Distributed Ledgers, Blockchains & Cryptocurrencies

DCBS | Consumer and Business Services

Division of Financial Regulation

Today’s Presentation

- Overview of the Technology
- Risks of Cryptocurrency
  - Trading/Investment
  - Transactions

Appendix: State of Regulations on Cryptocurrency

New Bottles, Old Beverages

- The technology reflects existing concepts:
    - How?
        - Distributed networks
        - Encrypted “keys” - cryptography
    - What?
        - Money transmission
        - Commodities/Securities
    - Why?
        - Financial Incentives

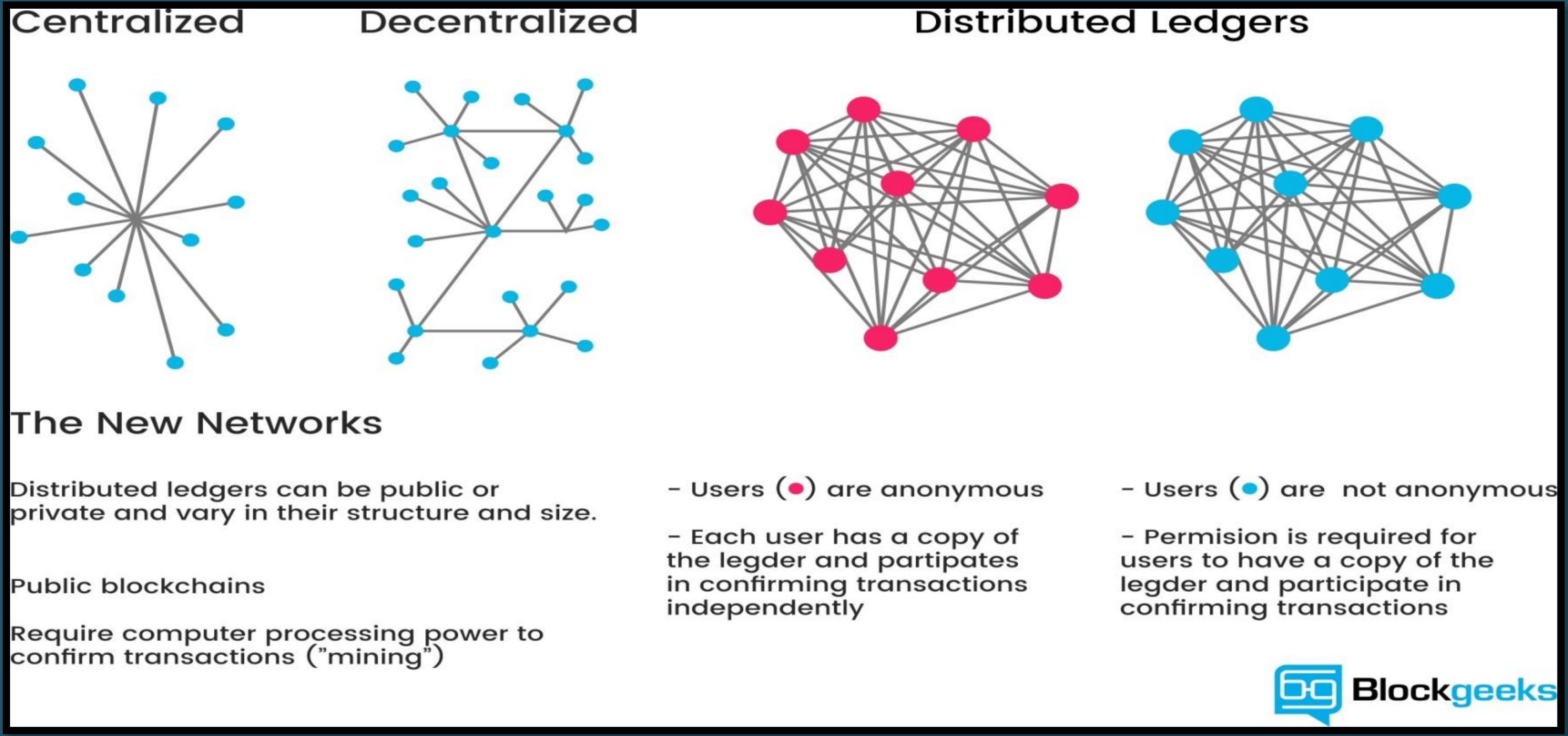
Centralized Networks Today

- Traditional centralized systems for transactions rely on a single trusted record keeper:
  - Banks, credit unions, etc.
  - Federal Reserve/Fedwire
- Central networks maintain a single master ledger with all activities.
- Central networks are tracked and controlled by third-party identification procedures and policies:
  - Payment Processor/ISO/MSP
  - Automated Clearinghouse (ACH)

Distributed Networks

- Distributed networks do not have a central administrator or centralized data storage.
- A peer-to-peer network is required as well as consensus algorithms to ensure replication across the network.
- Each computing device (“node”) replicates and saves an identical copy of the data. Each participant node of the network updates itself independently.

Centralized vs Decentralized Networks



Centralized

Decentralized

Distributed Ledgers

The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions (”mining”)

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

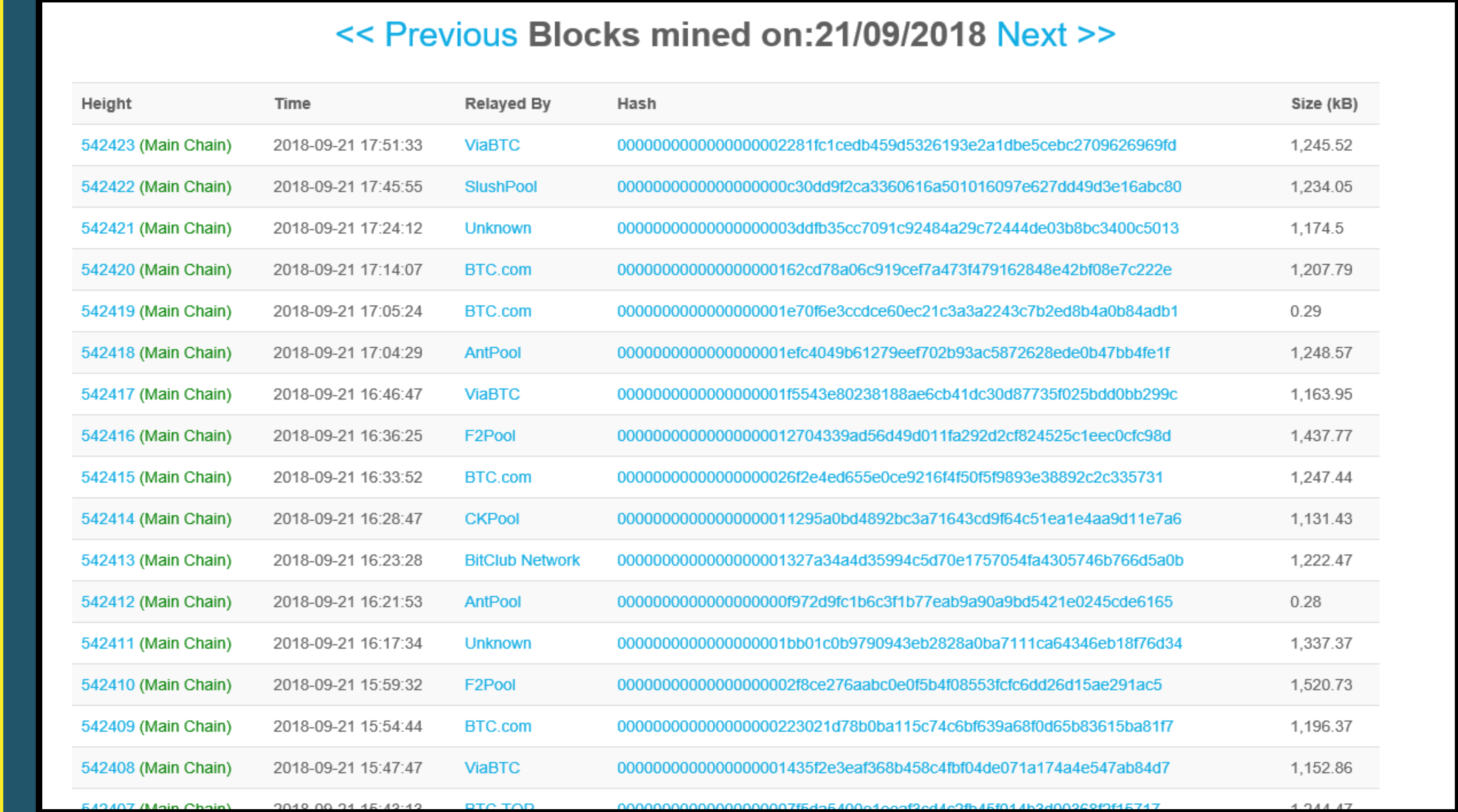
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Distributed Ledger Technology (DLT)

- Distributed ledger technology allows for a database not maintained by any central authority.
- Implementer still controls the network's structure, purpose, and function.
- Updates to the ledger are independently constructed and recorded by each node.
- Nodes vote on updates through a consensus algorithm to ensure that the majority agrees with the conclusion.
- Once consensus is reached, the distributed ledger updates itself.
- The latest, agreed-upon version of the ledger is saved on each node separately.

Blockchains

- A blockchain is a step further toward decentralization than distributed ledger technology.
- A blockchain ledger is shared among a network of users which records all data being transferred between them.
- All participants can view, but only updated upon agreement by a majority of participants.
- A blockchain organizes data in blocks, and updates the entries using an add-only structure.
- Ensures that transactions are unique.



<< Previous Blocks mined on:21/09/2018 Next >>

Height	Time	Relayed By	Hash	Size (kB)
542423 (Main Chain)	2018-09-21 17:51:33	ViaBTC	0000000000000000002281fc1cedb459d5326193e2a1dbe5cebc2709626969fd	1,245.52
542422 (Main Chain)	2018-09-21 17:45:55	SlushPool	0000000000000000000c30dd9f2ca3360616a501016097e627dd49d3e16abc80	1,234.05
542421 (Main Chain)	2018-09-21 17:24:12	Unknown	00000000000000000003ddfb35cc7091c92484a29c72444de03b8bc3400c5013	1,174.5
542420 (Main Chain)	2018-09-21 17:14:07	BTC.com	000000000000000000162cd78a06c919cef7a473f479162848e42bf08e7c222e	1,207.79
542419 (Main Chain)	2018-09-21 17:05:24	BTC.com	0000000000000000001e70f6e3ccdce60ec21c3a3a2243c7b2ed8b4a0b84adb1	0.29
542418 (Main Chain)	2018-09-21 17:04:29	AntPool	0000000000000000001efc4049b61279eef702b93ac5872628ede0b47bb4fe1f	1,248.57
542417 (Main Chain)	2018-09-21 16:46:47	ViaBTC	0000000000000000001f5543e80238188ae6cb41dc30d87735f025bdd0bb299c	1,163.95
542416 (Main Chain)	2018-09-21 16:36:25	F2Pool	00000000000000000012704339ad56d49d011fa292d2cf824525c1eec0cfc98d	1,437.77
542415 (Main Chain)	2018-09-21 16:33:52	BTC.com	00000000000000000026f2e4ed655e0ce9216f4f50f5f9893e38892c2c335731	1,247.44
542414 (Main Chain)	2018-09-21 16:28:47	CKPool	00000000000000000011295a0bd4892bc3a71643cd9f64c51ea1e4aa9d11e7a6	1,131.43
542413 (Main Chain)	2018-09-21 16:23:28	BitClub Network	0000000000000000001327a34a4d35994c5d70e1757054fa4305746b766d5a0b	1,222.47
542412 (Main Chain)	2018-09-21 16:21:53	AntPool	0000000000000000000f972d9fc1b6c3f1b77eab9a90a9bd5421e0245cde6165	0.28
542411 (Main Chain)	2018-09-21 16:17:34	Unknown	0000000000000000001bb01c0b9790943eb2828a0ba7111ca64346eb18f76d34	1,337.37
542410 (Main Chain)	2018-09-21 15:59:32	F2Pool	00000000000000000002f8ce276aabc0e0f5b4f08553fcfc6dd26d15ae291ac5	1,520.73
542409 (Main Chain)	2018-09-21 15:54:44	BTC.com	000000000000000000223021d78b0ba115c74c6bf639a68f0d65b83615ba81f7	1,196.37
542408 (Main Chain)	2018-09-21 15:47:47	ViaBTC	0000000000000000001435f2e3eaf368b458c4fbf04de071a174a4e547ab84d7	1,152.86
542407 (Main Chain)	2018-09-21 15:43:13	BTC.TOP	00000000000000000007f5da5400e1eeaf3cd4c2fb45f014b3d00368f2f15717	1,244.47

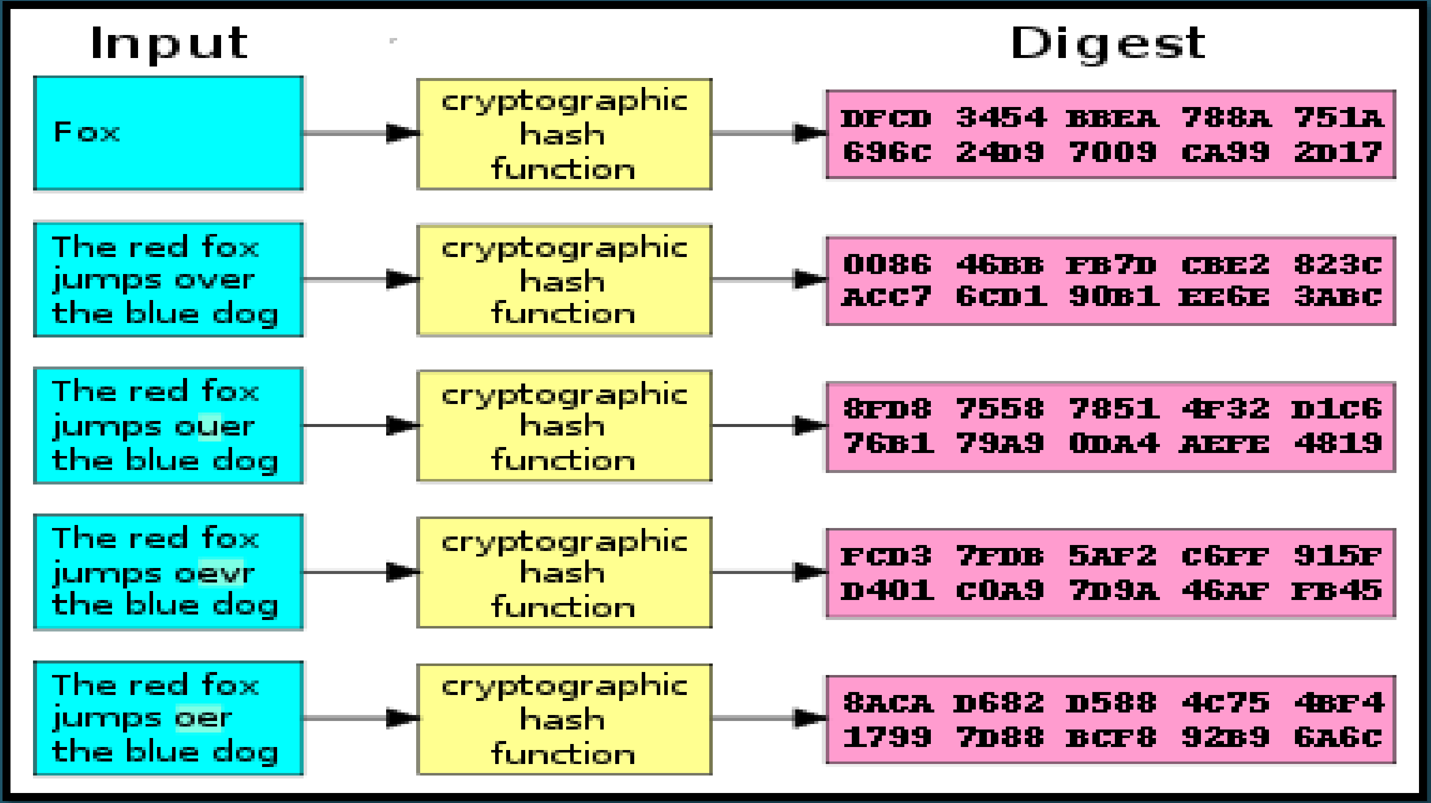
Cryptography

- The basis of blockchains and cryptocurrencies is cryptography.
    - Cryptography: the computerized encoding and decoding of information
    - Algorithms: a procedure for solving a mathematical problem (as of finding the greatest common divisor) in a finite number of steps that frequently involves repetition of an operation, following a particular protocol.
- Cryptographic problems are hard to solve, but easy to verify.

Cryptography: Hash Functions

- A cryptographic hash = an algorithm that maps data of any size to a bit string of a fixed size. Bitcoin uses the SHA256 algorithm to ‘hash’ data into a 256-bit string of characters.
- Data entered into the Bitcoin algorithm will result in a unique string of characters representing the data input.
- For example, information on a transaction:
    - History;
    - Description of the transaction;
    - Time;
    - Public key; and
    - Private key

Cryptography: Hashing



Input

Digest

Fox

cryptographic hash function

DFCD 3454 BBEA 788A 751A
696c 24D9 7009 CA99 2D17

The red fox jumps over the blue dog

cryptographic hash function

0086 46BB FB7D CBE2 823c
ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog

cryptographic hash function

8FD8 7558 7851 4F32 D1c6
76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog

cryptographic hash function

FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45

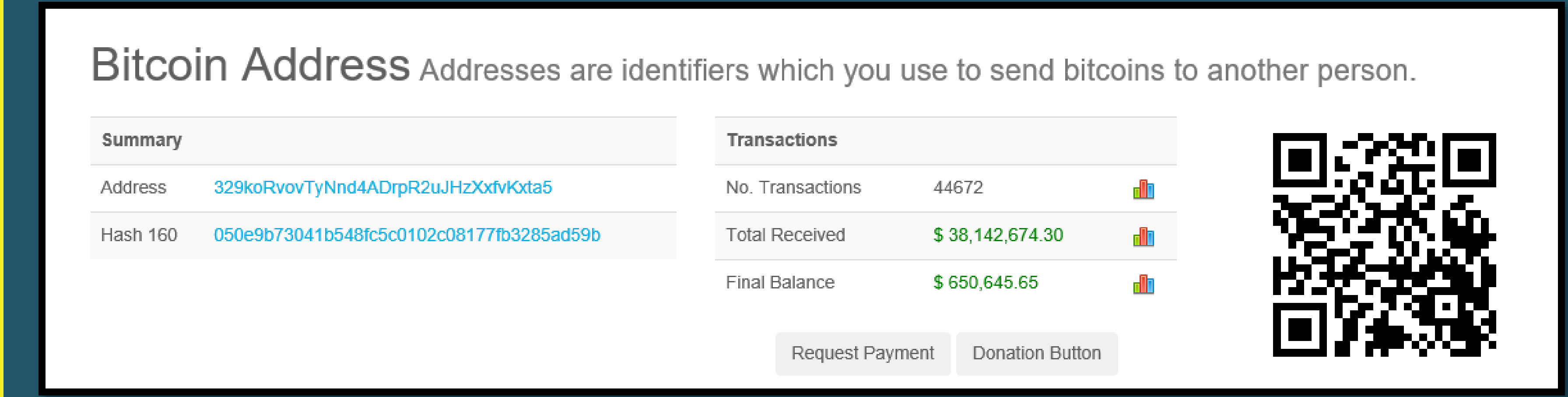
The red fox jumps oer the blue dog

cryptographic hash function

8ACA D682 D588 4c75 4BF4
1799 7D88 BCF8 92B9 6A6c

Cryptography: Public/Private Keys

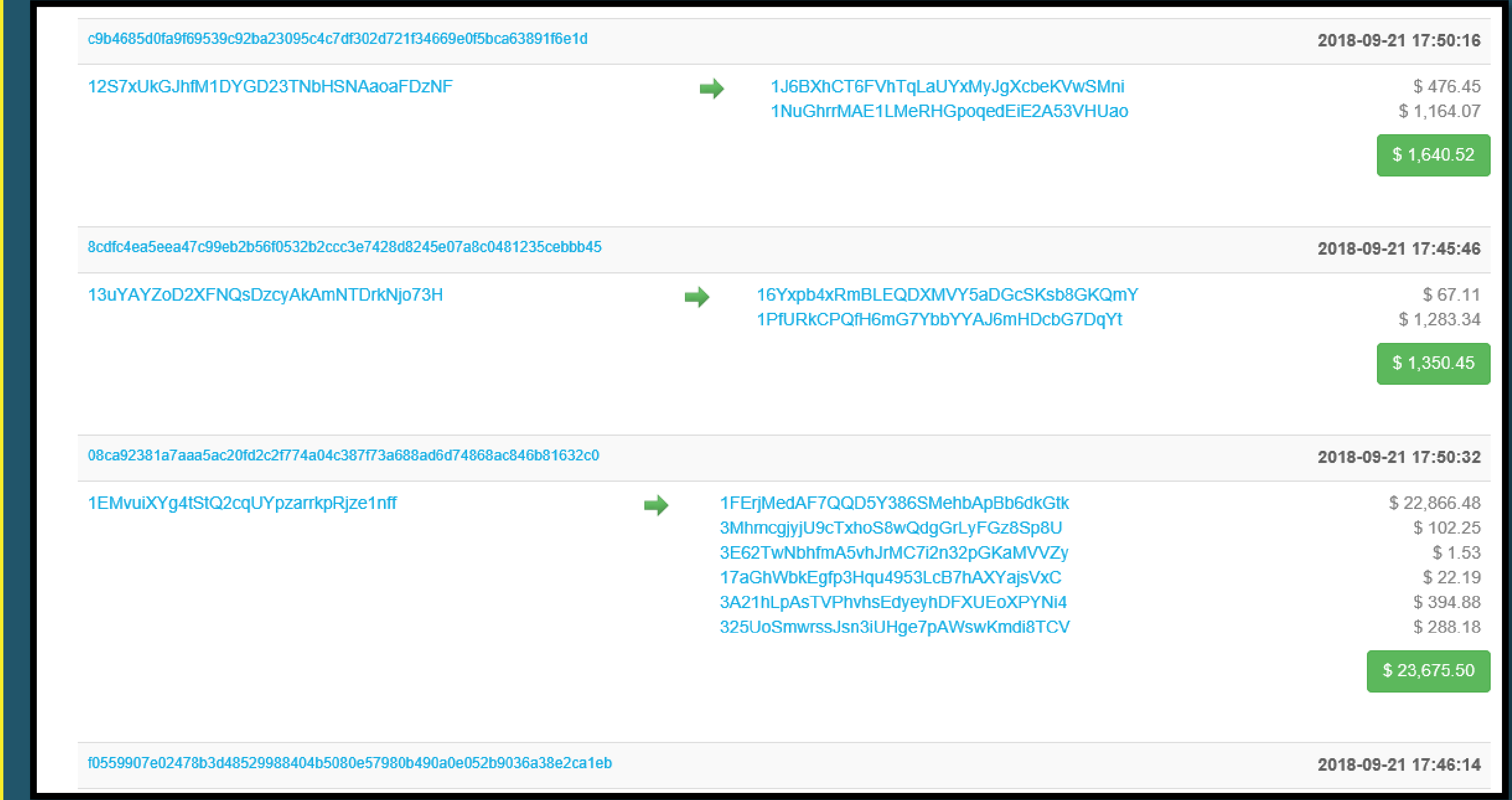
- Also called asymmetrical cryptography, because the keys are related but not identical. Two parts:
  - A public key is like an address - only used to encrypt
    - Published so that anyone can send to a particular receiver a secure message.
  - A private key is used to decrypt messages encrypted with a related public key.
    - Kept secret because it controls access
    - If someone gains access to your private key they gain access to all your cryptocurrency.



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	329koRvovTyNnd4ADrpR2uJHzXxfvKxta5
Hash 160	050e9b73041b548fc5c0102c08177fb3285ad59b

Transactions	
No. Transactions	44672
Total Received	$ 38,142,674.30
Final Balance	$ 650,645.65



c9b4685d0fa9f69539c92ba23095c4c7df302d721f34669e0f5bca63891f6e1d 2018-09-21 17:50:16

12S7xUkGJhfM1DYGD23TNbHSNAaoaFDzNF → 1J6BXhCT6FVhTqLaUYxMyJgXcbeKVwSMni $ 476.45
1NuGhrrMAE1LMeRHGpoqedEiE2A53VHUao $ 1,164.07

$ 1,640.52

8cdfc4ea5eea47c99eb2b56f0532b2ccc3e7428d8245e07a8c0481235cebbb45 2018-09-21 17:45:46

13uYAYZoD2XFNQsDzcyAkAmNTDrkNjo73H → 16Yxpb4xRmBLEQDXMVY5aDGcSKsb8GKQmY $ 67.11
1PfURkCPQfH6mG7YbbYYAJ6mHDcbG7DqYt $ 1,283.34

$ 1,350.45

08ca92381a7aaa5ac20fd2c2f774a04c387f73a688ad6d74868ac846b81632c0 2018-09-21 17:50:32

1EMvuiXYg4tStQ2cqUYpzarrkpRjze1nff → 1FErjMedAF7QQD5Y386SMehbApBb6dkGtk $ 22,866.48
3MhmcgjyjU9cTxhoS8wQdgGrLyFGz8Sp8U $ 102.25
3E62TwNbhfmA5vhJrMC7i2n32pGKaMVVZy $ 1.53
17aGhWbkEgfp3Hqu4953LcB7hAXYajsVxC $ 22.19
3A21hLpAsTVPhvhsEdyeyhDFXUEoXPYNi4 $ 394.88
325UoSmwrssJsn3iUHge7pAWswKmdi8TCV $ 288.18

$ 23,675.50

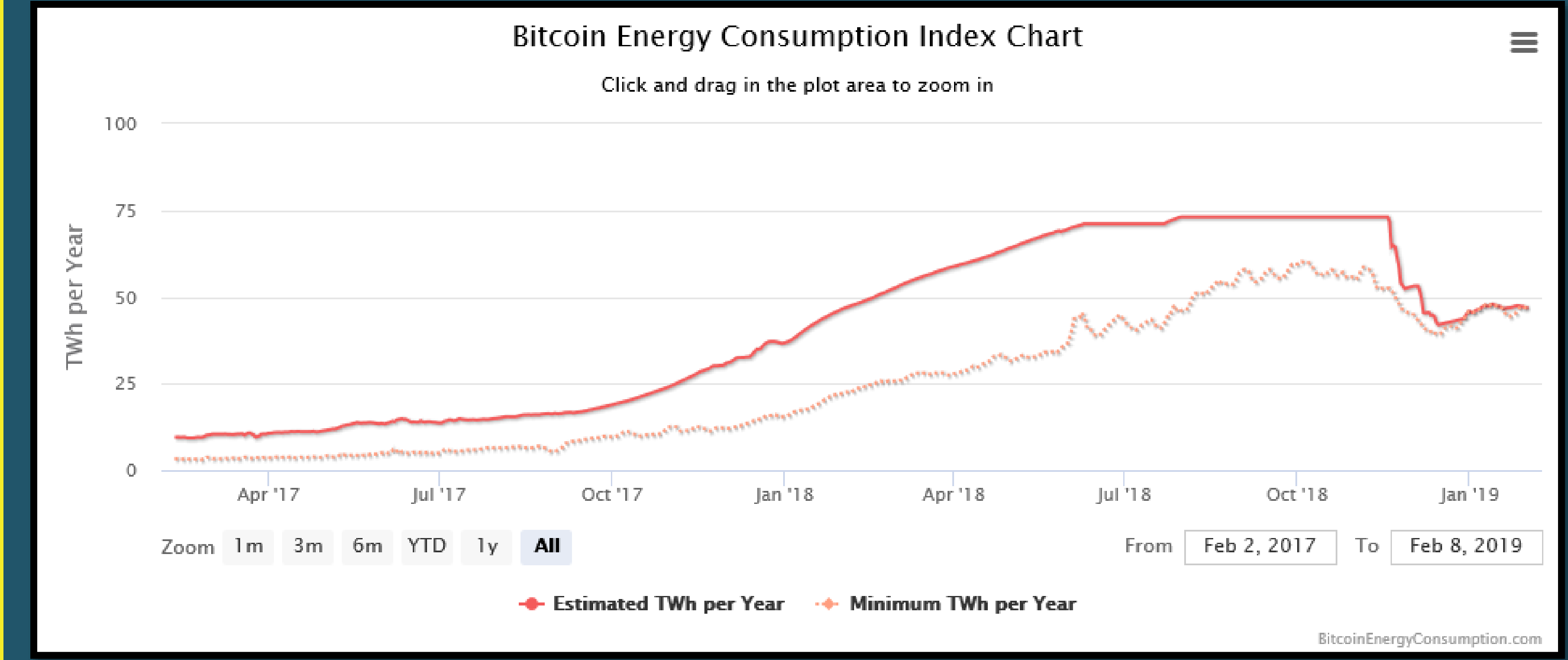
f0559907e02478b3d48529988404b5080e57980b490a0e052b9036a38e2ca1eb 2018-09-21 17:46:14

Blockchains: “Immutability”

- The “block” contains the who and what for every transaction and they are all linked in a “chain.”
- Precludes “chargebacks” – any one average user should unable to reverse transactions linked into the chain.
- True of all transactions that use the blockchain ledger.
- “51% Attack” on etherium Classic – January 5 2019

Financial Incentives for the Network

- Implementations of blockchain/DLT need a way to make sure that all the records are accurate across the entire network. But how?
- In the cryptocurrency implementations, the network rewards the nodes that solve the complex mathematical problems needed to verify the transaction with a unit of cryptocurrency.
- This is what is known as “mining.” Mining operations are increasingly complex and CPU intensive [the math problems are much harder than before as the network grows], leading to larger, industrial-scale operations.



Blockchain is Versatile

- Because the record is largely immutable, DLT/blockchain can be used for many “back office” functions:
  - Financial firms can use to track ownership of securities.
  - Power companies can use to track consumption and production.
  - Companies can use to track items through a supply chain;
  - Healthcare providers can use to streamline the sharing of medical records.

Application of Blockchain: Smart Contracts

- Self-executing computer code
- Relies upon a blockchain to include the operational terms of an agreement, terms are written into and executed by the lines of code.
- The code contains the "if-then" conditions of the contract.
- Data is received that triggers the set the terms and conditions that produce the contract's outcome. The contract language essentially becomes computer code, without the ability to change it (blockchain).
- In theory, smart contracts avoid the costs of contract drafting, judicial intervention, opportunistic behavior, and unclear language.
- But see: The DAO (June 2016).

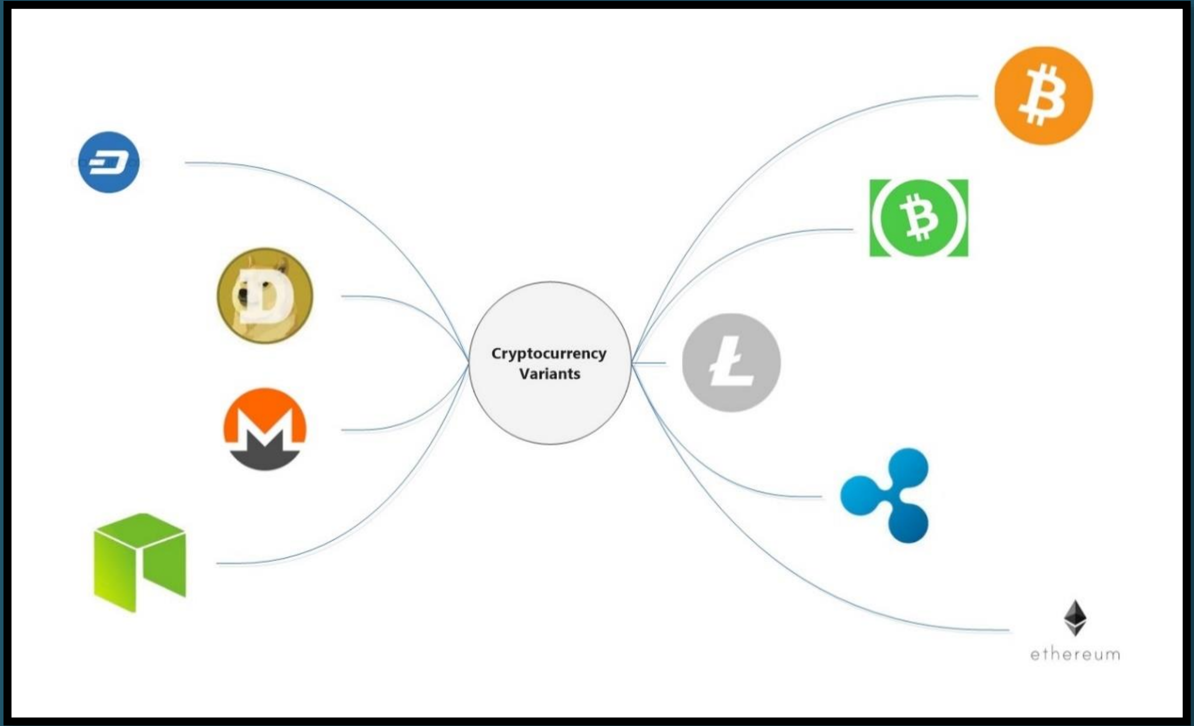
Application of Blockchain: Cryptocurrency

- Cryptocurrency is the most well known example of blockchain usage.
- A digital asset originally designed to work as a medium of exchange
- Uses cryptography and blockchain technology to:
  - secure financial transactions,
  - track ownership
  - verify the transfer of assets, and
  - control the creation of additional units.

Application of Blockchain: Bitcoin

- Created in 2008 by “Satoshi Nakamoto”
- Envisioned as a peer-to-peer payment system.
- Designed as a "decentralized currency of the people," taking centralized banks out of the equation.
- Individuals using their computers solve complex algorithms are rewarded with bitcoins (or portions).
    - Bypasses government currency controls and simplifies online transactions
    - Removes third-party payment processing intermediaries
- 21 million Bitcoins total; subunits termed “satoshis”

Other Cryptocurrencies



...and a thousand others.

E-Wallets

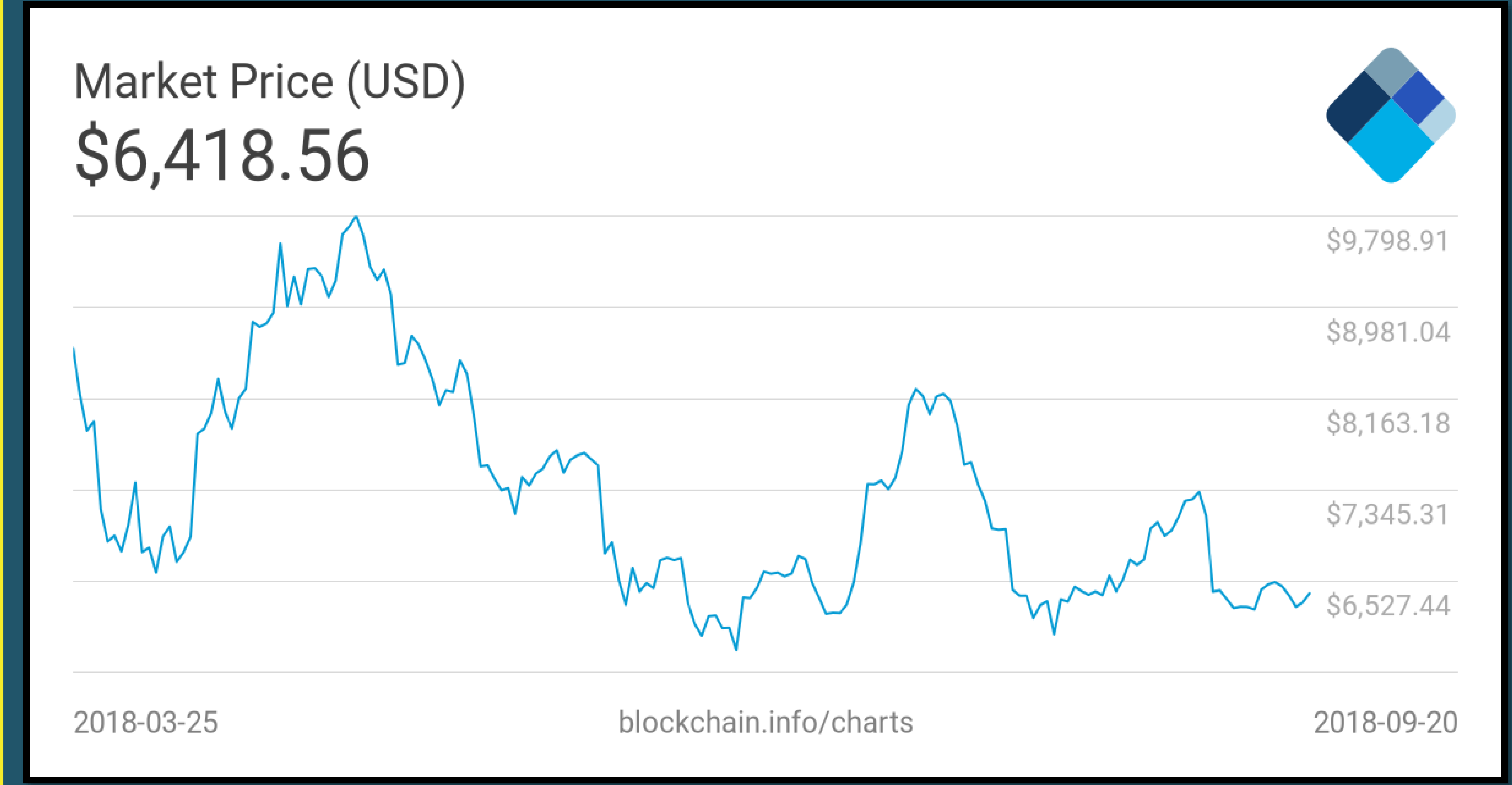
- Cryptocurrency is stored in a “wallet”
- Can be paper (cold) or electronic and connected to the Internet (hot)
- An e-Wallet is a digital system that allows payments online via a computer or mobile device
- A means to stores the public and private keys which can be used to receive or transmit a cryptocurrency.
- Different wallets support different cryptocurrencies

Risks: Payment vs. Investment

- Bitcoin was designed for payment
- More and more it is used for speculation and as a store of value.
- Very dynamic, fast-growing market for investors and speculators.
- Exchanges like Okcoin, poloniex, or shapeshift enable the trade of hundreds of cryptocurrencies.

Risks: Valuation Volatility

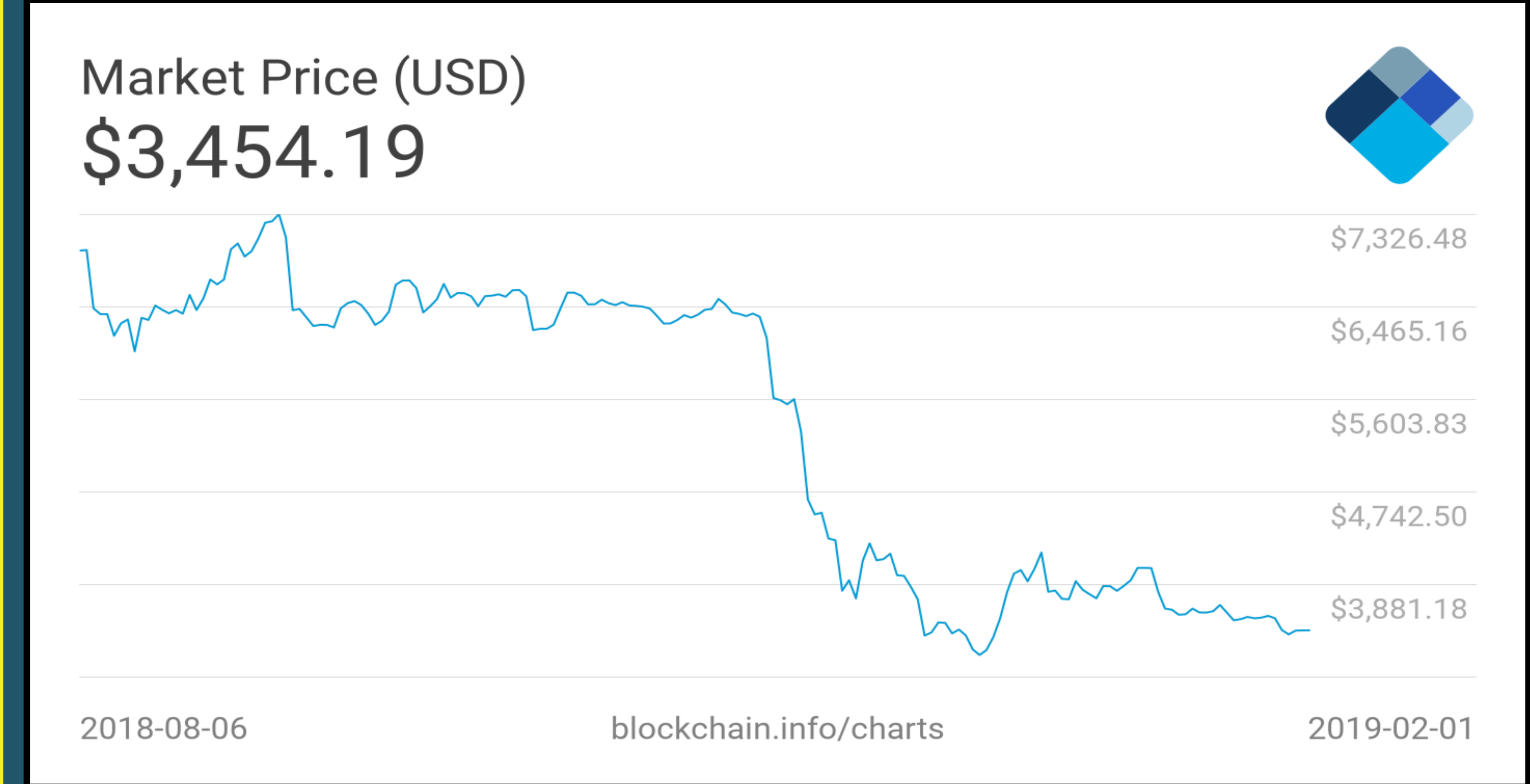
- Cryptocurrencies can be extremely volatile
- **2018 Labor Day Crash**: Bitcoin dropped sharply
  - Falling $500, (about 5%) in just over an hour
  - Lost almost $1,000 in value in a 24-hour period
- Others fell even more sharply,
  - Ether and Ripple's XRP lost about 12%
  - ethereum lost 20% in a 24-hour period



Market Price (USD)

$6,418.56

blockchain.info/charts


Market Price (USD)
$3,454.19
$7,326.48
$6,465.16
$5,603.83
$4,742.50
$3,881.18
2018-08-06
blockchain.info/charts
2019-02-01

Questions and discussion

Appendix: State of Regulations on Cryptocurrency

State of Regulations on Cryptocurrency

- Initial Considerations:
  - Virtual currencies lack the status of “money;” not issued and backed by a governmental entity
  - They are digital representations of value that function as a medium of exchange
  - Virtual currencies cannot be deposited into a bank account and are not covered by federal deposit insurance
  - Stored on computers or held by a purchaser or a third party in an e-wallet

State of Regulations on Cryptocurrency

- Risks
  - No recourse should the virtual currency disappear
    - Misplaced or stolen private key
    - Fraud
  - Rapid valuation changes
  - May not be redeemable if network becomes defunct
- Balance between innovation and consumer protection, using existing models.

Money Exchange

- Money exchange – crypto for fiat or vice versa
- The U.S. Treasury Department (FinCEN) requires exchanges to register as Money Services Businesses (MSB)
- FinCEN also regulates Money Transmitters as MSBs
  - Must have anti-money laundering policies
  - Pseudoanonymous because the MSB must be able to attach the account to a person to prevent money laundering.

Cryptocurrencies Exchanges: Money Transmission

- Legislative Assembly addressed cryptocurrency exchanges in 2015
- Senate Bill 277 added definition of “money.”
- Means a medium of exchange that:

> “(a) The United States or a foreign government authorizes or adopts; or
>
> (b) Represents value that substitutes for currency but that does not benefit from government regulation requiring acceptance of the medium of exchange as legal tender.”

Cryptocurrencies Exchanges: Money Transmission

- ORS 717.200: “In the business of receiving money for transmission, or transmitting money within the United States or to locations abroad by any and all means[.]”
  - Payment processors
  - Merchant service providers that act as an intermediary so merchant can accept cryptocurrencies
- Does not include simple currency exchange

Cryptocurrencies as Commodities

- Purchase/sale for investment purposes
  - Similar to stocks – buy low, sell high
- Regulated by U.S. Commodity Futures Trading Commission
  - Bitcoin and other virtual currencies have been determined to be commodities under the Commodity Exchange Act
  - General anti-fraud and manipulation enforcement authority

Cryptocurrencies as Securities

- An “investment contract” under the *Howey* test:
  - It is an investment of money
  - There is an expectation of profits from the investment
  - The investment of money is in a common enterprise
  - Any profit comes from the efforts of a promoter or third party
- SEC recently announced cryptocurrencies like bitcoin are not a security. Those without utility could be securities.

Cryptocurrencies as Securities

- If the virtual token or coin is a security, federal and state securities laws require investment professionals and their firms who offer, transact in, or advise on investments to be licensed or registered.
- Recent actions: *In the Matter of Tokenlot, LLC*
  - “ICO Superstore” operated as an unregistered broker-dealer offering customers the ability to buy, sell and trade digital assets connected with ICOs.
  - SEC charged TokenLot with violating broker-dealer registration requirements under the Exchange Act and the offering and sale of unregistered.

Investment Risks

- Not originally designed as investment but as a peer to peer system
- Trendy: some are just adding “blockchain” or “crypto” to existing processes
- Investments tied to virtual currency are unsuitable for most investors:
  - No cash flows;
  - Do not pay dividends;
  - No way to systematically determine demand growth for them.
- Companies may not accurately or fully disclose the risks that price fluctuations may have on business operations.

Initial Coin Offerings (ICOs)

- Similar to an initial public offering of securities,
  - Uses blockchain technology to issue customized tokens that entitle bearer to future benefits
  - Proceeds of an ICO can provide kick-start funding to develop the technology and platforms for the token holder's access.
- Legitimate ICOs provide easy transferability of tokens and the potential for those tokens to be traded on exchanges or resold and converted to government-issued legal tender (e.g., US dollars).
- ICO nearly always a security

ICO Risks

- Platforms facilitating trading in ICO tokens are not registered exchanges
  - One study found $400 million in funds raised in ICOs in 2017 was lost or stolen.
  - Hackers have accessed investors' personal information
  - Often promise that the ICO will become a “utility token” outside the scope of securities laws.

Decreasing the Risk

- Consumers can visit Investor.gov to check the registration status and background of investment professionals.
- Warning Signs of Investment Fraud
  - “Guaranteed” high investment returns.
  - Unsolicited sales pitches.
  - Unlicensed sellers.
  - No net worth or income requirements.
  - Too Good to Be True

Additional Regulatory Efforts

- New York adopted specific regulations for a “BitLicense” that regulates all aspects of cryptocurrency, except development and use.
- Uniform Law Commission approved the Uniform Regulation of Virtual Currency Businesses Act (1-9-18)
- Increasing scrutiny by the SEC and CFTC
- OCC Special Fintech Charter
  - Would preempt state regulation