BLOCKCHAIN

TRAINING ALLIANCE

BLOCKCHAIN
TRAINING ALLIANCE

Blockchain Overview

www.blockchaintrainingalliance.com

Let's Start

At the Beginning

No prior knowledge of Blockchain required

The course provides an overview of Blockchain Technology

Start with a simplified overview of how it all works, then dive deeper into each section

Course Modules

- Modules covered:
  - What is Blockchain – The Basics
  - Blockchain and Cryptocurrency
  - Why Use Blockchain
  - Decentralized Networks and Ledgers
  - Types of Blockchain
  - How Blocks are Created
  - Cryptography and Hashing
  - Mining a Block
  - Types of Consensus
  - Blockchain 2.0 and Ethereum
  - Blockchain Use Cases
  - Blockchain Adoption
  - Web 3.0
  - Blockchain Implementation

What is Blockchain?

The Basics

Immutable

Security

Trustless

The Core Principles of Blockchain

Distributed Ledger

Decentralized

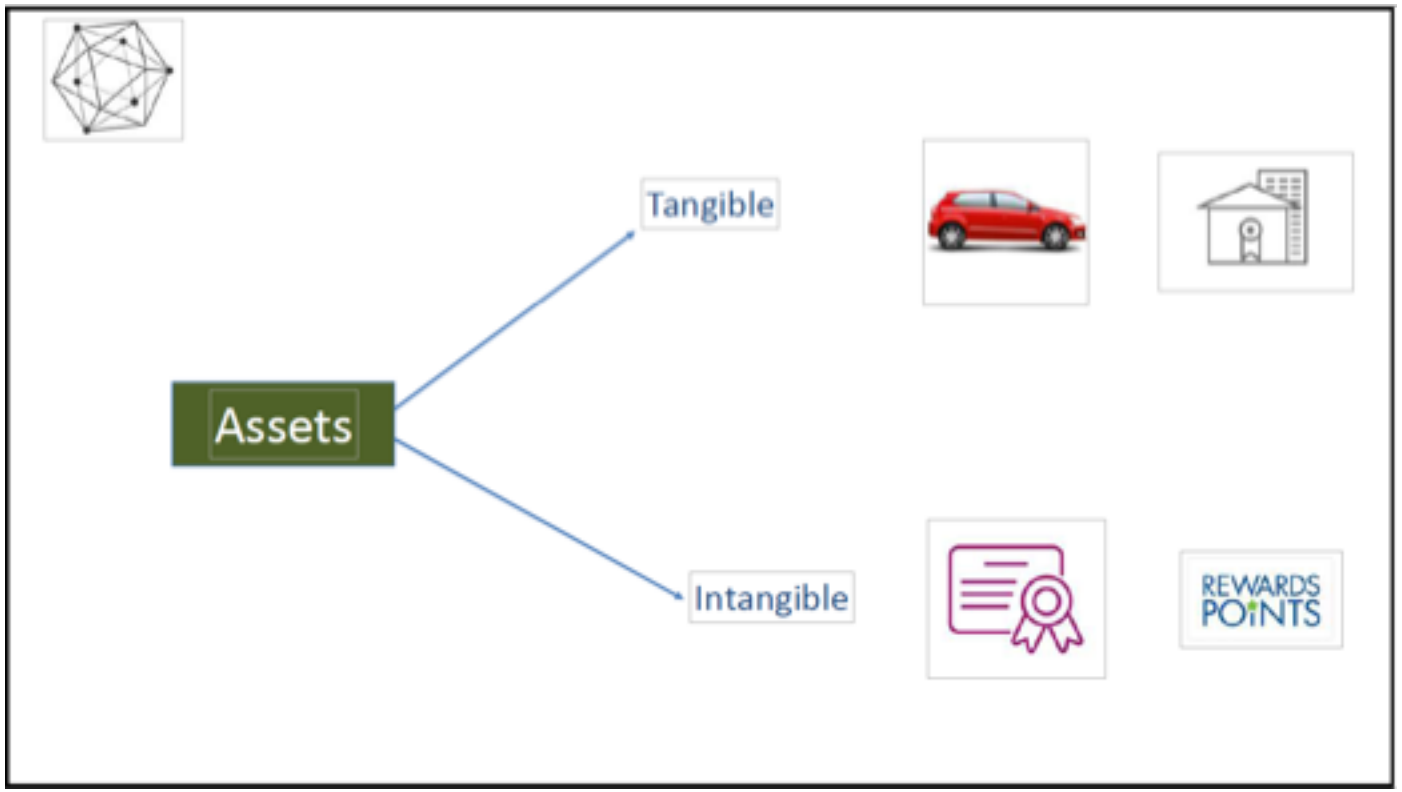
Group Consensus

Blockchain Defined

- In its simplest form, Blockchain is a distributed database, an unchangeable record (or Ledger) of asset ownership.

- Blockchain is primarily defined as a shared immutable ledger, or just an "unchangeable record of who owns what"
  - Global, peer to peer, and distributed immutable record of transactions.
  - Used to transfer and permanently record any change of assets between two or more parties without intermediaries.
  - Assets are defined as anything of value that requires accountability of ownership, i.e. money, cryptocurrency, real estate, records of any kind, identities, personal property, etc.

Assets Further Defined



Blockchain Uses Old Technology

- Blockchain is a combined use of existing older technology.
  - **Ledger** – 7,000 year old technology, triple-entry accounting
  - **Cryptography** – "coding messages" has been used for thousands of years, and still used in complex S/W algorithms for military and business applications like Blockchain
  - **Computer Networking Technology** – Blockchain makes extensive use of P2P networking architectures

The History of Ledgers

Sidebar - A Brief History of Accounting

- Ledgers appear around 5,000 BC
  - Single entry only
- 300 BC – Chanakya
  - First documented accounting standards
- Double-entry ledger appears in 1340 A.D.
  - Track debits and credits
  - Tell the story of a transaction from both / all sides
- Triple-entry ledger appears in 2009
  - aka Blockchain!
  - Debits, credits, and an immutable link to all past debits and credits

Blockchain Rules

- Once something has happened, and a record is created, the fact that it happened never changes
- Data written into a blockchain is a historical record and is immutable
- Blockchains have to prove they haven't been tampered with
- All the nodes (computers) running on a blockchain must agree (i.e. have consensus) on ALL the data stored on it

Blockchain is

- A record keeping system
  - To record the transfer of “tokens” or “coins” representing wealth (Monetary/currency)
    - Bitcoin and other cryptocurrencies such as Ether, LiteCoin, Monero, etc.

Blockchain is

- A record keeping system (for any kind of data)
  - To record the transactions of importance (Non-Monetary)
    - Update to a medical record
    - Transfer of ownership
    - Training certification on Blockchain
    - Recording important single-party announcements

Transferring Assets, Building Value

- Anything that is capable of being owned or controlled to produce value, is an asset
- Two fundamental types of asset
  - Tangible, e.g. a house
  - Intangible e.g. a mortgage
- Intangible assets subdivide
  - Financial, e.g. bond
  - Intellectual e.g. patents
  - Digital e.g. music
- Cash is also an asset
  - Has property of anonymity

14

Blockchain is:

Blockchain is:

- An event tracking system
  - Announcements mark events
- Events are actionable
- Smart Contracts running on the Blockchain allow actions to be taken on events/transactions
- Blockchain is a workflow platform
  - Now being implemented in financial contracts, manufacturing supply chains, quality tracking, shipping and international transactions, international currency exchange/transfers.

    Unlimited Possibilities!

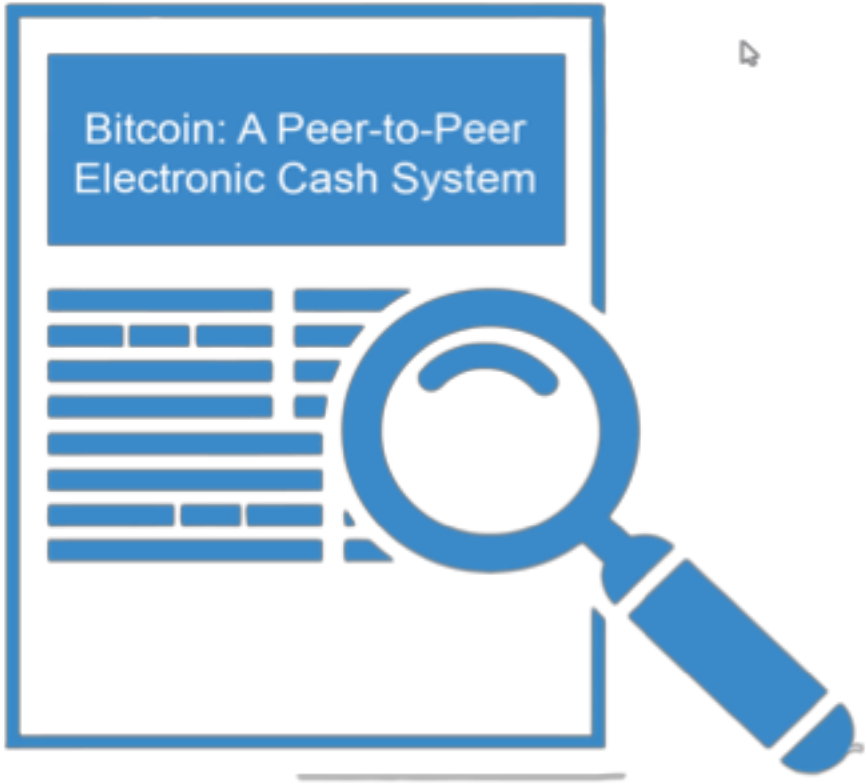
Blockchain is Immutable

- Cannot change the data once it's committed to the ledger
- Data is auditable
- Change by issuing offsetting transaction
- Smart contract code

Consensus in Distributed Networks

- In order to update the ledger, the network needs to come to consensus using an algorithm
- Consensus: what does it mean to come to consensus on a distributed network?
- Consensus methodologies will be discussed a little later

Blockchain Beginnings



In 2008 “Satoshi Nakamoto” published a whitepaper which outlined the architecture of Bitcoin

Interesting Blockchain Dates

- 2009 first block created
- Satoshi disappears December 2010 - date of last post
- 2015 – Ethereum and Hyperledger both go live
- 2018 – 14 open jobs for every blockchain developer
- 2019 – Walmart requires produce suppliers to be using blockchain
- 2021 – Dubai hosts all gov't operations and record-keeping on blockchain

Blockchain and Cryptocurrency

Blockchain's Relationship to Bitcoin

Bitcoin is a digital, decentralized, disintermediated, trustless currency

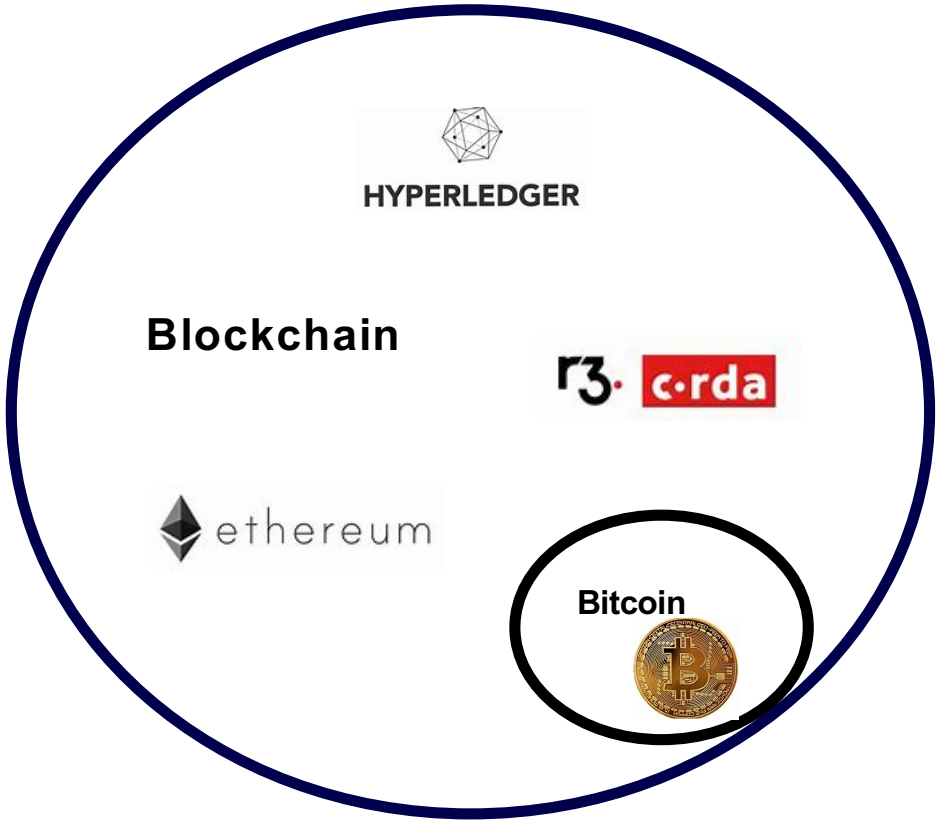
Blockchain is the underlying security software that manages and controls the WW Bitcoin Network, allowing for safe, trustless, and secure P2P transfer of Bitcoin, or any other cryptocurrency.

Bitcoin/Cryptocurrencies have *some* similar characteristics as a fiat currency

- **Durability** -
- **Portability** - Safe for long term storage
  (crypto - susceptible to individual coin market volitivity)
- **Divisibility**
  Easy to move around and spend
  (crypto - can be exchanged P2P with small transaction fee)
  -
  So you can spend small amounts
  (crypto - used in fractional amounts generally based on Bitcoin)
- **Fungibility**
  Each unit of value is equal
  (crypto - based on market value fluctuations - BTC/U.S.$ based)
  -
  To preserve value
  (crypto - based on market capitalization at time of ICO)
- **Scarcity** -
  So you can actually spend it
  (crypto - solely based on country monetary policy and merchant acceptability, plus transaction fees)
- **Acceptability** -

Bitcoin is a Blockchain Application

Bitcoin was the first Blockchain



Bitcoin is an application that runs on the Blockchain.

Blockchains can be either public or private but share the same technology.

Similar to Facebook, where Facebook is simply an application that runs on the Internet.

You Control Access to Bitcoin

- Nobody actually ‘has’ bitcoins – they can’t be download, or stored on a computer
- Remember: The Blockchain is a ledger - it records the transfer of bitcoin or other assets between people or other entities i.e. companies, groups, etc.
- The records stay on the Blockchain - what is transferred is the ‘control’ of the bitcoin or asset.
- An example would be if ‘Alice gives Bob 2btc’ i.e. ‘Alice transfers control of 2 of her bitcoins to Bob’
- Control is enabled through cryptography

Control via Cryptography

- When someone sends you coins they publicly place them under the control of your public key (in the form of an Address)
- If you can prove that you have the matching public key, and the matching private key, the network lets you control the coins

Why Use Blockchain

Decentralization

KEY CONCEPT: Decentralization

- Decentralized - Peer-to-Peer data sharing, hosting hardware owned by many not few, fault tolerant, secure, lower performance
- Distributed - Solution components spread across hardware assets, solution components and data maintained and controlled by central authorities
- Centralized - Solution components, data, and control all maintained by a central authority

Benefits of Blockchain

What are the benefits of Blockchain?

- Publicly verifiable
  - Accountability to customers and end-users
  - (permission-less)
- Secure
  - Control who sees what data when (permissioned)
- Quality assurance
  - Track origin of all supply chain components
  - Example – Food origin and/or safety recalls
  - Smart Contracts as a replacement for middlemen operators
- Lower transactions costs
  - Removing middlemen reduces cost

Benefits of Blockchain

What are the benefits of Blockchain?

- Tokenization
  - Create trade-able tokens backed by real-world value
  - Fractional ownership
    - Example - Own 1 car in 1 city, or 100 cars in 100 cities

- Trade, commerce, and business process automation
  - Smart Contracts as a replacement for middlemen operators

Drawbacks of Blockchain

What are the drawbacks of Blockchain?

- Very new technology
  - Constantly changing, evolving
  - Not very many trained resources
  - High cost for trained resources
- Best practices, recommended patterns still being formed
- Scalability, transaction speed / cost

Drawbacks of Blockchain

What are the drawbacks of Blockchain?

- Still learning good and bad use cases
- Stigma and history of Blockchain
  - Cryptocurrency and the dark web
  - ICO/ITO scams
- Anonymity of origin – Satoshi Nakamoto
- Data in the blocks

Drawbacks of Blockchain

Because All global nodes must validate all transactions, speed, scalability and cumulative power consumption are critical issues facing Blockchain.

Why Not a Database

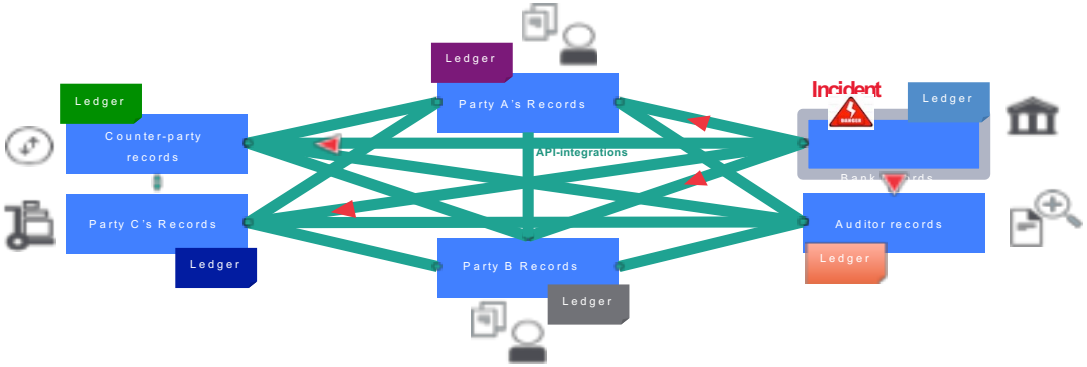
Blockchains solve specific problems:

- Fully distributed - highly fault tolerant
- No centralized authority
- Low barrier to entry
- Instant, global transactional capability
- No double spending
- Very low transaction costs

- Traditional Databases have centralized control and do not perform these functions.

Conventional System Problem

Problem - Difficult to monitor asset ownership and transfers in a trusted business network



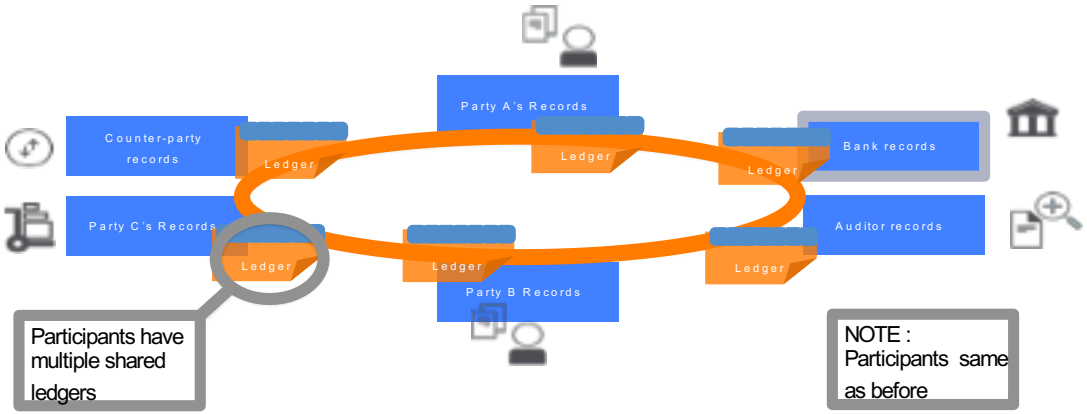
34

Inefficient, expensive, vulnerable

Blockchain Shared Ledger Solution

Solution – a permissioned, replicated, shared ledger

ALL Nodes have (and share) the same exact copy of the ledger



35

Consensus, provenance, immutability, finality

Decentralized Networks and Ledgers

Blockchains as Distributed Databases

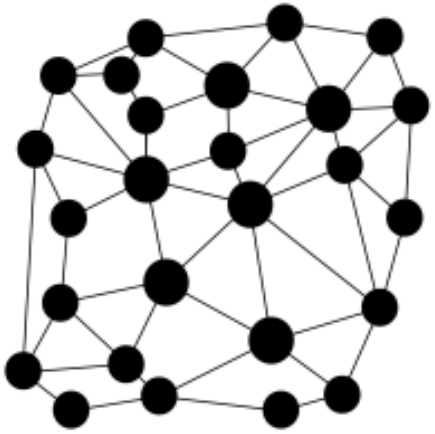
- In Blockchain, everyone has a copy of the Ledger
  - Everyone running a Blockchain node is part of the network
  - New transactions are broadcast to and recorded by the network
  - Everyone updates their local copy of the blockchain
  - If everyone has a copy of the blockchain, when queried, everyone gets the same answer

Centralized vs Decentralized Ledger

- If the single copy of the ledger were changed by any means, wealth would be lost unfairly
- With a decentralized ledger, nobody has to trust anyone else
  - Trustless environment is assumed from the beginning

Why Decentralized?

- Distributed network
- Many nodes or peers that are connected in a network with no single point of failure or centralized control
- Security and resiliency: design the network so that if some peers crash or attack the network maliciously, the network can still operate (Byzantine Fault Tolerance)



A distributed network.

Types of Blockchain

Blockchain as History

Blockchain as History

- Immutable, cannot be changed
  - Remember, each block contains the hash of the previous block
- Append-only
  - Data on the Blockchain cannot be deleted or edited, only additions can be made
  - This provides a detailed history of ALL events, not just a snapshot of the current state!

Types of Blockchains

- Public vs Private
  - Who can **write** data to the Blockchain?
  - Public – everyone can add a record
  - Private – only certain participants can write data

- Open vs Closed
  - Who can **read** data from the Blockchain?
  - Open – everyone can read Blockchain data
  - Closed – only certain participants can read data

Public or Private Blockchain

- Should the solution be a permissioned or permission-less Blockchain
  - Are all participants considered equal, or should some have abilities that others do not?
  - Election chairperson can add candidates to an election = permissioned
  - A digital currency which can exchanged and traded by all = permissionless
- Do customers understand the tech well enough to trust it with their data?
  - Great solutions may not be accepted until they have been socially normalized
  - Credit cards and early e-commerce

Public or Private Blockchain

- Hyperledger vs Ethereum
  - These are discussion points, NOT absolutes

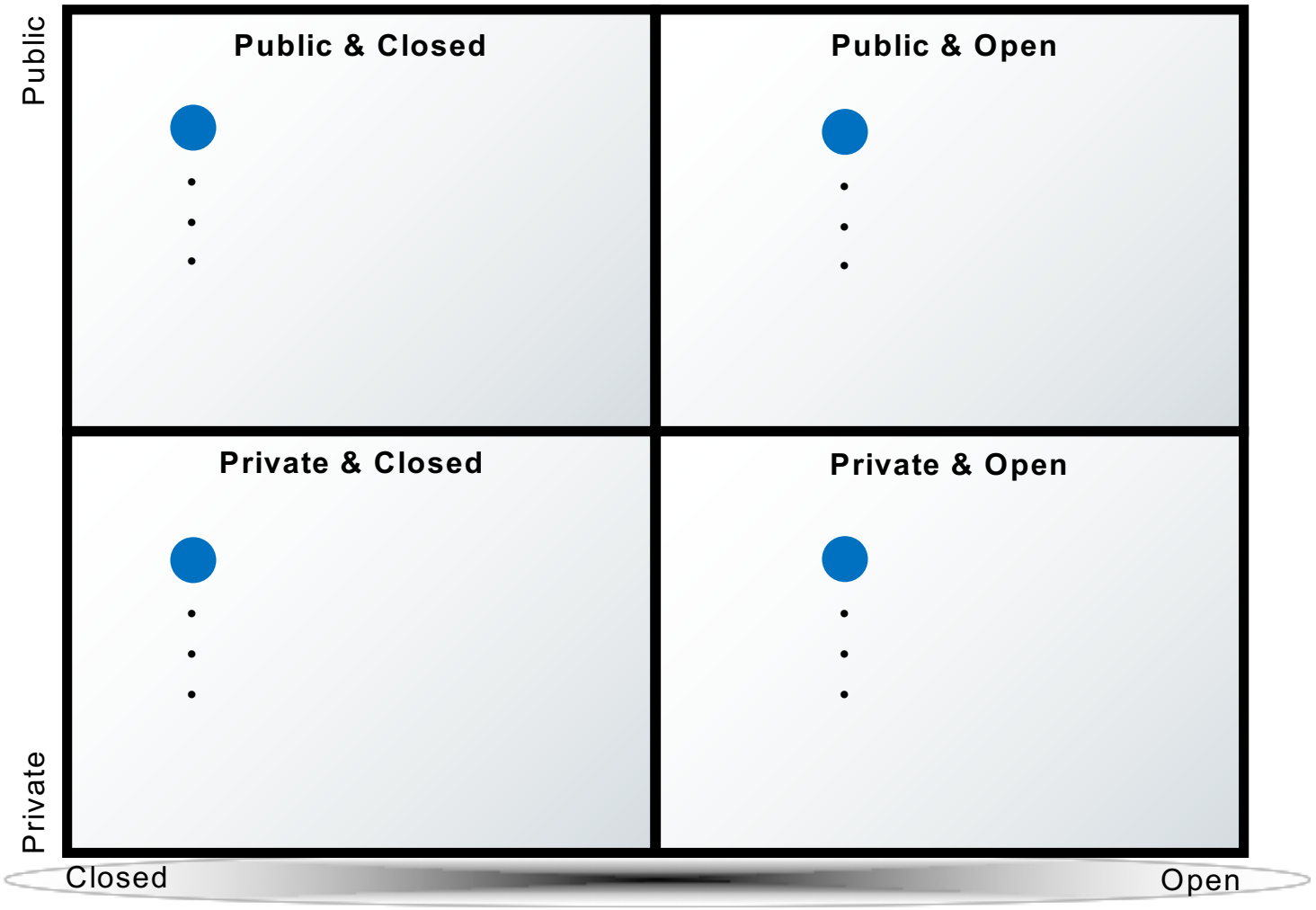
- Ethereum
  - Music and content distribution
  - Digital currency or asset-backed token
  - Blockchain-enabled mobile data service
  - Gambling and on-line gaming
  - Authoring, editing, and amending a piece of legislation
  - Group consensus is needed/required

Public or Private Blockchain

- Hyperledger vs Ethereum
  - These are discussion points, NOT absolutes

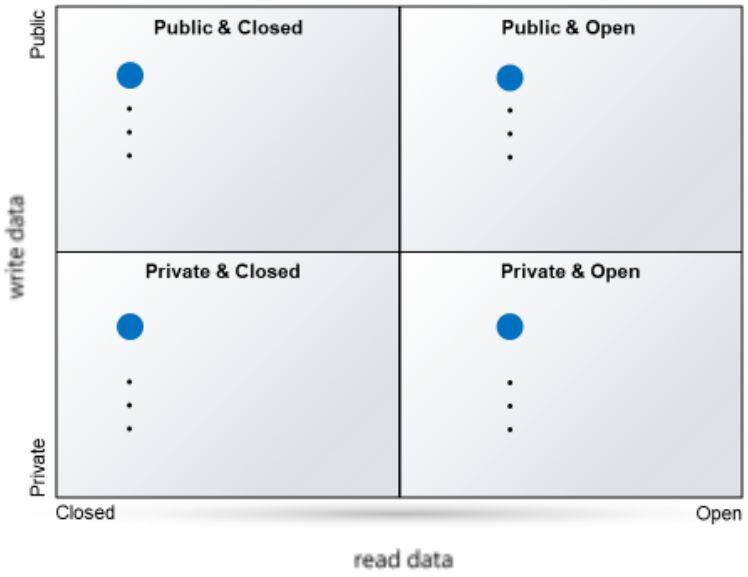
  - Hyperledger
    - Supply Chain
    - Supplier / Manufacturer inventory management
    - Managing internal business processes across geographically distributed locations
    - Allowing elected officials to vote on initiatives without being present

Blockchain Decision Worksheet

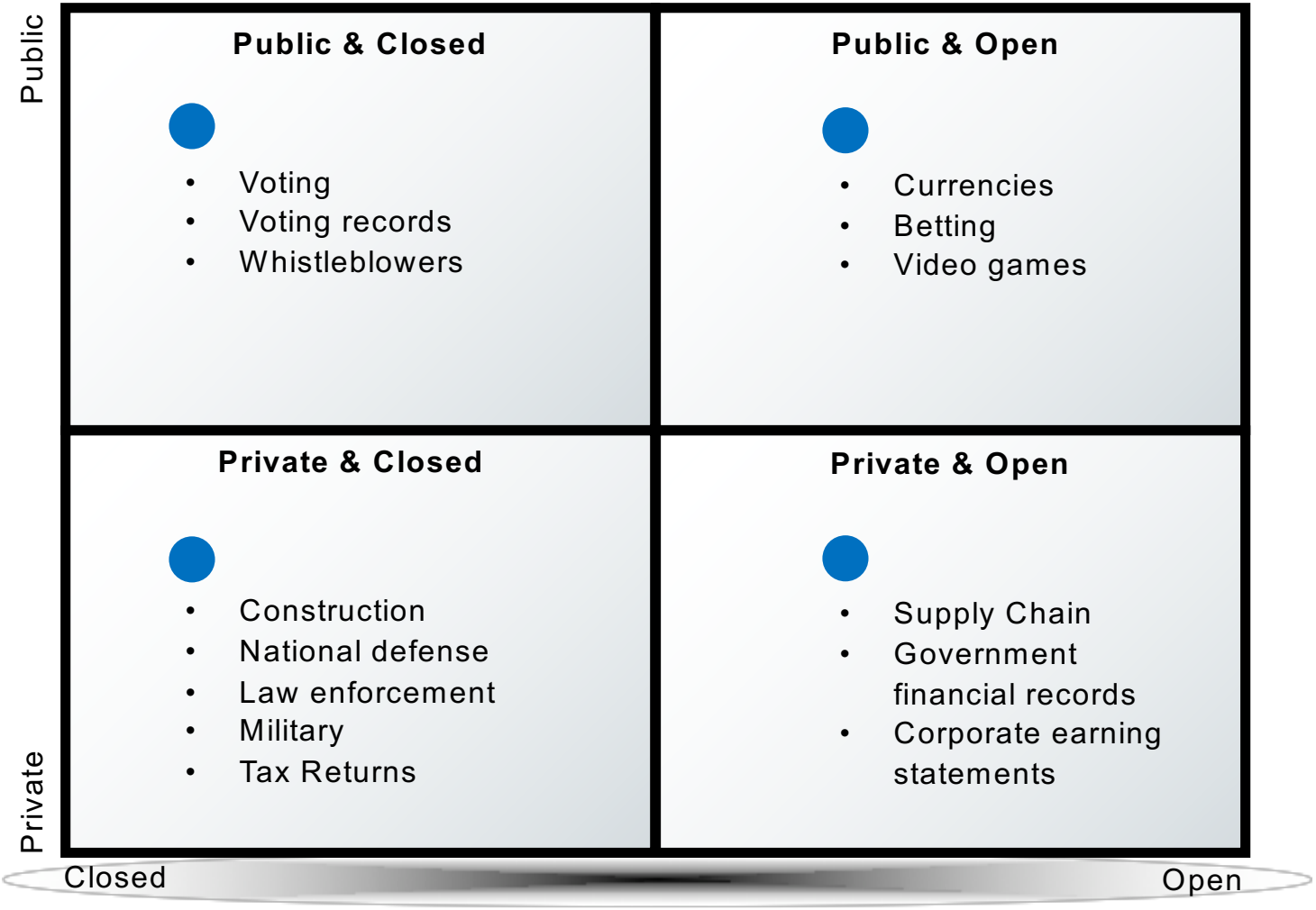


Blockchain Decision Lab

- Currency
- Securities exchange
- Betting
- Video game
- Voting records
- Supply chain data
- Government financial records
- Corporate earnings statements
- Construction tracking
- Defense programs
- Law enforcement agencies
- Others?



Blockchain Decision Matrix



Public Blockchains

- What is blockchain? (public, open, permissionless)
  - Decentralized ledger
    - Can store any type of data
    - Shared ledger
  - Immutable
  - Anonymous
  - Fully-Transparent
  - Group Consensus
    - Nodes only verify data was recorded correctly
    - No ability to verify truth of the data itself
  - Smart Contracts
    - Ability to automate processes
    - Blockchain as workflow / BPM

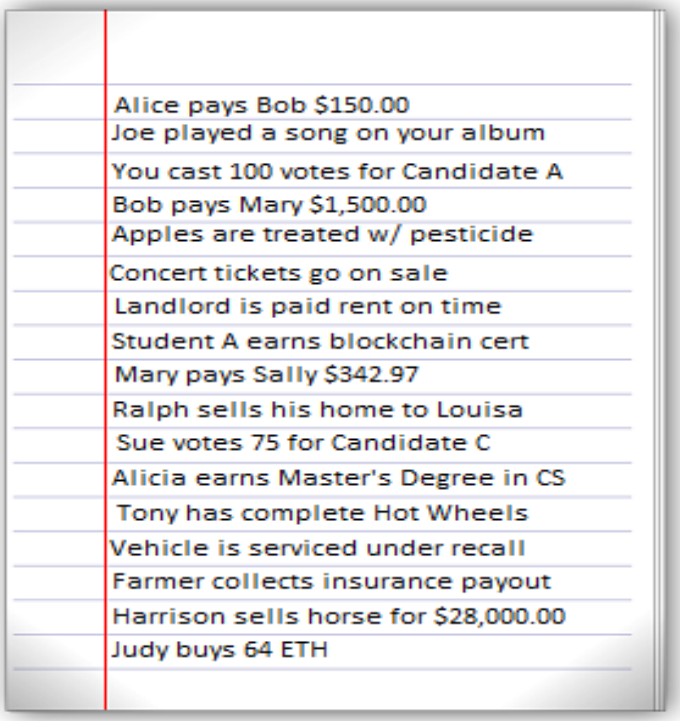
Blockchain for Business

- Are these properties good or bad?
  - Decentralized ledger
    - Can store any type of data
    - Shared ledger
  - Immutable
  - Anonymous
  - Fully-Transparent
  - Group Consensus
    - Nodes only verify data was recorded correctly
    - No ability to verify truth of the data itself
  - Smart Contracts
    - Ability to automate processes
    - Blockchain as workflow / BPM

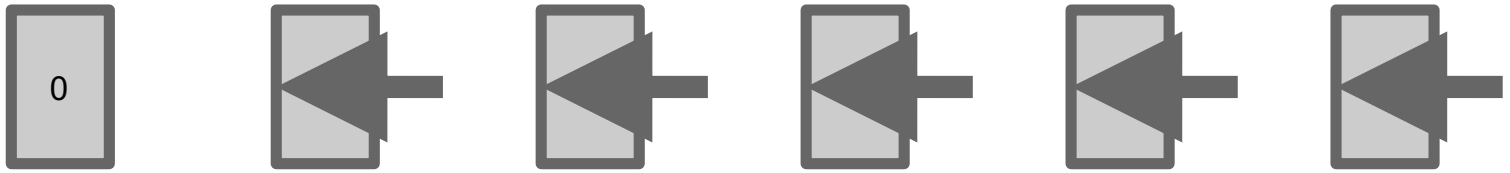
How Blocks are Created

The “Blocks” of a Blockchain

- Think of a “Block” as a sheet of paper with 25 recorded transactions
  - Each of the 25 lines has a complete transaction record
  - Each record is complete with time, data, all transaction details
  - When a sheet is filled (25 transactions), the Nodes “validate” the transactions on the current page and post it on the Blockchain
  - All Nodes must agree (have Consensus) on the transaction content

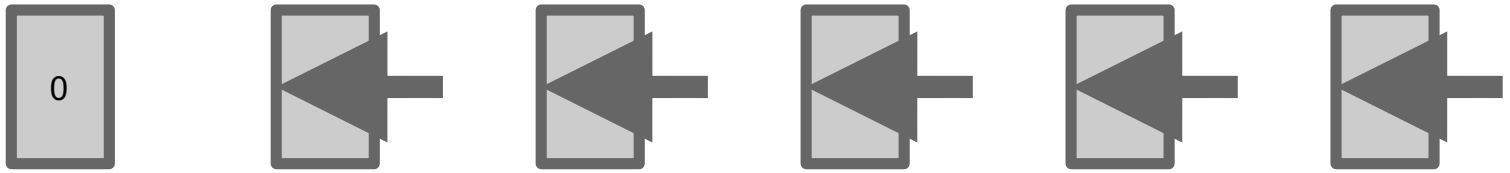


Blockchain Blocks



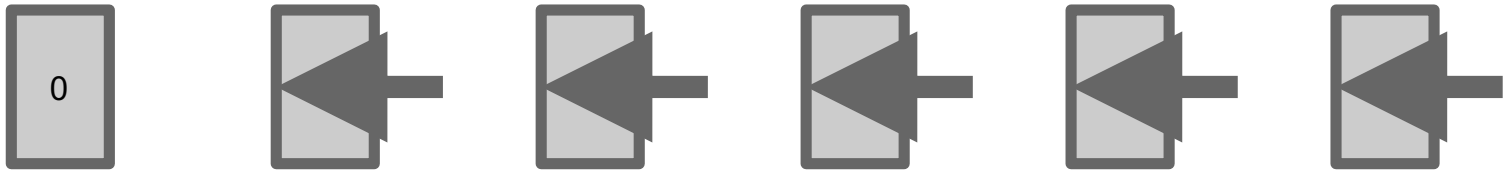
- Blocks are numbered in ascending order, 0 is first/oldest
- The number is the ‘height’ of the block
- Arrows only go from newer to older blocks - a block only directly links to the one immediately before it
- Once a block is stored, it’s read-only (which is why it doesn’t link to the ones after it - that would require you to update it)

Blockchain Blocks



- Blocks store data, in Bitcoin, it's the transactions, but it could be any digital data
- Blocks are created periodically (on average, 10mins for Bitcoin) by a process called 'mining'
- A block represents a set of events that have occurred over a particular time frame (usually, since the previous block)

Blockchain Blocks



- Block id is the hash of the **data** in the block

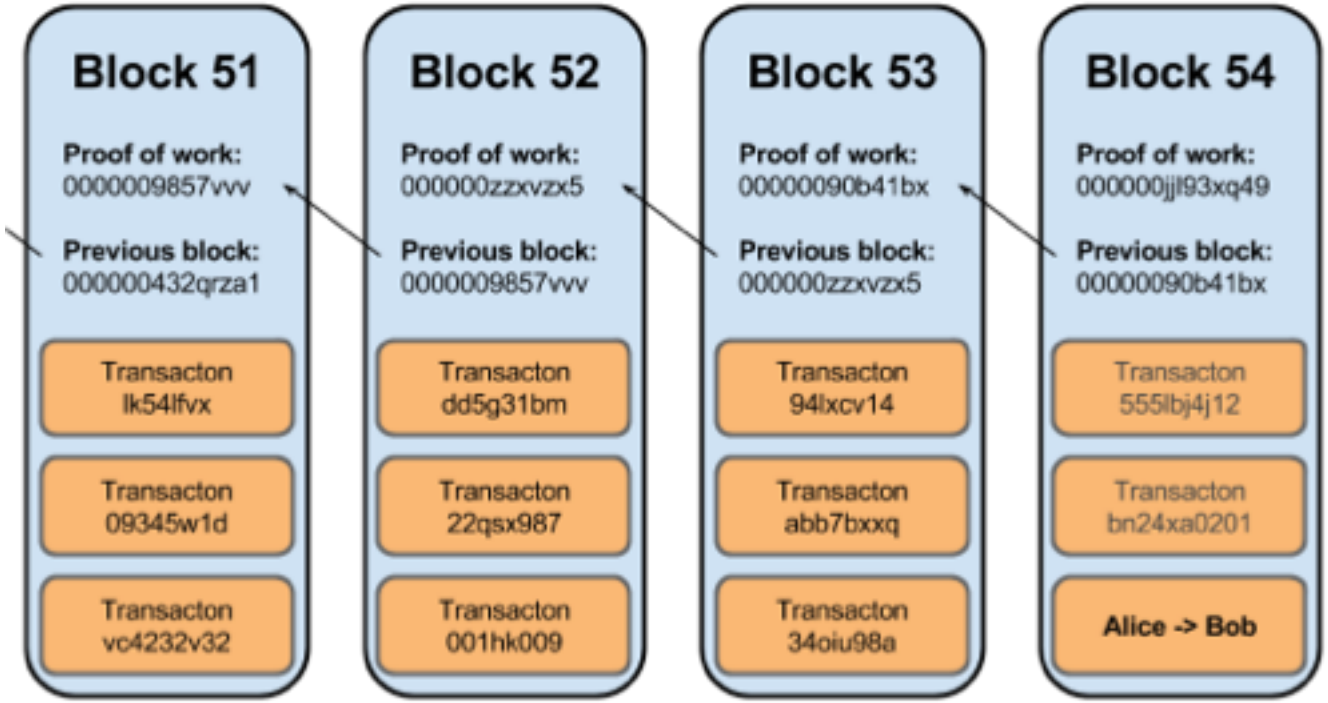
- 0=000000000019D6689C085AE165831E934FF763AE46A2A6C172B3F1B60A8CE26F
- 1=00000000839A8E6886AB5951D76F411475428AFC90947EE320161BBF18EB6048
- 2=000000006A625F06636B8BB6AC7B960A8D03705D1ACE08B1A19DA3FDCC99DDBD

- Block id is a digital fingerprint of that block

What is in a Block?

- A size number to specify how much data is contained in the block
- Some metadata:
  - A version number of the block format
  - A link to the previous block that came immediately before it
  - Merkle root of all the transactions in the block
  - Timestamp of when the block was created
  - Mining difficulty (more about this later)
  - Nonce for proof-of-work (more about this later)
  - All the data of the transactions recorded in this block

What is in a Block?

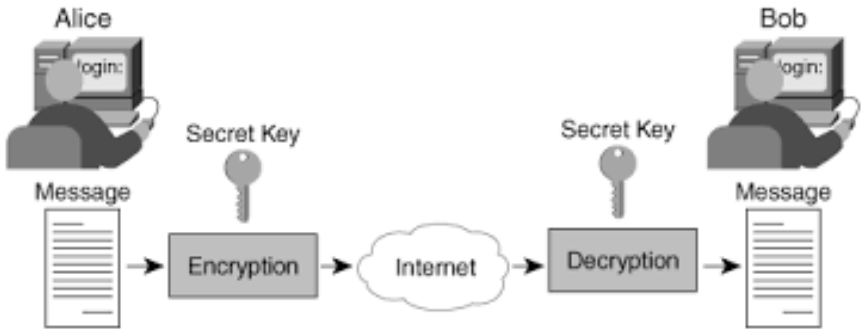


The connection between blocks means that the Blockchain is much more *tamper-proof* than standard database structures. Since Blockchain is a ledger of records, this tamper-proof record of assets is known as an “Immutable Ledger”.

Cryptography and Hashing

Cryptography

- Cryptography can be used to address the issue of privacy
- What is cryptography?
  - The study of how to send information back and forth securely in the presence of adversaries



Cryptographic Function

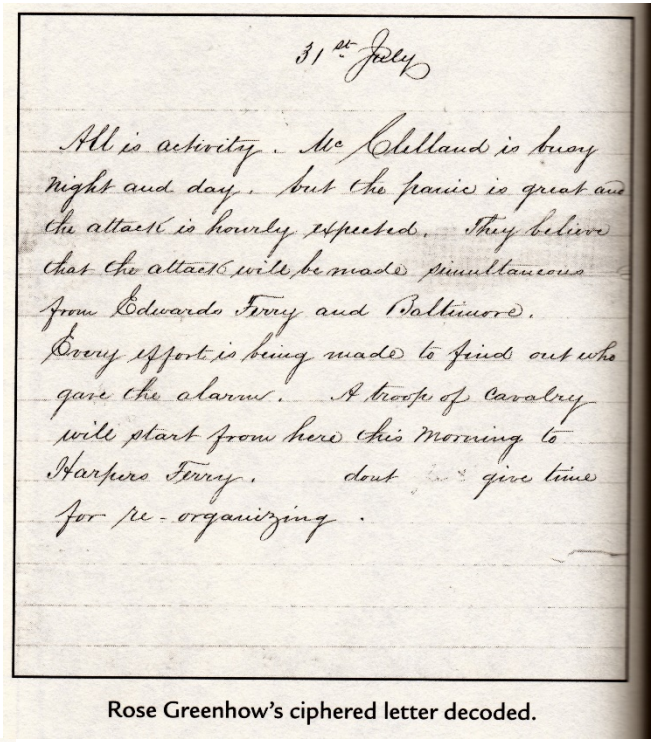
What is a cryptographic function?

- A function for encoding or encrypting data to protect the contents from adversaries

- Simple example function:
  - The Secret - “Blockchain Training Alliance”
  - The Function – Swap each letter in the secret with a new letter according to the Key
  - The Key - “+2”
  - The Cipher = “Dnqemejckp Vtckpcpi Cnnkcpeg”

Cryptographic Function

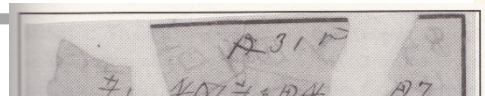
- Real World Example: Rose Greenhow
  - Renowned confederate spy during US Civil War
  - Socialite in Washington D.C.
  - Used cryptography to communicate



31st July

All is activity. McClelland is busy night and day, but the panic is great and the attack is hourly expected. They believe that the attack will be made simultaneous from Edwards Ferry and Baltimore. Every effort is being made to find out who gave the alarm. A troop of cavalry will start from here this morning to Harpers Ferry. dont give time for re-organizing.

Rose Greenhow's ciphered letter decoded.



Cryptographic Function

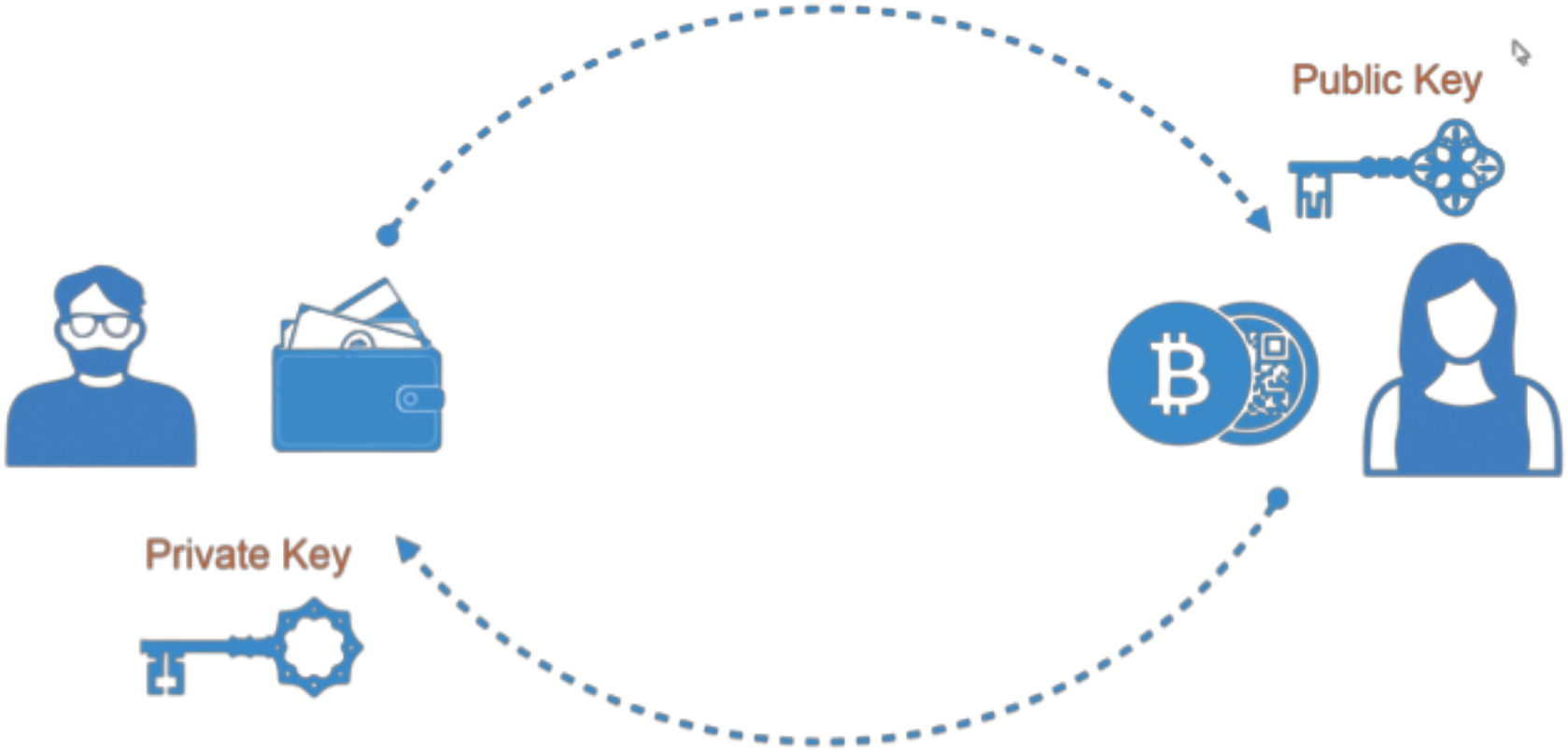
Public Key Cryptography

- Provides identity & transaction approval
- Public Key
  - Verify the digital signature of a given key pair
- Private Key
  - Sign/approve any transaction/action that might be made by the holder of the key pair

PUBLIC/PRIVATE KEY CRYPTO

- 2 uniquely related cryptographic keys
- Data encrypted with the public key can only decrypted with the private one (and vice versa)
- Main aim is confidentiality (in messaging)
- Also used for digital signatures

Public and Private Keys



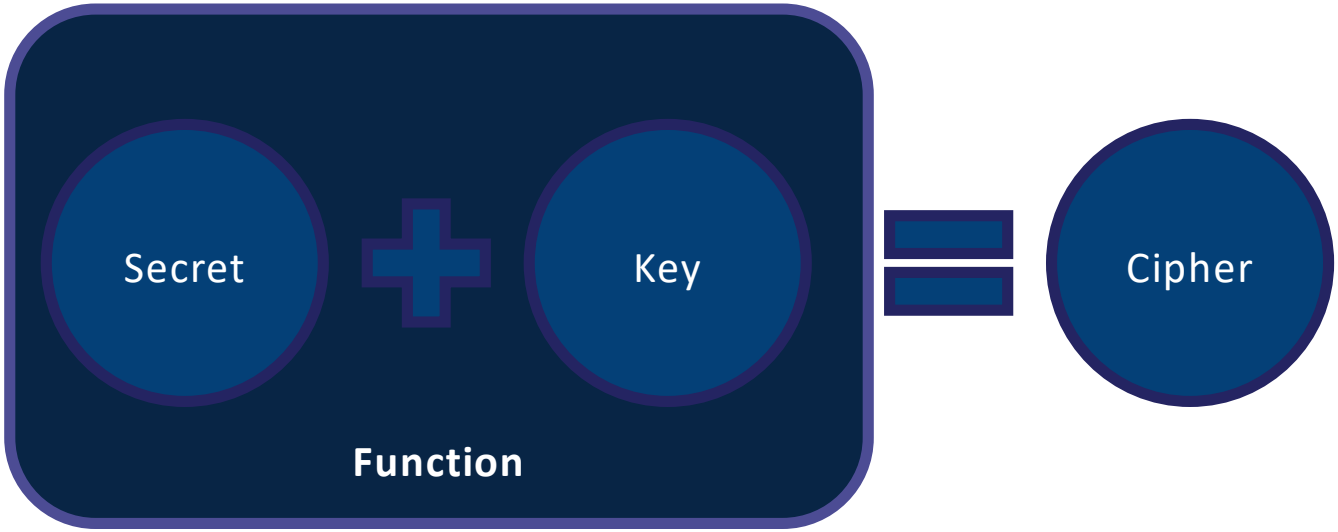
Important Terms

Terms:

- The Secret – The data which we are trying to protect
- The Key – A piece of data used for encrypting and decrypting the secret
- The Function – The process or function used to encrypt the secret
- The Cipher – The encrypted secret data, output of the function

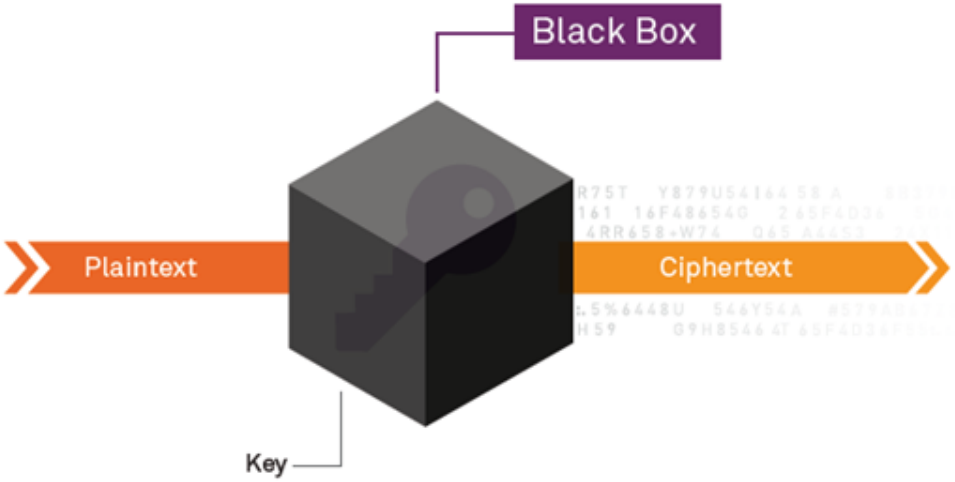
Cipher

- The Secret and the Key are passed into the Function to create the Cipher



Cryptographic Hash

- What is a cryptographic hash function?
  - A hash is a one-way function, encrypted information CANNOT be decrypted
  - Each unique input generates a unique output



Cryptographic Hash

- Why would I want to use a hash?
  - Address privacy concerns by making net worth private with a "digital thumbprint"
    - This would NOT be acceptable:
      - Sally - $418,013.45
      - John - $93,247.89
      - Mary - $9,423.11
    - This WOULD be acceptable:
      - 0376189a740845f75bde8260416b3812ab6d4377 - $418,013.45
      - 5753A498f025464d72e088a9d5d6e872592d5f91 - $93,247.89
      - 94F85995c7492eec546c321821aa4beca9a3e2b1 - $9,423.11
    - Nobody knows Sally's net worth, but Sally can always prove which account is hers

Cryptography Example

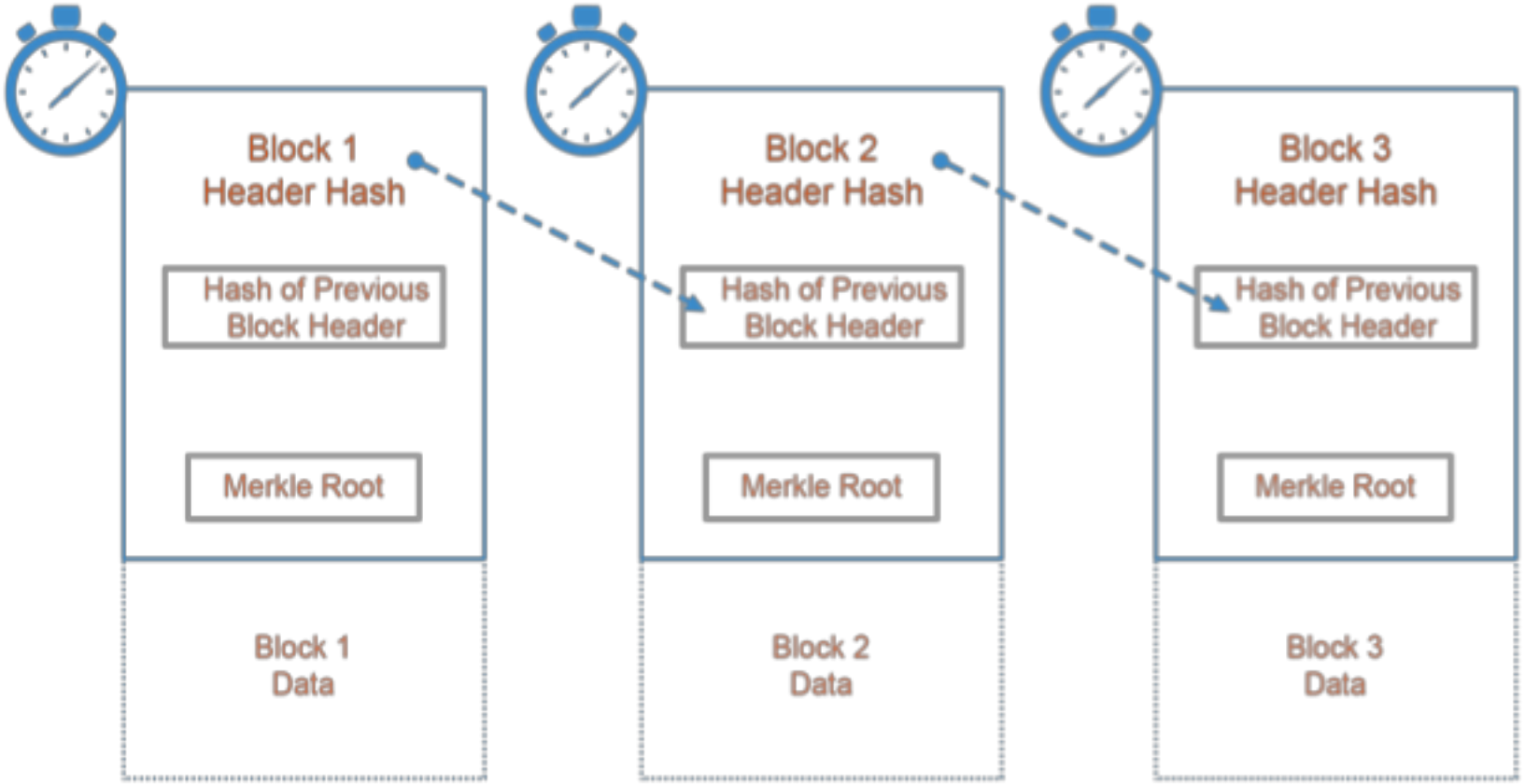
- Cryptographic Hashing example
  - Try it out (using SHA256)
  - Go to: www.anders.com/blockchain/hash.html

    (or: bit.ly/2HnJS6O)
  - Demo:
    - Let's eat, Grandma
      - 45b09eea07b7896d836308e89d01986ea92227ea41d5239dc42650c66393cc01
    - Let's eat Grandma
      - aab9185e406446c4700be80ae8c274778a15e9f2914303ae803ecfa2eca19b5a

Cryptographic Hash

- Why would I want to use a hash?
  - Landlord and tenant can compare lease documents
  - Verification of software
    - If there's ANY difference between what should be and what is, it's easy to identify
      - Malware which makes slight changes to the original codebase can be easily detected
      - Important for self-driving cars, automation, IoT, etc..
  - Instantly compare two or more LARGE volumes of data to ensure they're the same
    - Has 1 bit been flipped in a 100TB file?

Blockchain Basics - recap



Mining a Block

Transaction Implications

- Transactions take time to ‘confirm’
- Each transaction, once it’s in an accepted block has a height
  - The height of a block is the **number of blocks in the chain between it and the genesis block**
- Each increase in blockchain height is called a confirmation
- A transaction 5 blocks below the top of the chain is said to have ‘6 confirmations’
- Wait for 6 confirmations for anything of value

Blockchain Forks

- Upgrades to the protocol can cause problems – but can be managed
- Blocks that are created have a version number
- New blocks using the new protocol use a different version number
- If the upgrade is backward compatible, it's a soft fork
- If the upgrade isn't backward compatible, it's a hard fork
- Hard forks are much harder and we try to avoid them

Types of Consensus

Consensus

- Proof of Work Consensus
  - When a block is full, each node competes to solve a guessing game problem
    - This problem requires computational resources to quickly guess the “Nonce” of the transaction block
    - Miners try to guess the “nonce”
      - All block data plus the current guess (nonce) are run through a cryptographic hash
  - If the result matches the current level of “difficulty”, the miner has guessed the right answer
  - The miner with the answer shares it with all other miners, Miners will confirm the answer is correct by using the nonce with their block data to try and get the correct result. When 51% of the miners confirm the nonce is correct, the transaction is added to the Blockchain
  - The result is Proof of Work Consensus

Proof of Stake (PoS)

- Proof of Stake Consensus
  - Proposed as an alternative to Proof of Work
  - Attempt to overcome scalability concerns imposed by PoW consensus
  - Removes the guessing game from consensus
  - Mining no longer requires specialized and powerful hardware
    - Many feel that specialized hardware requirements lead to centralization
      - Blockchain is about de-centralization
  - Less energy intensive form of consensus
    - Addresses concerns about “green” mining

Proof of Stake (PoS)

- Proof of Stake Consensus
  - Ok, how does it work?
    - Block of transactions created
    - When it's time for group consensus, all who wish to participate lock up funds in a stake
    - A random 'player' is selected
    - That player's block data is shown to all other participants
    - Other players stake on the validity of the block transactions

Proof of Stake (PoS)

- Proof of Stake Consensus
  - If the majority agree with the proposed block, the random player is rewarded, as are all who staked on that player
  - If the majority disagree, the random player gets no reward AND loses their stake!
  - Then a new player is randomly selected to share their block data

Proof of Stake (PoS)

- Proof of Stake Consensus
  - No “computing” is ever performed during consensus, only staking/wagering
  - Any kind of device can stake, regardless of computing power
  - Some argue that this also leads to centralization as only players who can afford to stake are able to participate in consensus

PoW vs PoS

- PoW vs PoS
  - Work for a reward vs make a safe bet for a reward
  - Security vs Speed
  - Centralization vs Decentralization
  - Proven vs New
  - Capital spent on hardware vs capital spent on staking funds

- Ethereum – quickly moving to PoS
- 0.1.0 Released May 2018

Other Consensus Mechanisms

- Other consensus mechanisms
  - Proof of Activity
    - Hybrid of PoW and PoS
    - Empty template blocks are mined (PoW), then filled with transactions which are validated via PoS
  - Proof of Burn
    - Coins are “burned” by sending them to an address where they cannot be retrieved
    - The more coins you burn, the better your chances of being selected to mine the next block
    - Eventually, you must stake more by burning more coins

Other Consensus Mechanisms

- Other consensus mechanisms
  - Proof of Capacity (aka Space)
    - Pay to play with hard drive space or memory
    - The most space you ‘stake’ the better your odds of being selected to mine the next block
    - Consensus algorithm generates large data sets called ‘plots’ which consume storage
    - Major criticism – this method has no real deterrent for bad actors

Other Consensus Mechanisms

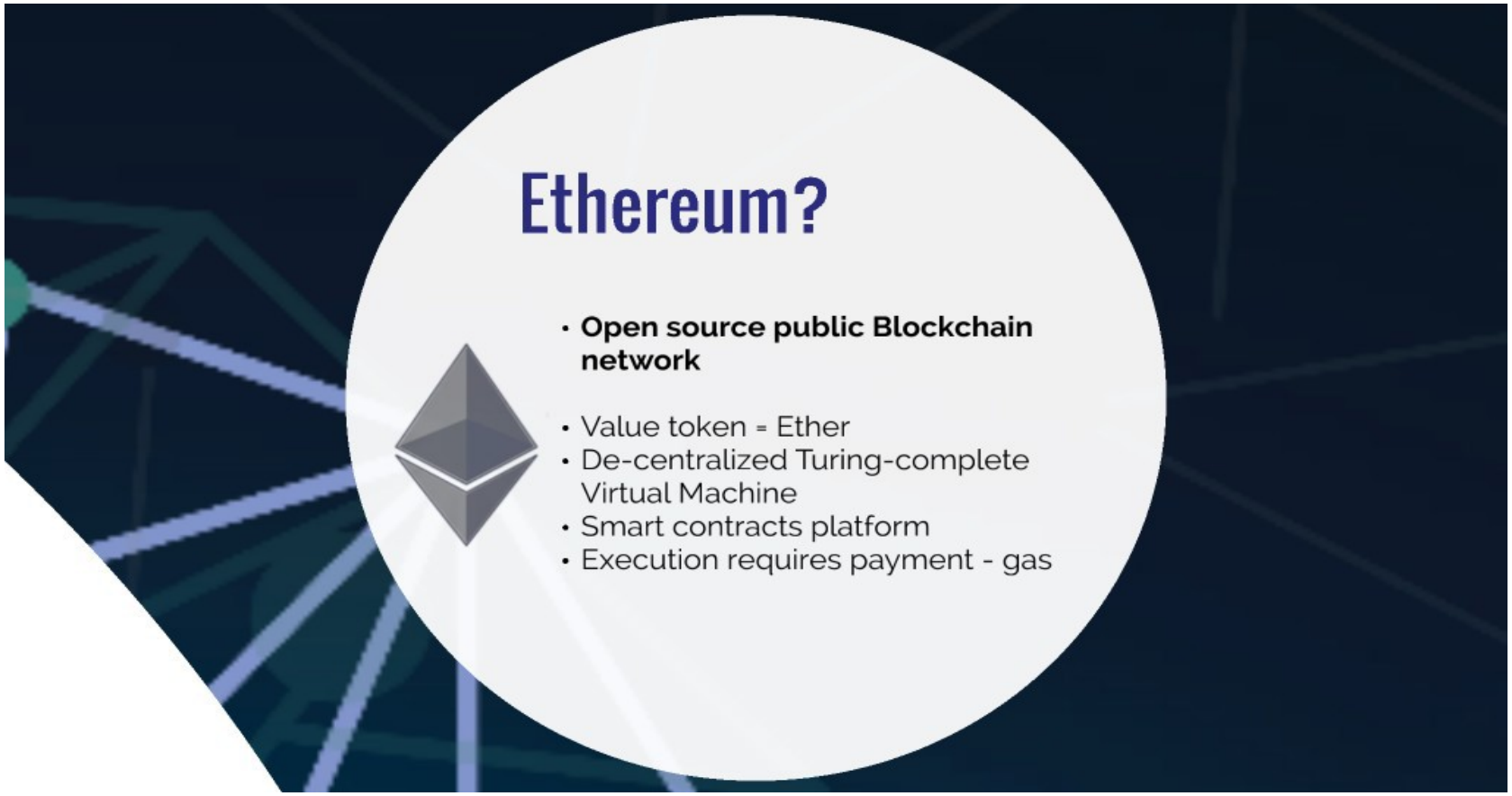
- Other consensus mechanisms
  - Proof of Elapsed Time
    - Created by Intel to run on their trusted execution environment
    - Similar to PoW, far more energy efficient
    - Major criticism – requires trust in Intel, places power back in the hands of a central authority
  - Proof of Authority
    - Uses a set of “authorities” – nodes that are explicitly allowed to create new blocks and secure the blockchain
    - Replacement for PoW - Private blockchains only
    - Earn the right to become a validator/authority

Consensus Mechanisms

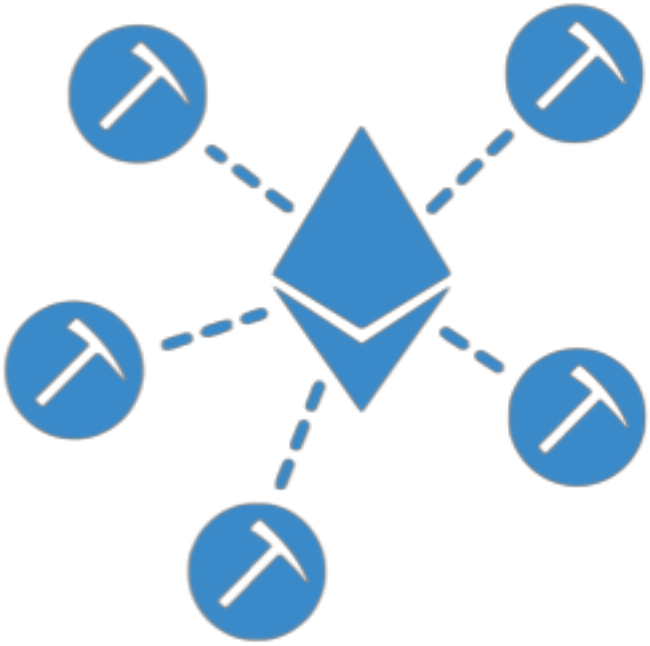
- Consensus protocols are the key to Blockchain!
  - Blockchain consensus mechanisms are the nuts and bolts of validation.
  - Think Internet & TCP/IP – transmission of bytes of data across the Internet
- PoW is the only tried and true (9+ years in use). PoS is coming, rolling out now.
- The rest are concepts and development ideas that different developers are working on. Some are in a test trial phase.

Blockchain 2.0 and Ethereum

Ethereum Overview

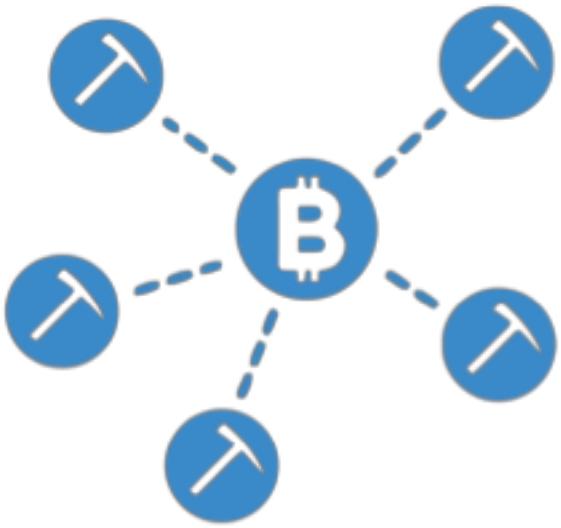


Blockchain - Ethereum

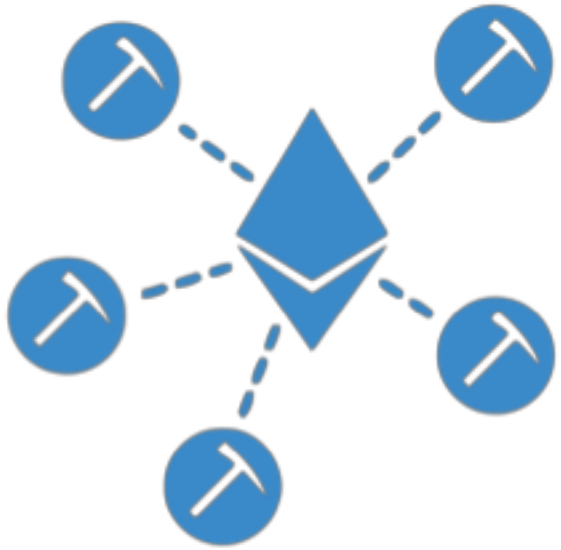


It provides a decentralized Turing-complete virtual machine, which can execute computer programs using an global network of nodes

Blockchain – Current Transactions per Second



TPS = 7



TPS = 15

Visa can process over 70,000 TPS, Facebook can handle 175,000 TPS

Ethereum Smart Contract

Smart Contract

Computer code, written in multiple languages

- Contract lives on the network
- Enforces rules
- Performs negotiated actions

ETH Valuations

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

ETH Supply

Ethereum EVM Software

EVM

- An software that can execute Ethereum Bytecode
  - Follows the EVM specifications (Ethereum protocol)
  - Runs as a process on a computer/sever

- EVM implemented in multiple languages

Ethereum Gas

Gas

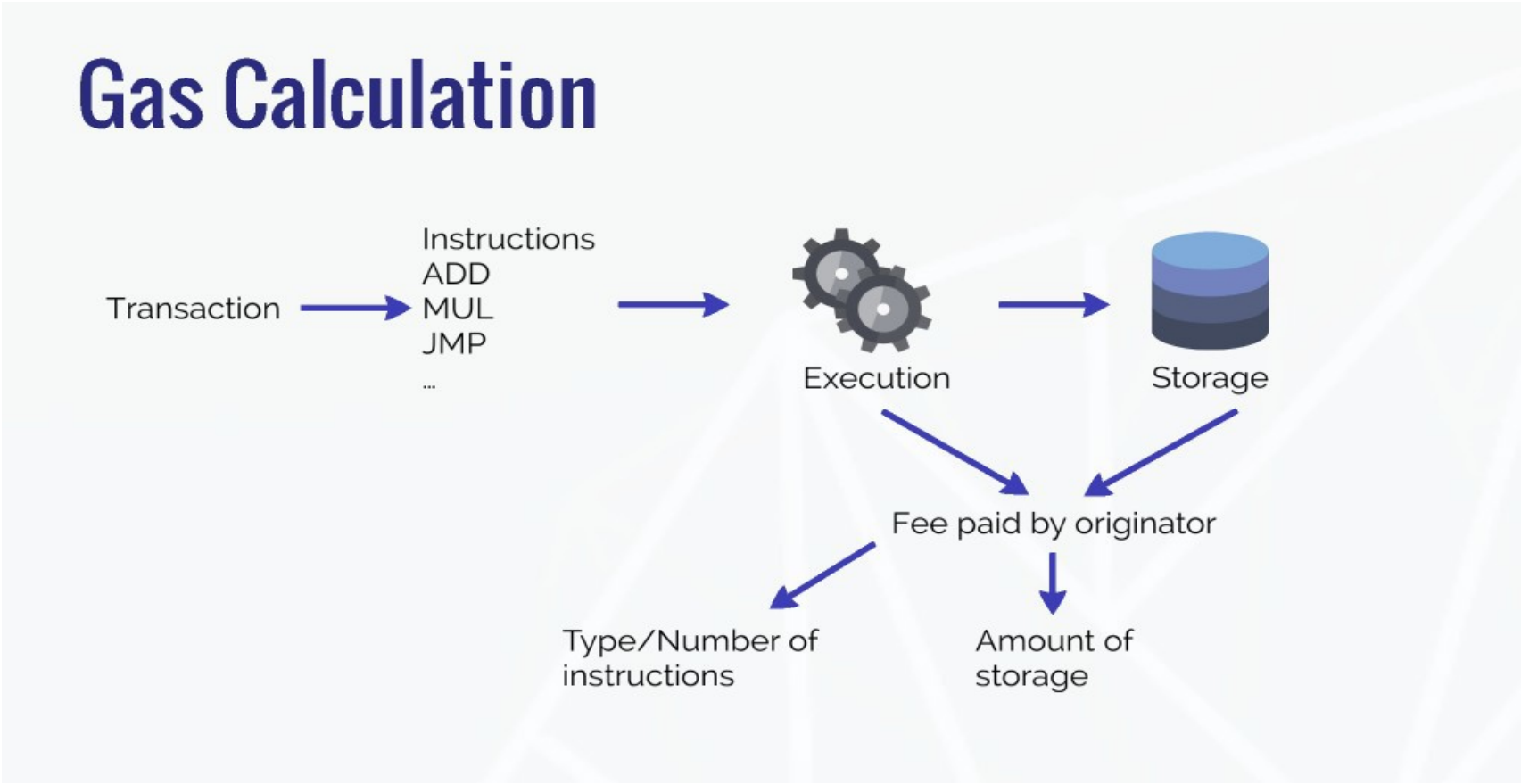
- User invoking the transaction pays for the execution

Measures: kWH used

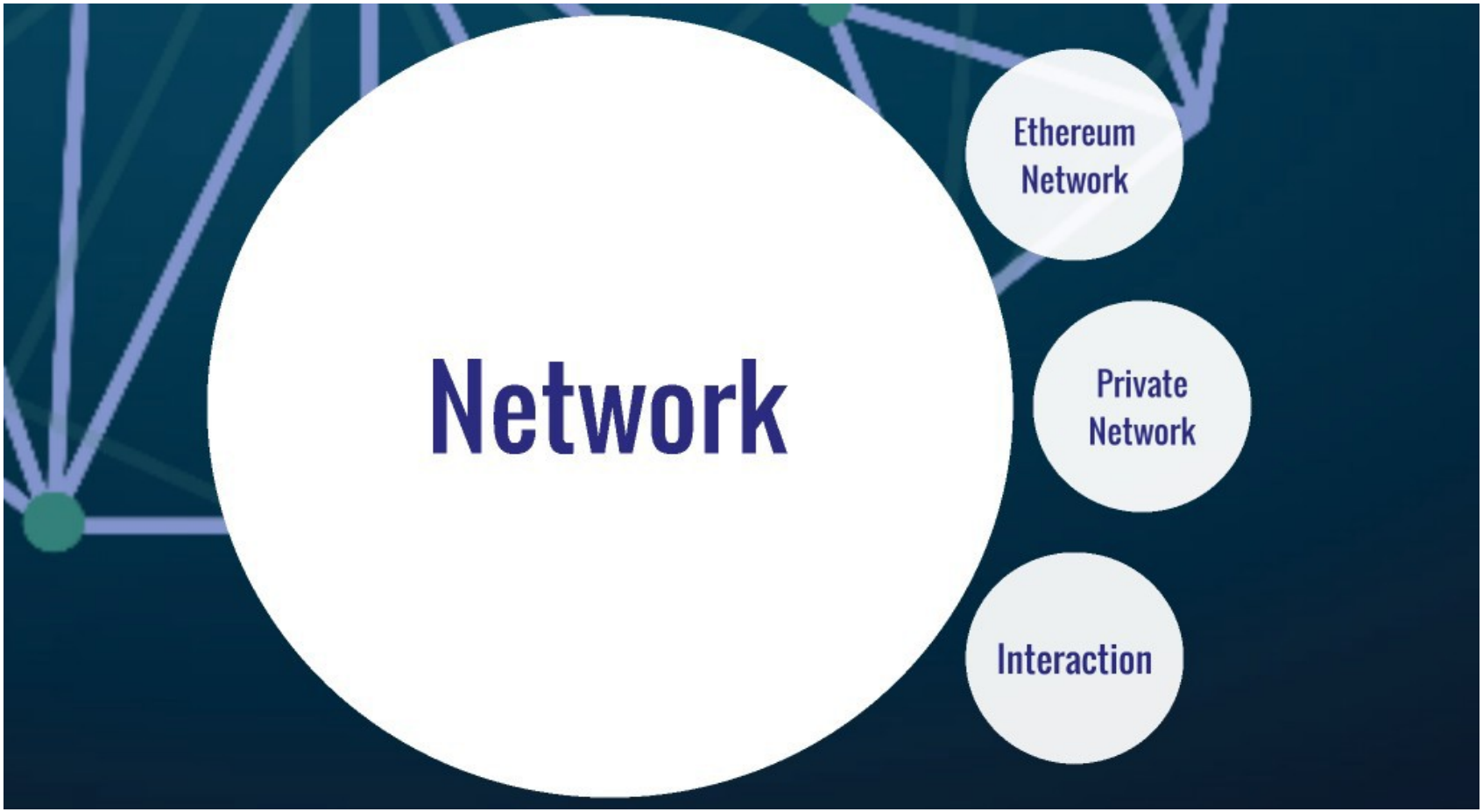
Measures: Gallons of water used

- Gas is the unit in which EVM resource usage is measured

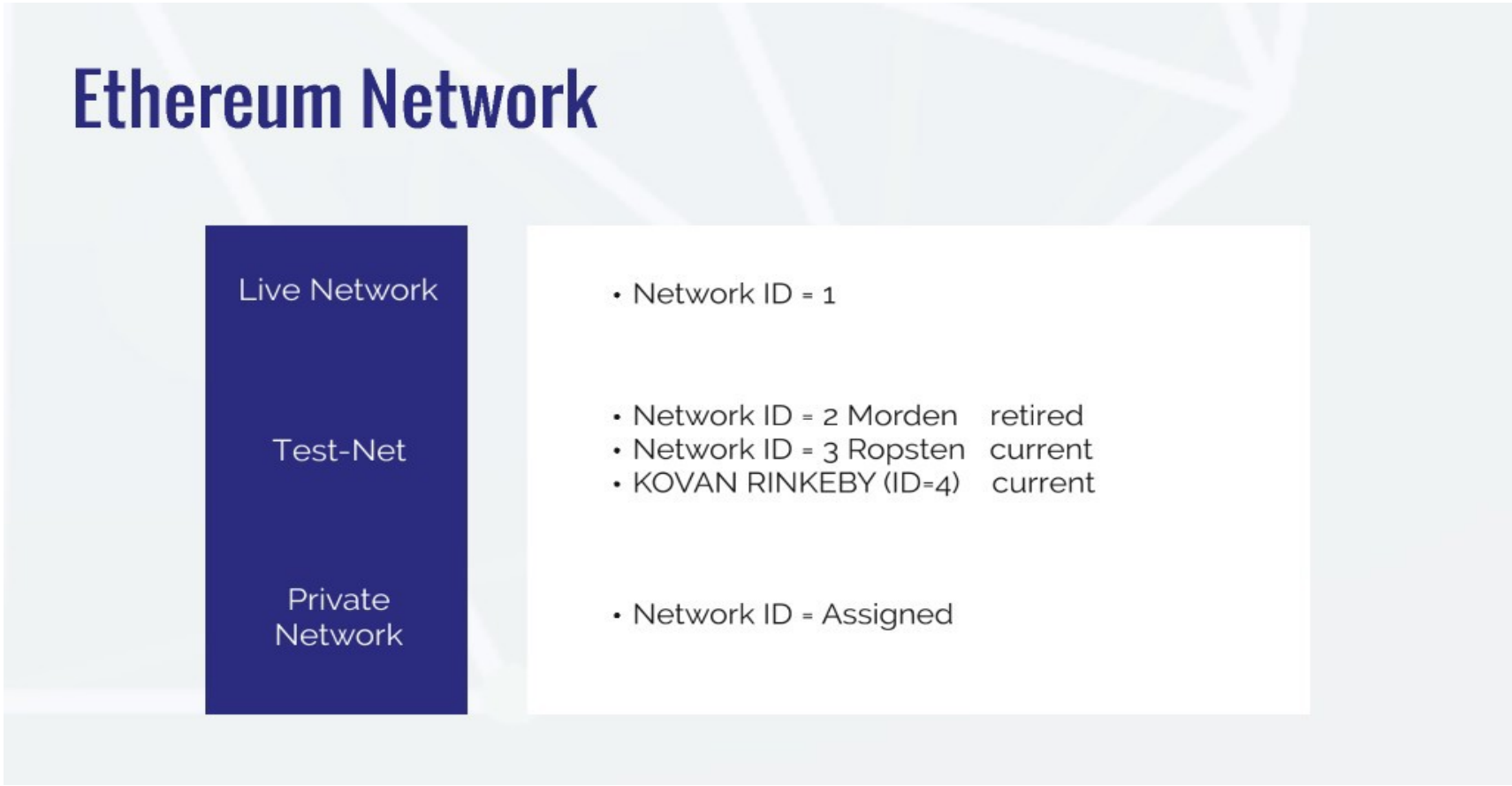
Ethereum Gas



Ethereum Network



Ethereum Network



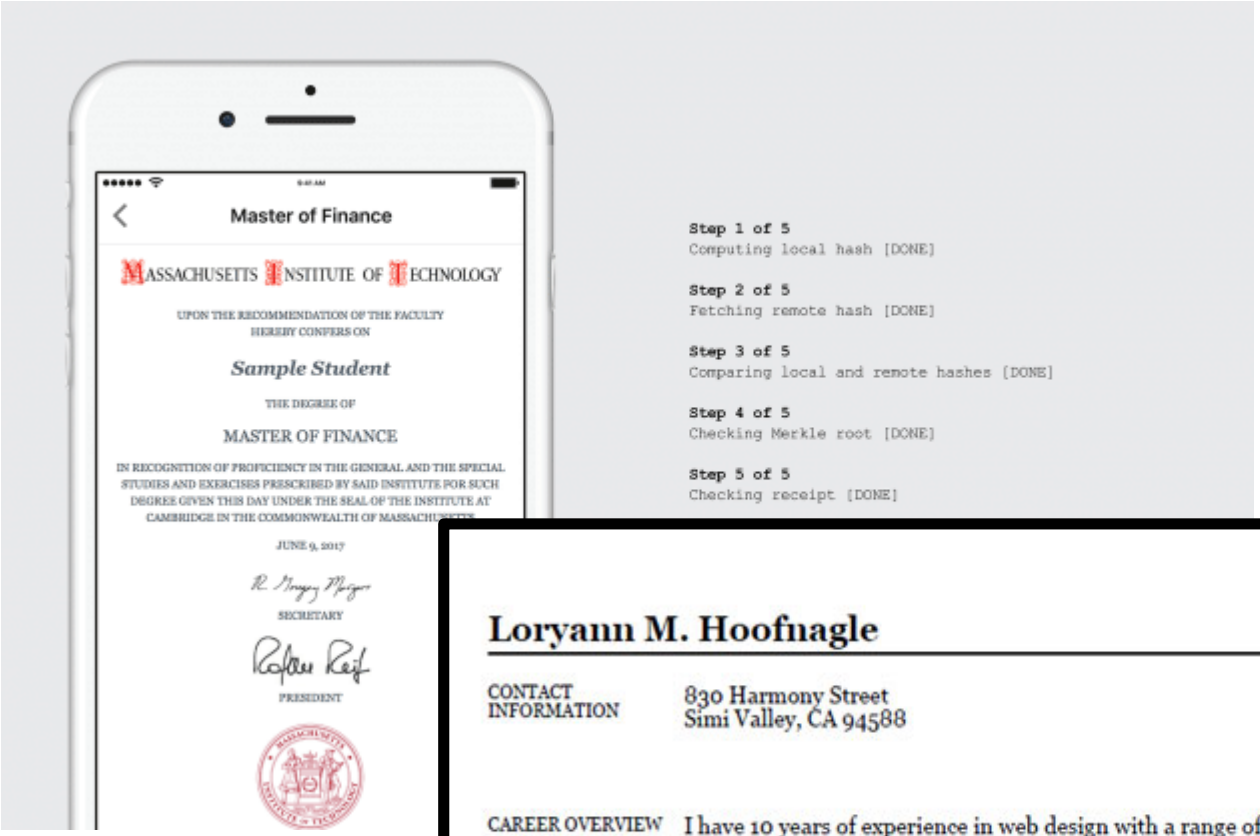
Blockchain Use Cases

Just a Few Use Cases

- Background checks: education credentials, criminal records
- Secure document storage: home deed, auto title
- Birth registries
- Land registries
- Financial services: securities clearing, syndicated loans
- Global supply chain: automotive recalls and counterfeit airbags
- Healthcare: EMRs, insurance claims, genome research
- Airlines: registration, re-booking, vouchers, loyalty
- Tokenized economy: Tech Coworking space 1 token = 1 seat
- Payment channels: Starbucks or for bandwidth consumption

Background Checks

MIT Digital Certificates (diplomas); Criminal Records

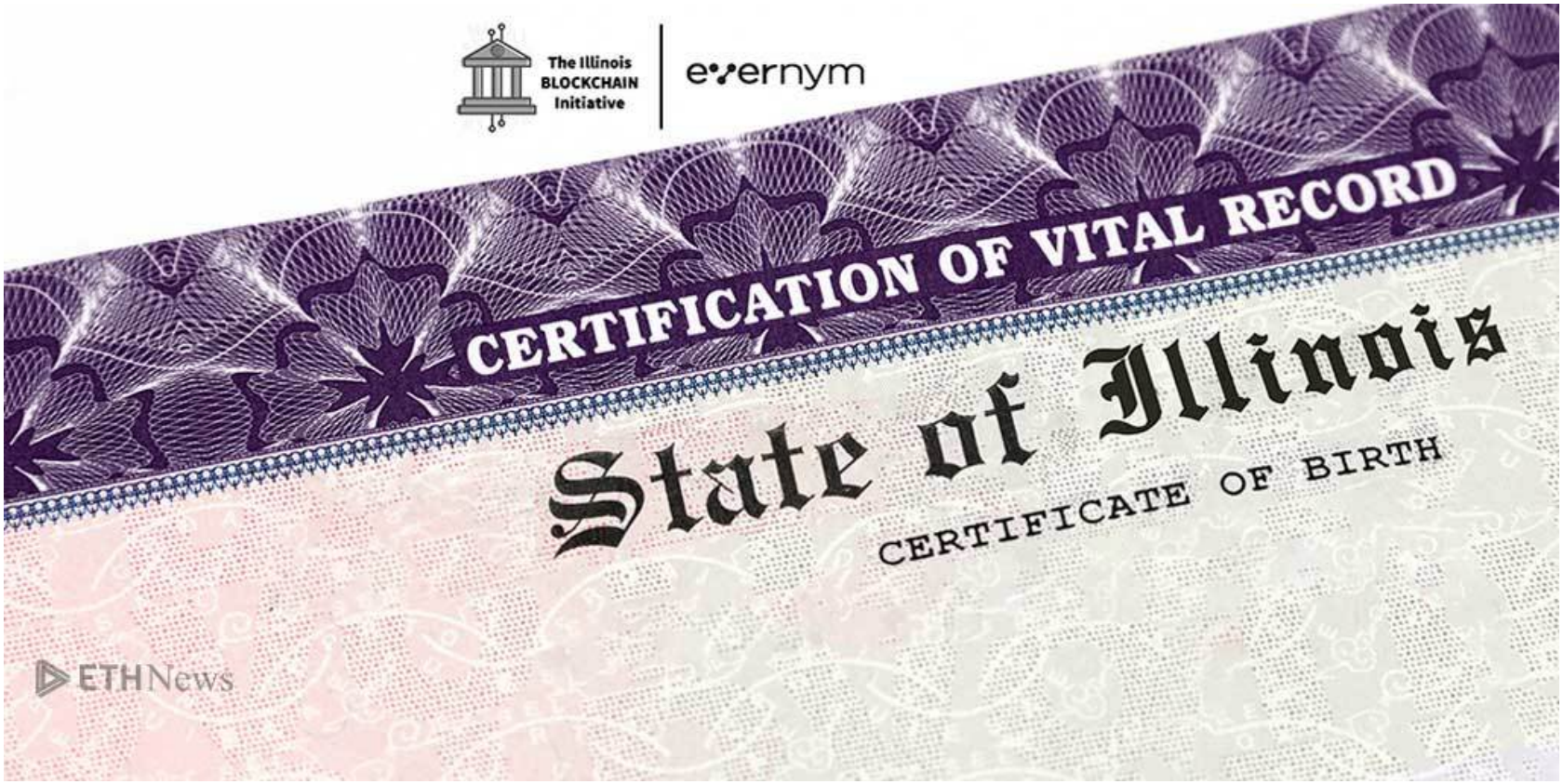



```
Step 1 of 5
Computing local hash [DONE]

Step 2 of 5
Fetching remote hash [DONE]

Step 3 of 5
Comparing local and remote hashes [DONE]

Step 4 of 5
Checking Merkle root [DONE]

Step 5 of 5
Checking receipt [DONE]
```

Loryann M. Hoofnagle

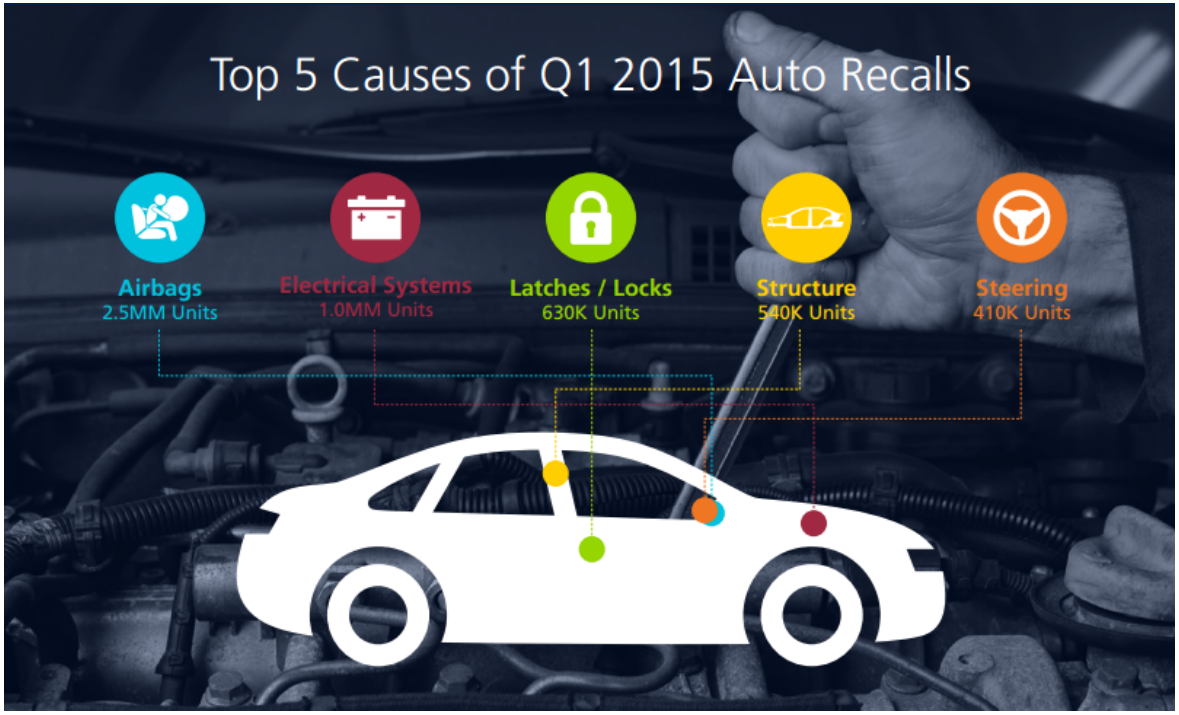
CONTACT INFORMATION	830 Harmony Street Simi Valley, CA 94588	home: 805-960-6116 work: 805-990-1747 email: demo@opresume.com website: http://OPResume.com/demo
CAREER OVERVIEW	I have 10 years of experience in web design with a range of clients including small private companies, medium-sized e-commerce shops, and large online magazines. My main focus is on design, usability and SEO optimization.	

Birth Registry



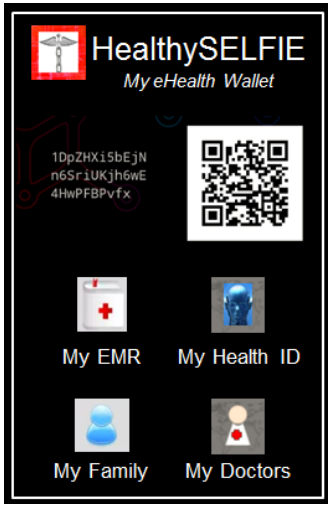
Global Supply Chain

- Automotive Industry Recalls and Counterfeit Airbags
- Business case: 30% global airbags sold and installed are counterfeit
- Solution: Single shared process for airbag registration and lookup



Healthcare

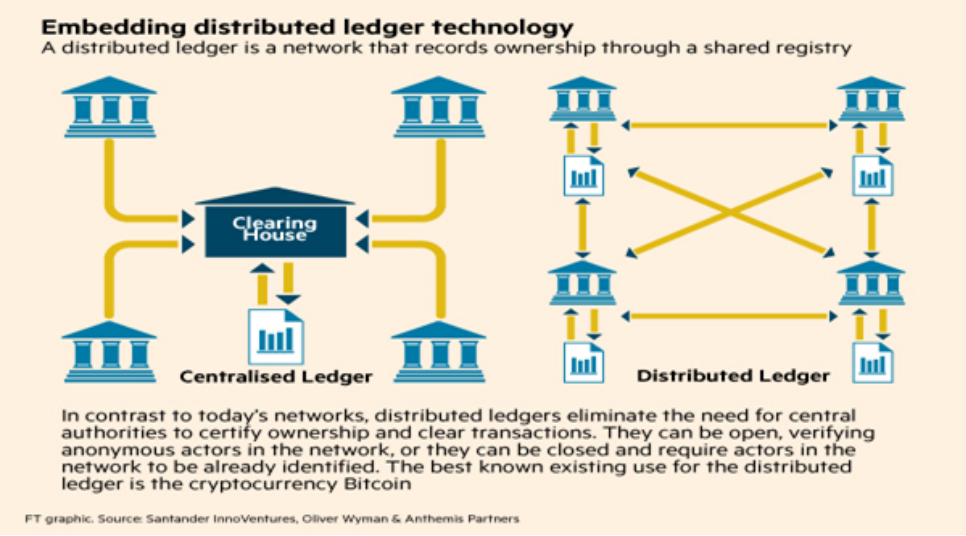
- Electronic Medical Records (EMRs)
  - Digital health wallet
    - Identity credentials + EMR + health insurance + payment information
- Health insurance claims
  - Automated claims billing, validation, payment, and settlement
  - Multi-party value chain: patient, service provider, billing agent, insurance company, payor, government, collections
- Genomic research
  - Files too large (20-40 Gb) for centralized research repositories
  - Need secure validated access



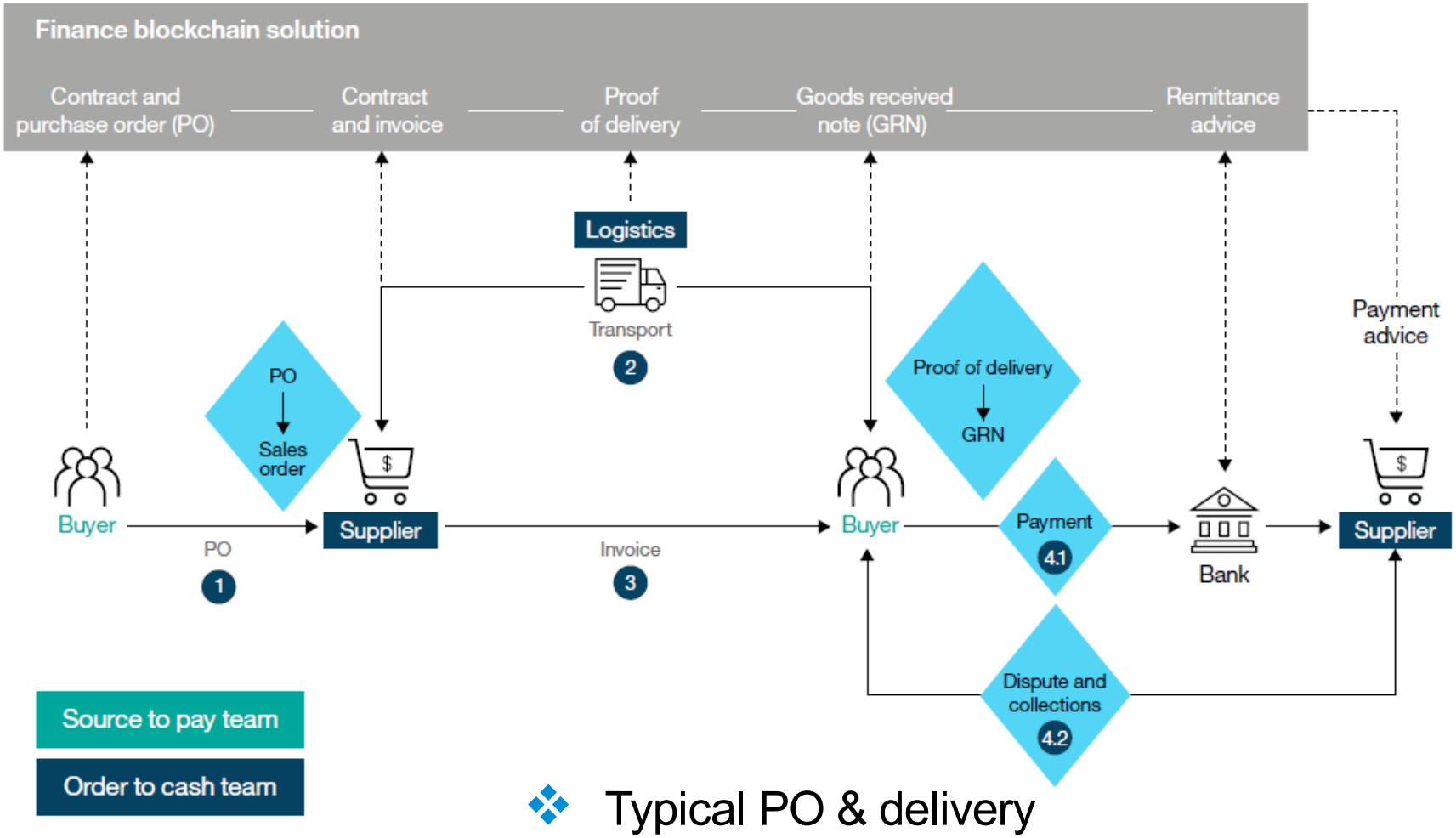
Digital health wallet

Financial Services

- Clearing and Settlement
- Issuance, Ownership, and Transfer of Financial Instruments
- Servicing of Instruments
- Payments and Remittance
- KYC/AML Compliance
- Regulatory Reporting
- Audit and QA
- Back-office Reconciliation



Financial Services - PO



- Typical PO & delivery

Airlines

- Registration System (like SABRE)
- Cross-airline flight re-booking
- Loyalty programs
- Flight cancellation smart contract vouchers

Smart contracts automatically issue vouchers to customers when flights are delayed or cancelled

Real Estate Services

Blockchain and Home Purchases

- Save by eliminating transaction fees for buyer/seller agent, banks and any other intermediaries
- Minimize turnaround time
- Eliminate escrow as Blockchain is only a source of trust
- Eliminate manual process for requesting mortgages

Blockchain and Political Systems

- Elections and Voting
- Liquid Democracy / Delegative Democracy
  - Voters can transitively delegate their votes
- Futarchy and Voting Prediction Markets
  - 2-tier voting for project area and approach
- Participatory Budgeting
  - Residents collectively decide how to spend their local government's budget
- Self-directed Public Finance
  - $500/$1000 personal bond offerings
- Virtual Democracy
  - Instant elections among machine learning models of real voters to address the challenge of ethical decision making

Blockchain Adoption

One of the fastest-moving technology adoptions

Blockchain Adoption

- Blockchain (distributed ledger technology) is being considered by more than half of the world's big corporations, according to a Juniper market research survey released Jul 2017
  - 57 percent of large corporations – defined as any company with more than 20,000 employees – were either actively considering or in the process of deploying blockchain
  - Two-thirds of companies surveyed by Juniper said that they expected the technology to be integrated into their systems by the end of 2018
- IDC: $2.1 billion estimated global blockchain spend 2018

https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html

The Future of Blockchain

Transforming Society

- Blockchain technology is bringing us the Internet of value: a new platform to reshape the world of business
- It transcends all physical and geographical barriers and uses math and cryptography to enable transactions globally
- The uniqueness of blockchain lies in its capacity to store and retain person-to-person transactional history, so that chances of fraud, hacking, and third-party interference are greatly reduced

Many Blockchains/Crypto currencies

- It's easy to create your own, and there are many.

- Each is separate and runs its own blockchain
- The value transferred in each blockchain is primarily in its own cryptocurrency

Parallels to the Internet

Blockchains today have been likened to the Internet in 90s.

- Only faster growing WW investment occurring!
- Touching a larger scope of business and society
- Exploiting Web 3.0 with unlimited uses (IoT)

History doesn't repeat, but it rhymes: We expect similar...but

- Faster path to maturity – continued expansion
- Wider – Faster Adoption curve
- Evolution of protocol and applications touching the lives of people previously unreached by the Internet

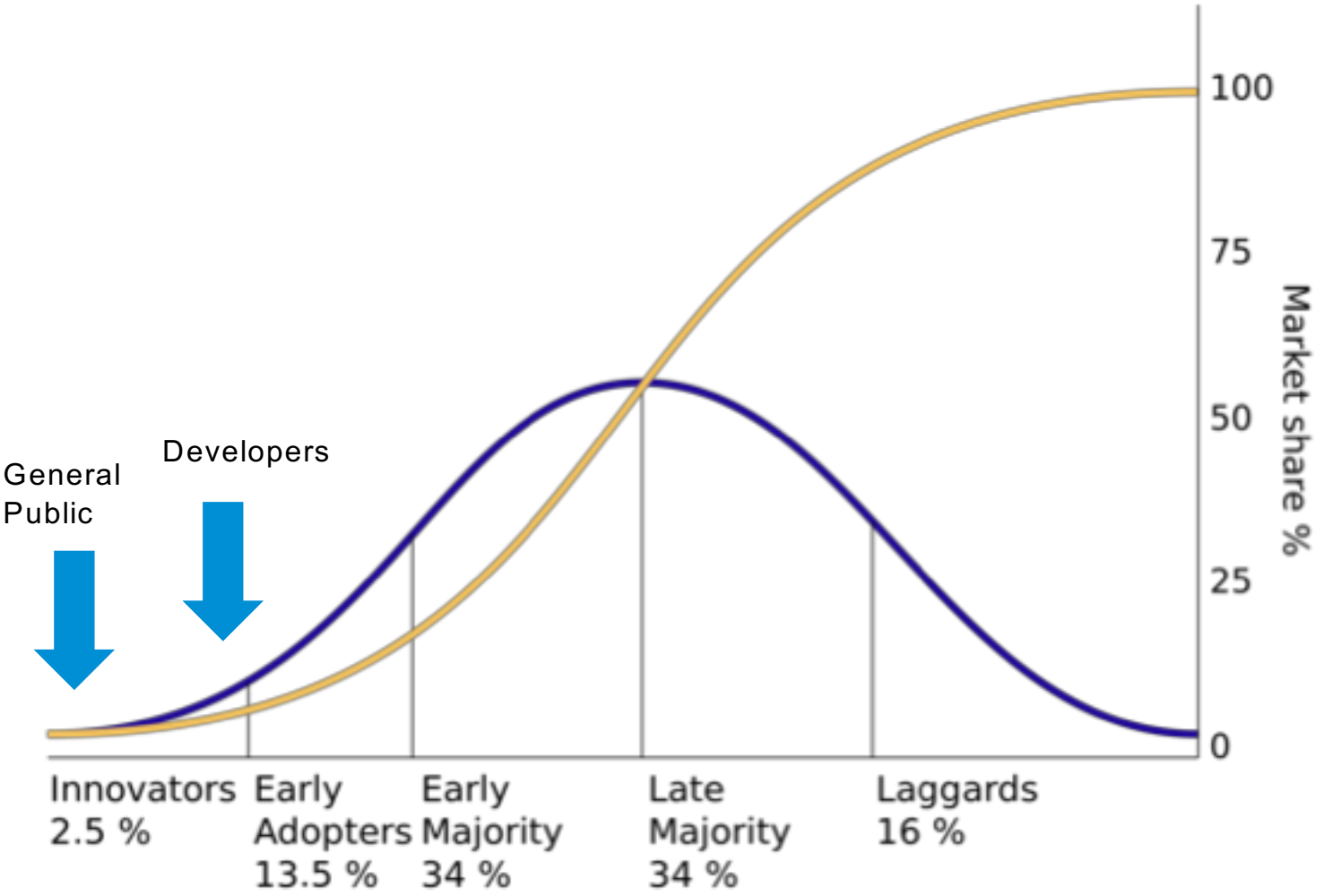
Parallels to the Internet

Just as the internet 1.0 revolutionized access to information, Blockchain is doing the same to multiple industrial verticals:

- Finance and Commerce first
  - It's what Blockchain's purpose is
  - It's where the money is
  - Greatest opportunity to reduce business cost
- Non-finance uses
  - Specialist Blockchains dedicated to one task
  - Typically tied to a cryptocurrency
  - Generalist Blockchains to be used as a 'platform'

Blockchain Technology is moving very fast – still a lot to learn and new opportunities on many levels, industries, services, and trade!!

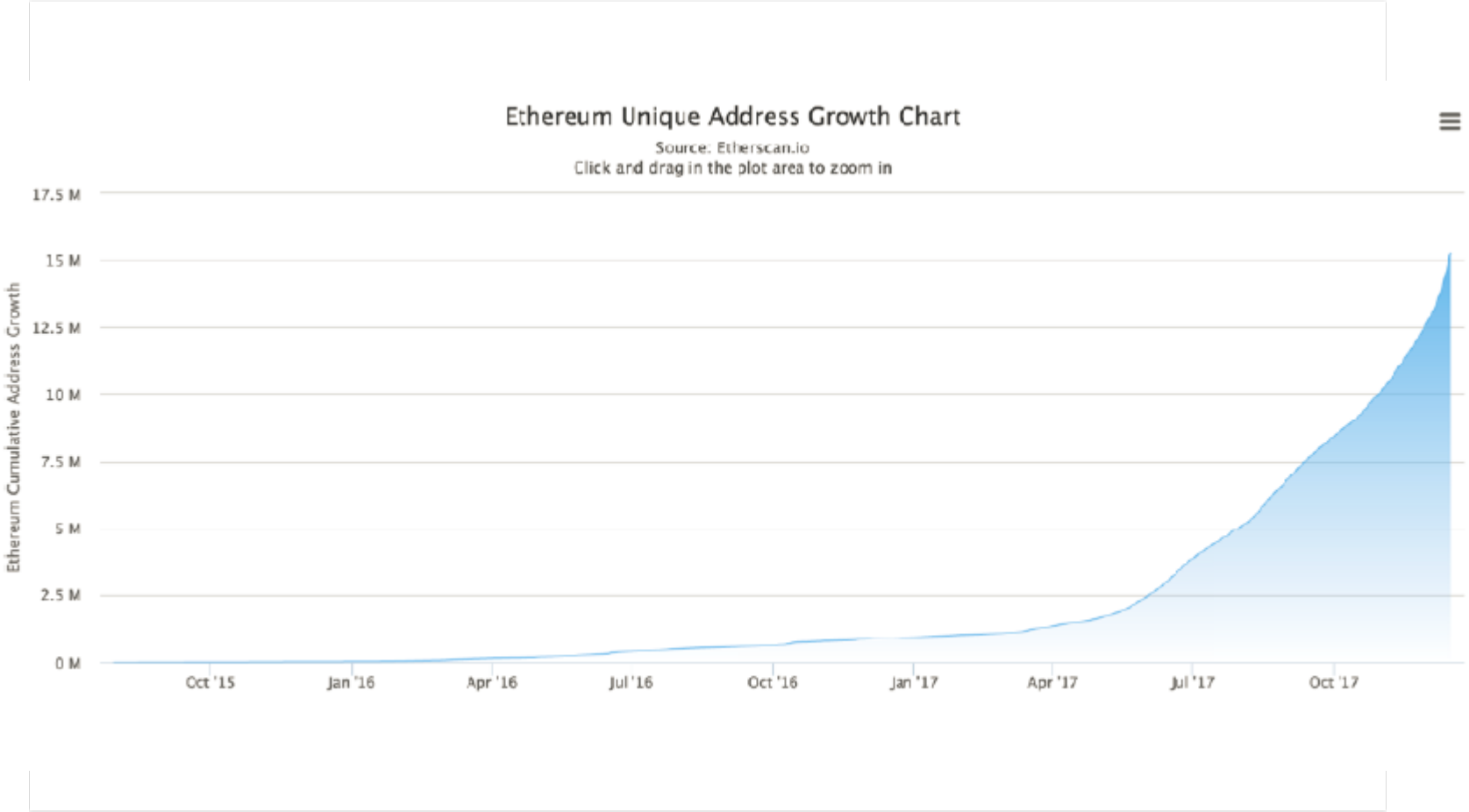
Where Are We Now?



Investment Into the Sector

- Reid Hoffman (LinkedIn) Invested US$20M in Blockstream
- Sir Richard Branson backed BitPay (Exchange) in a US$30 Million
- Circle (Exchange) raised US$50 Million - led by Goldman Sachs
- NYSE led a US$75 Million Investment in Coinbase (Exchange)
- Large BaaS (Blockchain as a Service) investments by IBM, SAP, Cisco, AWS (2017 -2018)
- Mercedes Benz invests $110 million to explore blockchain use cases
- Blockchain investments are extending to the underdeveloped countries and underbanked areas of the world quickly, providing a way to do personal business, as well as commerce

Growth in CryptoAddresses



Wall Street Blockchain Investment Growing

BARCLAYS

Three blockchain startups selected for Barclays Accelerator, with one aiming to provide blockchain solutions for the insurance industry

citi

Citi wants "to [accelerate] emerging technologies that have the potential to transform financial services experiences for Citi's customers"

UBS

UBS is set to open a London-based research lab to explore the application of blockchain technology in the financial services industry

Sources: CoinDesk, Bank Innovation

Web 3.0

Internet Technology Progression

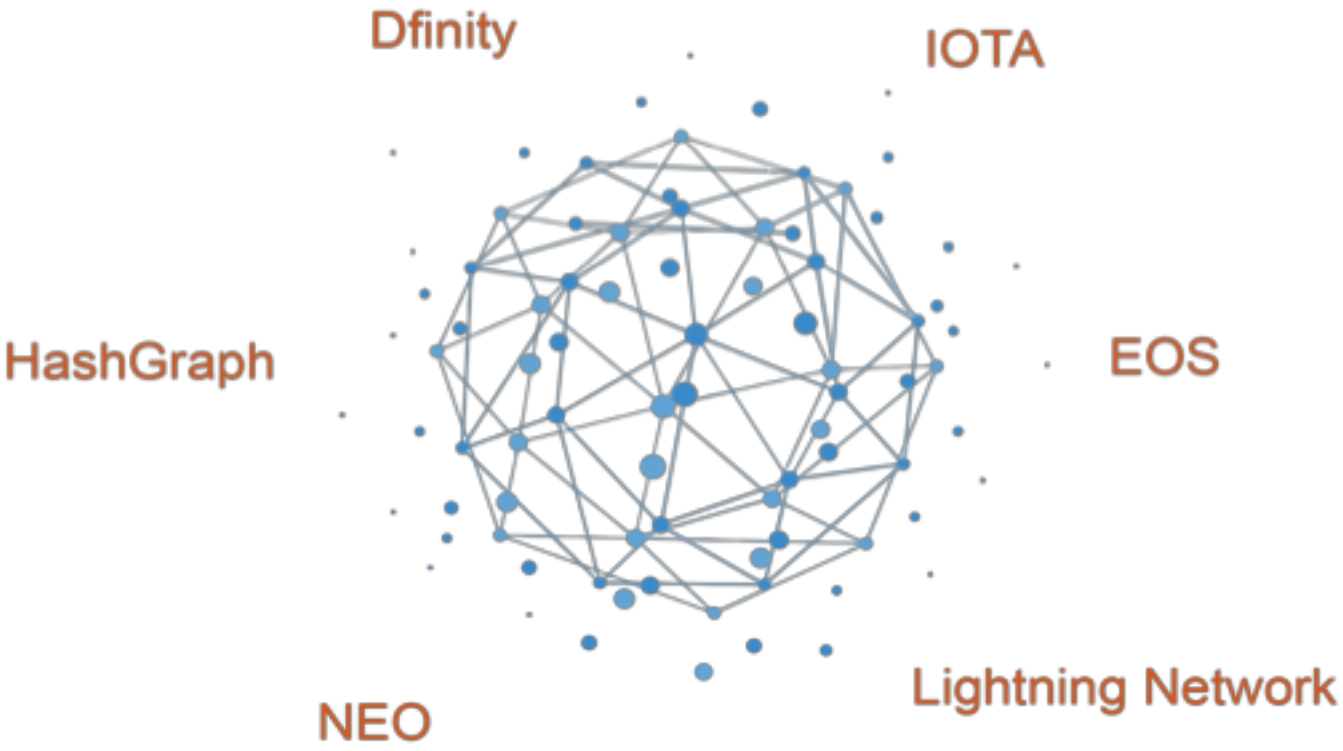
Internet 1.0
Static Information
WW Explosion of Information

Internet 2.0 Social Engagement
Twitter, Facebook, New Voice of
People Worldwide

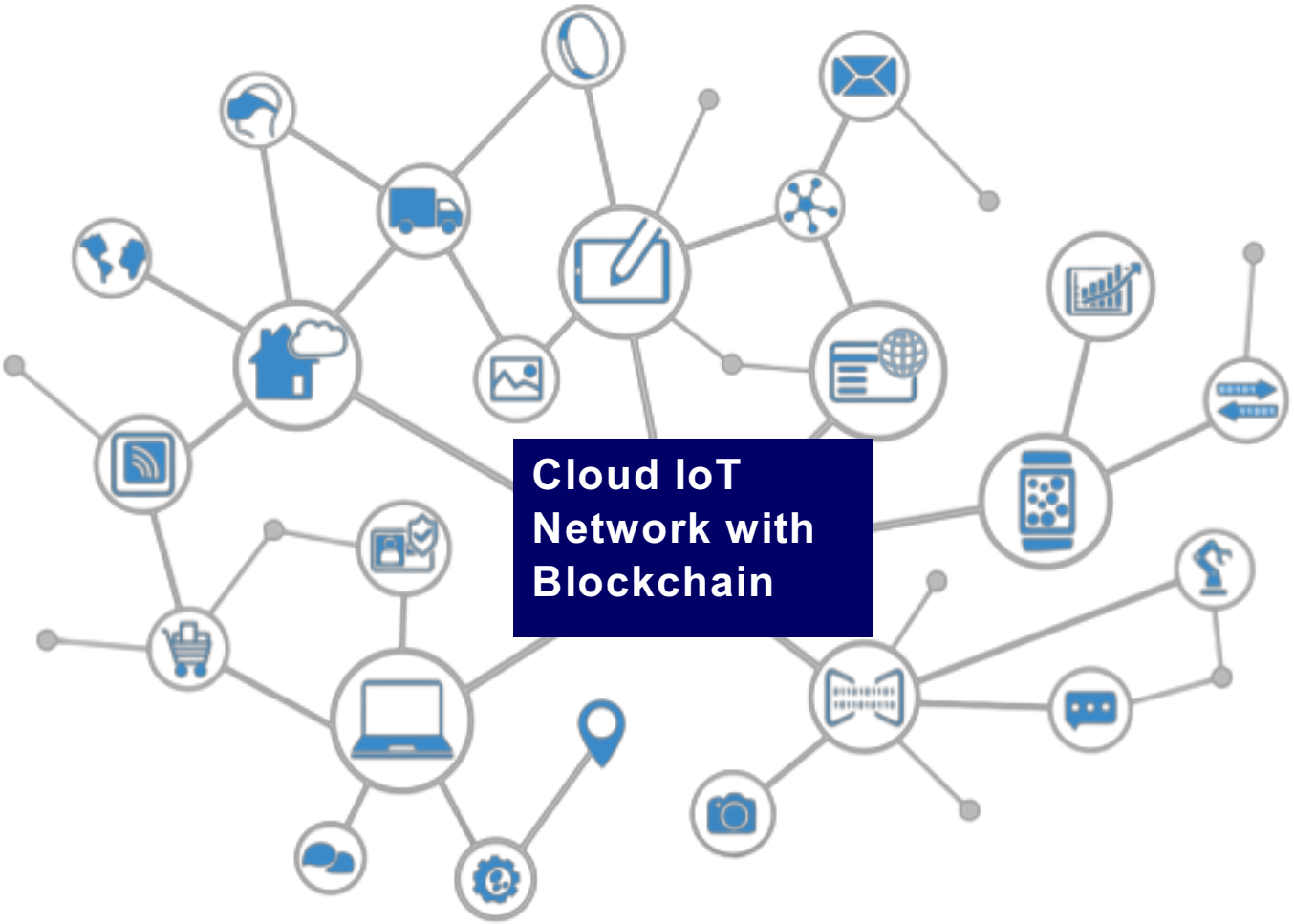
Internet 3.0 The Internet of Value. Communication, commerce, and participation at all levels. i.e. The Internet of Things (IoT)

Blockchain – New 3.0 Solutions

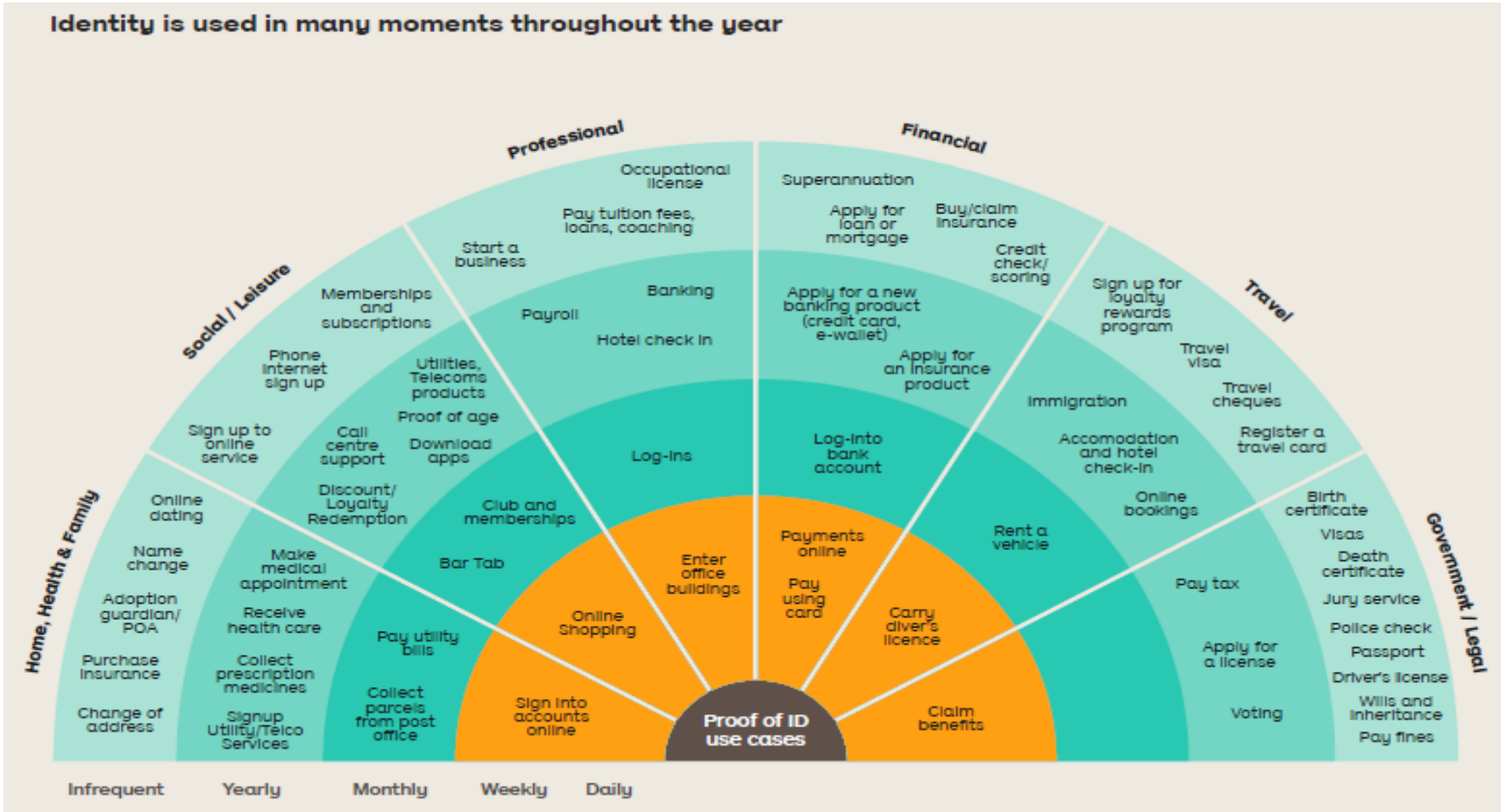
Many new Blockchain networks are evolving to provide scalability and solve many of the current problems. New protocols such as Lightning's Off-Chain solution, and IOTA's parallel transactions are just two of the schemes being developed and tested.



Blockchain – Future Internet 3.0



Digital Identity Touch Points using Blockchain



Blockchain Implementation

Top 5 Blockchain Platform Features

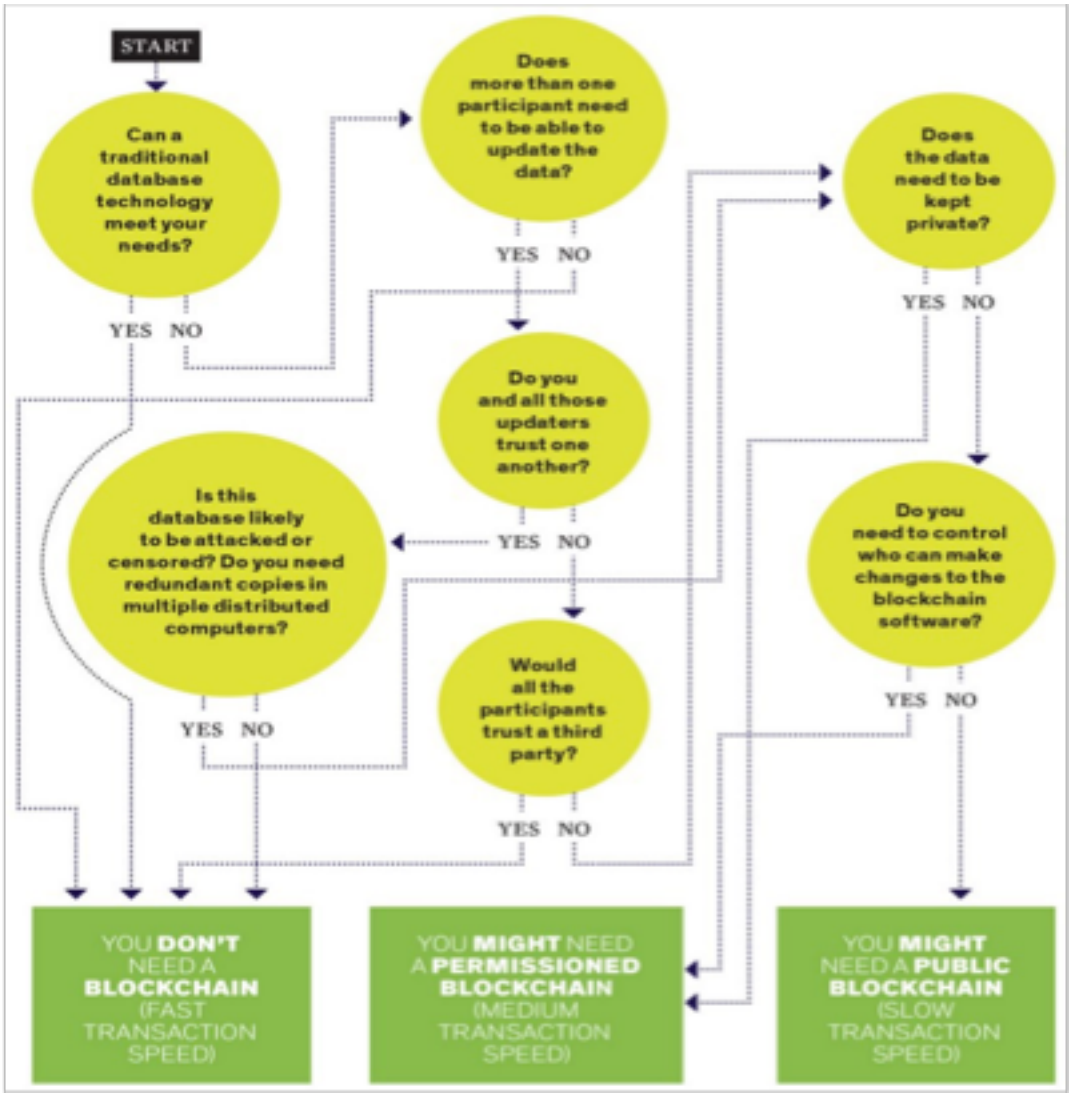
Summary of Features of top 5 Blockchain Platforms for Enterprises

	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry-focus	Cross-industry	Cross-industry	Financial Services	Financial Services	Cross-industry
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum developers & JP Morgan Chase
Ledger type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Cryptocurrency	Ether (ETH)	None	None	Ripple (XRP)	None
% providers with experience[1]	93%	93%	60%	33%	27%
% share of engagements[2]	52%	12%	13%	4%	10%
Coin Market Cap[3]	$91.5 B (18%)	Not applicable	Not Applicable	$43.9 B (9%)	Not Applicable
Consensus algorithm	Proof of Work (PoW)	Pluggable framework	Pluggable framework	Probabilistic voting	Majority voting
Smart contract functionality	Yes	Yes	Yes	No	Yes

1. *Based on responses from 15 leading blockchain service providers*
2. *Based on a random sample of set of 50 enterprise blockchain engagements across multiple industries*
3. *Coinmarketcap.com as of Feb 20, 2018, 6:20 PM UTC*

Source: HfS Research, 2018

When to use Blockchain



When to use Blockchain

- Database?
  - Centralized
  - Decentralized
- Secure network transfer?
  - # parties, frequency
  - Information
  - Money (value)
- Business process automation?
  - QA/Compliance/Audit
  - Always-available information
  - Data sovereignty

Use Case Example: **Factom: Health insurance claims billing**

- Automated claims billing, validation, payment, and settlement
- Multi-party value chain: patient, service provider, billing agent, insurance company, payor, government, collections

When to use Blockchain

- Large Business Network
- Need for multiple ledgers
- Public Verification
- Coin / Token
- Audit / Review
- Can’t be solved with a database
- Non-technical (human) problems / barriers
- Systems integration

Requirements Definition

- Where would having a single shared set of trusted information help in value chain ecosystem?
  - Blockchain is a single shared database of information and transactions between parties in a value chain.
- What are obvious ways to deliver customer value?
  - Financial: What is the cost of transactions/information transfer now? What is the business case for moving to a blockchain solution?
  - QA Regulation/Compliance: audit-log demonstrates compliance; assures chain of custody.

Next Steps

- Identify 2-3 Blockchain use cases that would address your business requirements
- Design and Implement Pilot Project
- Deployment Strategy
- Competitive Edge: lead blockchain single shared database and processes in your industry ecosystem
- Resources
  - Blockchain consultants, system integrators/vendors