Bitcoin: Learning in a contentious environment

Mark Nesbitt
Denver Crypto Group
11/29/2017

Summary

- Why should traders care how crypto works?
- Avoiding pitfalls when learning
- Learning resources

Why should traders care how crypto works?

Mark Nesbitt
Denver Crypto Group
11/29/2017

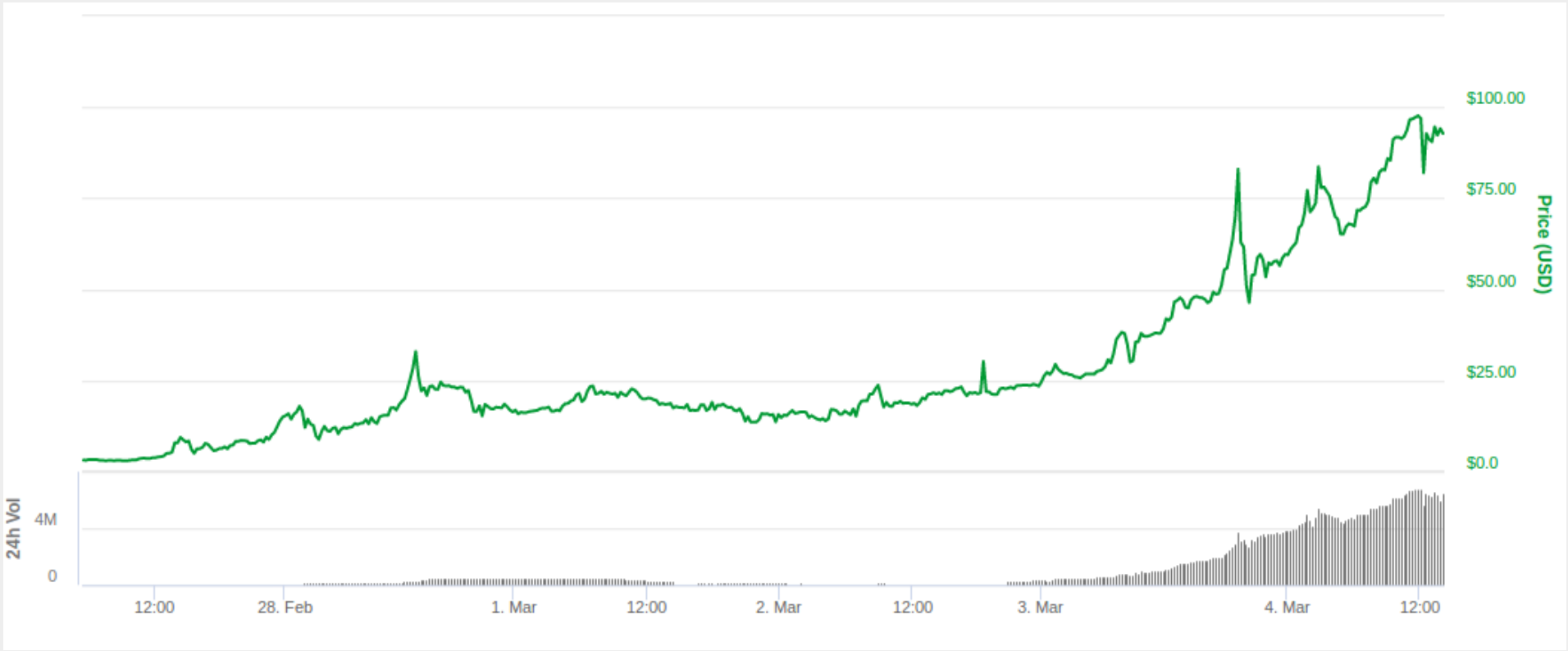
Why should traders care about the underlying protocol?

- Don’t trade tulips

Why should traders care about the underlying protocol?

- Don’t trade tulips
- Auroracoin

Auroracoin



Mark Nesbitt
Denver Crypto Group
11/29/2017

Auroracoin

Mark Nesbitt
Denver Crypto Group
11/29/2017

Auroracoin

Mark Nesbitt
Denver Crypto Group
11/29/2017

Auroracoin

Mark Nesbitt
Denver Crypto Group
11/29/2017

Why should traders care about the underlying protocol?

- Don’t trade tulips
- Auroracoin
- Bitcoin Cash recent price movement

Bitcoin Cash: Big blocker exodus after Segwit 2x called off?

Mark Nesbitt
Denver Crypto Group
11/29/2017

Bitcoin Cash: Subsequent price action maintaining new price level

Mark Nesbitt
Denver Crypto Group
11/29/2017

Why should traders care about the underlying protocol?

- Don’t trade tulips
- Auroracoin
- Bitcoin Cash recent price movement

Understanding the technology will help you more intelligently deploy your assets

Avoiding pitfalls when learning

Mark Nesbitt
Denver Crypto Group
11/29/2017

Avoiding pitfalls when learning

- The current environment is highly divided with many different opinions
- Much of what you hear will be wrong or agenda-driven interpretations
- How do you come to an opinion on common claims that you hear?
  - “Transaction fees are too high and are strangling bitcoin”
  - “Miners have too much power”
  - “Blocks are too small”
  - “The network is at risk of centralization”

Seek facts, not narratives

Mark Nesbitt
Denver Crypto Group
11/29/2017

Think independently

Mark Nesbitt
Denver Crypto Group
11/29/2017

Avoiding pitfalls example

- Why shouldn’t I store my coins on an exchange?

Avoiding pitfalls example

- Why shouldn’t I store my coins on an exchange?
  - “Because you should control your own money!”
  - “Because exchanges can’t be trusted!”
  - “Because the whole point is to ditch banks!”

Avoiding pitfalls example

- Why shouldn't I store my coins on an exchange?
  - ~~"Because you should control your own money!"~~
  - ~~"Because exchanges can't be trusted!"~~
  - ~~"Because the whole point is to ditch banks!"~~
  - Whoever has the private keys controls the coins
  - There are numerous examples of exchanges losing or stealing millions in crypto

Avoiding pitfalls summary

- Seek facts not narratives → Be willing to change your mind
- Think independently → Seek out people who disagree with you

Learning Resources

Mark Nesbitt
Denver Crypto Group
11/29/2017

Brief Bitcoin overview

- Bitcoin as a protocol: computers exchanging properly formatted information
- Transactions: confirmed vs. unconfirmed
- Nodes: mining vs. non-mining
- A transaction is confirmed when a mining node includes a transaction in a block
- The collection of all sequential blocks is the blockchain
- Consensus is key
  - Network participants need to be in agreement on the state of the network. (e.g. which blocks are valid, what constitutes a valid transaction, what is the latest block)
  - Any node or group of nodes that deviates from this consensus “forks” onto a different blockchain

Running a node

- Anyone can download the software and run a node
  - Miners must have a copy of the blockchain and be connected to the network to produce and disseminate valid blocks
  - Users can do this to validate transactions. This may be very important for certain businesses or individuals that engage in large and/or frequent transactions
  - Learners should do this as it is a great way to learn about the network
  - Hot topic: Do non-mining nodes help support the network? To what degree do non-mining nodes influence network consensus?
- https://bitcoin.org/en/download
  - Use an old computer, download and run the software
  - NB: This is not mining

Blockchain.info

- *Block explorer* service with charts and data about the network
- Nearly all data is pulled from nodes
  - Blockchain status (shows node is up to date. Consensus!)
  - Tie out older block data to the node
  - Show charts
- “Segwit transactions are allowing for increased capacity”
  - Segwit.party

Mempool statistics

- Blockchain.info mempool data
  - Confirm against node
- https://jochen-hoenicke.de/queue/#24h
  - Confirm against node
- “There is a spam attack going on”

Fork and hashpower information

- https://fork.lol/pow/hashrate
- The mining algorithm for Bitcoin and Bitcoin Cash are the same, allowing miners to quickly move between mining one coin or the other
- “Hashpower follows price”

Resource list: Reading/Research

- Original Bitcoin whitepaper (https://bitcoin.org/bitcoin.pdf)
- Mastering Bitcoin (ISBN 978-1491954386)
- Andreas Antonopolous youtube channel (youtube.com/user/aantonop)
- Emin Gun Sirer blog (http://hackingdistributed.com/)
- https://www.mycryptopedia.com/cryptocurrencies/
- http://www.openbitcoinprivacyproject.org/
- https://oxt.me/history
- Small block perspective: https://www.youtube.com/watch?v=cZp7UGgBR0I
- Large block perspective: https://www.bitcoin.com/info/bitcoin-cash-is-bitcoin
- Reddit:
  - /r/bitcoinbeginners
  - /r/bitcoin and /r/btc. These two communities have very different perspectives and I recommend that you read both. This speaks to my principles from before-- don't fall into a camp, seek people who disagree with you.

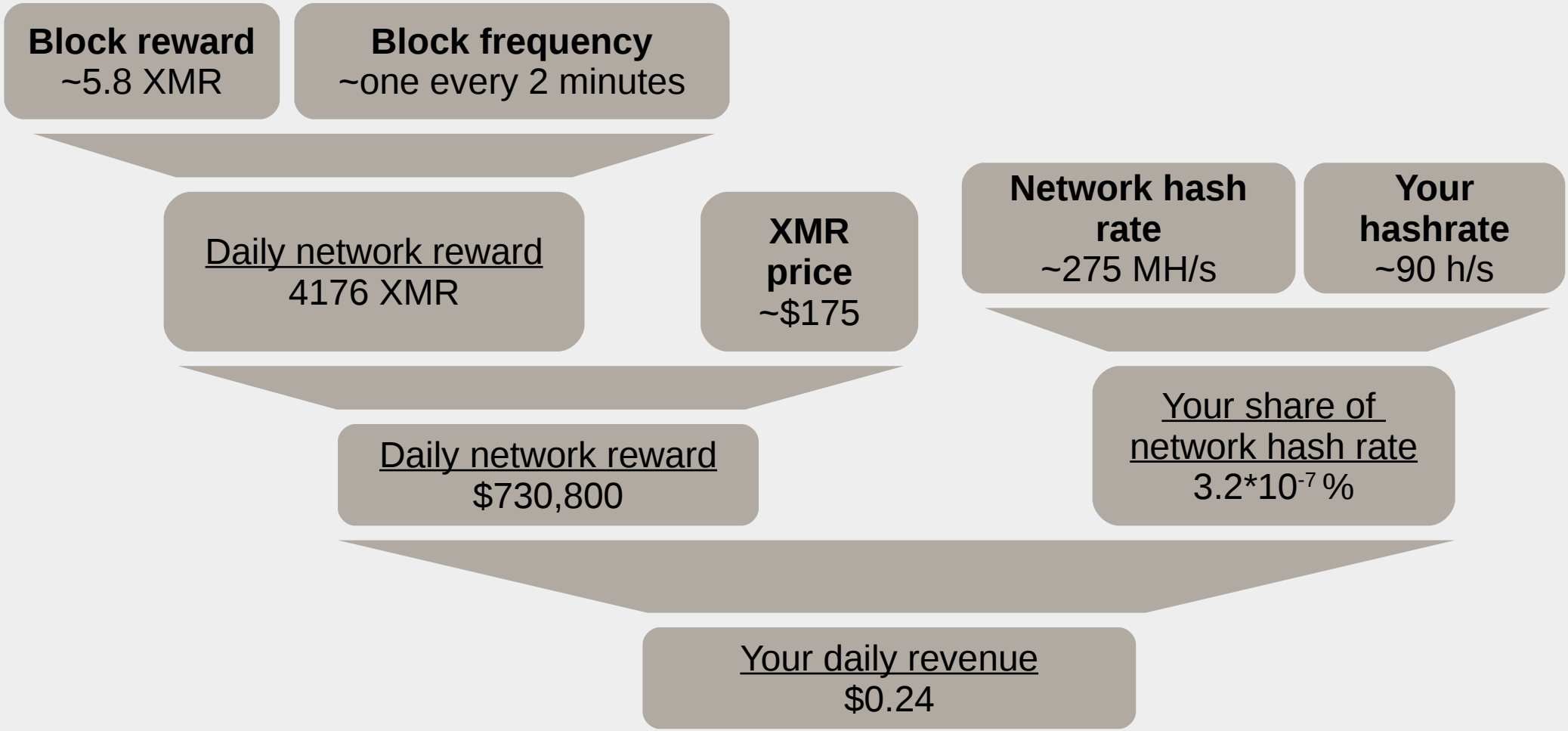
Note: There are many, many resources online. These are a select few that I've found helpful in the past. Google is your friend.

Resource list: Data/Charts

- Coin.dance
- Nodecounter.com
- Bitcoinity.org
- Tradeblock.com/markets
- Blocktrail.com/btc
- Bitcoinwisdom.com
- Blockchair.com
- https://cryptothis.com/diff/

Note: There are many, many resources online. These are a select few that I've found helpful in the past. Google is your friend.

Exercise: How much can I make mining Monero?



Mark Nesbitt
Denver Crypto Group
11/29/2017

Exercise: How much can I make mining Monero?

Block reward
https://whattomine.com/coins/101-xmr-cryptonight

Block frequency
https://whattomine.com/coins/101-xmr-cryptonight

XMR price
https://coinmarketcap.com/currencies/monero/

Network hash rate
https://www.coinwarz.com/network-hashrate-charts/monero-network-hashrate-chart

Your hashrate
Must be measured by you on your hardware, but estimates exist
https://coinhive.com/#hash-rate

Mark Nesbitt
Denver Crypto Group
11/29/2017

Slides available on github

github.com/mwnesbitt/DenverCryptoGroup