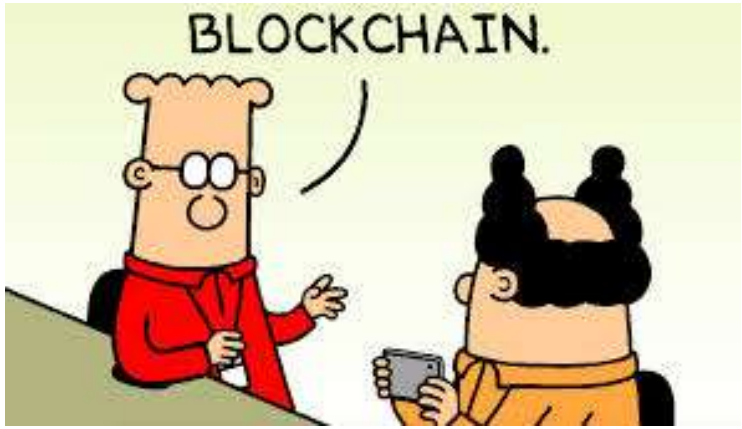
Blockchain, Bitcoin & Ethereum

David McCoy, CPA

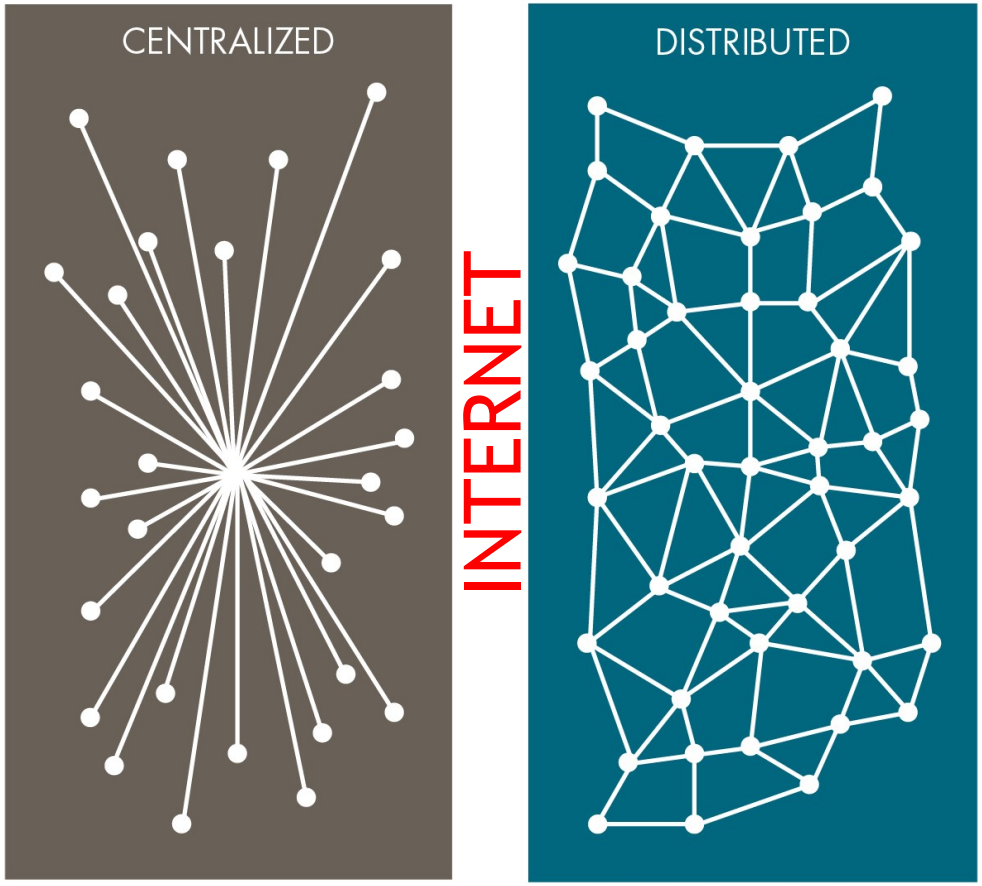

BLOCK CHAIN
TECHNOLOGY



- **Protocol** that runs over the internet (like tcp/ip or http)
- **Blockchain is a shared database** that is **distributed** over a peer-to-peer network. **Open-Source.**
- **Cryptography** and **economic incentives** are built in.
- A key goal is to facilitate transactions between individuals/entities who would otherwise have no means to trust one another – aka **Trust Protocol**

Centralized Network vs. Distributed Network

Centralized is a million times more cost efficient than Distributed



- **Bitcoin & Ethereum**

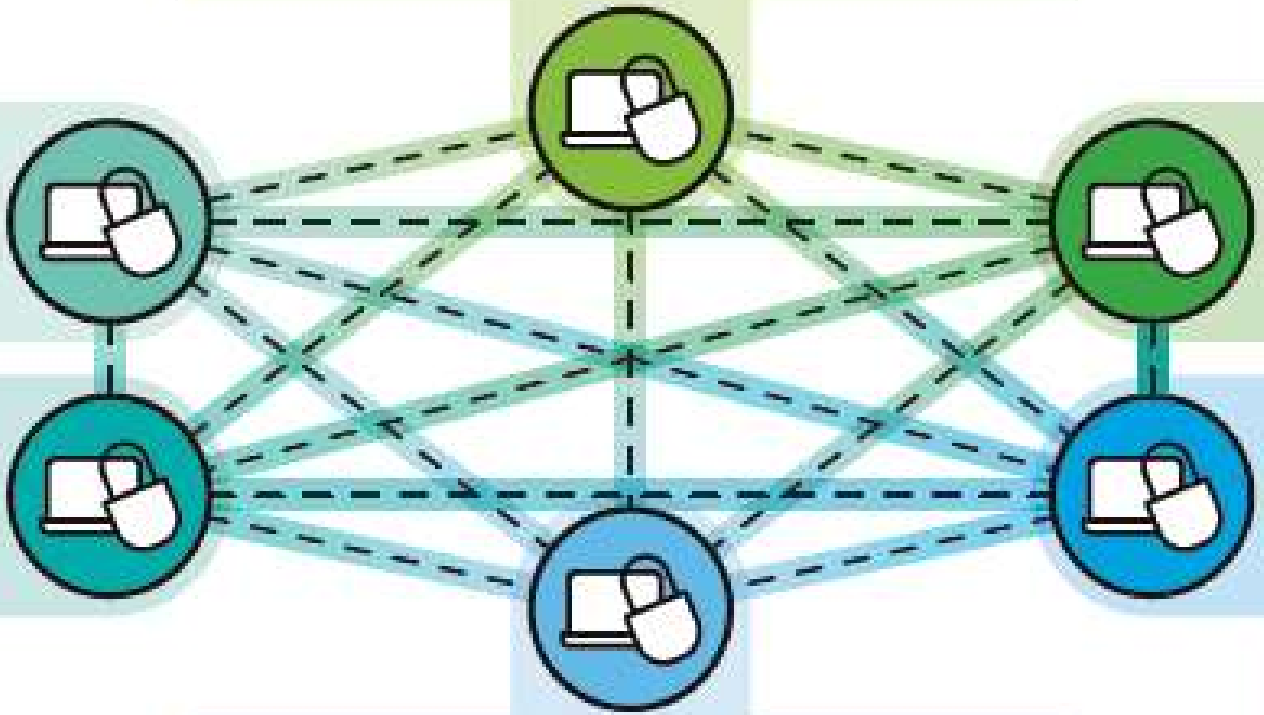
- No single entity controls it
- No central point of failure
- Behaves like a single computer
- Each full node has a copy of the database

Close-up

A **system of computers**, connected via the Internet, in which users at any one computer can receive or send value to another computer

Digital signatures and cryptography is used **to secure** the transfer

It facilitates peer-to-peer transfer of value **without a central intermediary** e.g. a bank



Data is replicated across the systems over a **peer-to-peer** network

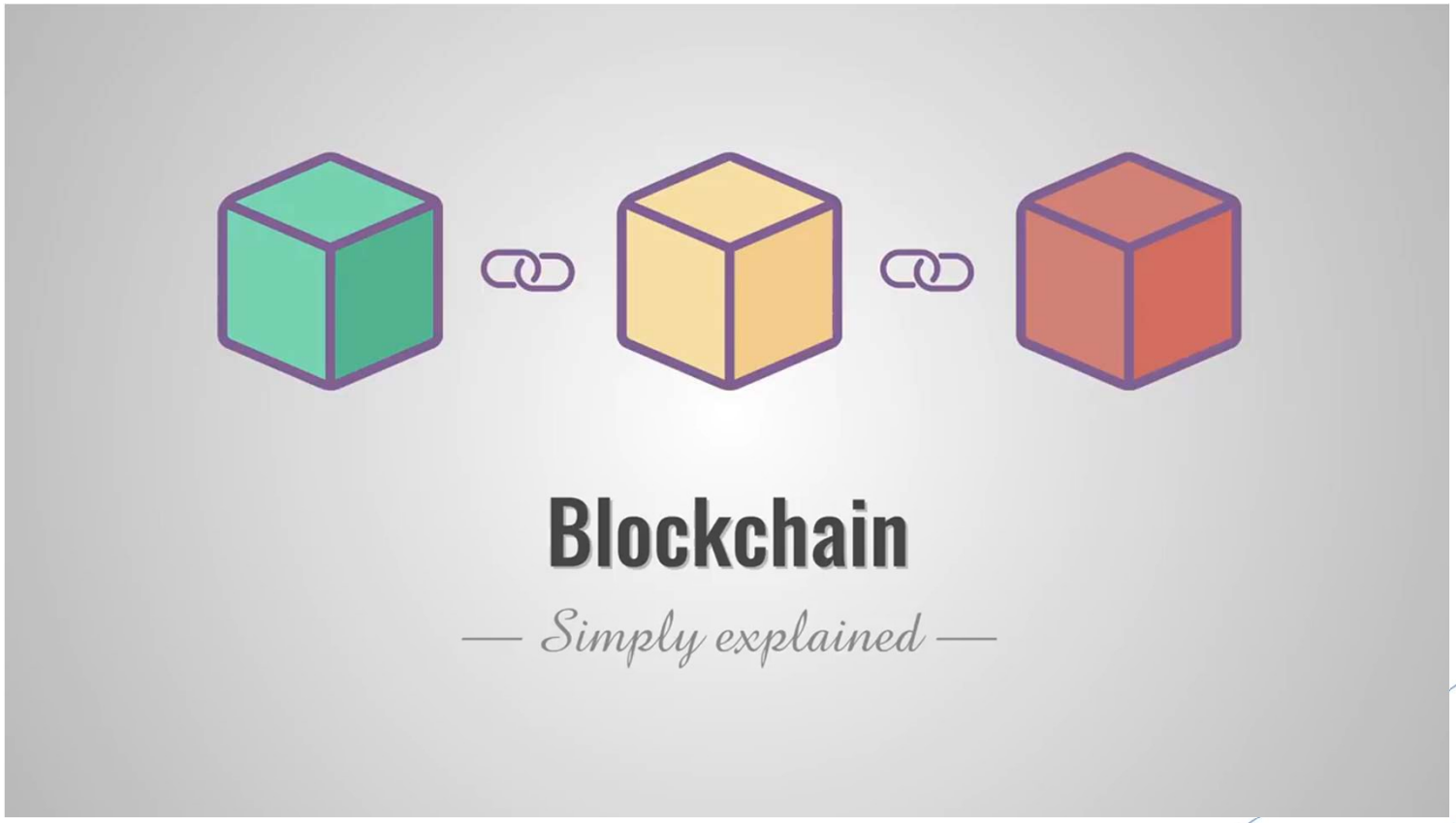
Transactions are recorded in chronological order on a **continuously growing database**

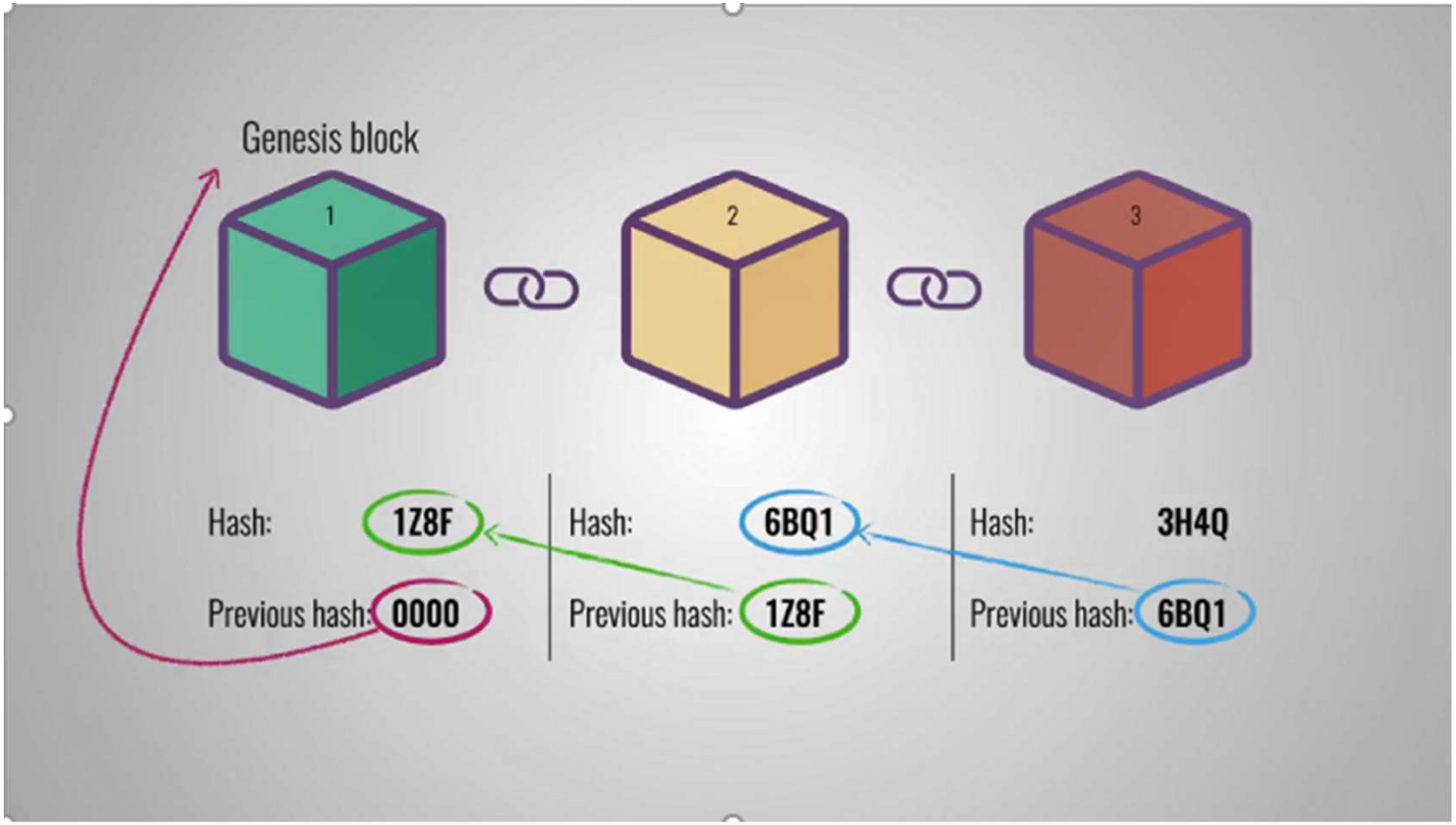
Can be **written** and **read** by certain participants and entries are **permanent, transparent, and searchable**

Some Critical Terms

- Hash : A formula that will take a specific series of numbers and create a single number called a hash total that is unique. That hash total can only be calculated by the specific series of numbers. AND, the specific series of numbers can not be calculated from the hash total.
  - The hash total is unique
  - The specific series of numbers can not be calculated from the hash total
- Proof of Work : Something that is done that demonstrates that a new block in the chain is valid and it can only be done by doing work on that new block. The harder the work is to do, the longer it will take and therefore, the harder it is to add an invalid block to the chain.

Video: Blockchain Security with Hashing Explained




Genesis block
1
2
3
Hash:
1Z8F
Previous hash:
0000
Hash:
6BQ1
Previous hash:
1Z8F
Hash:
3H4Q
Previous hash:
6BQ1

Blockchain Disadvantages

- **Currently too slow to serve a mainstream user base in billions - a scaling solution is needed**
- **Proof of Work** mining calculations are energy intensive
  - Electricity used would power a small country
- Early stage infrastructure (foundation poured & plumbing)
- Changes to the infrastructure require widespread adoption
  - Hard Fork or Soft Fork (backward compatible)
- Steep learning curve, clunky user interfaces, not easy to use
- Different kinds of risks - user is responsible for private key, transactions are not reversible (no stop payment), no dispute arbitration
- BLOCKCHAIN WILL BE DISRUPTIVE (eliminating middlemen)

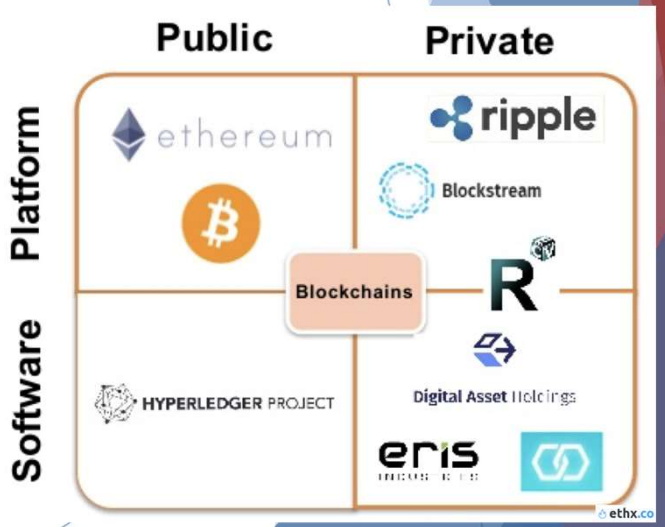
Public vs. Private Blockchains

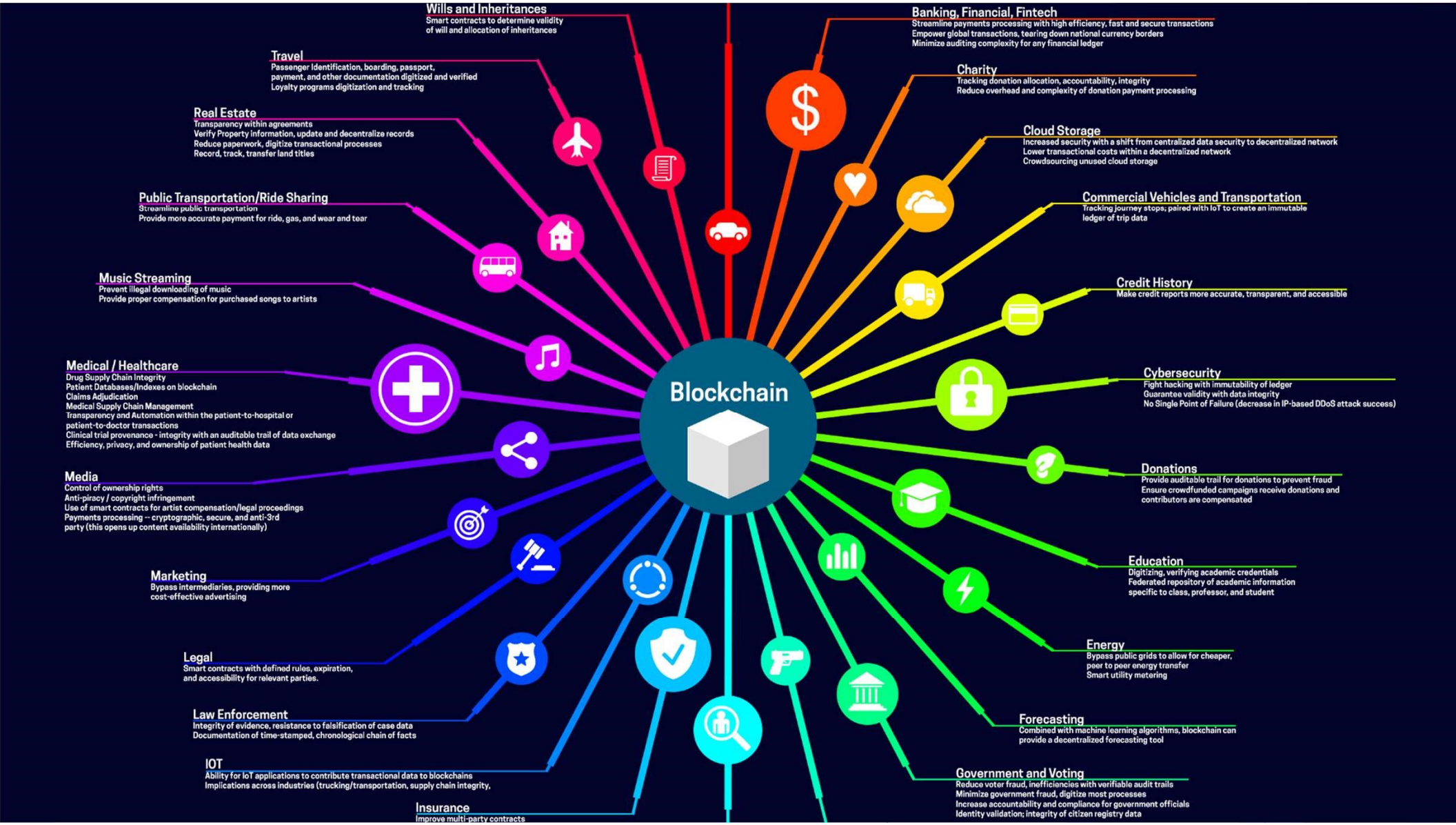
Public (BTC, ETH)

- Many public nodes
- Data transparency
- Throughput is slow
- Public hardware
- Compensates miners in cryptocurrency

Private (Permissioned)

- Only permissioned nodes
- Data confidentiality
- Much faster
- Private enterprise hardware
- May or may not use cryptocurrency (IT budget)




Blockchain
Wills and Inheritances
Smart contracts to determine validity of will and allocation of inheritances
Travel
Passenger Identification, boarding, passport, payment, and other documentation digitized and verified
Loyalty programs digitization and tracking
Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles
Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear
Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists
Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data
Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing -- cryptographic, secure, and anti-3rd party (this opens up content availability internationally)
Marketing
Bypass intermediaries, providing more cost-effective advertising
Legal
Smart contracts with defined rules, expiration, and accessibility for relevant parties.
Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts
IOT
Ability for IoT applications to contribute transactional data to blockchains
Implications across industries (trucking/transportation, supply chain integrity,
Insurance
Improve multi-party contracts
Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger
Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing
Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage
Commercial Vehicles and Transportation
Tracking journey stops, paired with IoT to create an immutable ledger of trip data
Credit History
Make credit reports more accurate, transparent, and accessible
Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)
Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and contributors are compensated
Education
Digitizing, verifying academic credentials
Federated repository of academic information specific to class, professor, and student
Energy
Bypass public grids to allow for cheaper, peer to peer energy transfer
Smart utility metering
Forecasting
Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool
Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data

Video: IBM Fabric / Linux Hyperledger
Private (Permissioned) Blockchain

BLOCKCHAIN Takeaway

- Protocol that runs on the Internet
- Distributed database (shared ledger)
- Entries are timestamped, signed, permanent, transparent and searchable
- Secured by cryptography and consensus mechanisms to achieve trust
- Contiguous chain of blocks containing transactions
- Can transform business processes where trust is critical

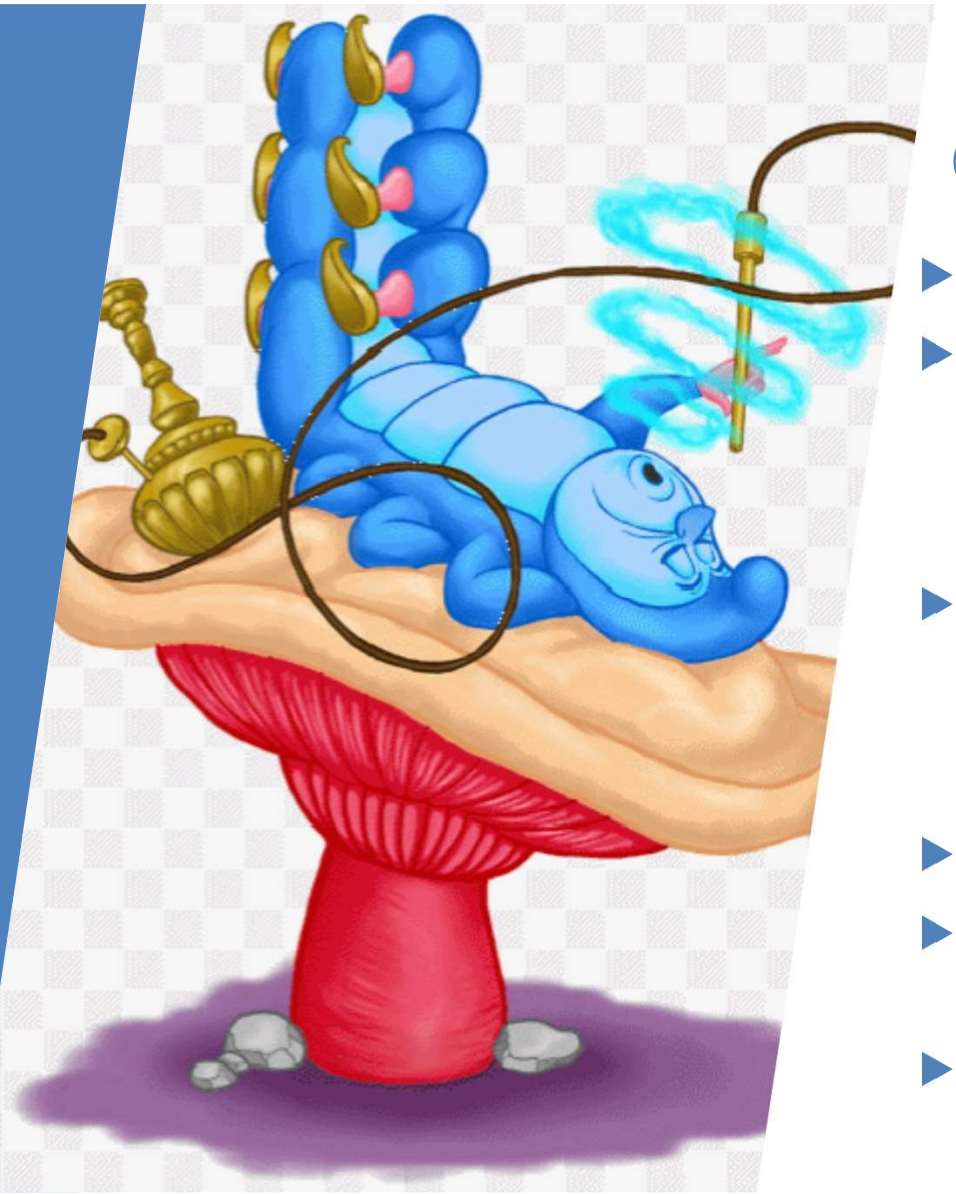
Bitcoin

- Intangible
- Ledger
  - Immutable
  - Permanent
  - Transparent
  - Searchable
- Open Source
- Digital payment system with no central authority

Bitcoin is the 1st computer technology to solve the social issue of TRUST, without a 3rd party

- **Satoshi Nakamoto's** white paper* in 2008:
  - **Solved double spend problem - a coin cannot be copied**
  - **Blockchain and Proof Of Work consensus protocol**
- Currency based on cryptographic proofs instead of trusted banks

* *Bitcoin: A Peer-to-Peer Electronic Cash System*



Checkered Reputation

- Cyberpunk & libertarian roots
- Anyone can open a bitcoin wallet (address). Not Anonymous. Pseudo-anonymous.
- Early on, used for drug purchases on dark web. Silk Road shut down in 2013. Now 90% legit.
- Ransom, Cyberjacking
- Chainalysis tool used by law enforcement
- Bitcoin maximalist cult

FBI makes record $28 million Bitcoin bust

Published time: 26 Oct, 2013 08:57 Get short URL

Reuters/Jim Urquhart © Reuters

Follow RT on Google News

US authorities have reported their largest-ever Bitcoin bust amounting to $28 million of the digital currency. It was seized from the owner of the controversial Silk Road website, which was shut down three weeks ago.

A Friday statement by federal prosecutors in New York details the seizure of 144,336 bitcoins, which were discovered on the computer belonging to Silk Road founder Ross William Ulbricht, alias “Dread Pirate Roberts,” Reuters reports. Ulbricht was arrested Oct. 1 in San Francisco on several charges of conspiracy.

Video: Digital Signature Cryptography

Bank Reconciliation
Before and After Blockchain

Company A Books

- BoA Bank Statement
- Deposits cleared
- **Deposits in transit**
- Checks cleared
- **Checks outstanding**
- **Bank fees, NSF, other**

Company B Books

- WF Bank Statement
- Deposits cleared
- **Deposits in transit**
- Checks cleared
- **Checks outstanding**
- **Bank fees, NSF, other**

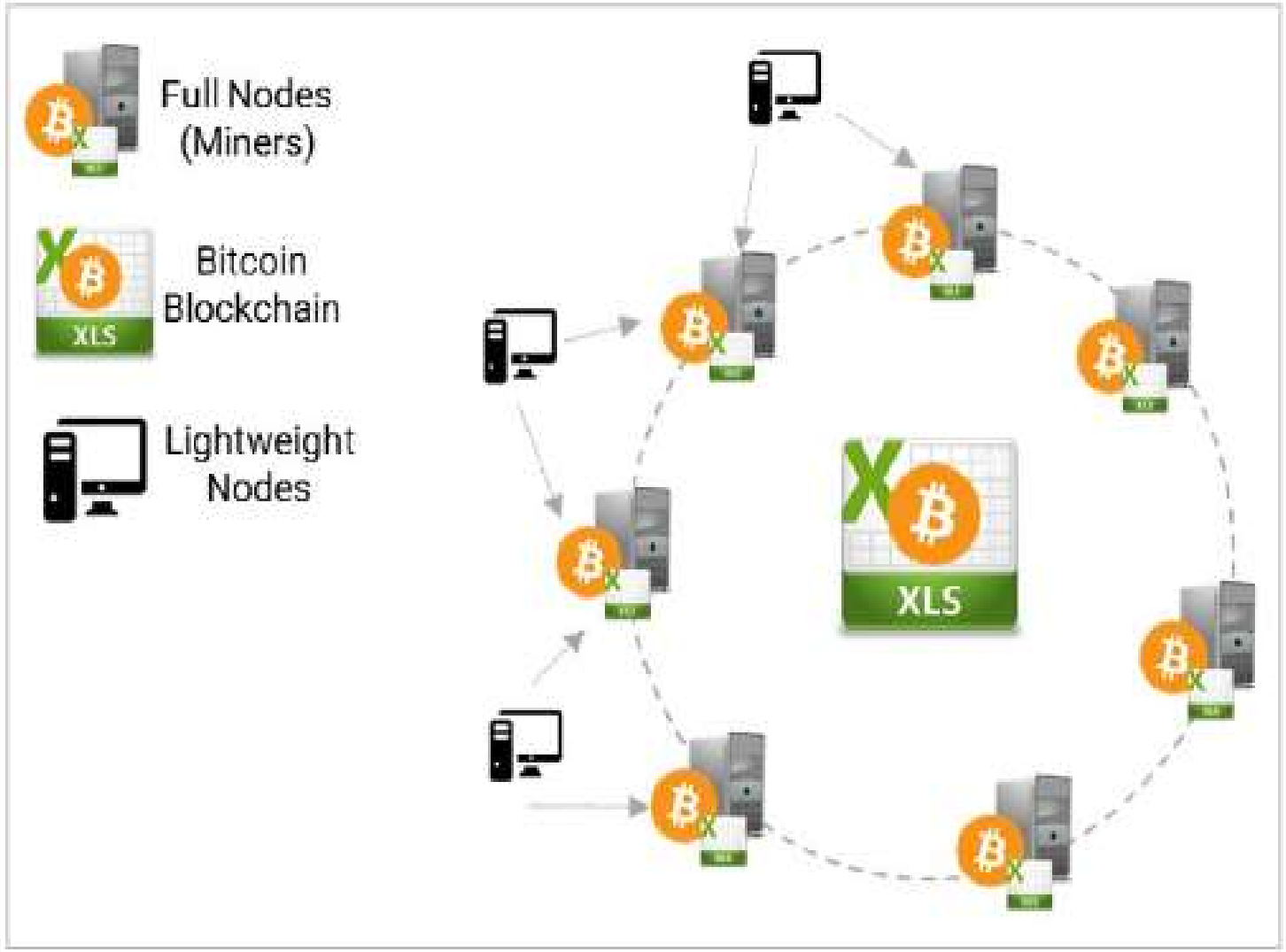
Company A Books/Wallet

Company B Books/Wallet

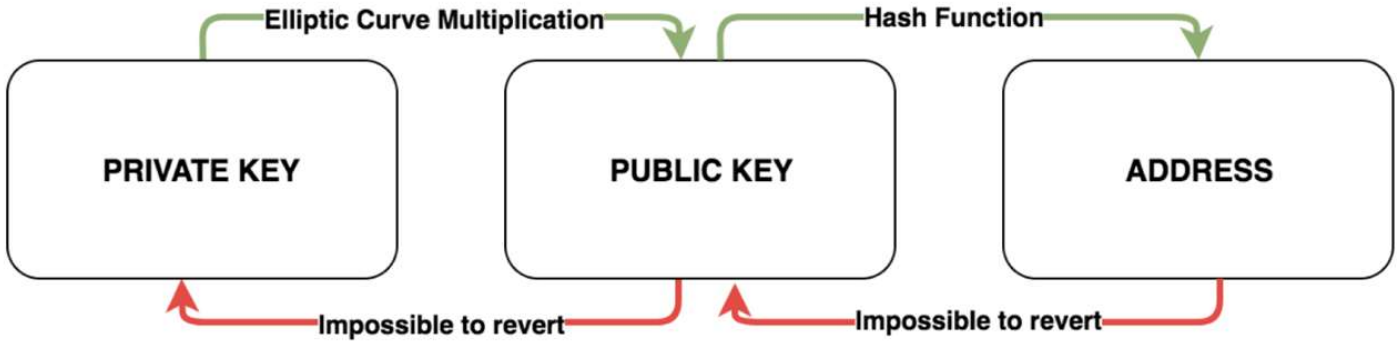
- **Blockchain Transaction Ledger (Send or Receive)**

How Does Bitcoin Work?

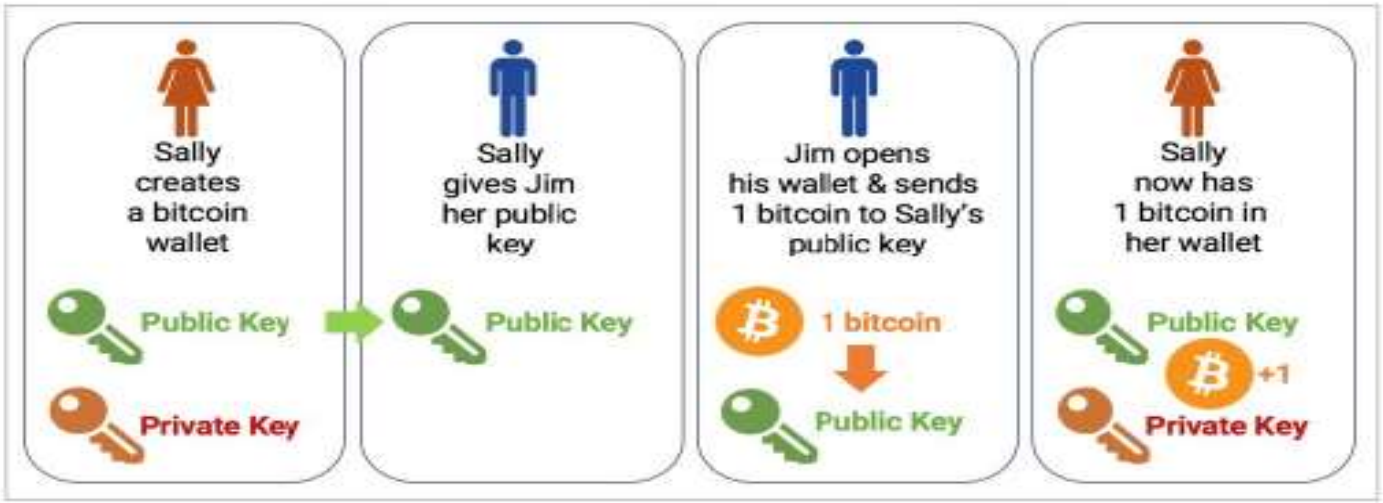
- Bitcoin ledger is kept in transaction records like an excel spreadsheet.
- Transactions are lumped into blocks and a new block is added to the blockchain about every 10 minutes.
- When the block is added to the chain, all of the transactions in the block are completed, can never be changed, can not be reversed.
- The block is added to the chain when a Bitcoin miner solves a very hard math problem. The miner is also responsible for “validating” that all the transactions in the block are valid – that is, there are enough bitcoins in the accounts to cover the transactions and there are no other outstanding transactions that would use the same bitcoins.
- Anyone can create a “wallet” which means they are given a Private Key. From the private key, they create a public key which is then then their address. Their wallet contains the portion of block chain related to their transactions.

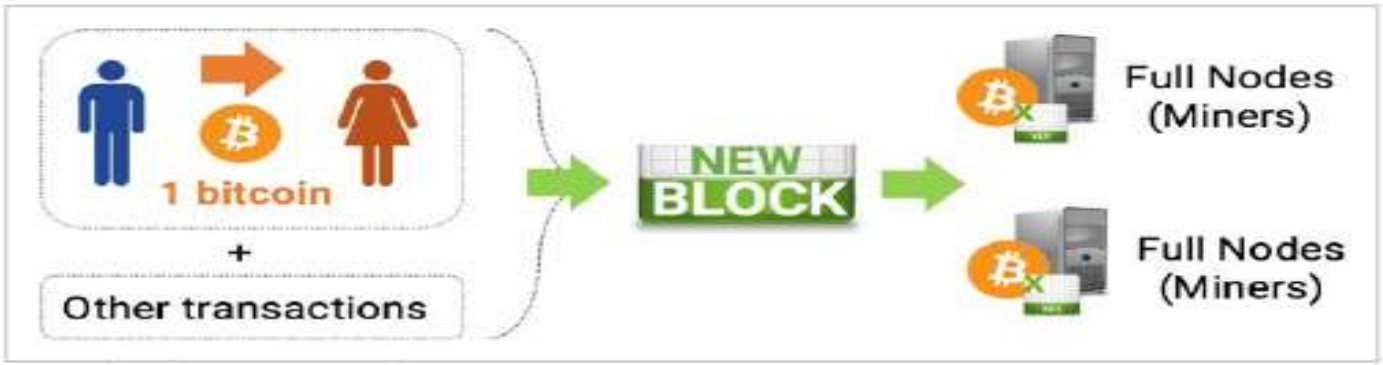

Full Nodes
(Miners)
Bitcoin
Blockchain
XLS
Lightweight
Nodes
XLS

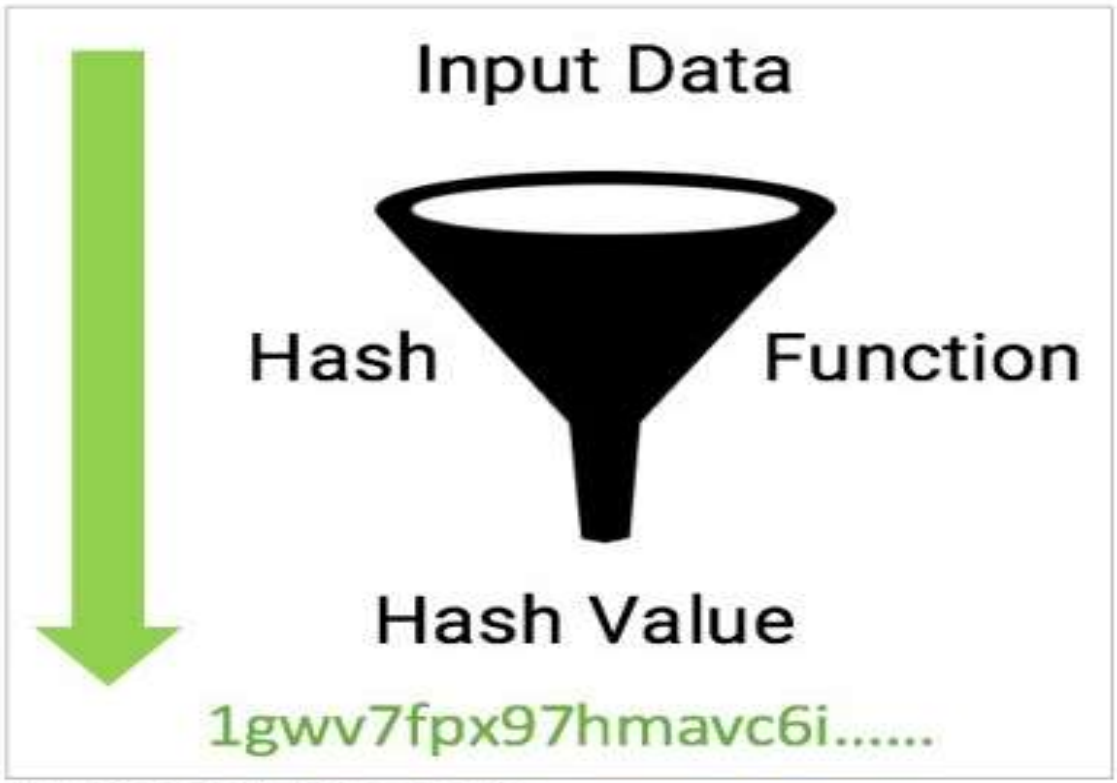
Public Key Cryptography Close-up

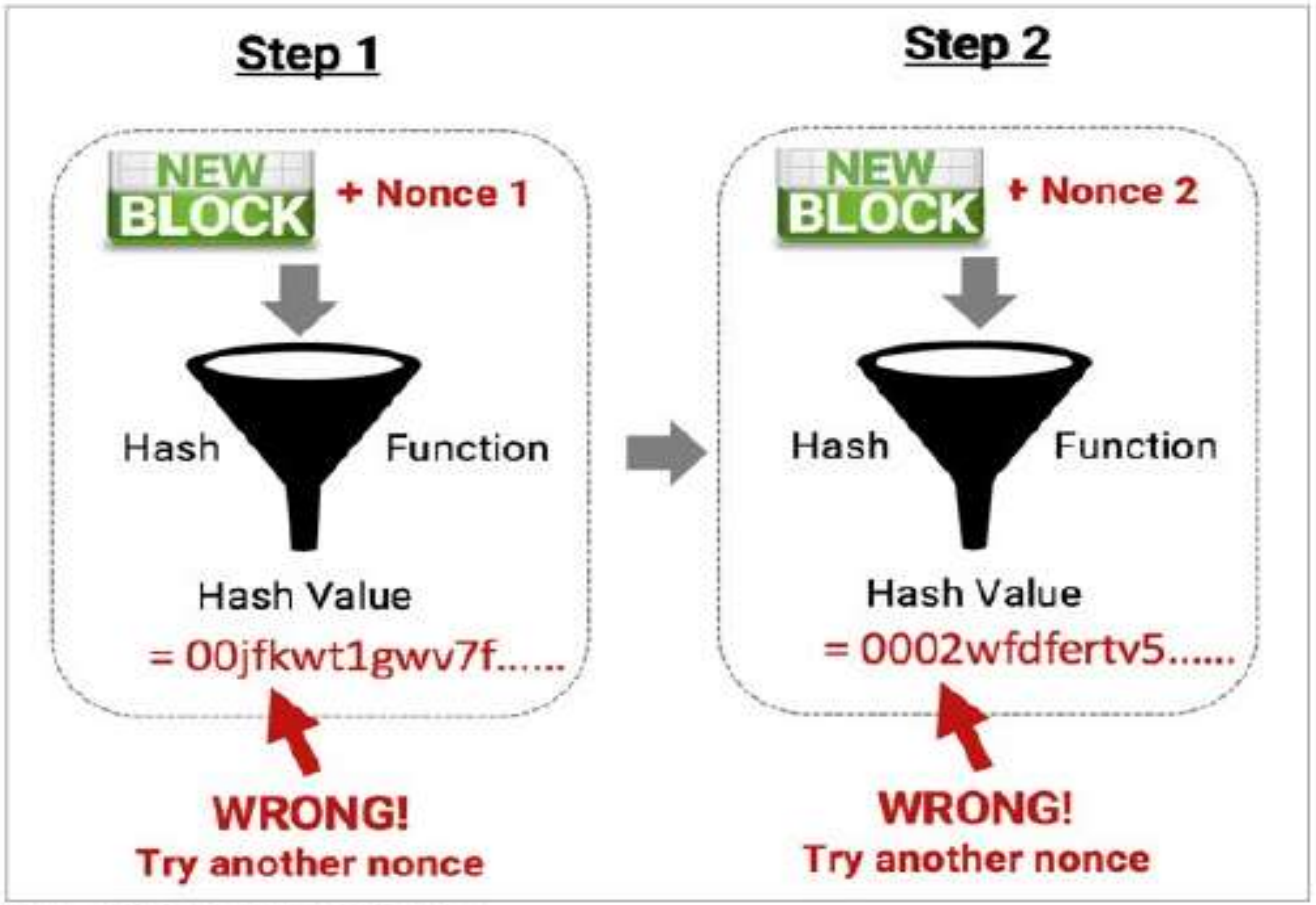


- Private key generates a public key, not reversible
- NEVER share private key – it is like a bearer asset
- Private Key (64 characters):
- F5064ec3af07035d673a8d906a2cf579c3fc0a89c67d02e4eb2c62d13d5a5b32
- The public key address may be shared with others
- Public Key Address (42 characters):
- 0x0115D3215067dCf2357D8B3Eb3CBAe8b522F7873

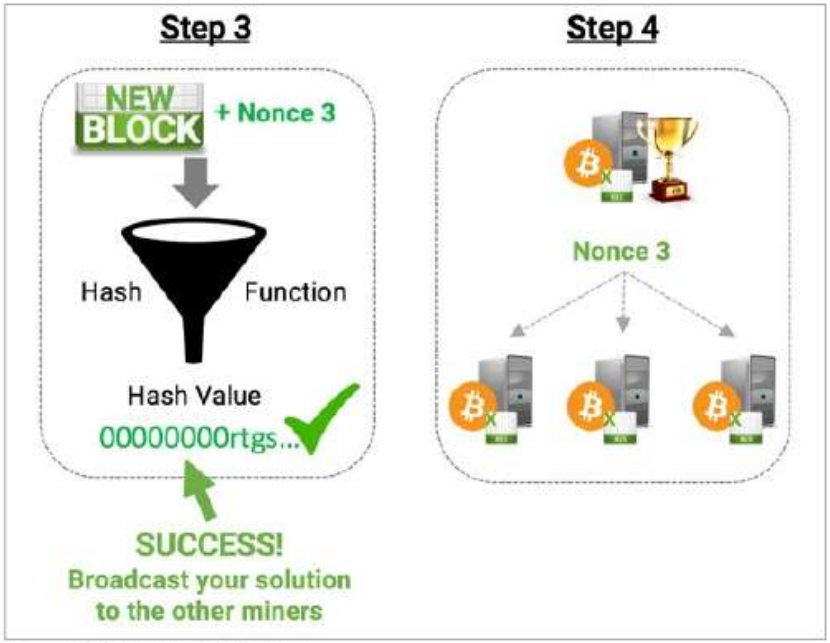

Sally creates a bitcoin wallet
Public Key
Private Key
Sally gives Jim her public key
Public Key
Jim opens his wallet & sends 1 bitcoin to Sally's public key
1 bitcoin
Public Key
Sally now has 1 bitcoin in her wallet
Public Key
+1
Private Key
www.stansberryresearch.com

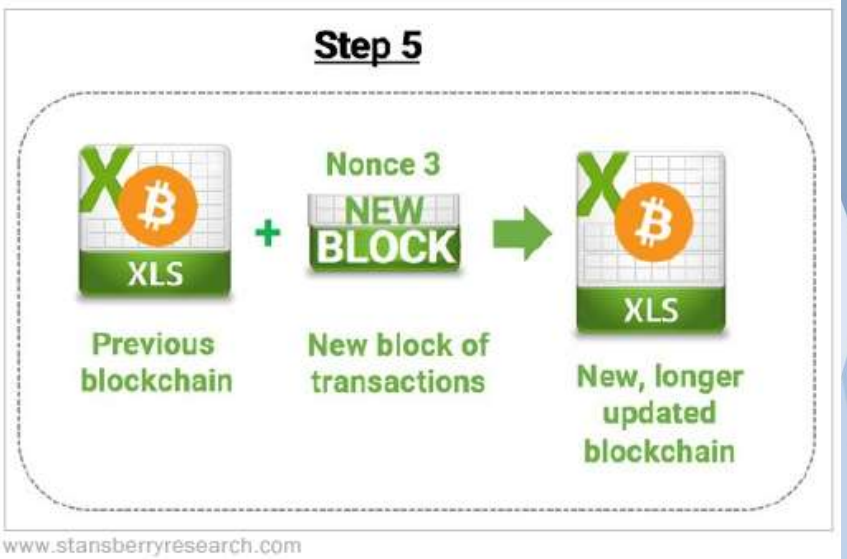

1 bitcoin
+
Other transactions
NEW BLOCK
Full Nodes (Miners)
Full Nodes (Miners)
www.stansberryresearch.com


Input Data
Hash
Function
Hash Value
1gwv7fpx97hmavc6i.....
www.stansberryresearch.com

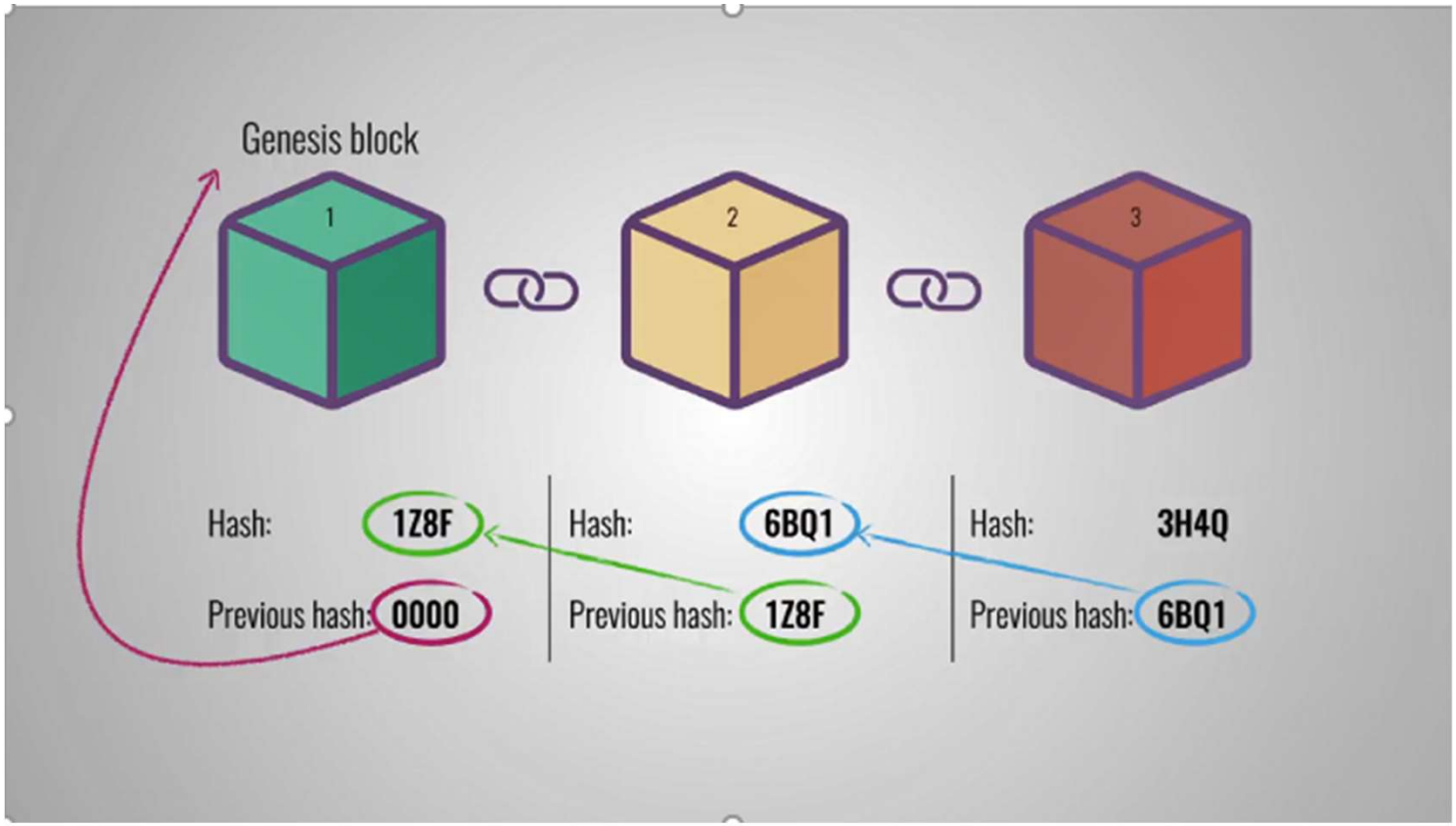


www.stansberryresearch.com





The first miner with the solution wins a certain number of bitcoins and whatever transaction fees are listed in the transactions that go into the block



Each Block in the Bitcoin chain has

- Some number of ledger transactions
- Its Hash total
- The previous block Hash total
- It's "Nonce"

Bitcoin Mining Costs
Hardware, Electricity, Cooling, Admin.

ASICs

Application-Specific Integrated Circuit

China 60%, Georgia 15%, Sweden 8%, USA 3%, all others 14%

Bitcoin – what is it good for?

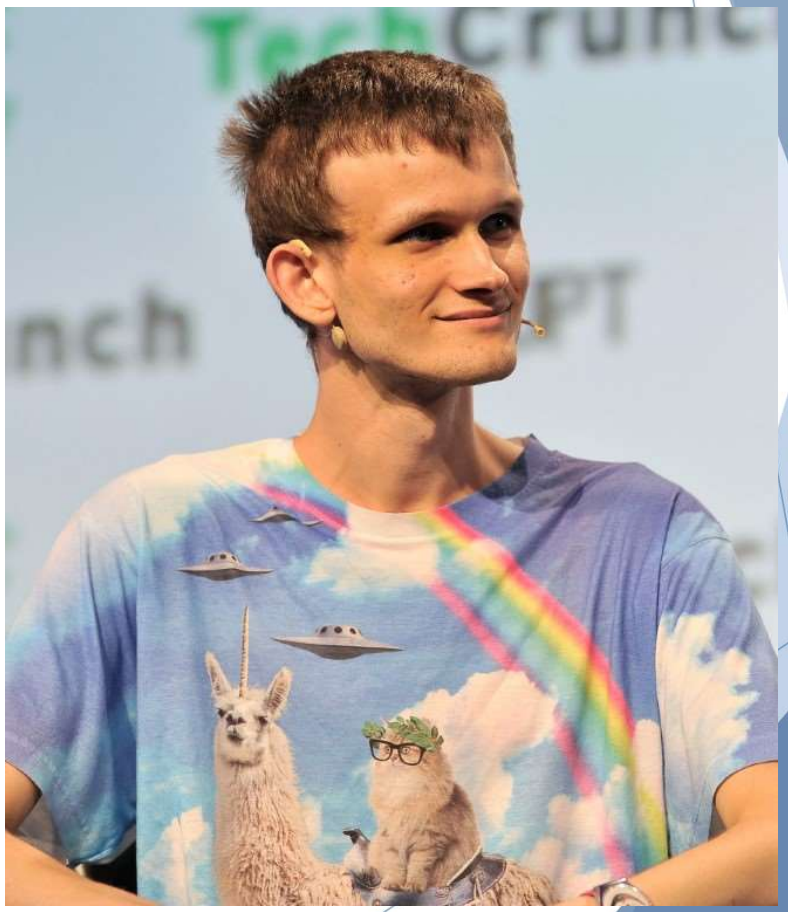
- Retail adaption slowed due to high transaction fees ($1-$40) and slow transaction speed (10 min.+)
- **Speculation**, volatile market value
- **Store of Value**, **Digital Gold** - useful in countries with high inflation – Argentina, Venezuela, Turkey
- **Global Currency**, transfer funds across borders
- Dark web transactions

BITCOIN (BTC) Takeaway

- Solved double-spend problem for digital assets
- Automates trust without a bank or middleman
- Most mature cryptocurrency blockchain (10 yrs)
- Most famous cryptocurrency
- History of nefarious uses (Notorious BTC☺)
- POW security mechanism wastes energy
- Mixed acceptance by retailers
- Speculation or Store of Value?

A Brief History of Ethereum and Ether (ETH)

- Invented by Vitalik Buterin when he was 19
  - Russian born Canadian
  - Co-editor of Bitcoin Magazine
  - Univ. of Waterloo drop-out
- 2013 Issued White Paper
- 2015 Launched Ethereum global distributed blockchain protocol
- Includes Turing-complete programming language Solidity
- Runs smart contracts
- Runs decentralized apps (DApps)



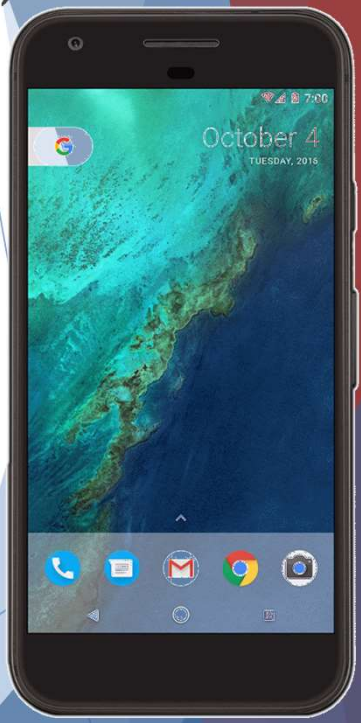
Compare and Contrast

Bitcoin (currency)

- The ‘Gold Standard’ of blockchains
- Asset: bitcoin (BTC)
- 10 Minute block time
- Simple and robust
- Proof-of-Work
- Primary purpose is payments, competes with fiat currencies, gold

Ethereum (general)

- Smart Contract Blockchain Platform
- Asset: ether (ETH)
- 14 Second block time
- Complex and feature-rich
- Moving to Proof-of-Stake
- Primary purpose is to fund computation on Earned Value Management and align incentives



Video: Smart Contract Example
Commodity Trading of 1 Ton of Copper

Where is all this going?

- Real projects for supply chain – Walmart/IBM tracking produce
- Real potential in MANY hard problems
  - Electronic Voting
  - Diamond Tracking
  - Property Sales
- Facebook – Libra
  - Worldwide crypto currency
  - Facebook has 2.4 billion users
  - Moving to separate Libra management from Facebook management
  - Jerome Powell – “very high hurdles for approval”

Questions?

Blockchain, Bitcoin and Ethereum

David McCoy, CPA