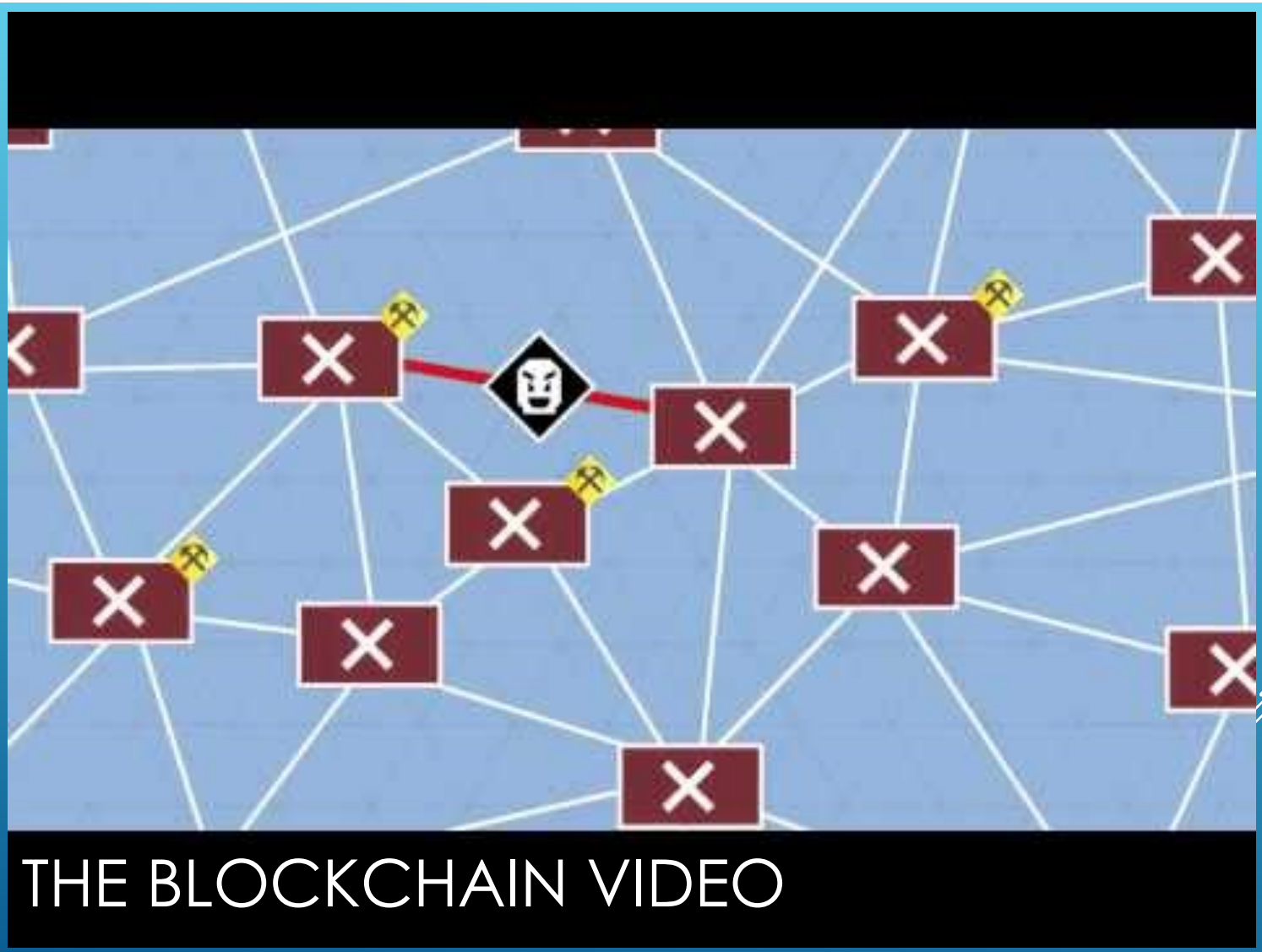
THE BLOCKCHAIN

Ethan Kinory, Ph.D.

Sean Stein Smith, DBA, CPA



THE BLOCKCHAIN VIDEO

WHAT IS THE BLOCKCHAIN?

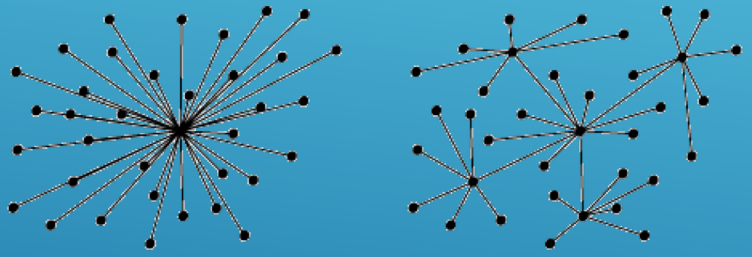
- In simple terms: a blockchain is a transparent database that does not permit modification of previously approved transactions.
- New transactions, once approved, are packaged into blocks. The block is then appended to the ordered chain of preexisting blocks. In this way, we form a chain of blocks. (hence BLOCK + CHAIN).
  - Picture a train being elongated as new cars are added
- The method by which new blocks are approved can vary by design.
  - The bitcoin blockchain requires that a complex cryptographic challenge be solved.
- More formally: The blockchain is an decentralized distributed ledger that utilizes cryptography to ensure the immutability of data.

1. **Decentralized**
2. Distributed
3. Encrypted
4. Immutable

- "Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system *behaves* like a single computer)."

-Vitalik Buterin

(Co-founder of Ethereum)



Centralized Decentralized

DECENTRALIZED

Image credit: Wikimedia Commons

1. Decentralized
2. **Distributed**
3. Encrypted
4. Immutable

DISTRIBUTED

- The ledger is distributed across the network.
- A full copy of the blockchain is replicated and maintained on each node in the network.
- Nodes possess a complete and up to date copy of the blockchain.
- Communication between participants does not pass through a centralized point
- Also referred to as peer to peer

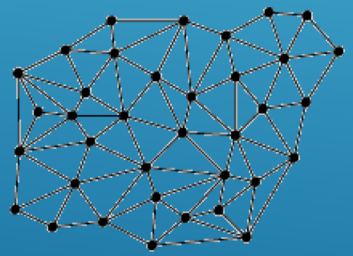
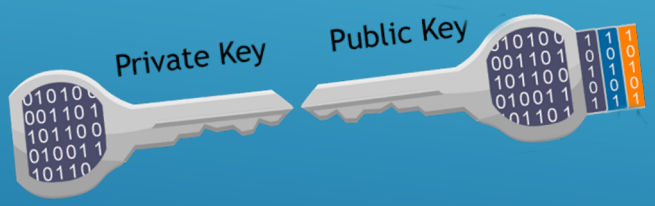
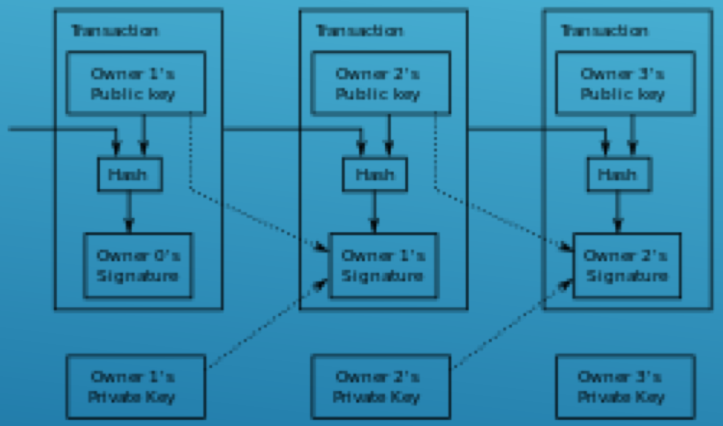


Image credit: Wikimedia Commons

1. Decentralized
2. Distributed
3. **Encrypted**
4. Immutable

- Cryptography and digital signatures helps safeguard the data on the blockchain and ensure its authenticity.
- Each block is cryptographically linked to its predecessor.





ENCRYPTED

Image credit:Wikimedia Commons

1. Decentralized
2. Distributed
3. Encrypted
4. **Immutable**

IMMUTABILITY

- Data on the blockchain cannot be overwritten.
- Append to database only, no rewrites, overwrites or deletes
- By design, any efforts to modify data will be quickly detected and rejected.
- Changing a preexisting block is extremely difficult, but not theoretically impossible.
  - Collusion can circumvent the immutability characteristic
  - Advent of quantum computing can threaten existing cryptographic techniques

TYPES OF BLOCKCHAINS

- Permissionless blockchains – Public blockchains that anyone can access and participate in.
  - Low level of trust
  - Characterized by (pseudo) anonymity
  - Requires additional rigor to ensure legitimacy of transactions

- Fully Permissioned blockchains – Private blockchains restrict access. Write permissions are limited to select parties. Think of an internal private blockchain at a company.
  - Trust level is high
  - Higher transaction and validation speed
  - Anonymity not a characteristic

TYPES OF BLOCKCHAINS

- Consortium Blockchains – The consensus process is restricted to a pre-selected set of nodes. For example, Company A, Company B, and the SEC must all agree to add a block to the chain.

LIMITATIONS OF THE BLOCKCHAIN

- Little standardization
- Little or nonexistent regulation (e.g., SEC)
- Adoption issues – Implementation costs, integration with pre-existing systems, etc.
- Scaling issues – the ability to efficiently process transactions

CONSENSUS

- Participants in a public permissionless blockchain are
  1. Not trusted
  2. Not known.
- Specific verification protocols can vary depending on the design of the blockchain, but a process is in place to ensure that additions to the ledger are approved.
- In order to prevent any nefarious manipulation of the blockchain, new blocks are subject to a validation process before they are added.
- The process of accepting a proposed block and adding it to the distributed ledger is called “consensus”.

CONSENSUS ALGORITHMS

1. **Proof of work (PoW)**
2. Proof of stake (PoS)
3. Delegated PoS (DPoS)
4. Proof of elapsed time

- Examples of algorithms used to arrive at consensus
  1. Proof of work (PoW):
     - A. Requires only a single node to submit a solution to an algorithmic problem.
     - B. This solution is very difficult to achieve but easy to verify.
     - C. Rewards incentivize participants to seek out a solution.
       - Greater participation accelerates the verification process
       - Greater participation reduces the risk that a bad actor will corrupt the integrity of the chain
     - D. Subject to 51% attack
     - E. PoW is utilized in the Bitcoin, Litecoin, Monero, and Ethereum* blockchains

* Ethereum is planning a switch to PoS

CONSENSUS ALGORITHMS

1. Proof of work (PoW)
2. **Proof of stake (PoS)**
3. **Delegated PoS (DPoS)**
4. Proof of elapsed time

2. Proof of stake (PoS):
   A. A lottery determines which stakeholders will approve the transaction. The probability of being selected varies directly with the stake held.
   B. Ethereum is moving from proof of work to proof of stake
   C. Cardano and Neo are the largest cryptocurrencies using PoS

3. Delegated proof of stake algorithm (DPoS):
   A. Similar to proof of stake except that participants can delegate their stakes to increase their representation in the lottery.
   B. EOS is the largest cryptocurrency using DPoS

1. Proof of work (PoW)
2. Proof of stake (PoS)
3. Delegated PoS (DPoS)
4. **Proof of elapsed time**

4. Proof of Elapsed Time (PoET):
   A. Uses a random, or election, based model to determine who will approve the block
   B. Validator with the shortest wait time wins the lottery
   C. Validator has to wait a certain amount of time before mining another block
   D. Miners have to run Intel Software Guard Extensions (SGX).
   E. Requires some reliance on Intel for the hardware

CONSENSUS ALGORITHMS

BITCOIN

- We will consider Bitcoin because it allows us to observe a fully functional public blockchain.
- Bitcoin is an application that utilizes blockchain technology
- Bitcoin is a cryptocurrency that can be transferred within a peer-to-peer network
  - There are over 1,500 cryptos
  - Total market cap exceeded $500 billion in January 2018
  - Total market cap plummeted in 2018 and stood at just $200 billion in September 2018
  - Approximately one-half of this market capitalization is attributable to Bitcoin
- Devised by Satoki Nakamoto as a peer to peer electronic cash system
- Shorthand for 1 Bitcoin is “BTC”

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

BITCOIN: FROM GENESIS TO NOW

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

BITCOIN WHITE PAPER

Source: Bitcoin.org

BLOCKCHAIN

The steps to run the network are as follows:

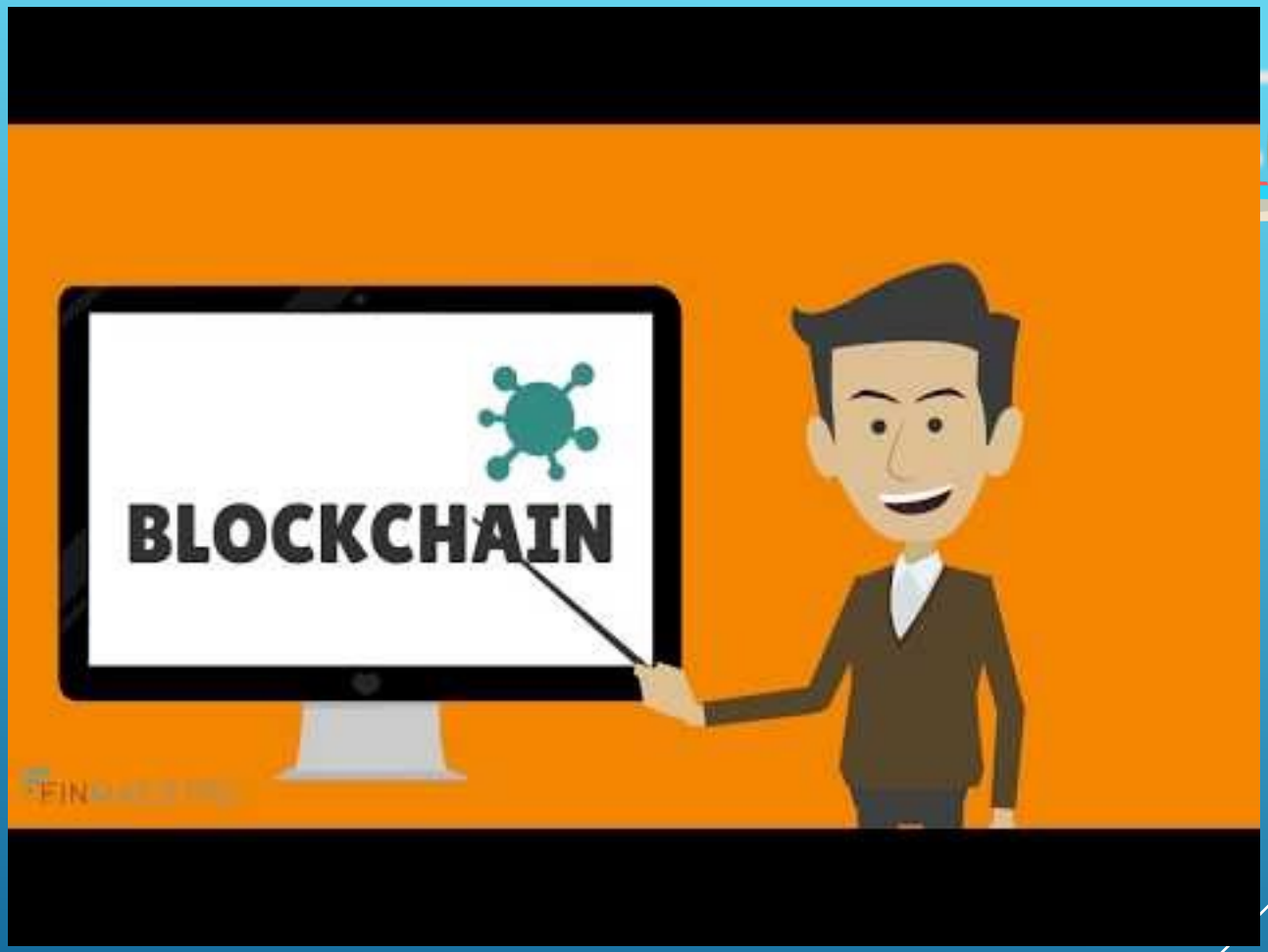
1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

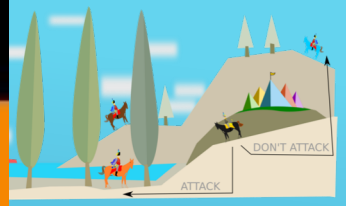
ADDING A BLOCK TO THE BITCOIN BLOCKCHAIN

- Transactions are packaged into blocks.
- Miners determine which transactions to package
- Transactions cannot be packaged into more than 1 block in order to prevent the double spend problem
- Block limit is 1MB, thus the number of transactions in a block is limited
  - A new block is added every ten minutes
  - Scalability problem (3.3 – 7 transactions per second).

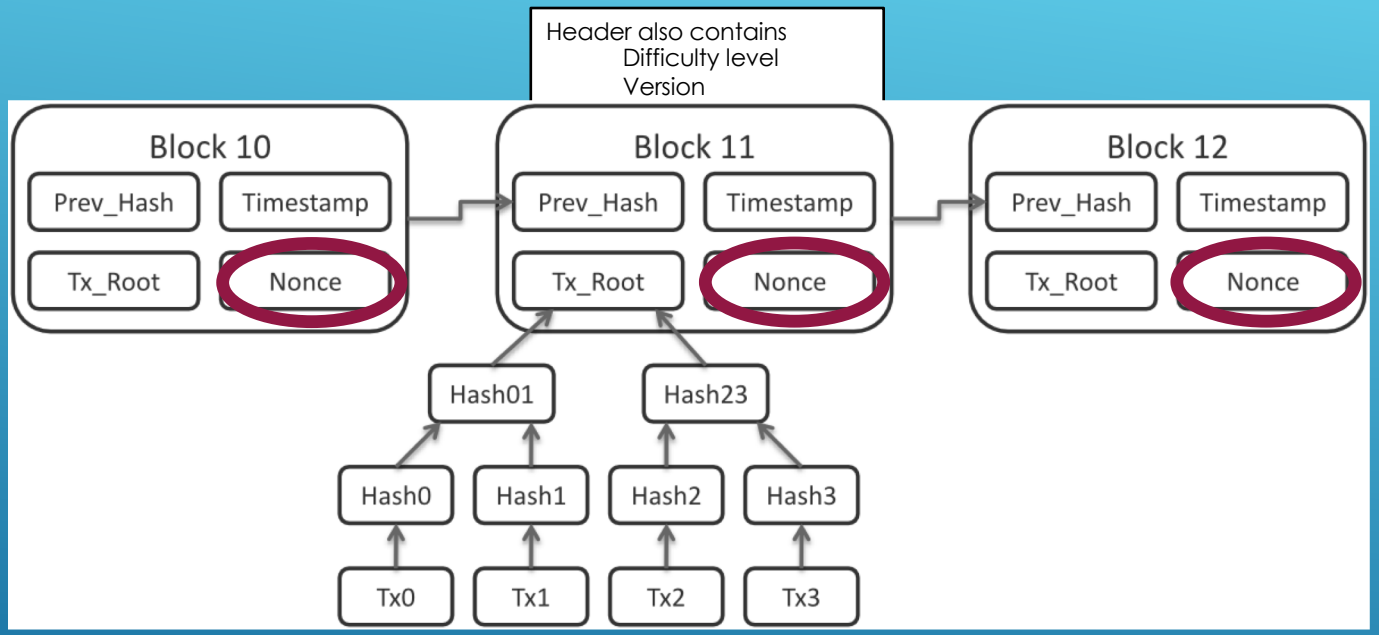
CRYPTOGRAPHIC HASH FUNCTIONS

- Individual transactions are cryptographically hashed
- Hashing is the process of converting data of arbitrary size to a fixed size
- Hashing properties
  - Easy to calculate for any input
  - Extremely difficult to identify the input if given the hash
  - Highly improbably that a hash will be the same for 2 slightly different messages
- Cryptographic hashing appears random but is deterministic
- Go to http://passwordsgenerator.net/sha256-hash-generator/ and try!



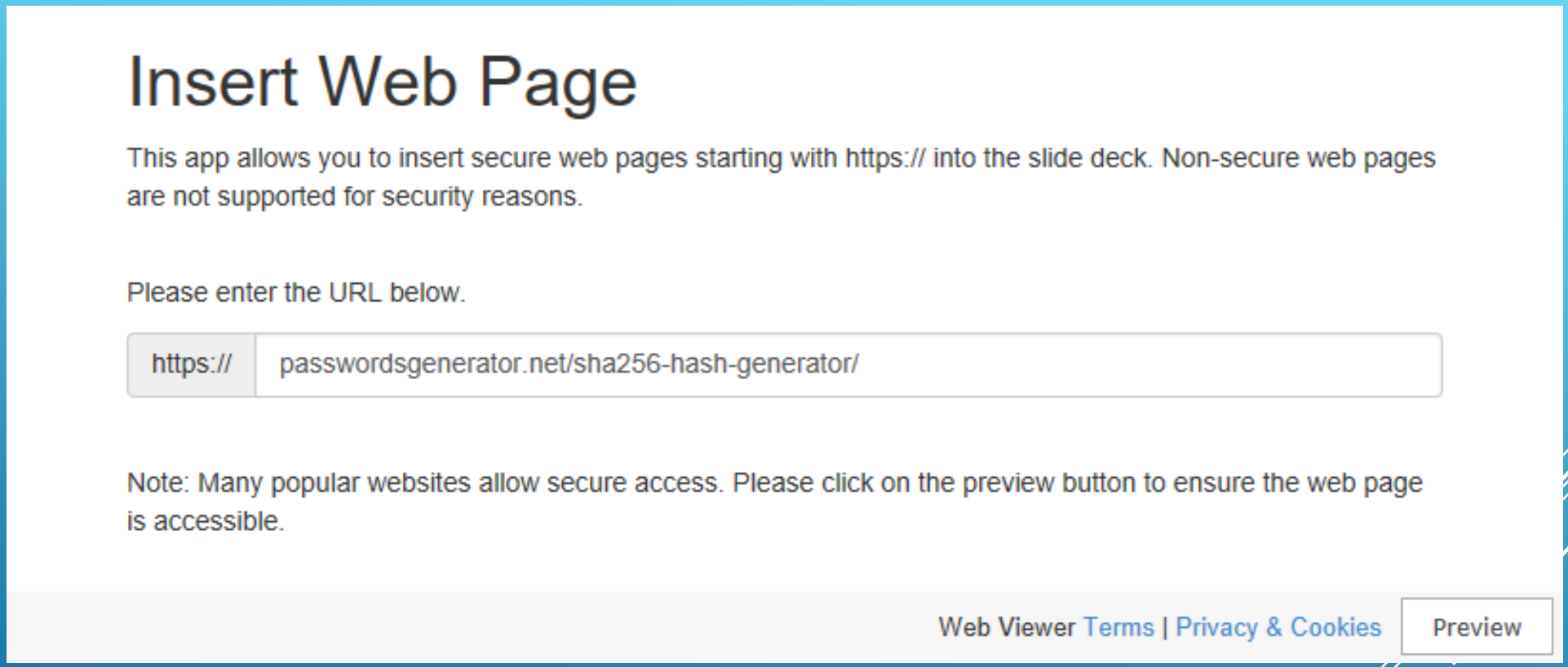


CRYPTOGRAPHY



BITCOIN BLOCKCHAIN HEADER

Image credit: Wikimedia Commons



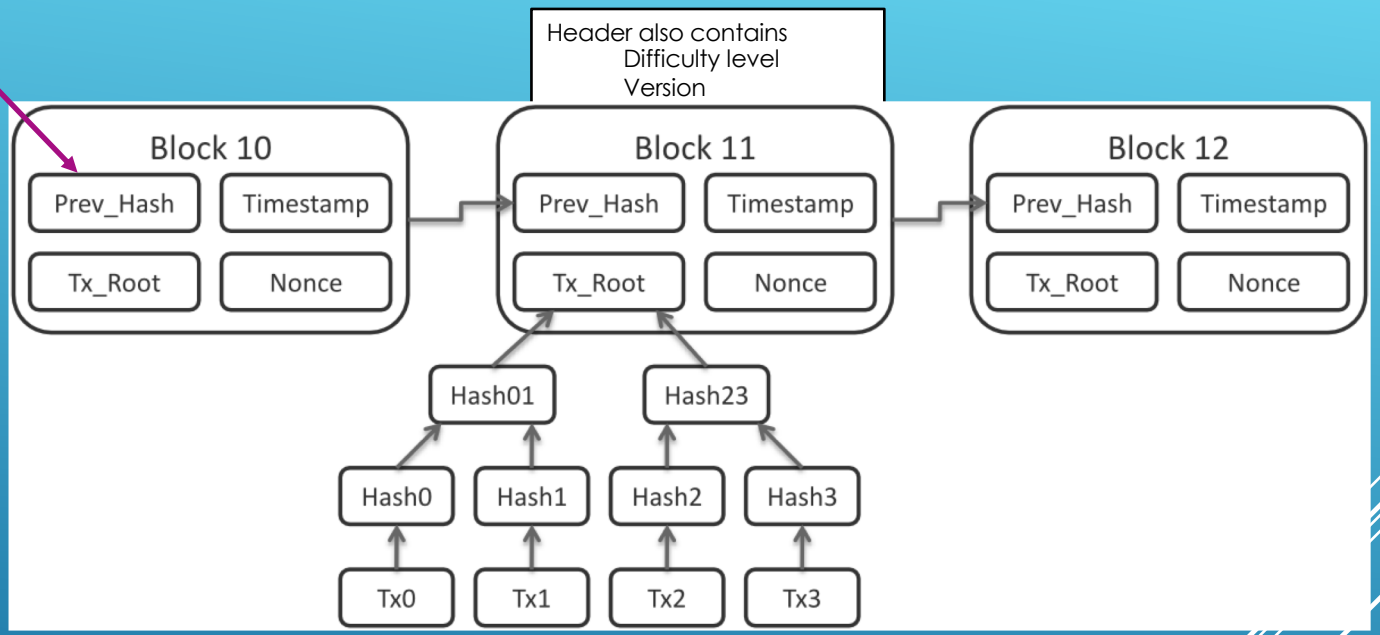
SHA 256 HASH GENERATOR

HTTP://PASSWORDSGENERATOR.NET/SHA256-HASH-GENERATOR/

Currently, nonce should yield 18 leading 0's

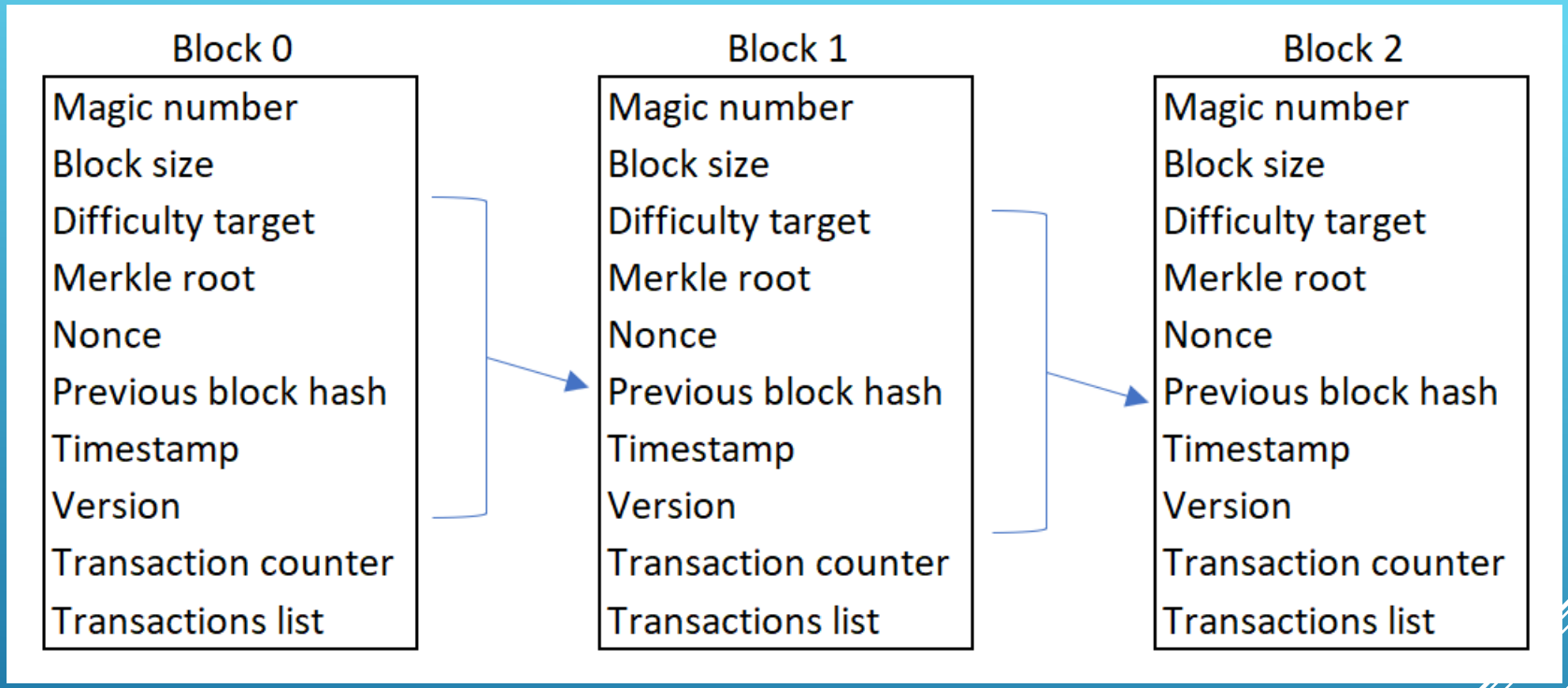
A hash of the following information from the previous block:

- Version
- Previous block's hash
- Merkle root
- Time stamp
- Difficulty (hexed to bits)
- Nonce

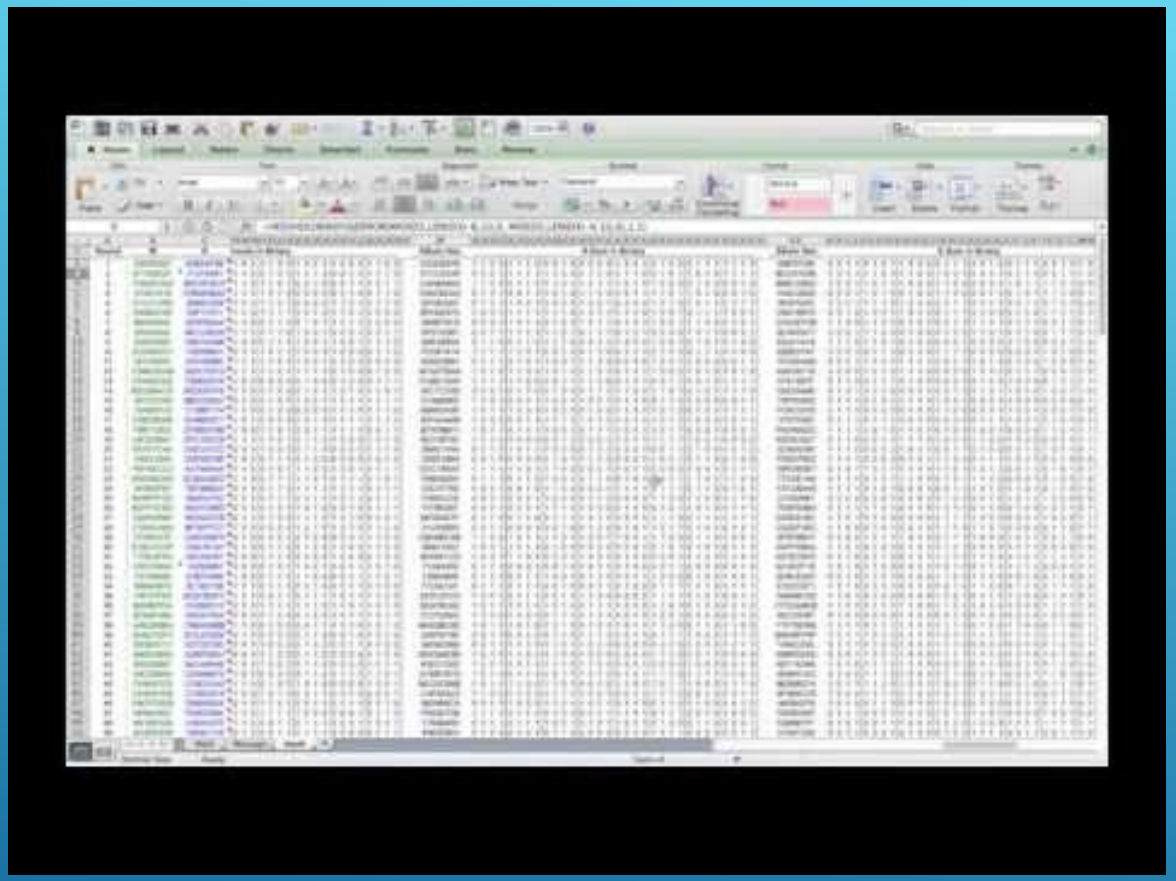


BITCOIN BLOCKCHAIN HEADER

Image credit: Wikimedia Commons



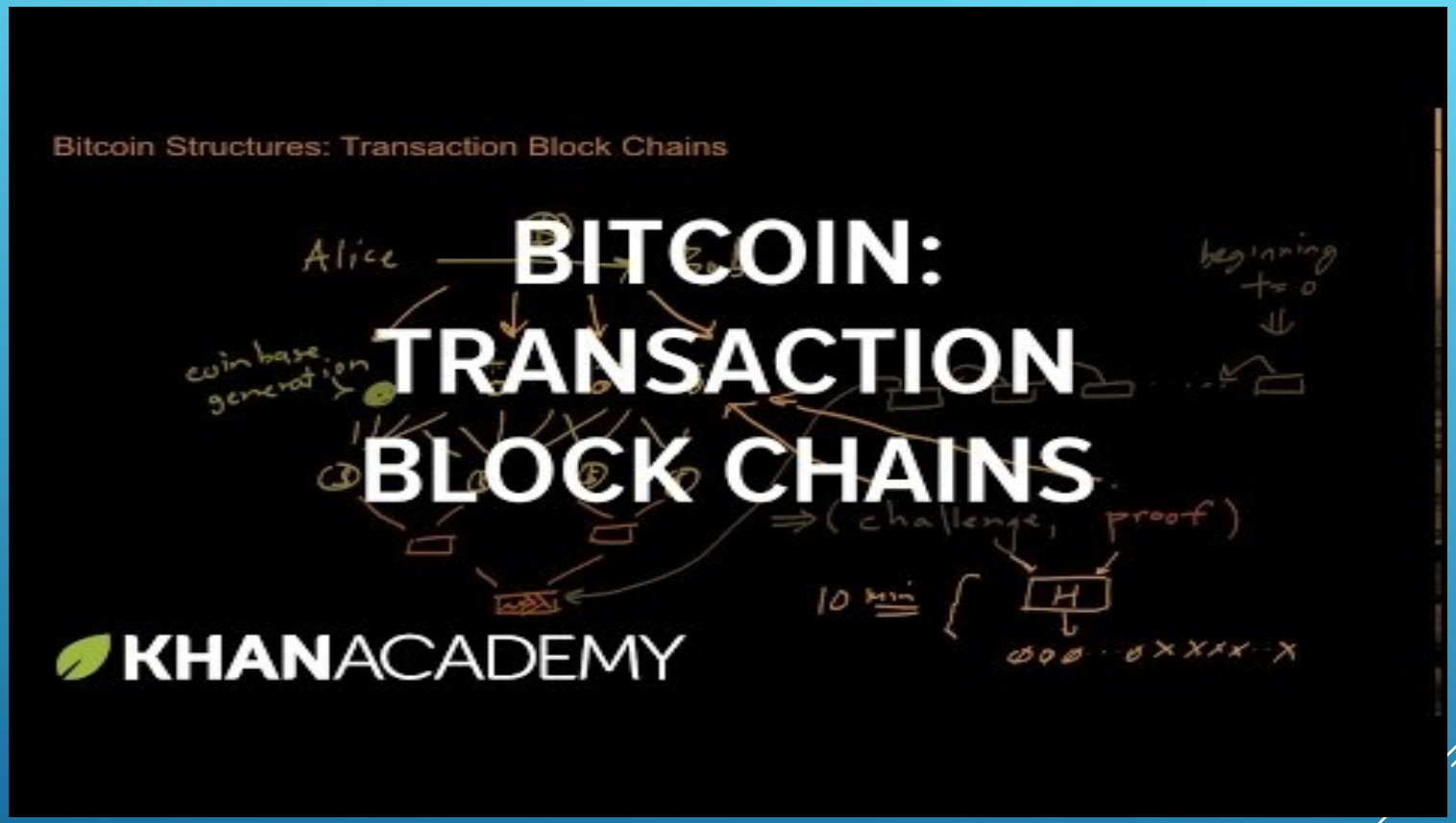
CONNECTING THE BLOCKS



MINING BITCOIN WITH EXCEL

- Open Bitcoin Proof of Work Algorithm.xlsx

LET'S CONFIRM A NONCE

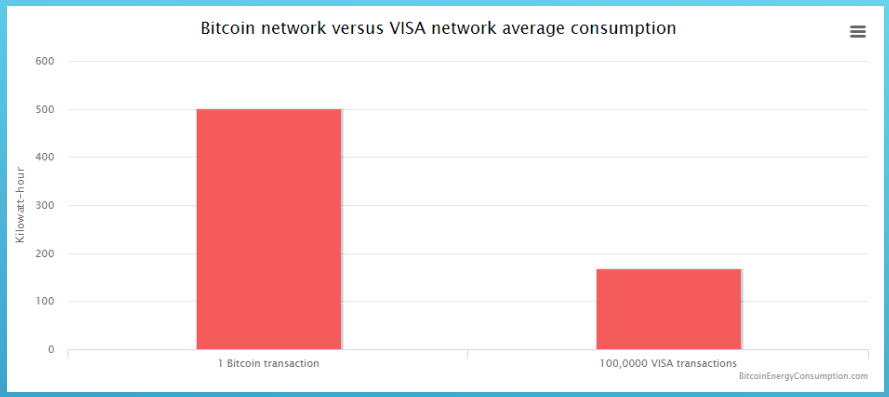

Bitcoin Structures: Transaction Block Chains
BITCOIN:
TRANSACTION
BLOCK CHAINS
Alice
coinbase generation
beginning tx 0
(challenge, proof)
10 min
KHANACADEMY

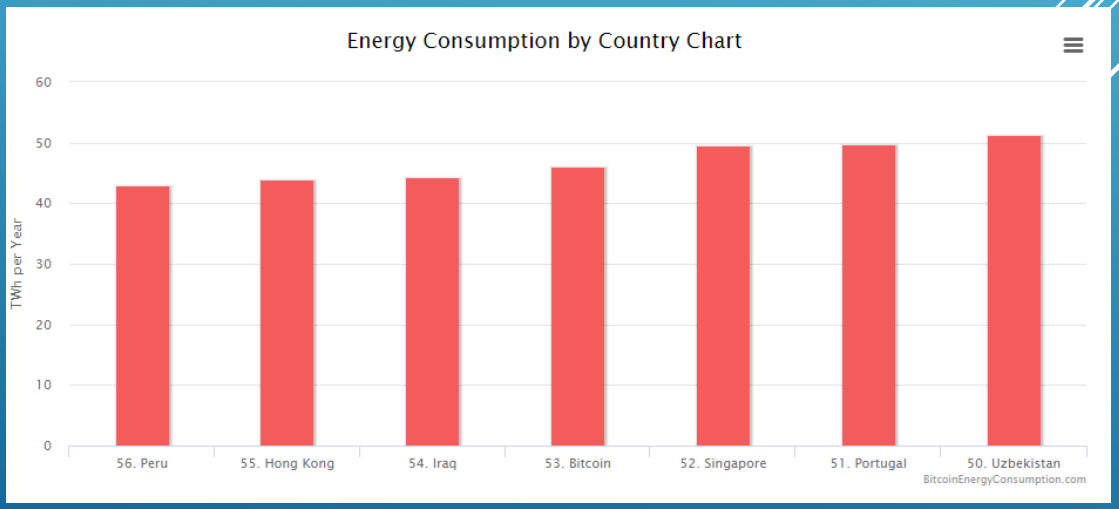
INCENTIVES

The world's cryptocurrency mining uses more electricity than Iceland

By Mark Coppock — Posted on July 7, 2017 11:32 am

- Bitcoin miners are rewarded for their efforts
  - Transaction fees
  - Reward of12.5 BTC (halved every 210k blocks)
  - Rewards will end circa 2140





INCENTIVES

- CPU time and electricity
  - ASICs (Application Specific Integrated Circuit)
  - Mining Pools

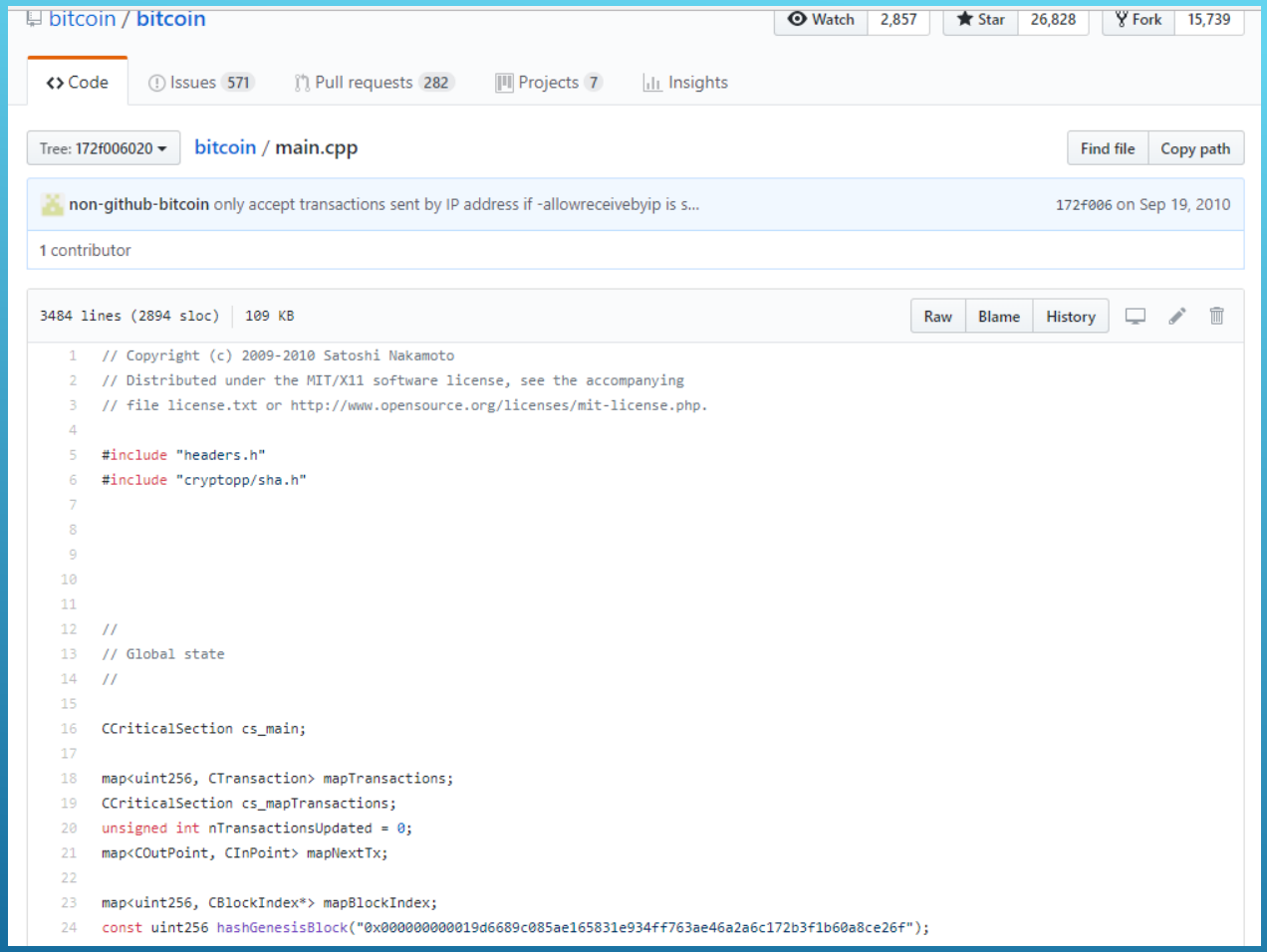
Exercise: Find an online calculator and determine profitability

Image credit: Wikimedia Commons

WHAT GIVES BITCOIN VALUE?

- Limited circulation
- Supply and demand
  - Supply
    - Limited to 21,000,000 coins (1/100,000,000 is called a Satoshi)
  - Demand comes from the following characteristics
    - Speculation
    - Deregulated
    - Anonymous
    - Legitimate transactions (e.g., Microsoft, NewEgg, Jay Z, 50 Cent*, etc.)
    - Illicit transactions

* When listing his assets in a bankruptcy filing, 50 Cent denied ownership of bitcoin.



Written in C++

THE BITCOIN BLOCKCHAIN

Blocks by date.

Height	Timestamp	Transactions	Mined by	Size
507035	Jan 31, 2018 9:20:35 PM	702		991502
507034	Jan 31, 2018 9:16:08 PM	793		992262
507033	Jan 31, 2018 9:10:31 PM	461		992948
507032	Jan 31, 2018 9:07:39 PM	584		992221
507031	Jan 31, 2018 9:03:17 PM	626		988332
507030	Jan 31, 2018 8:59:44 PM	283		996986
507029	Jan 31, 2018 8:58:15 PM	1372	AntMiner	989033
507028	Jan 31, 2018 8:49:04 PM	1892	AntMiner	982013
507027	Jan 31, 2018 8:42:11 PM	2477		979314
507026	Jan 31, 2018 8:35:57 PM	2164	BTCC Pool	982633

Blockchain.info, TradeBlock.com, BlockExplorer.com

BITCOIN LEDGER

BITCOIN TECHNOLOGY NOVEMBER 06, 2017 23:53

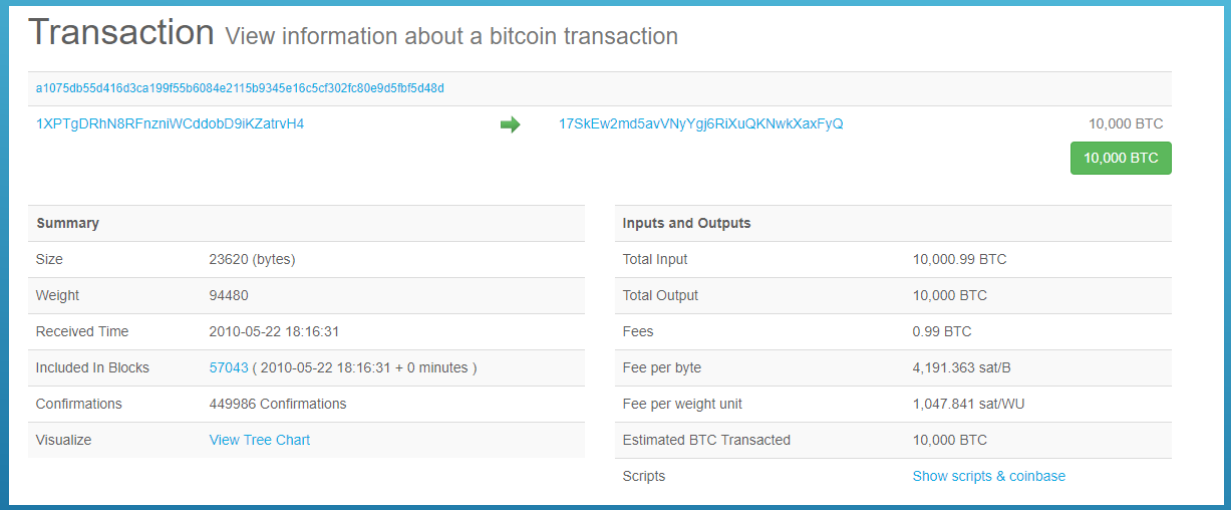
Stampery Demonstrates Timestamping on Public Blockchains like Bitcoin and Litecoin

- Stampery allows us to create an "immutable record of existence, integrity and ownership" by immortalizing documents on the blockchain.
- Let's do it! Go to https://stamp.io/ and create an account.

LET'S ADD TO THE LEDGER

THE FABULOUSLY EXPENSIVE PIZZA

- On May 17th 2010 Laszlo Hanyecz made the first documented purchase of a good with bitcoin…two Domino's pizzas. How much money would Laszlo have in USD today if he had saved his bitcoin?



Transaction View information about a bitcoin transaction

a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

1XPTgDRhN8RFnznWCddobD9iKZatrvH4 → 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ 10,000 BTC

10,000 BTC

Summary	
Size	23620 (bytes)
Weight	94480
Received Time	2010-05-22 18:16:31
Included In Blocks	57043 (2010-05-22 18:16:31 + 0 minutes)
Confirmations	449986 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	10,000.99 BTC
Total Output	10,000 BTC
Fees	0.99 BTC
Fee per byte	4,191.363 sat/B
Fee per weight unit	1,047.841 sat/WU
Estimated BTC Transacted	10,000 BTC
Scripts	Show scripts & coinbase

Bitcoin Forum
https://bitcointalk.org/?topic=137.0

BUYING BITCOIN

- Bitcoin exchanges
  - Coinbase
  - Bitfinex
  - Kraken
  - Bitstamp
  - Many others
- Bitcoin ATM's

Image credit: Wikimedia Commons

STORING BITCOIN

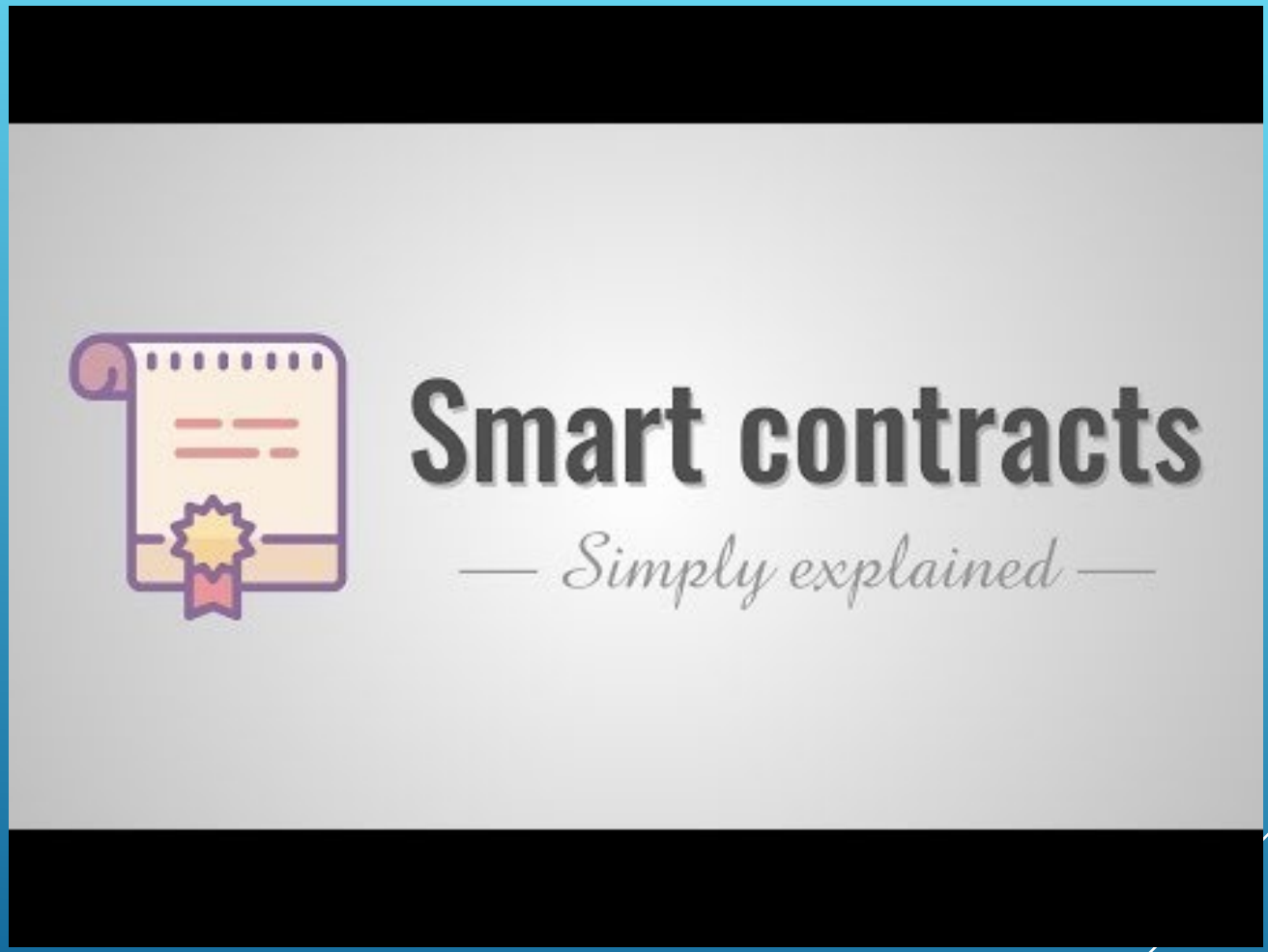
- Wallets store your public and private keys
- Hot wallets
  - Web wallets (exchange wallets)
  - Desktop wallets
  - Mobile wallets
- Hot wallets are subject to hacking and other vulnerabilities

- Cold Wallets
  - Hardware (Keepkey, Ledger Nano S, Trezor)
  - Paper wallets

ETHEREUM

- Ethereum is also a cryptocurrency.
- Designed by Vitalik Butterin
- More robust at handling smart contracts than Bitcoin

Image Credit: Wikimedia Commons



SMART CONTRACTS

SMART CONTRACTS CHARACTERISTICS

- Automated execution based on predetermined software code
  - No third party is required to execute the contract
  - However, reliance on third party data is potentially problematic (e.g., weather.com, interest rates)
- Reliable
  - e.g., grain contract adjusts price based on preestablished parameters if weather dips
- Encrypted contract detail

BENEFITS OF SMART CONTRACTS

- Lower costs
- Possibly fewer third parties
- Increased speeds
- Higher accuracy since coded
- Lower execution risk (execution is managed automatically)

LIMITATIONS ON SMART CONTRACTS

- Delaware and Arizona are the only 2 states that have laws that allow enforcement of smart contracts.
- Some reliance on third party information
- No legal recourse if something goes haywire since the blockchain can't be modified.
- On a public blockchain there is risk that someone could identify the parties involved and/or divulge proprietary information.

- Not anonymous. Businesses must have additional information about their counterparty (e.g., to comply with tax, money laundering laws, etc.)
- Businesses demand smart contracts
- Business blockchains are more transparent since the details are imperative

DIFFERENCES BETWEEN CURRENCY BLOCKCHAINS AND ENTERPRISE BLOCKCHAINS

ENTERPRISE APPLICATIONS

- What makes the blockchain useful for businesses?
  - Track materials, inventory, etc.
  - Track effort, direct labor hours, etc.
  - Track money, transfers, payments, receivables, payables
  - Track provenance

PROVENANCE

1. Provenance provides us with a record of ownership
    A. Diamonds
    B. Food (Fish) – Salmonella outbreaks, and other health concerns
    C. Merchandise
    D. Supply chain
    E. Collectibles

2. Likely to incorporate sensory data
    A. Temperature
    B. Location

IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com

Roger Aitken, CONTRIBUTOR
FULL BIO

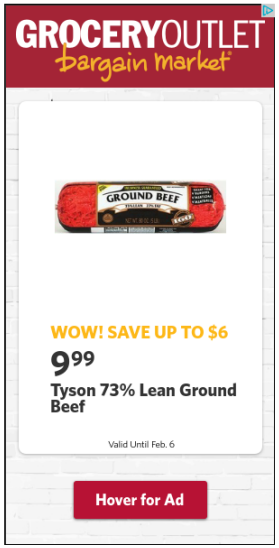
Opinions expressed by Forbes Contributors are their own.

In further move to apply Blockchain technology for food traceability to support offline and online consumers, IBM, Walmart and Nasdaq-listed Chinese retailer JD.com together with Tsinghua University National Engineering Laboratory for E-Commerce Technologies have announced a Blockchain Food Safety Alliance collaboration to improve food tracking and safety in China.

By collaborating with one of China's largest retailers, JD.com, a member of the NASDAQ-100 and a Fortune Global 500 company, and their suppliers, the latest effort is touted as helping to bring a safer food supply to China, and an extension of the work initiated by Walmart and IBM earlier this year in August in the US.

Through the latter initiative, ten food suppliers and retailers - Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart - signalled their intention to collaborate. And, Walmart's food safety solution has been working with IBM and its Blockchain Platform.

That initiative is designed to bring the requisite efficiency, transparency and authenticity to food supply chains around the world. The solution from 'Big Blue' is global - reflecting the global nature of supply chains.



PROVENANCE

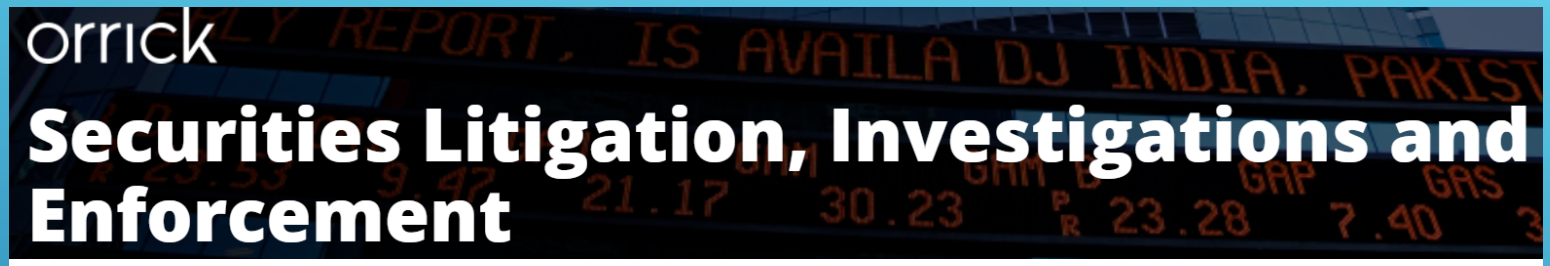
Source: Forbes.com

FEDERAL AGENCY BLOCKCHAIN USE CASES

Federal agencies blockchain use cases

- Financial management
- Procurement
- IT asset and supply chain management
- Patents, Trademarks, Copyrights, Royalties
- Government-issued credentials like visas, passports, SSN and birth certificates
- Federal personnel workforce data
- Appropriated funds
- Federal assistance and foreign aid delivery

From <https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain>



- **Data security:** Blockchain uses decentralized record keeping and advances in cryptography to safeguard data and protect against cyberattacks.
- **Investor Autonomy:** End-users will be able to control who receives and has permission to access their financial data, investment and transaction history.
- **Efficiency:** Blockchain speeds up transactions by eliminating the need for a centralized authority to act as a clearinghouse for financial transactions. It can also reduce transaction costs by replacing clunky accounting and payment networks.
- **Real-Time Regulation:** Regulators will be able to detect and counteract predatory and deceptive practices at a much earlier stage because transaction data becomes available on the Blockchain ledger instantaneously.

BLOCKCHAIN APPLICATIONS IN FINTECH

Source: https://blogs.orrick.com/securities-litigation/2017/10/18/the-sec-wants-to-know-whats-next-for-blockchain-are-you-keeping-up/

REGULATOR INTEREST AND CONCERNS

- Potential Regulator Oversight
  - Regulators can access transaction detail
  - Regulators can monitor transactions in real time
  - Regulators could prevent consensus
  - Regulators could unveil actors seeking anonymity

I. Financial Instruments, Records and Models

- Currency
- Private equities
- Public equities
- Bonds
- Derivatives (futures, forwards, swaps, options and more complex variations)
- Voting rights associated with any of the above
- Commodities
- Spending records
- Trading records
- Mortgage / loan records
- Servicing records
- Crowd-funding
- Micro-finance
- Micro-charity

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

II. Public Records

- Land titles
- Vehicle registries
- Business license
- Business incorporation / dissolution records
- Business ownership records
- Regulatory records
- Criminal records
- Passports
- Government/non-profit accounting/transparency
- Death certificates
- Voter IDs
- Voting
- Health / Safety Inspections
- Building permits
- Gun permits
- Forensic evidence
- Court records
- Voting records
- Non-profit records
- Birth certificates

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

III. Private Contracts

- Contracts
- Signatures
- Wills
- Trusts
- Escrows
- GPS trails (personal)

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

IV. Other Semi-Public Records

- Degree
- Certifications
- Learning Outcomes
- Grades
- HR records (salary, performance reviews, accomplishment)
- Medical records
- Accounting records
- Business transaction records
- Genome data
- GPS trails (institutional)
- Delivery records
- Arbitration

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

V. Physical Asset Keys

- Home / apartment keys
- Vacation home / timeshare keys
- Hotel room keys
- Car keys
- Rental car keys
- Leased cars keys
- Locker keys
- Safety deposit box keys
- Package delivery (split key between delivery firm and receiver)
- Betting records
- Fantasy sports records

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

VI. Intangibles

- Coupons
- Vouchers
- Reservations (restaurants, hotels, queues, etc.)
- Movie tickets
- Patents
- Copyrights
- Trademarks
- Software licenses
- Videogame licenses
- Music/movie/book licenses (DRM)
- Domain names
- Online identities
- Proof of authorship / Proof of prior art

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

VII. Other

- Documentary records (photos, audio, video)
- Data records (sports scores, temperature, etc.)
- Sim Cards
- GPS network identity
- Gun unlock codes
- Weapons unlock codes
- Nuclear launch codes
- Spam control (micro-payments for posting)

BLOCKCHAIN APPLICATIONS

Source: ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list

Discussion: can you brainstorm some income tax applications for the blockchain?

BLOCKCHAIN APPLICATIONS

CRYPTOCURRENCY REGULATOR CONCERNS

- The SEC has seen filings from several registered funds seeking to hold cryptocurrencies.
  - Would retail investors have sufficient information to consider these products and to understand the risks?
  - When thinking about cryptocurrencies and other blockchain offerings as fund assets, are differences in their features important?
  - How would these funds fit into the existing regulatory scheme?
  - What regulatory structure or structures apply to the market for the underlying instrument?

From <https://www.sec.gov/news/speech/blass-keynote-ici-securities-law-developments-conference-2017>

QUESTIONS FOR DISCUSSION

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!*

- 1. How does someone in the blockchain know whether to approve a transaction?

A: Consensus is the process by which a miner proposes a solution to a cryptographic puzzle, the block he/she resolved is then accepted by participating nodes, and the state of the ledger is updated. The puzzle itself is a cryptographic algorithm that is very difficult to solve, but easy to verify.

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 2. How and why do forks occur? If the blockchain is immutable why are their examples of changes to the historic ledger?

A: Hard forks occur when there is a change in the blockchain protocol, leading to a divergence between the nodes that adapt the new protocol and those that do not. It is not backwards compatible. In contrast, a soft fork is backwards compatible. These forks can occur for a variety of reasons including scalability, privacy, safety, etc. A recent example includes the fork of bitcoin to form bitcoin cash which allows for a block size of 8mb vs. 1mb.

Immutability is a characteristic of the blockchain but it can be circumvented. Ethereum experienced a hard fork as a way of recouping millions of dollars that had been stolen.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 3. The blockchain invites many parties to approve transactions. Why is it superior to having one third party?

A: Decentralization eliminates the need to put all trust in one party. The blockchain is decentralized and does not require that nodes be entrusted.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 4. When bitcoin are completely mined (22 million), what will be the incentive to miners?

A: Miners will continue to receive transaction fees. Transactions fees can increase if necessary, and with scalability (increased use) the number of transactions will increase. Lower mining costs can also lower the compensation miners demand.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 5. How do participants approve transactions if they are encrypted?

A: An encrypted private key is required, and a validation process ensures that adequate funds are in place.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

QUESTIONS FOR DISCUSSION

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 6. Looking at the private blockchain it seems that it has the power to reduce cost and improve controls. What potential use cases can you identify for private blockchains?

Supply chain / Provenance. Forbes magazine reported that Walmart put their supply chain for mangos on the blockchain to track provenance.

Title searches, transactions between banks, etc.

Another use case, Delaware allows stock ownership to be accounted for using blockchain. This could allow proxy voting and dividend payments would be more accurate since it would be more clear as to who owns the shares on a given date/time.

Audit Application: A/R verification process could be possible

Transactions between banks such as syndicated loans.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 7. How is a permissioned blockchain different than a permissionless Blockchain?

A: A permissionless blockchain is decentralized, anonymous, and equally accessible to all nodes. Level of trust is low or nonexistent. A permissioned blockchain is more centralized, lacks anonymity, and has a high level of trust. For these reasons, the method utilized for consensus is likely to differ.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 8. How do people convert dollars to bitcoin?

A: Generally, buy bitcoin from an exchange.

The process of acquiring bitcoin depends on the country. Japan has a loosely regulated market because of the Mt. Gox debacle (850,000 bitcoins "disappeared" in 2014).

Exchanges exist but since they are unregulated there are often different prices (opportunity for arbitrage).

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 9. How do the smart contract actually work? Is there a written contract? How is it in the blockchain?

A: The details of the contract are programmed into the blockchain. It is not as robust a traditional contract because it is not easily modified.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 10. Is there a role of a miner on a permissioned blockchain?

A: No. Not necessary because you know the parties and have trust and compensating someone adds cost.

QUESTIONS FOR DISCUSSION

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

QUESTIONS FOR DISCUSSION

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 11. What if there is a mistake in the blockchain who do you contact? How do your rectify a problem?

A: There is little you can do. The money will move because it is based on an algorithm. On a permissioned blockchain it is easier since you can contact the parties involved and resolve the concern.

Theft, error, or ransom money are irreversible unless there is consensus to alter the state of the ledger.

- Note: Answers provided in these slides either reflect the actual response provided by FASAC, or they were constructed by the authors.

QUESTIONS FOR DISCUSSION

These are actual questions raised by participants at a Financial Accounting Standards Advisory Council meeting, held on December 14, 2017. Let's answer them!

- 12. Can you think of how the adoption of blockchain might impact accounting treatment (i.e., changed to GAAP, or other regulations)?

A: Mandated accounting treatment could change once we can more easily track transactions. For example the retail inventory method is permitted because of the recognized difficulty in inventory costing using alternative means. Maybe with more precise tracking of the supply chain, the acceptability of this method will be reconsidered.

Should we allow LIFO, FIFO, etc. if there is a low cost of adopting a more accurate system? Think about how overhead application is estimated. This could lead to changes in accounting practices.

Voluntary disclosures: Supply chain application of the blockchain could aid in allowing for more precision in accounting disclosure. As the cost of computing has gone down an increase in voluntary disclosures has occurred. The information tracked by the blockchain could result in much more voluntary information disclosure (e.g., provenance, etc.).

BLOCKCHAIN AND FUTURE FINANCIAL REPORTING

- How will increase use of blockchain technologies influence financial reporting requirements?

1. The nature of the information required (e.g., potentially more rollforwards and quantitative information; less qualitative information)

2. The amount of detail required (would investors use more granular information about individual transactions; impact on the cost of equity?)

3. The frequency (e.g., real time updates)? (What are the implications to investors and would this create potential advantages for sophisticated investors?)

4. The use of accounting conventions (accounting for transactions vs. estimations)

Source: http://www.fasb.org/cs/ContentServer?c=Document_C&cid=1176169665221&d=&pagename=FASB%2FDocument_C%2FDocumentPage_

How has (or will) the application of blockchain technologies (or other technologies, such as artificial intelligence) change the processes around preparing financial statements, program resources, and timing/frequency of delivering financial information? Specifically:

- A. In the next 5 years, how likely is that we will see organizations utilize a blockchain between their customers and vendors?
- B. How prevalent will blockchain be for tracking stockholders for voting and dividend purposes?
- C. If more supply chains move to a blockchain based solution with their vendors, how does this alter the risk and process?

THINK ABOUT THE FUTURE

Source: http://www.fasb.org/cs/ContentServer?c=Document_C&cid=1176169665221&d=&pagename=FASB%2FDocument_C%2FDocumentPage_

What are the impediments (or catalysts) to companies adopting and investing in blockchain (or other technologies)?

- a) The anticipated costs (how would smart contracts change the costs in the financial reporting systems?)
- b) The regulatory status and regulation
- c) Use by peers/competitors
- d) The anticipated pace of technology advances (and potential obsolescence).

THINK ABOUT THE FUTURE

Source: http://www.fasb.org/cs/ContentServer?c=Document_C&cid=1176169665221&d=&pagename=FASB%2FDocument_C%2FDocumentPage_

IMPACT ON AUDITORS

ACCOUNTING FOR CRYPTOCURRENCY

The Chamber of Digital Commerce sent a letter to FASB asking them to add cybercurrency issues to the EITF's agenda. There is no specific guidance in existing GAAP regarding how to account for cybercurrencies. Referencing extant GAAP, an argument for at least 4 alternative accounting treatments can be advanced:

Argument 1: Digital currencies should be accounted for under ASC 305, Cash and Cash Equivalents.

Argument 2: Digital currencies should be accounted for as financial instruments under ASC 825, Financial Instruments.

Argument 3:. Digital currencies should be accounted for as intangible assets under ASC 350, Intangibles – Goodwill and Other.

Argument 4: Digital currencies should be accounted for as inventory under ASC 330, Inventory.

Source: http://fasb.org/cs/BlobServer?blobkey=id&blobnocache=true&blobwhere=1175835064585&blobheader=application%2Fpdf&blobheadername2=Content-Length&blobheadername1=Content-Disposition&blobheadervalue2=1273310&blobheadervalue1=filename%3DAR-2017.UNS.001.CHAMBER_OF_DIGITAL_COMMERCE_PERIANNE_BORING.pdf&blobcol=urldata&blobtable=MungoBlobs

ACCOUNTING FOR CRYPTOCURRENCY

Digital currencies should be accounted for under ASC 305, Cash and Cash Equivalents

- Seems to be consistent with the common perception of cybercurrency
- Cash equivalents are short-term, highly liquid investments that have both of the following characteristics:
  A. Readily convertible to known amounts of cash
  B. So near their maturity that they present insignificant risk of changes in value because of changes in interest rates.

➢Question: Cryptocurrency is not legal tender, not issued by a country, and do not have to be accepted. Is that problematic?

Source: http://fasb.org/cs/BlobServer?blobkey=id&blobnocache=true&blobwhere=1175835064585&blobheader=application%2Fpdf&blobheadername2=Content-Length&blobheadername1=Content-Disposition&blobheadervalue2=1273310&blobheadervalue1=filename%3DAR-2017.UNS.001.CHAMBER_OF_DIGITAL_COMMERCE_PERIANNE_BORING.pdf&blobcol=urldata&blobtable=MungoBlobs

ACCOUNTING FOR CRYPTOCURRENCY

Digital currencies should be accounted for as financial instruments under ASC 825, Financial Instruments

- Financial instruments are cash, evidence of an ownership interest in an entity, or a contract that both:
  - Imposes on one entity a contractual obligation either:
    A. 1) To deliver cash or another financial instrument to a second entity
    B. 2) To exchange other financial instruments on potentially unfavorable terms with the second entity.
  - Conveys to that second entity a contractual right either:
    A. 1) To receive cash or another financial instrument from the first entity
    B. 2) To exchange other financial instruments on potentially favorable terms with the first entity. […]

Question: Is cryptocurrency cash? Is it ownership interest in an entity? Is it a contract establishing a right or obligation to deliver or receive cash?

Source: http://fasb.org/cs/BlobServer?blobkey=id&blobnocache=true&blobwhere=1175835064585&blobheader=application%2Fpdf&blobheadername2=Content-Length&blobheadername1=Content-Disposition&blobheadervalue2=1273310&blobheadervalue1=filename%3DAR-2017.UNS.001.CHAMBER_OF_DIGITAL_COMMERCE_PERIANNE_BORING.pdf&blobcol=urldata&blobtable=MungoBlobs

ACCOUNTING FOR CRYPTOCURRENCY

Digital currencies should be accounted for as intangible assets under ASC 350, Intangibles – Goodwill and Other.

- Assets (not including financial assets) that lack physical substance
- Question: Does cryptocurrency meet this definition?

Treating cryptocurrency as an indefinite life intangible asset would require entities to record the currency at original cost and perform annual impairment testing.

Question: Intangibles are recorded at cost less impairment. Does the volatility in cryptocurrency value undermine seem incompatible with cost basis accounting?

Source: http://fasb.org/cs/BlobServer?blobkey=id&blobnocache=true&blobwhere=1175835064585&blobheader=application%2Fpdf&blobheadername2=Content-Length&blobheadername1=Content-Disposition&blobheadervalue2=1273310&blobheadervalue1=filename%3DAR-2017.UNS.001.CHAMBER_OF_DIGITAL_COMMERCE_PERIANNE_BORING.pdf&blobcol=urldata&blobtable=MungoBlobs

ACCOUNTING FOR CRYPTOCURRENCY

Digital currencies should be accounted for as inventory under ASC 330, Inventory.

- Inventory is the aggregate of those items of tangible personal property that have any of the following characteristics :
  A. Held for sale in the ordinary course of business
  B. In process of production for such sale
  C. To be currently consumed in the production of goods or services to be available for sale.

Question: Is Cryptocurrency tangible personal property?

Note: Treating cryptocurrency as inventory would necessitate lower of cost and net realizable value accounting – not fair market value.

Source: http://fasb.org/cs/BlobServer?blobkey=id&blobnocache=true&blobwhere=1175835064585&blobheader=application%2Fpdf&blobheadername2=Content-Length&blobheadername1=Content-Disposition&blobheadervalue2=1273310&blobheadervalue1=filename%3DAR-2017.UNS.001.CHAMBER_OF_DIGITAL_COMMERCE_PERIANNE_BORING.pdf&blobcol=urldata&blobtable=MungoBlobs

TAXATION OF CRYPTOCURRENCY

IRS Notice 2014-21 describes how existing tax principles apply to cryptocurrencies:

- Virtual currency is treated as **property** for tax purposes
- Tax regulations concerning foreign currency gains/losses are irrelevant
- Taxpayers receiving virtual currency as payment must include its fair market value in gross income
- Fair market value is determined based on exchange rate in established market

TAXATION OF CRYPTOCURRENCY

IRS Notice 2014-21 describes how existing tax principles apply to cryptocurrencies:

- Gain or loss is recognized on exchanges
  - Use it to buy something? Calculate the gain/loss!
- Character of gain or loss depends on the nature of the holding
  - Investment (e.g., capital)
  - Business (e.g., inventory, etc.)
  - Personal (e.g., using it for every day purchases)
- The miner of the currency realizes gross income equal to the fair market value at the date of receipt
- The miner is subject to self employment tax unless he/she is acting as an employee
- IRS order Coinbase to turn over identifying information for over 10,000 accounts worth at least $20,000 during 2013 to 2015

LEARNING MORE: BLOCKCHAIN COUNCIL

- A free-to-join membership and advisory council focusing on promoting blockchain implementation and use cases among different organizations
- Great source of information and articles on blockchain, including information on other open source platforms
- https://www.blockchain-council.org/about-us/

AICPA AND BLOCKCHAIN

- The most high profile development of blockchain by the AICPA is the partnership with the Wall Street Blockchain Alliance (WSBA)
- Lots of articles and information on blockchain as well
- Excellent articles there summarizing the changes coming to the profession

What You're Doing Now	The Disruption	Your New Job
Examining statements to ensure accuracy	Blockchain technology inherently ensures accuracy of the ledger	• Examining the accuracy of blockchain inputs to ensure data is based on accurate information • Reviewing blockchain outputs for accuracy to ensure data has not been tampered with
Documenting financial transactions by entering account information	Blockchain captures transactions on the distributed ledger	• Analyzing transactions rather than entering them
Overseeing budget and financial management	Blockchain tracks transactions that can be easily viewed for analysis, and organizations can set rules in blockchain smart contracts to ensure money is spent on what it has been allocated for	• Monitoring and providing real time financial recommendations based on blockchain data • Recommending rules to govern the blockchain • Partnering with business units to provide insights and data interpretation
Summarizing current financial status by collecting information; preparing balance sheet, profit and loss statement, and other reports	Blockchain holds financial information in one location so it is easily collected and prepared into reports	• Using data from the blockchain to generate reports and financial statements • Analyzing reports, as the blockchain creates efficiencies in report generation

AICPA – THE BLOCKCHAIN TRANSITION

Source: http://blog.aicpa.org/2017/11/your-new-blockchain-supported-job-1.html#sthash.MUGSusrX.dpbs

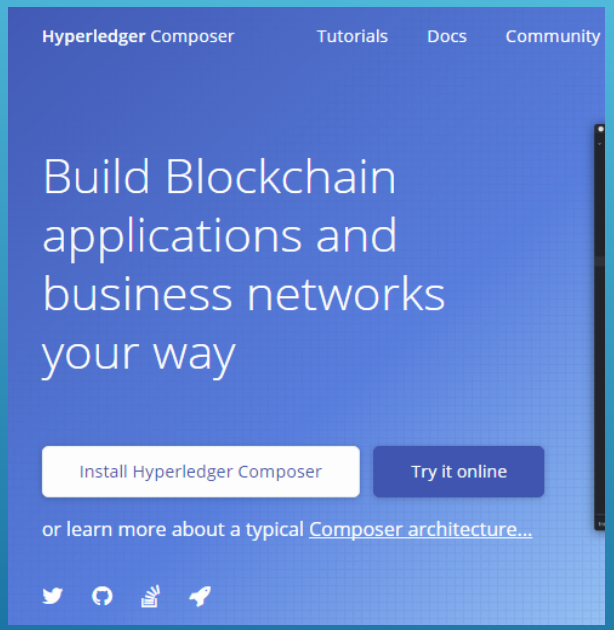
IBM COURSERA

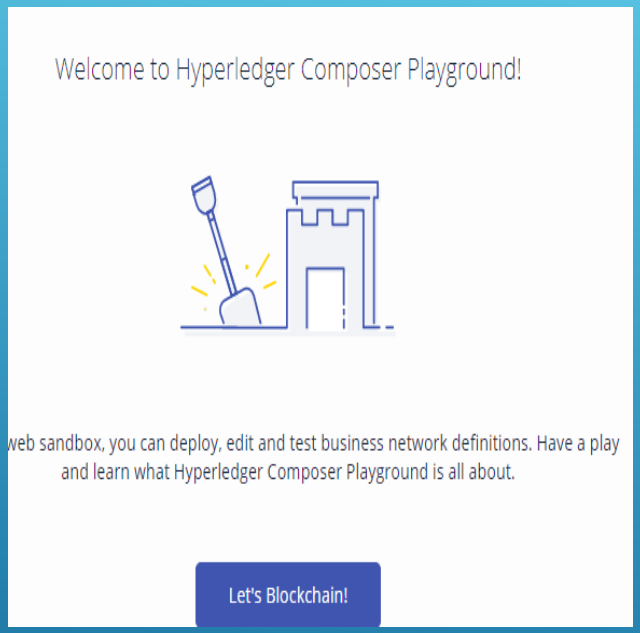
- IBM has partnered with Coursera to put together a course on how to get started with using blockchain
- You can try these courses for free!
- Especially the first part of this course, focusing on concepts and high level applications, is a great introduction
- "IBM Blockchain Foundation for Developers"
- https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers/lecture/DA8WS/ibm-and-hyperledger-relationship-blockchain-for-business

HANDS ON LEARNING

- Reading about topics and attending seminars is great, but what about some hands on practice with these tools?
- Open source platforms are free to use and allow you to experiment and play around with blockchain technology before investing in it significantly
- In other words, you can mess it up and be OK ☺
- Hyperledger is an open source collaborative blockchain platform hosted by The Linux Foundation. It is not cryptocurrency based.

1. https://hyperledger.github.io/composer/stable/index.html
2. http://composer-playground.mybluemix.net/





- You can either install Hyperledger on your device or experiment with it entirely online
- Refer to the accomanying supplementary resources (slides and video) for a step by step walk through on how to build and manipulate a Hyperledger blockchain in real time

HANDS ON LEARNING: HYPERLEDGER COMPOSER

- Refer to the accomanying supplementary resources (slides and video) for a step by step walk through on how to experiment with a Ethereum based blockchain in real time

HANDS ON LEARNING: ETHEREUM BLOCKCHAIN

CONCLUDING VIDEO

Source: Fortune.com