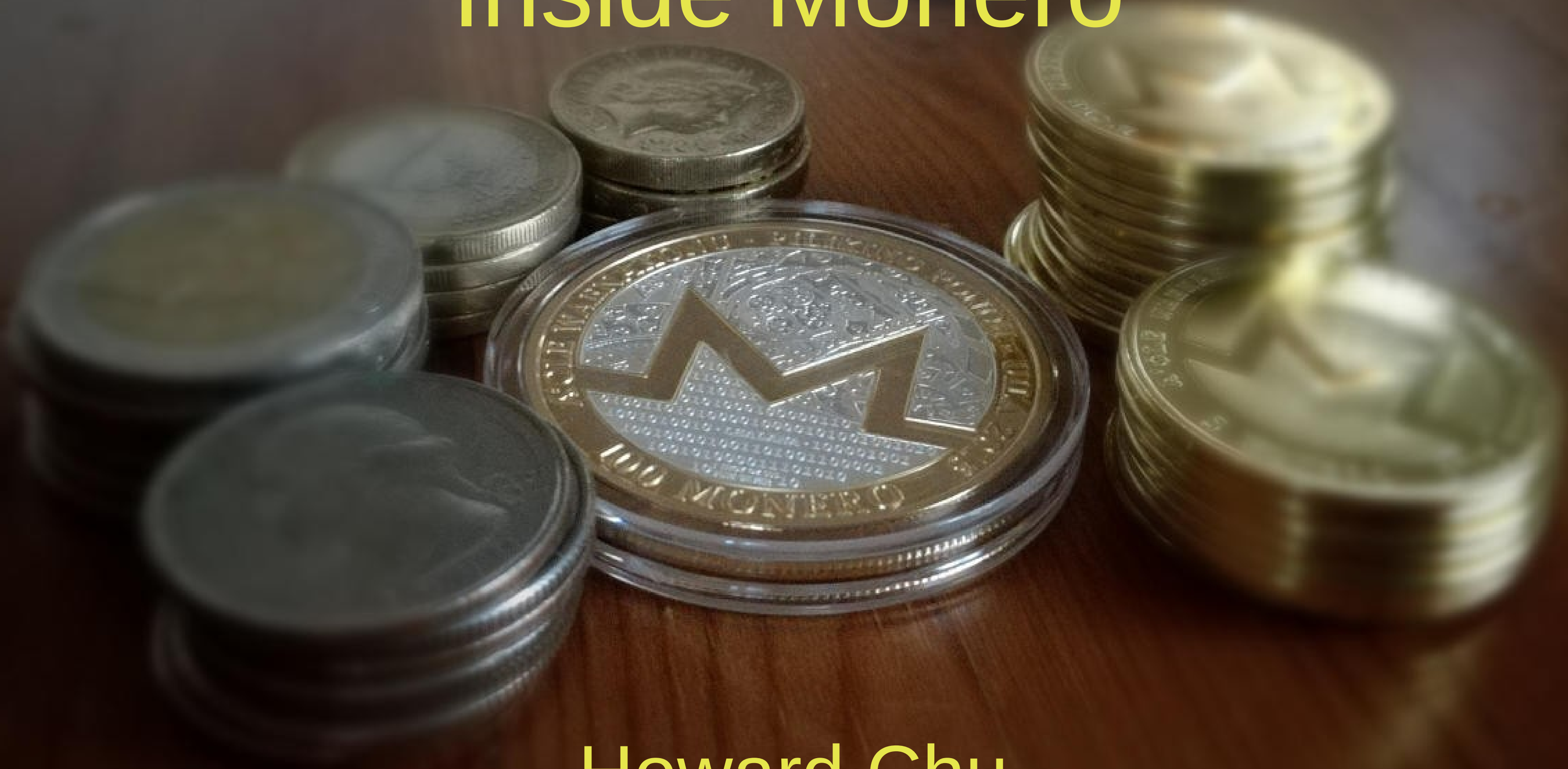
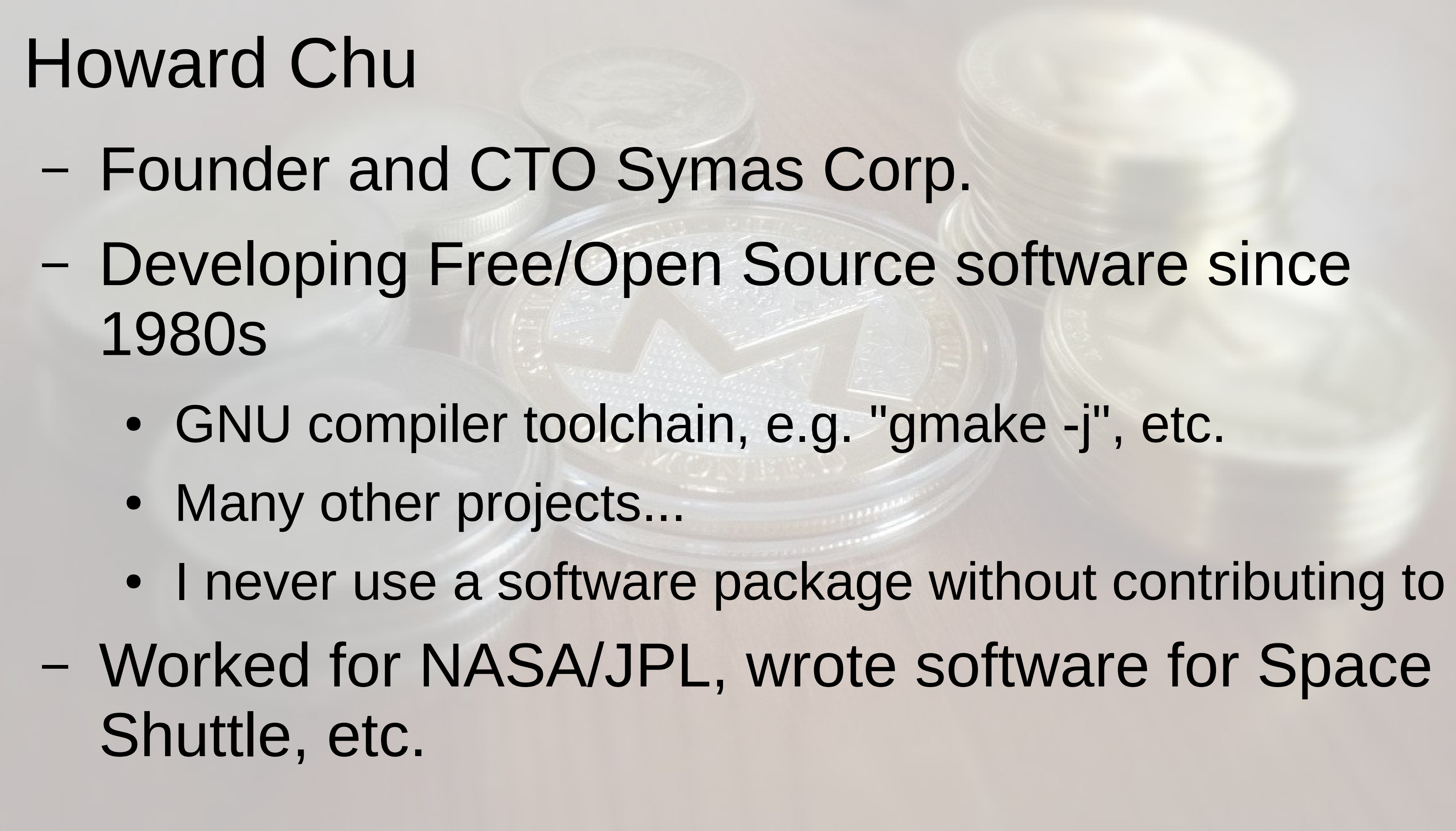
Inside Monero



Howard Chu
CTO, Symas Corp. hyc@symas.com

2018-02-04

Personal Intro



- Howard Chu
  - Founder and CTO Symas Corp.
  - Developing Free/Open Source software since 1980s
    - GNU compiler toolchain, e.g. "gmake -j", etc.
    - Many other projects...
    - I never use a software package without contributing to it
  - Worked for NASA/JPL, wrote software for Space Shuttle, etc.

Personal Intro

- Career Highlights
  - 2011- Author of LMDB, world's smallest, fastest, and most reliable embedded database engine
  - 1998- Main developer of OpenLDAP, world's most scalable distributed data store
  - 1995 Author of PC-Enterprise/Mac, world's fastest AppleTalk stack and Appleshare file server
  - 1993 Author of faster-than-realtime speech recognition using Motorola 68030
  - 1991 Inventor of parallel make support in GNU make

Personal Intro

- Security-related Highlights
  - 2015- Contributor to Monero
  - 2010- Maintainer of RTMPdump, reverse-engineering Adobe Flash encryption
  - 1996- Contributor to OpenSSL, including multi-precision math functions for Motorola 68020
  - 1995- Contributor to Kerberos
  - 1994- Discovered weakness in Andrew File Server's password hashing scheme
  - 1991 Co-inventor of TCPwrappers, used to secure internet server connections on Unix

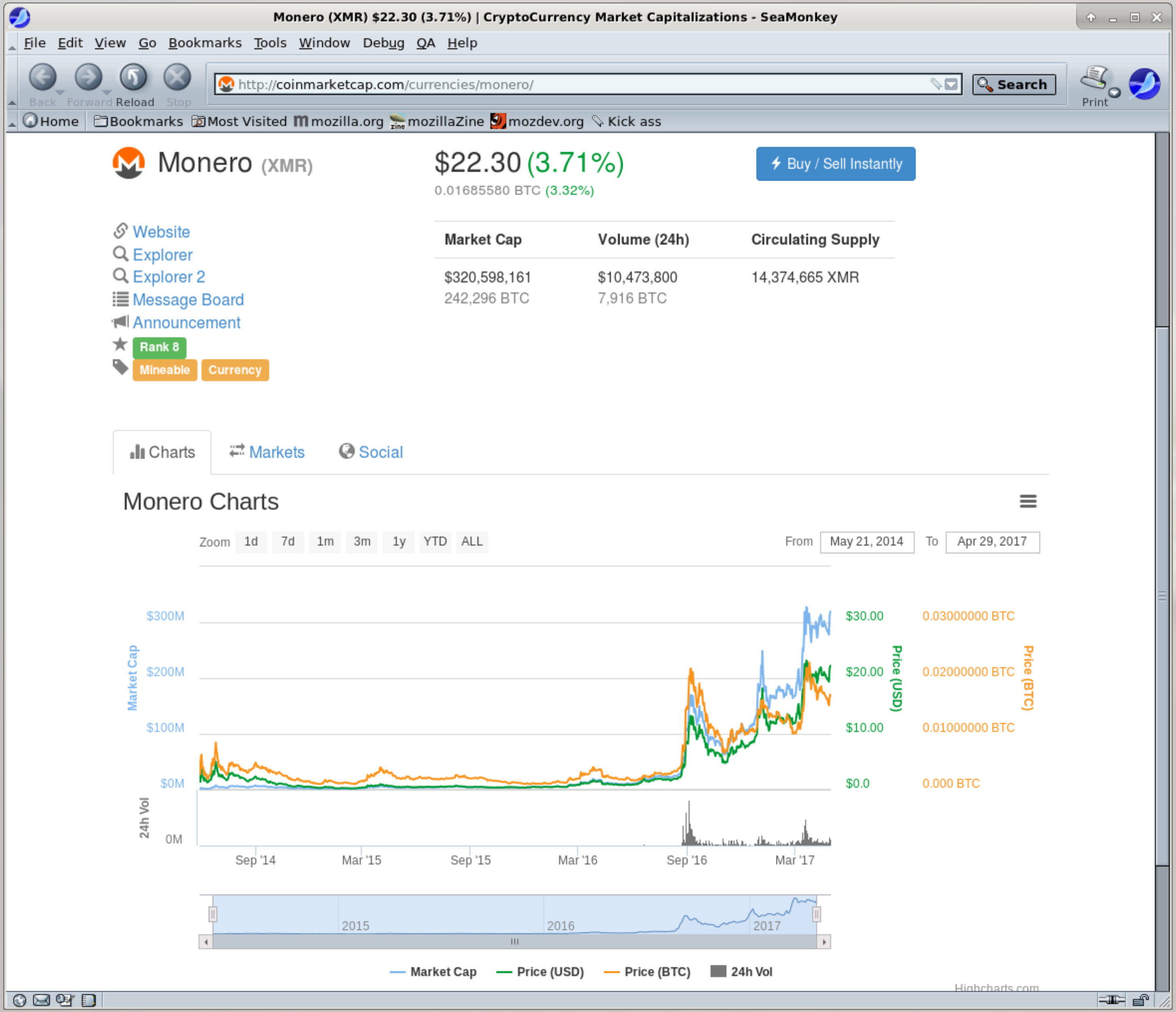
Topics

- What is Monero?
  - What is a cryptocurrency?
  - How does Monero work?

What is Monero

- A totally private cryptocurrency
  - Built on a public blockchain
  - But all transactions are completely opaque
- The name is the Esperanto word for "money"
- Started in 2014

What is Monero



Monero (XMR) $22.30 (3.71%) | CryptoCurrency Market Capitalizations - SeaMonkey

http://coinmarketcap.com/currencies/monero/

Monero (XMR)

$22.30 (3.71%)

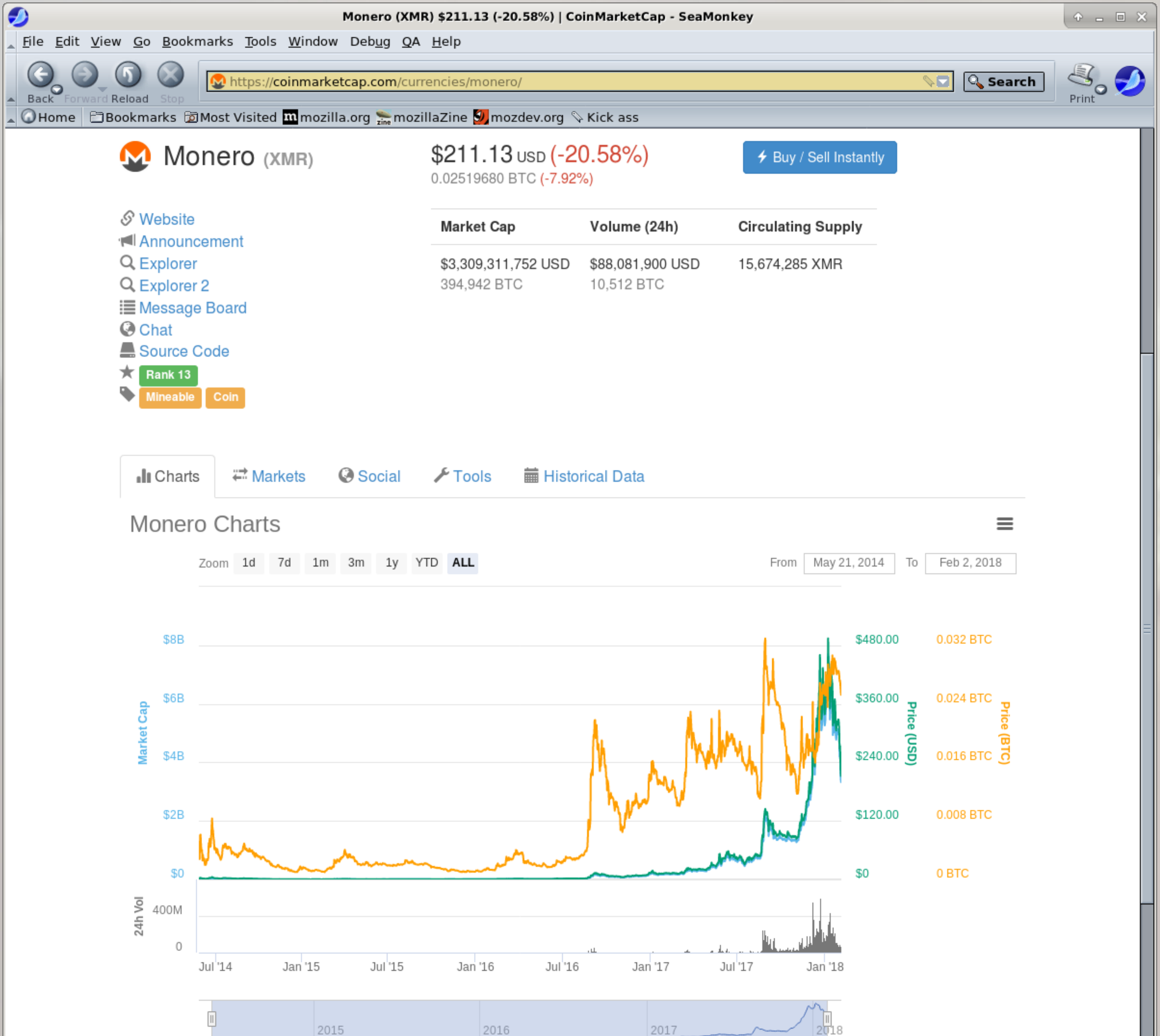
0.01685580 BTC (3.32%)

Market Cap	Volume (24h)	Circulating Supply
$320,598,161 242,296 BTC	$10,473,800 7,916 BTC	14,374,665 XMR

Monero Charts

From May 21, 2014 To Apr 29, 2017

What is Monero


Monero (XMR) $211.13 (-20.58%) | CoinMarketCap - SeaMonkey
File Edit View Go Bookmarks Tools Window Debug QA Help
Back Forward Reload Stop
https://coinmarketcap.com/currencies/monero/
Search
Print
Home Bookmarks Most Visited mozilla.org mozillaZine mozdev.org Kick ass

Monero (XMR)

$211.13 USD (-20.58%)
0.02519680 BTC (-7.92%)

- Website
- Announcement
- Explorer
- Explorer 2
- Message Board
- Chat
- Source Code
- Rank 13
- Mineable Coin

Market Cap	Volume (24h)	Circulating Supply
$3,309,311,752 USD 394,942 BTC	$88,081,900 USD 10,512 BTC	15,674,285 XMR

What is a Cryptocurrency

- "A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency." (Wikipedia)
  - Most cryptocurrencies in existence today are forks of Bitcoin, released in 2009
  - Cryptography is used to enforce "digital scarcity" and prevent forgery of assets using public key crypto and digital signatures
  - Transactions are stored in a blockchain, a public distributed ledger

What is a Blockchain

- Essentially, a distributed database using group commit
  - Transactions are grouped into "blocks" and committed together
  - Typically high commit latency, usually timed on the order of minutes
    - E.g., Bitcoin uses 10 minute block times
    - Monero uses 2 minute block times
  - Each block carries the signature of its preceding block, thus enforcing a chain of validations

What is a Blockchain

- Blocks and transactions are transmitted across a peer to peer network of participating nodes
  - Every node in the network validates the signatures of each block
  - Highly redundant processing, but decentralization ensures that no single bad actor can corrupt the data without being detected

What is a Blockchain

- Blocks are compiled by "miners" competing to produce the next block
  - Mining is extremely compute-intensive (Proof of Work)
  - The cost of mining is essential to protecting the integrity of the blockchain
  - The miner that generates the next block wins a reward for that block
- Race conditions occur frequently
  - Blockchain provides eventual consistency
  - Eventually one longest chain wins

What is a Cryptocurrency

- Bitcoin's aim was to be a trustless, permissionless, decentralized system of money
  - Trustless - the system requires no trusted 3rd party for operation (as opposed to the modern banking system)
  - Permissionless - anybody can use the system anywhere
  - Decentralized - no single person or organization is in charge of the system

What is a Cryptocurrency

- Bitcoin fails as a currency, on a number of points
  - It is not permissionless - coins and transactions have been censored, and users have been banned
  - It is not decentralized - majority of control is in the hands of a few mining organizations
  - It doesn't behave like cash - spending it reveals to the buyer and seller exactly how much money each other possesses

What is a Cryptocurrency

- Bitcoin fails as a technology, on a number of points
  - It is claimed to support up to 7 transactions per second, but measurements show that the network clogs at around 3-4 transactions per second
    - Compare to credit card networks at 1000s of transactions/second
  - It has hard-coded constants that constrain its scalability
    - 1MB blocksize limit has been debated for the past 2-3 years at least
  - It has a fixed coin supply, and no guarantee that the network will continue to function when the final coin is created

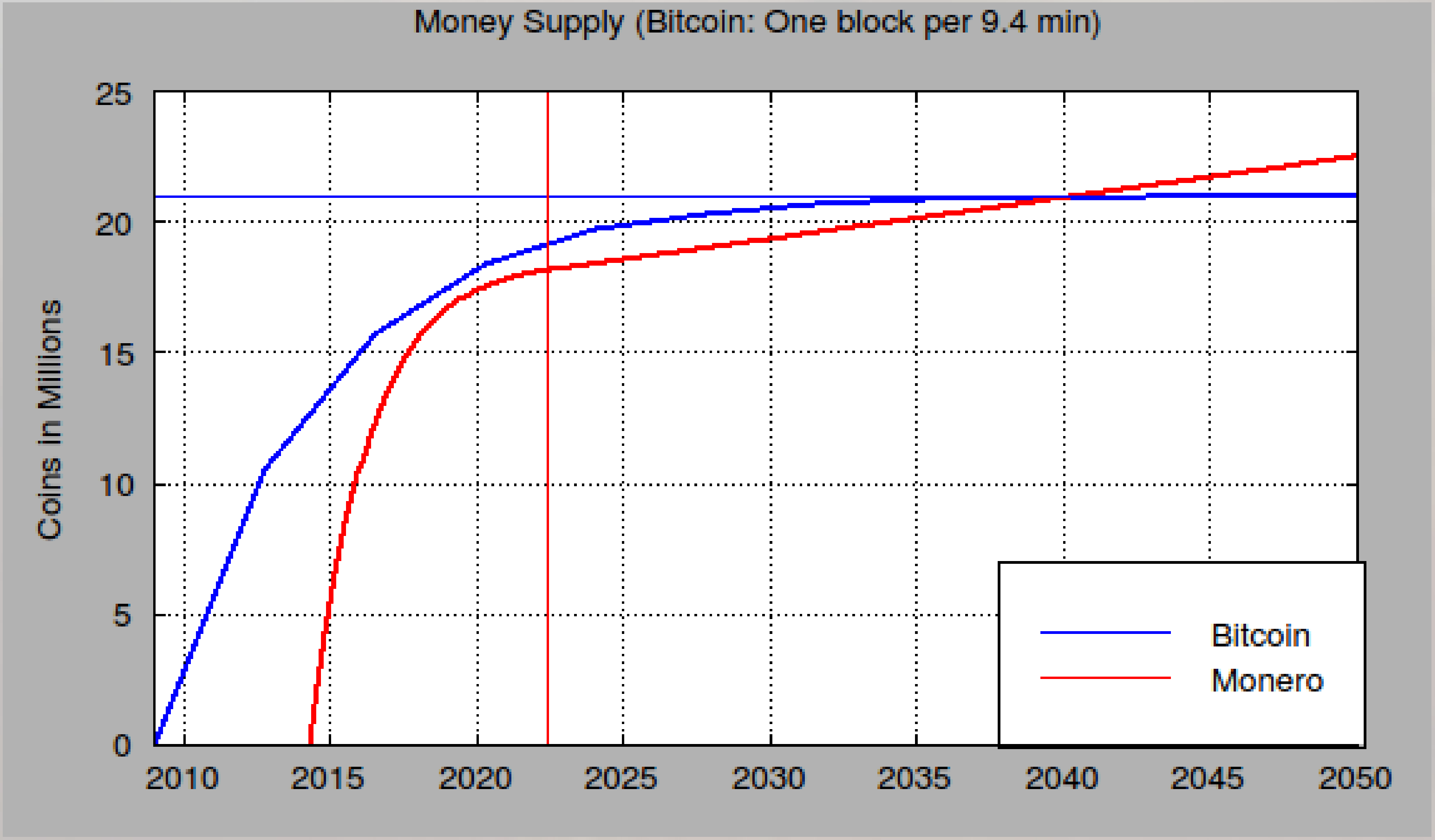
What is Monero

- Monero is essentially Bitcoin 2.0
  - It is permissionless - coins are completely fungible so they cannot be banned or censored
  - It is decentralized - the proof of work algorithm makes centralization difficult
  - It behaves like cash - spending it reveals nothing to the buyer and seller about how much money each other possesses

What is Monero

- Monero is essentially Bitcoin 2.0
  - It is dynamically scalable
    - No hard-coded parameters constraining operation
  - It has a perpetual tail emission
    - The emission rate gradually declines to a minimal amount, ensuring that miners still have incentive to operate
  - It is based on CryptoNote, a completely independent codebase from Bitcoin
    - inherits none of Bitcoin's bugs
    - but also cannot leverage any of Bitcoin's infrastructure

What is Monero



How does Monero work

- How does Monero ensure permissionless operation?
  - Ensuring uncensorability requires fungibility
    - 1XMR = 1XMR - any coin must be indistinguishable from any other coin

How does Monero work

- Monero ensures privacy and anonymity of all transactions
  - Thus, since no coin has any obvious history, none can be singled out for censorship
  - In contrast, in Bitcoin and most of its derivatives, all transactions are public
    - the sender and receiver address are public
    - the transaction amount is public
    - any coin's history can be traced completely from creation to latest use

How does Monero work

- Fungibility requires privacy and anonymity for all transactions
  - Some cryptocurrencies provide optional privacy, obscuring the sender or receiver or amount of a transaction
  - But since use of privacy is optional, those transactions are glaringly obvious, and can easily be censored
  - In practice, when privacy is optional, only a tiny proportion of users will use it (typically less than 5%)

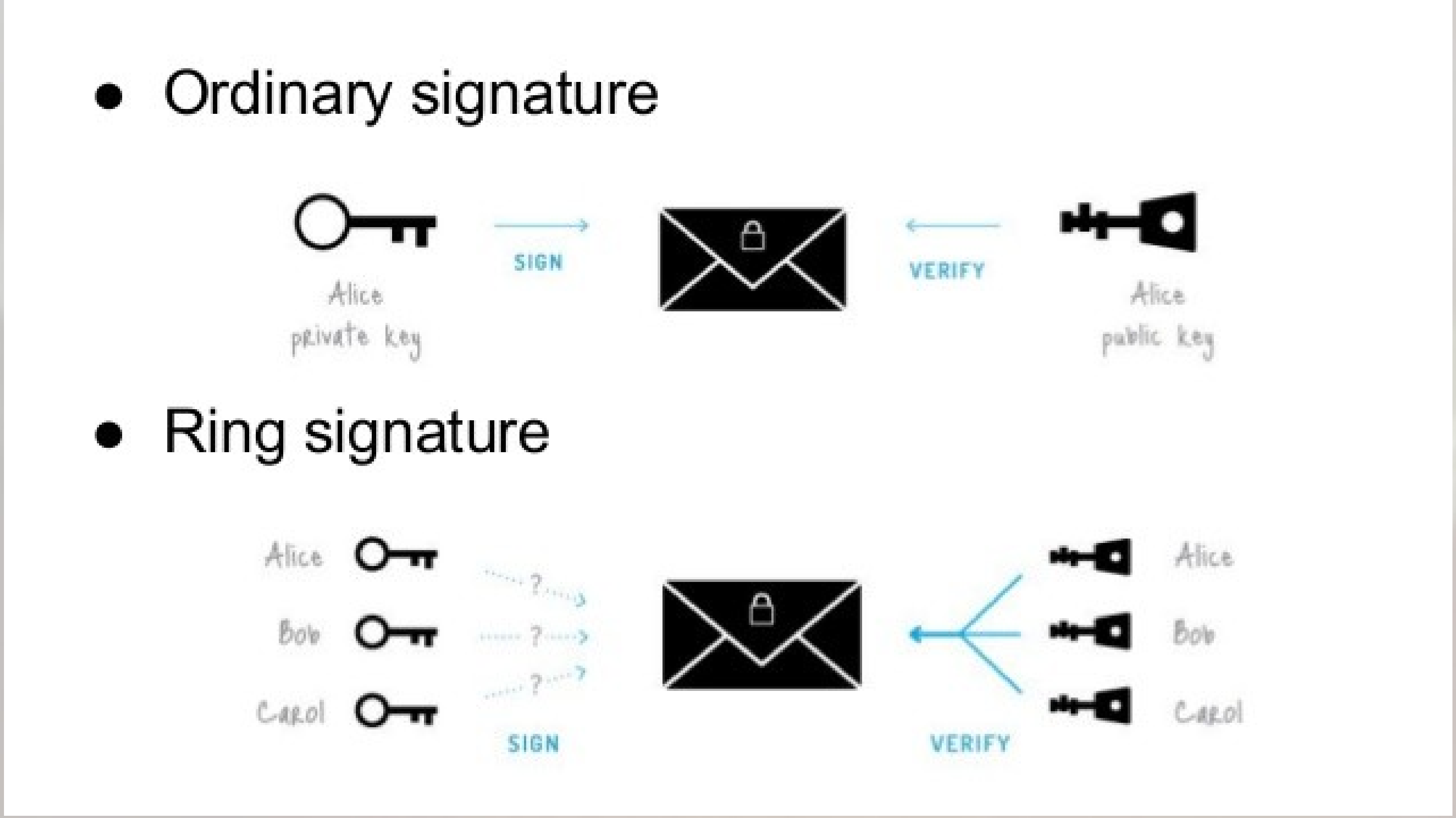
Privacy in Monero

- Stealth Addresses
  - Senders' and recipients' public addresses are never used in actual transactions
  - Randomly generated one-time addresses are used
  - Transactions recorded in the blockchain can never be linked to an actual wallet address

Privacy in Monero

- Ring Signatures
  - Transactions don't contain just a sender's coin, they contain multiple decoys as well
  - Using traceable ring signatures, only the sender knows which coin in the transaction is the real one
  - However, each transaction carries a "key image" of the real coin, which allows the network to detect double-spend attempts

Privacy in Monero



- Ordinary signature
- Ring signature

Privacy in Monero

- Ring Confidential Transactions (ringCT)
  - Transaction amounts are totally hidden
  - Confidential Transactions (CT) were first defined by Greg Maxwell for use in Bitcoin
  - Adapted for use with Monero's ring signatures
  - CT is itself based on ring signatures

Privacy in Monero

- CT basics
  - Amounts encoded in Pedersen Commitments
    - commitment = hash(blinding factor || data)
    - commitments can be added, and the sum of a set of commitments is equal to the commitment of the sum of the data
    - so it can be independently verified that the sum of inputs and outputs to a transaction are equal, i.e. no coins are magically created
    - C(BF1, data1) + C(BF2, data2) = C(BF1+BF2, data1+data2)
    - C(BF1, data1) - C(BF1, data1) = 0

Privacy in Monero

- CT basics
  - Amounts constrained by range proofs
    - the data can be arbitrary value, but we only want values up to 2^64
    - use range proofs to assert that values are in a valid range
    - A value is expressed in binary, and 2-element ring signature is created for each digit:
    - C1 is 0 or 1 || C2 is 0 or 2 || C3 is 0 or 4 || C4 is 0 or 8...

Privacy in Monero

- i2p Integration (WIP)
  - i2p = Invisible Internet Protocol
  - Comparable to TOR
  - Hides the true internet addresses of all participating network nodes
  - Work is ongoing in Kovri, a Monero sub-project implementing an i2p router in C++

Decentralization in Monero

- Cryptonight Proof of Work algorithm
  - Memory-hard: requires 2MB of RAM per hash
  - Uses multiple crypto primitives, including AES-256 and Keccak (SHA-3)
  - Resistant to ASIC implementation (primarily due to cost of embedded RAM)
  - Difficult for GPUs (due to random access pattern, GPUs optimized for sequential access)
- Bitcoin uses SHA2-256
  - Tiny memory footprint, trivial to build in dedicated hardware

Scalability in Monero

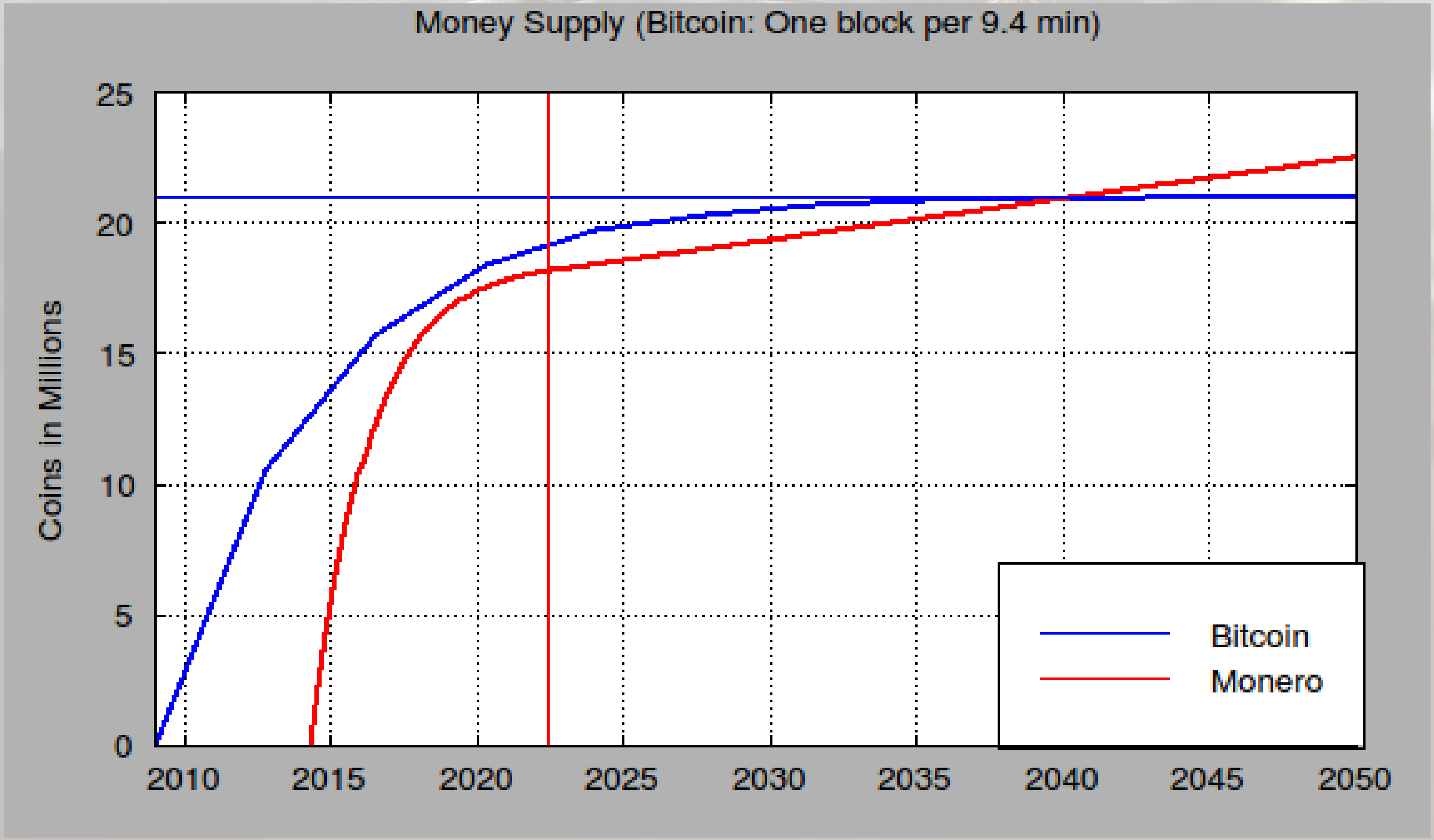
- Dynamic block size
  - based on median of previous 100 blocks
  - limit is designed to discourage spamming the network with huge transactions
  - transaction fee is calculated per kB of txn size
- Dynamic fee
  - based on median of previous 100 blocks and the current block reward

Scalability in Monero

- January 2015, blockchain took 5GB RAM; switching to LMDB took less than 10MB RAM
- January 2015, 585k blocks took 4.2 hours to sync; July 2015 >1M blocks took 10 minutes with LMDB
- Raspberry Pi 1b sync time today, for 1.3M blocks, estimated 150 days - CPU bound at ~10 seconds per block verification

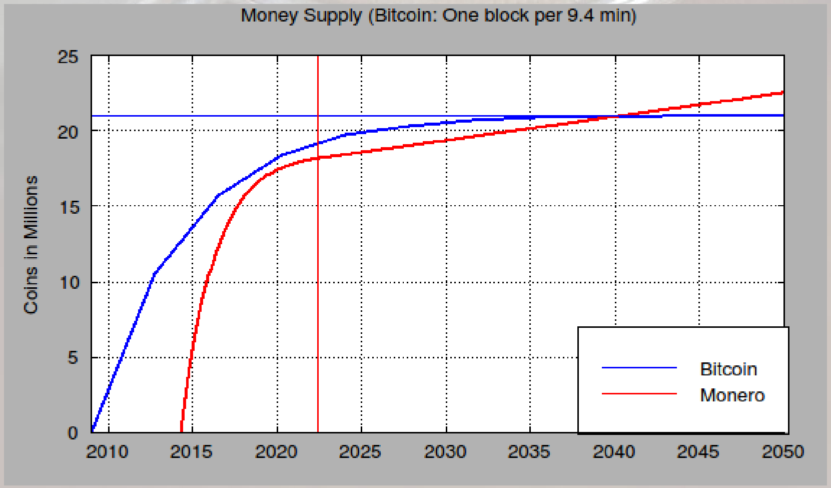
Future Issues

- Security and efficiency are diametrically opposed



Future Issues

- Security and efficiency are diametrically opposed
  - Mars colonies by 2030
  - The currency of the future will need to work at interplanetary scale...



Summary

- Monero is the world's first cryptocurrency that actually behaves like a real currency
  - fungible, private, anonymous
- The design benefited from observing and learning from Bitcoin's flaws
- It works today, but this is only one step on a long journey. It will continue to evolve.

Questions?