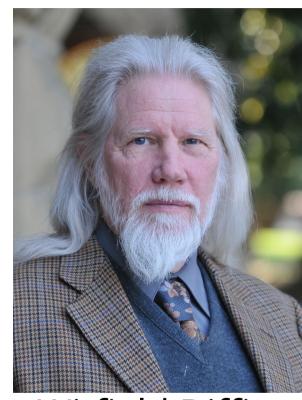


Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Crypto History of Bitcoin

- Public Key Cryptography, 1976 (Diffie-Hellman)
- DigiCash, 1990 1998
- Hashcash, Adam Back, 1997
- b-money, Wei Dai 1998
- Bit Gold, Nick Szabo, 2005? 2008?
- Bitcoin Whitepaper, 2008
- Bitcoin Genesis Block, 2009



Witfield Diffie



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Money History of Bitcoin

- Pre-gold*, ~100,000 BC Today
- Gold*, ~5000 BC
- Fractional Reserve Banking*, ~1000 AD
- Classical Gold Standard, 1870 ~1915
- Bretton Woods, 1944 1971
- Bitcoin, 2009



* Caveat: Rough estimate



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Rai Stones: Physical Bitcoin

- Quarried in Micronesia & Guam
- Used as money on Yap
- Stones do not move rely on oral history to track ownership
- Really difficult to make new ones can't just print them (without modern tech)
- Just like bitcoin: value comes from proofof-work, history of ownership is shared information



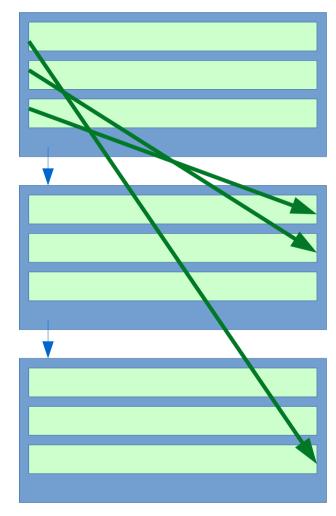


Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin Blockchain Overview

- Blocks contain transactions and a proof-of-work hash
- Each block links to previous block
- Each transaction links to outputs of earlier transactions



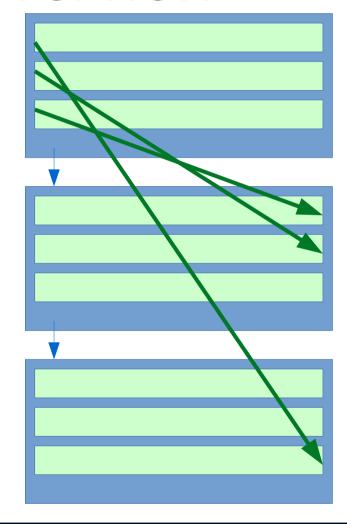


Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin Blockchain Overview

- Genesis Block:
 - The First Block
- Coinbase Transaction:
 - First transaction in a block
 - Mining reward
 - Has "null" inputs





Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin Blockchain Overview

Each block has:

- Proof-of-Work Hash (PoW)
- Nonce
- Meta data and transactions

Example PoW with data "test data"

- Nonce: 0, Hash: df59bb7272f144dc7d3620e6f9e14234
- Nonce: 1, Hash: 460142d2a0349c13a48b422261d708eb
- Nonce: 2, Hash: 71be158053f58c9e1f094fb3f7da282e
- •
- Nonce: 146, Hash: 00f82186722b46b2adb57f321793e44f



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin Blockchain Summary

- Transactions are digitally signed (public key cryptography).
 - Cannot fake a transaction must have private key to produce valid signature
- Hash functions used for proof-of-work on each block.
- "Encryption" has nothing to do with it just digital signatures and hash functions.
- Transactions grouped in blocks, one big chain back to the genesis block.
- Each transaction links to earlier transaction(s) back to Coinbase transaction(s).



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

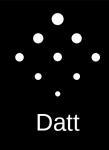


Important Concepts

- Bitcoins are mined. 50 new bitcoins per block for first four years,
 25 per block for next four years, etc. Total of 21 million.
- Miners perform proof-of-work hashing. CPUs → Graphics cards
 → FPGAs → ASICs.
- "full node" a fully-validating node. "light node", or "SPV" only validates block headers.
- **Bitcoin has no central authority.** The only way to change the rules is to change the software the miners, full nodes, and wallets run. Democratic by CPU power and economic power.
- Do you control your private keys?



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



The Creator: Satoshi Nakamoto

- Active on cryptography mailing list 2008
- Active on bitcoin forum 2009 2010
- Last known message late 2010
- Writings recorded at:
 - http://nakamotoinstitute.org/
- Highly recommended to read his writings!



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Byzantine Consensus

- Byzantine Generals Problem a well-known computer science problem.
- If generals want to attack a city, when no one is in charge, how do they arrive at consensus about what particular time to attack?
- Bitcoin is a solution to this problem (use proofof-work on times – most proof-of-work wins)
 https://bitcointalk.org/oldSiteFiles/byzantine.html



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



"The Blockchain"

- "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf
- The word "blockchain" does not appear in whitepaper or original source code. ("block chain", two separate words, does appear in original source code, but not whitepaper)
- "Blockchains," distributed consensus of transactions grouped into blocks, have become popular for reasons other than money, particularly other financial services & identity.
- Bitcoin was invented for one purpose: decentralized electronic cash. Other uses of blockchain are nice bonus.



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Altcoins

(The First Non-Bitcoin Blockchains)

- First appeared ~2012.
- Litecoin first popular altcoin.
- Dogecoin second popular altcoin.
- Almost all are forks of bitcoin, or a fork of a fork. Some, like NXT, are complete rewrites.
- Most do not have novel features.
 Some do.
- Bitcoin market cap: ~\$6.5 billion
- All alts put together: < \$1 billion





Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Alternative Uses of Blockchain (besides money)

- Stocks, bonds, fiat currencies, commodities decentralized ownership, but centralized backing
- Identity, names, rotating keys, revoking keys
- Smart contracts (money or other assets change hands according to complex conditions executed automatically)
- Smart property & Internet of Things (property perform actions, can be owned by cryptographically)
- Proof-of-existence, patents, trademarks, copyright
- DACs and DAOs (distributed autonomous corporations & organizations)
- If it involves distributed consensus, consider blockchain



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Permissioned Blockchains

- Bitcoin is **permissionless**. Anyone can use it. Anyone can mine it. No one owns it. (Although some actors have more power than others more bitcoin, more hash power, commit access, etc.)
- Banks are creating **permissioned** blockchains. Based on the same principles, but not open to the public. They are owned by the banks.
- Exploring monetary and non-monetary uses of blockchain technology.
- R3: http://www.coindesk.com/bitcoin-headlines-r3-blockchain-dream-team/



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Blockchains in a Box

- OpenChain easily produce a blockchain that is optionally attached to bitcoin https://www.openchain.org/
- MultiChain easily produce a blockchain with custom features as a fork of Bitcoin Core http://www.multichain.com/
- Can be permissionless (open, anyone can use) or permissioned (closed, only used by select parties)



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Blockchains in a Box

- OpenChain easily produce a blockchain that is optionally attached to bitcoin https://www.openchain.org/
- MultiChain easily produce a blockchain with custom features as a fork of Bitcoin Core http://www.multichain.com/
- Can be permissionless (open, anyone can use) or permissioned (closed, only used by select parties)



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Ethereum

- Bitcoin script is not Turing complete (there are some programs that cannot be written with it)
- Ethereum script is Turing complete can program any conceivable contract
- Bitcoin is designed to solve the problem of digital cash.
 Ethereum is designed to solve everything else.
- Bitcoin infrastructure better developed (companies, software, capital), but Ethereum potentially more useful
- See Gav Wood's recent article, "So Ethereum is released."
 https://medium.com/@gavofyork/so-ethereum-is-released-4291da4

 6b770



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Non-Blockchains

- Ripple a distributed ledger, based on similar cryptography to bitcoin, but NOT proof-of-work or proofof-stake
- Stellar a fork of Ripple
- Both of them can track arbitrary assets and rely on third parties to exchange for "real" assets, e.g. withdrawing dollars or bitcoin
- Fall under "cryptofinance" category, but they DO NOT have blockchains!



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



A Note on Security

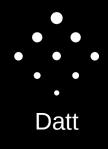
- Bitcoin miners are the world's most powerful supercomputer.
 (5 billion teraflops vs. 54 thousand teraflops*)
- Reversing bitcoin transactions requires having an enormous amount of computing power, only achievable by a State actor.
- Reversing a small, private blockchain requires far less computing power and is achievable by small actors. Beware.

* Conversion info: https://www.quora.com/How-to-convert-mflop-s-to-mhash-s ... I calculated assuming 700 million Ghash/s current hash rate, and 700 Mhash/s to 5340 Gflop/s

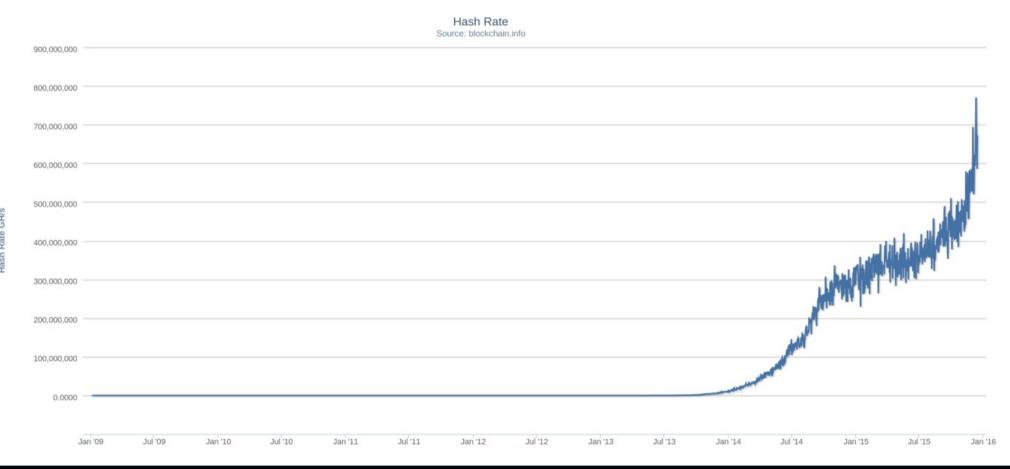
Current top super computers: http://www.top500.org/lists/2015/06/



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin's All-Time Hash Rate





Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Colored Coins

- Put meta data on bitcoin transactions to track assets (stock, bonds, whatever) on the bitcoin blockchain.
- Protocols: Open Assets, CoinSpark, Chromaway, Colu, others.
- Upside: Security of bitcoin.
- Downside: Limited block size and thus transaction count. Rules are not enforced by miners.



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Two-Way Pegged Sidechains

- Invented by Blockstream, theoretically allows transfer of bitcoin to other blockchains by "pegging" - proofof-peg lets you spend bitcoin on the sidechain, proofof-unpeg lets you retrieve bitcoin back on normal chain
- Upside: Security of bitcoin, network effect of bitcoin, unlimited advanced uses of blockchain.
- Downside: Not yet implemented.



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Technology Summary

- Bitcoin
- Altcoins
- Ethereum
- Non-Blockchain (Ripple, Stellar)
- Permissioned Blockchains (banks)
- Bitcoin-dependent: Colored Coins; Sidechains
- ...hard to beat bitcoin's security and network effect



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Bitcoin Economy

- Wallets
- Exchanges
- APIs and Developer Tools
- Payment Gateways
- Miners
- Storage
- Merchants
- Investment
- Non-Monetary Advanced Uses
- Financial Services



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Miners



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Wallets

WALLETS

"At Coinbase, we're excited about the progress made thus far but we're still in the early days of the technology and even more excited about the app ecosystem and what the future of Bitcoin applications will look like."

Adam White VP of Business Development, Coinbase



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Storage

STORAGE

"Bitcoin paved the way to decentralized security, and will jumpstart the usage of personal privacy devices."

> Eric Larchevêque CEO, Ledger

"Today there are more than 100,000
Bitcoin transactions per day for more
than \$100 million and there are more
than 5,000 servers acting as nodes of
the network: Bitcoin is a lot less likely to
disappear today than it was 2 years ago
when the price was over \$1,000 per
Bitcoin."



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles





Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Payment Processors



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Merchants



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Investment



INVESTMENT
Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Media & Advocacy



"We are privileged to be at the nexus where information meets technology, using a multimedia platform to support the adoption and innovation of Bitcoin and the blockchain. In only two years, the audience for digital currency news has exploded from Fintech specialists to the man on the street. This is now a mainstream media topic, and what happens in Bitcoin happens to the world."

David Bailey CEO, BTC Media



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Advanced Uses of Blockchain



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Financial Services



Graphics by BitPay, Bitcoin Magazine & Josh Dykgraaf



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles



Implementations of Bitcoin

- Bitcoin Core Original C++ implementation, maintained by "Core" developers
- BitcoinJ The first re-implementation
- Btcd A full implementation in Go
- bitcore, bitcoinjs, fullnode Javascript & Node.js
- rust-bitcoin Rust
- python-bitcoinlib, caesure Python



Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

