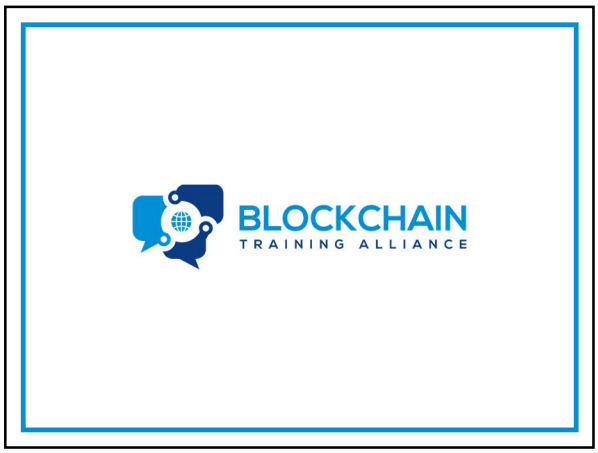

BLOCKCHAIN
TRAINING ALLIANCE

1


BLOCKCHAIN
TRAINING ALLIANCE
Blockchain Overview
Revision 1.3
www.blockchaintrainingalliance.com
© Copyright 2020 | All Rights Reserved

2


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

3

Logistics

- Class time: Approx. 6 hours
- 6 modules organized into
  - 45-minute sessions
  - 5 min Q&A (flexible)
  - 10-minute break
  - Start at top of the hour
  - Instructor available for additional Q&A at end of call

4

Course Objectives

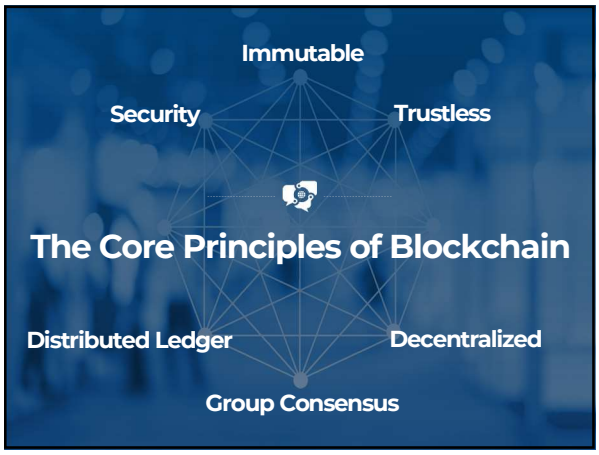
- Modules covered:
  - What is Blockchain – The Basics
  - Blockchain and Cryptocurrency
  - Why Use Blockchain
  - Decentralized Networks and Ledgers
  - Types of Blockchain
  - How Blocks are Created
  - Cryptography and Hashing
  - Mining a Block
  - Types of Consensus
  - Blockchain 2.0 and Ethereum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

5

What is Blockchain?

The Basics

6



7

Introduction

Blockchain Defined

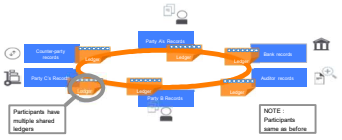
- In its simplest form, Blockchain is a distributed database, an unchangeable record (or Ledger) of asset ownership.
- Blockchain is primarily defined as a shared immutable ledger, or just an "unchangeable record of who owns what"
  - Global, peer to peer, and distributed immutable record of transactions.
  - 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.

8

Blockchain Defined

Blockchains are basically a network of computers (i.e. nodes) that have Blockchain software (applications) running on them to accomplish specific business functions. It's important to remember that not all Blockchain networks are the same. The example below is a private, permissioned Blockchain which will be discussed later.

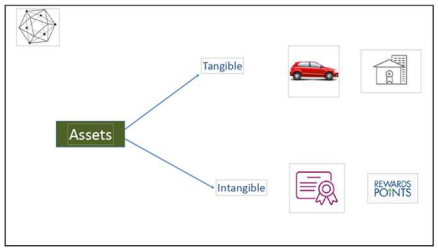
ALL Nodes however have (and share) the same exact copy of the transaction ledger



Consensus, Provenance, Immutability, Finality

9

Assets Further Defined



10

Blockchain Uses Old Technology

- Blockchain is a combined use of existing older technology.
  - **Accounting Ledger** – 1000's of years old, now triple-entry ledger with the internet and Blockchain S/W
  - **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
  - **Business Computer Network Technologies** – Blockchain makes extensive use of P2P networking architectures

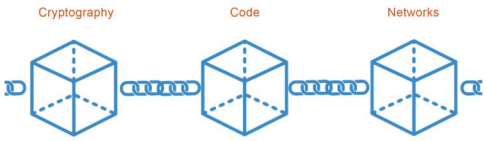
11

Blockchain Rules

- Once something has happened, and we create a record of that, the fact that it happened never changes
- Data written into a blockchain is a historical record and is immutable
- Blockchains have to prove that 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 (aka – The World State of the Blockchain)

12

Blockchain Basics



13

Blockchain is:

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

14

Blockchain is:

- A record keeping system – of Any Asset
  - 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

15

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

16

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!

17

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

18

Blockchain Provides Identity

- To use the network, you need a Cryptographic Identity
  - (similar to an email address)
  - If you want to access your email, you need the password, which functions similarly to a private key and your public key is like your address (more complicated)
- Authentication: peers sign transactions with their cryptographic identity, this enables account "ownership"

19

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?
  - It means that everyone agrees on the current state (e.g. how much money does each account have) and making sure that no one is double-spending money (easy in Bitcoin, more complex in Ethereum, business networks)
- Consensus methodologies will be discussed a little later.

20

Blockchain is based on Ledgers

Ledgers are Important

- Ledger [1] is THE system of record for a business
  - records asset transfer between participants.
- Business will have multiple ledgers for multiple business networks in which they participate.

[1] The principal book (or computer file) for recording and totaling financial transactions by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.

21

What is a Ledger?

- A ledger is like a database, a Google or Excel spreadsheet
- Add new records by appending rows
- Each row contains information
  - Account balances, who owns certain assets
  - Memory and execution state of a computer program

Ledger	
Alice	$500
Bob	$10
Charlie	$1,000

22

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

23

Blockchain Beginnings

In 2008 Satoshi Nakamoto created the first Blockchain and used in Bitcoin in 2009

24

Interesting Blockchain Dates

- 2009 first block created
- Satoshi Nakamoto was the person accredited with creating BC
- Early days, it was just him (and a few others)
- Then crypto-geeks, then early technology adopters
- Satoshi disappears December 2010 - date of last post
- Recent years have seen 'professionalism' of the ecosystem

25

Blockchain and Cryptocurrency

26

Blockchain's Relationship to Bitcoin

Bitcoin is a **digital**, **decentralized**, **disintermediated**, **trustless** currency

Digital Currency	Decentralized	No Intermediary	Trust-less
Bitcoins are completely digital in nature and operates like any independent currency.	Bitcoins are open source peer to peer money with data stored on multiple 'nodes' simultaneously	Bitcoin enables participants to transact between themselves without the need of an intermediary	Transactions are anonymous, thus ensuring a higher level of privacy

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.

27

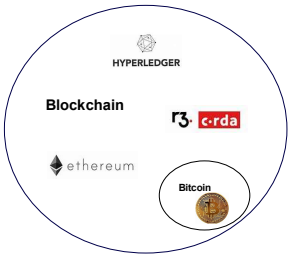
Bitcoin/Cryptocurrencies have *some* similar characteristics as a fiat currency

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

28

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. There are roughly 10,000 active nodes on the Bitcoin Blockchain WW (11/2018)
https://bitnodes.earn.com/dashboard/

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

29

You Control Access to Bitcoin

- Nobody actually 'has' bitcoins - you can't download them, or store them on your computer
- Remember that 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 actually 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

30

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
- This gets a bit technical, quite quickly. Don't panic if you don't get all of this in your first pass

31

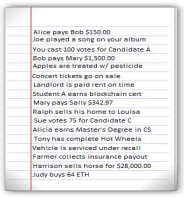
Control via Cryptography

- Because blockchain transactions are anonymous, there needs to be a way of enforcing control over the coins
- Transactions are programmable
- Each transaction contains a program that specifies conditions that must be met in order to spend i.e. transfer the coins

32

Transaction "BLOCKS" of Blockchains

- A standard Blockchain Block has roughly 25 transactions (1 MB limit)
  - Each record is complete with time, data, all transaction details.
  - When a Block has 25 complete transactions, the Nodes "validate" the transactions on the current page and post it on the Blockchain.



  - By comparison, the Bitcoin Blockchain can have up to ~ 2000 Bitcoin transactions per Block. (~ 500 data bytes per transaction)

33

WORLDS MOST EXPENSIVE PIZZA?

22nd May 2010 is Bitcoin Pizza day – Bitcoins first real-world transaction

- Laszlo Hanyecz offered 10,000 BTC for 2 pizzas
- Someone in the UK phoned through the order using their credit card
- Then worth US ~$24
- Currently worth (12/2018) U.S. ~$35.0m (varies hourly)

34

Addresses

Private key

↓

Public key

↓

Hash

Encode

↓

Address

35

Addresses

- Hides your public key (because of the hashing), but you still have both the public and private key
- This is your bitcoin 'Address' – must be shared with those who need to send coins to your address
- You will (can) have many Addresses
- Your digital wallet software keeps track of all payments made 'to' your Address

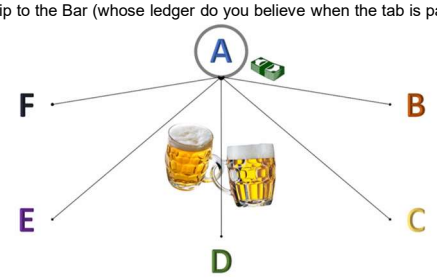
36

Why Use Blockchain

37

What problem does Blockchain solve?

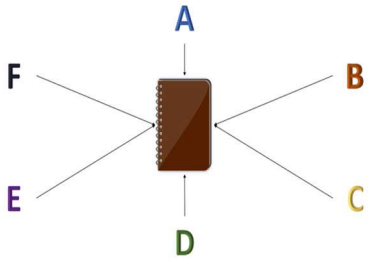
- Trip to the Bar (whose ledger do you believe when the tab is paid?)



38

What is Blockchain

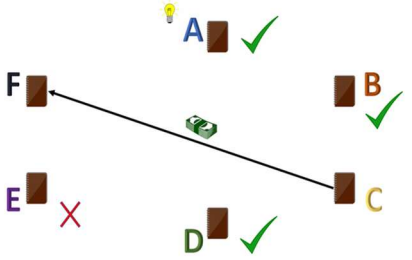
- Common Ledger (i.e. everyone has the same record)



39

What is Blockchain

- A More Common Ledger (consensus is reached by majority!)



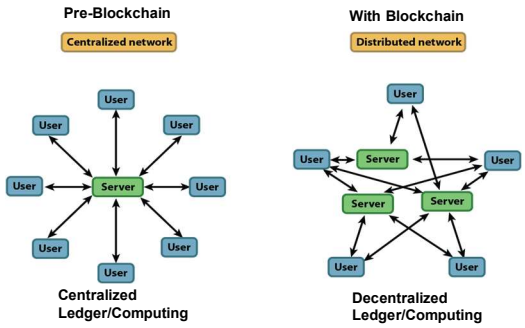
40

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

41

Benefits of Blockchain



42

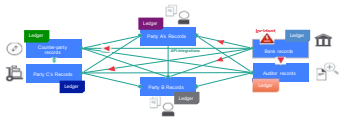
Benefits of Blockchain

- 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

43

Conventional System Problem

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



Inefficient, **expensive**, **vulnerable**

44

Drawbacks of Blockchain

- What are the drawbacks of Blockchain?
  - Slow adoption to newer technology
    - Quickly evolving making it difficult for companies to commit
    - BaaS (Blockchain as a Service) is expensive to use
    - High cost for trained developers to develop your own Blockchain
  - Best Blockchain solutions for industries is still evolving
  - Scalability, transaction speed / cost are still adoption concerns

45

Drawbacks of Blockchain

- What are the drawbacks of Blockchain?
  - Application Use Case adoption is slow. Fear of not working?
  - Stigma and history of Blockchain
    - Cryptocurrency Hacks and principal losses
    - ICO/ITO scams
  - Anonymity of origin – Satoshi Nakamoto
  - Data in the blocks
  - No Regulatory Agencies Governing International Blockchains

46

Drawbacks of Blockchain

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

47

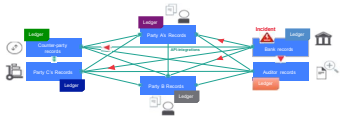
Why Not a Database

- Blockchains solve specific problems:
  - Fully distributed - highly fault tolerant
  - No centralized authority
  - 3rd party trust without trust (Relationship)
  - Low barrier to entry - computer + internet = win
  - Instant, Global transactional capability
  - No double spending
  - Very low transaction costs
- Traditional Databases have centralized control and do not perform these functions.

48

Conventional System Problem

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



Inefficient, Expensive, Vulnerable, Difficult Problem Resolution

49

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

50

Blockchain Shared Ledger Solution

Solution – a permissioned, replicated, shared ledger

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

Consensus, Provenance, Immutability, Finality

51

Trustless Environment

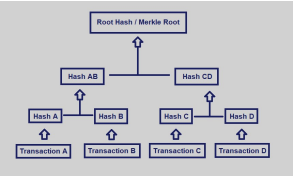
- KEY CONCEPT: Trustless environment
  - Traditional systems assume trust at the beginning, then provide safety measures to block the actions of bad actors
  - Blockchain assumes a trustless environment from the beginning, so requires no additional hardening***

*** - However, All developed Blockchain code should be reviewed for vulnerabilities by a cybersecurity professional !!

52

Trustless Environment

- KEY CONCEPT: Merkle Tree
  In common Blockchain design, Merkle trees are used to create a **lightweight digital fingerprint** of the state of all the transactions within a block.
  - Provides an 'index' of all transactions on the Blockchain.
  - Collectively, the "state" of ALL BC Blocks make up the "World State" of the Blockchain.



53

Four elements characterize Blockchain

Replicated ledger
- History of all transactions
- Append-only with immutable past
- ALL nodes have the same ledger

Cryptography
- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus
- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated
  - ALL Nodes Agree on ledger content

Business logic
- Logic embedded in the ledger
- Executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

54

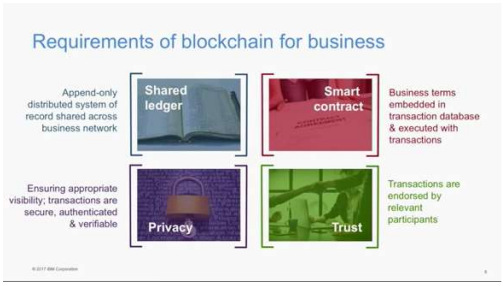
Shared Ledger Attributes

LEDGER

- Records all transactions across business network
- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- THE shared system of record
- Eliminates the Double Spend Problem
- The Ledger is APPEND ONLY

55

WHY Blockchain for Business



56

Decentralized Networks and Ledgers

57

Authorities

Authority

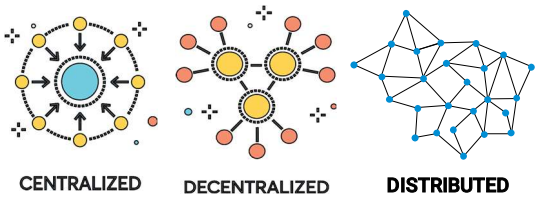
the power or right to give orders, make decisions, and enforce obedience

person or organization having power or control in a particular, typically political or administrative, sphere

the power to influence others, especially because of one's commanding manner or one's recognized knowledge about something

58

NETWORK EVOLUTION



CENTRALIZED DECENTRALIZED DISTRIBUTED

59

Single (no consensus) Authority

Centralized Systems

- Single Authority
- All processes are carried out at a single location
- Very susceptible to collapses

Point of Authority

60

Single (no consensus) Authority

Benefits

- Easy to implement and co-ordinate
- Economies of scale

Drawbacks

- The system can collapse if the central authority fails
- No transparency

Examples


Banking System

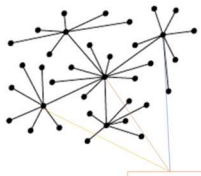

Food Franchise


Server CPU

61

Multiple (Flatter) Authorities

De-centralized Systems



- Multiple Authorities
- Less susceptible to collapses
- Flatter Hierarchy

Points of Authority

62

Multiple (Flatter) Authorities

Benefits

- Decisions made closer to the customer
- Not susceptible to collapses

Drawbacks

- Diseconomies of scale
- Not completely secure

Examples

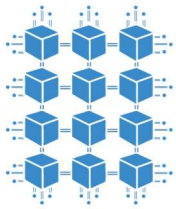

Johnson & Johnson Supply chain


Governments


Cloud database

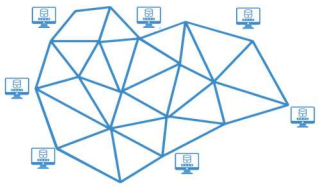
63

Blockchain Basics



64

Blockchain Basics



- Automatic Trust
- Tamper Proof
- Shared Data
- Transparent
- Resilient

65

Blockchains as Distributed Databases

- In Blockchain, everyone has a copy of the Ledger (assets).
  - Everyone running a Blockchain node is part of the network
  - New (transaction) blocks are broadcast to the network
  - Everyone updates their local copy of the blockchain
  - If you're behind the current height of the chain, you can ask other nodes for copies of the Blocks needed to catch-up
  - If everyone has a copy of the blockchain, when queried, everyone gets the same answer
  - Blockchains are a bit like read-only distributed databases

66

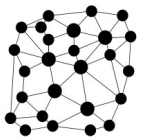
Centralized vs Decentralized Ledger

- 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

67

Why Distributed?

- 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)

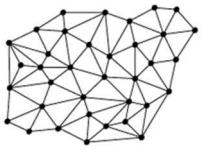


A distributed network.

68

Distributed System Authorities

Distributed systems



Every point has equal authority

- **No** Authority OR **Everyone** is an authority
- Virtually unsusceptible to collapses
- Completely flat Hierarchy

69

Types of Blockchain

70

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!

71

Types of Blockchains

- Who are the participants in the Blockchain?
  - ANYONE with an important announcement to make can be a Blockchain participant
    - Personal data
  - Groups of people can use the Blockchain to capture announcements that are important to them
    - Supply chain participants
  - Large groups of people can use Blockchain to capture important data which support critical social and economic functions
    - Voting records, land titles

72

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

73

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

74

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

75

Public vs. Private Blockchains

'Public' (Open) vs 'Private' (Closed) Blockchains: Generalized Features Comparison

	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-Stake	Pre-approved participants
Identity	Anonymous/ pseudonymous	Known identities
Asset	Native assets	Any asset

Note: some features can vary form platform to platform.
Sources: Chain, Chris Skinner's blog

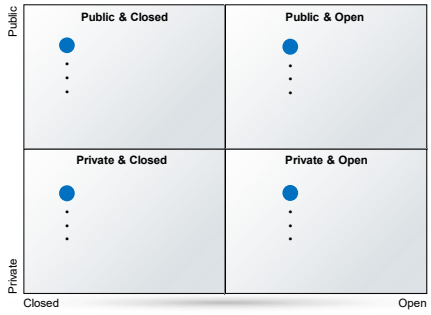
76

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

77

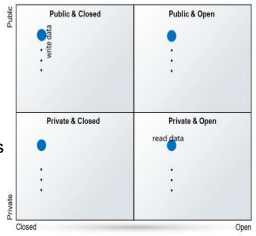
Blockchain Decision Worksheet



78

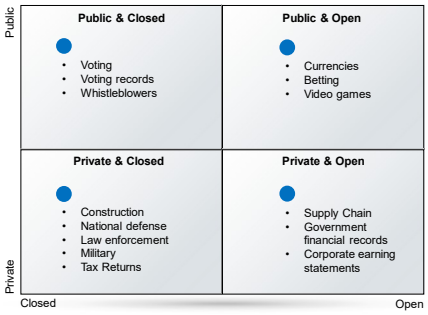
Blockchain Decision Lab

- 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?



79

Blockchain Decision Matrix



80

How Blocks are Created

81

Blockchain Basics

Blocks

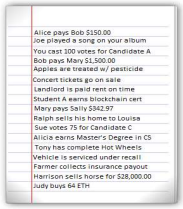
Mining

Consensus

82

The "BLOCKS" of a Blockchain

- Think of a "Block" as a sheet of paper with of 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



83

The "Blocks" of a Blockchain

Transactions are grouped together into a Block

25 Transactions per Block

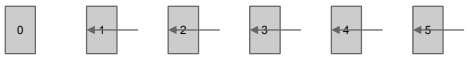
84

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)

85

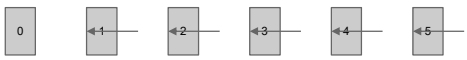
Blockchain Blocks



- 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)

86

Blockchain Blocks



- Blocks aren't identified by their height, but by their id
- 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

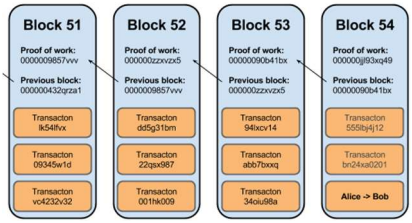
87

What is in a Block?

- A 'magic number' (0xD9B4BEF9) to show it's a Bitcoin block
- A size number to specify how much data is coming next
- 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 25 transactions recorded in this block

88

What is in a Block?

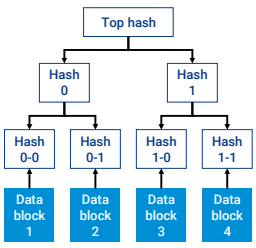


The connection between blocks means that the Blockchain is much more *tamper-proof* than standard database structures. Since Blockchain is a ledger of records, this tamper-proof record of assets is known as an "Immutable Ledger".

89

MERKLE TREE - HASH OF HASHES

- Multiple blocks of data, in a certain order, into a single hash
- Allows you to work out which block has changed



90

Tamper Evident

- Blocks are identified by their ID (hash of the metadata)
- Metadata in turn, contains Merkle Root of Transaction data
- Change the metadata, block id will change - broken chain
- Change the details of a transaction, the Merkle root will change, which in turn changes the metadata hash, which will change the block id
- Hashing data once is really quick, so easy to check the validity of each block as you go along

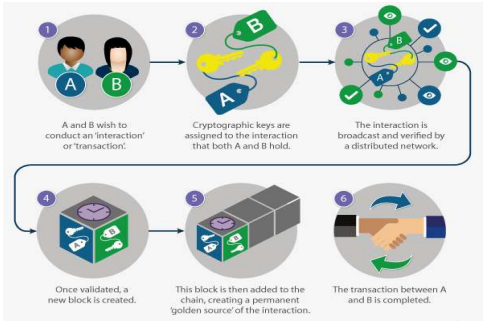
91

The "chain" of Blockchain

- What creates the chain?
  - Block header
    - Contains information about the block
      - Platform version, timestamp, difficulty level, nonce, etc.
      - Also contains the hash output of the previous block data
  - All data from the current block, including its header is hashed
  - The hash output for the current block will be stored in the header of the next block
  - All data from that block, including the header, will be hashed

92

The Lifecycle of a Blockchain



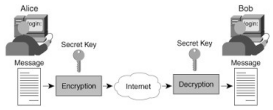
93

Cryptography and Hashing

94

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



95

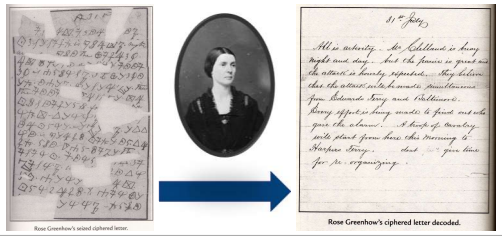
Cryptographic Function

- 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”

96

Cryptographic Function

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

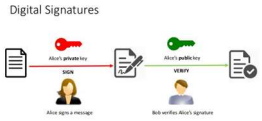


Rose Greenhow's ciphered letter decoded.

97

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



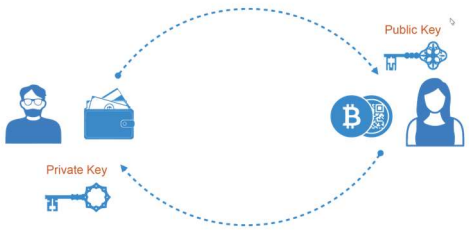
98

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)
- The mathematical computation behind it is complex
- Main aim is confidentiality (in messaging)
- Also used for digital signatures (the bit we're interested in)

99

Public and Private Keys



100

DIGITAL SIGNATURES

- Verify the messages came from the correct person
- Verify the messages hasn't been changed or tampered with
- Can be used to prove that you have the private key
- Main aim is confidence in identity (in messaging)

101

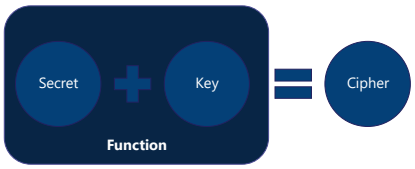
Important Terms

- 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

102

Cipher

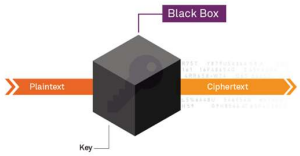
- The Secret and the Key are passed into the Function to create the Cipher



103

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



104

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

105

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

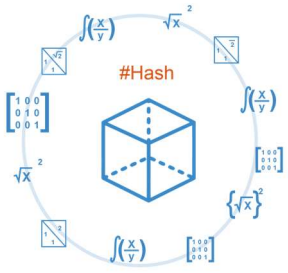
106

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?

107

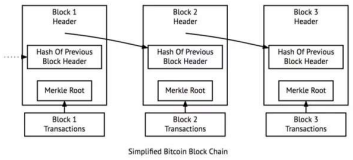
Blockchain Basics



108

The "chain" of Blockchain

- The "chain" of Blockchain
  - If I hash the data of any block, and the output matches the hash value from the header of the next block, I can trust the data has not been tampered with



Simplified Bitcoin Block Chain

109

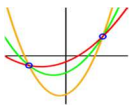
Using Multisignatures

- Digital signatures are heavily used in the blockchain
- Some transactions may need to be authorized by multiple parties
  - High value transactions, signing contracts, etc.
- Algorithms exist that require multiple secret keys to generate a digital signature
  - Based on Shamir Secret Sharing
  - At least K of a set of N users need to participate to create a valid signature
- Security Assumptions:
  - Secret keys are appropriately protected

110

Multisignatures: Shamir Secret Sharing

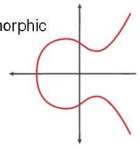
- Shamir Secret Sharing requires K of a set of N parties to generate a valid signature
- It's based on the number of points you need to define a line or curve
  - The shared secret is where the curve crosses the Y-axis
  - Each person is given the X,Y coordinates of a point on the curve
  - A shared signature can be pieced together from each individual signature



111

Confidential Transactions: Elliptic Curve Crypto

- Elliptic Curve Cryptography is a form of public key cryptography
  - Uses points on an elliptic curve
- Public key, P, is the product of a private key, x, and a point on the curve, G
  - It's impossible to derive x from P and G
- Elliptic curve cryptography is additively homomorphic
  - P1+P2=(x1+x2 (mod n))*G



112

Putting a BLOCK on the Blockchain

- Once the page has been validated, it is added to a stack of previously validated sheets
  - Each sheet on the stack can be assumed to be trustworthy
  - Once a sheet is validated it can't be changed, because of group consensus. i.e. Immutability!

113

Data Blocks of Blockchain

- How are blocks "chained" together?
  - Use of computers & cryptography
  - All data in a block is run through a cryptographic hash
    - We'll dive into the details later
  - Hashes create a unique output for a specific input
    - Can always recreate if use same inputs
    - Think Black Box
  - Chain is established by embedding the last block's data into the header of the current block

114

Mechanics of Blockchain

- Changing the data on any block will result in a different hash
  - The new hash will not match the hash in the next block header
  - If you try to change the next block header, it will change the hash of that block

115

The "chain" of Blockchain

- To summarize
  - The hash output will be stored in the header of the next block, etc.…
  - Changing the data in any block will result in the hash of that block not matching the hash value stored in the header of the next block
  - The next block will need to be changed too…
    - ...and the block after that, and the block after that, and the block after that…

116

Blockchain Basics - recap

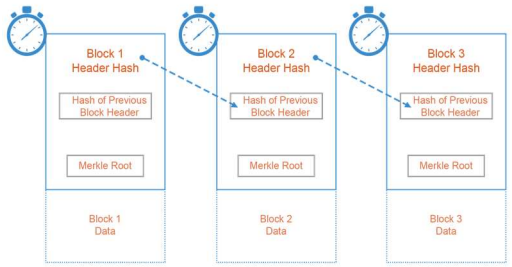
Block 1
Header Hash

nb41ad5047d95a70fbe410e3eba035e633b65d94

Hash of Previous Block Header

117

Blockchain Basics - recap

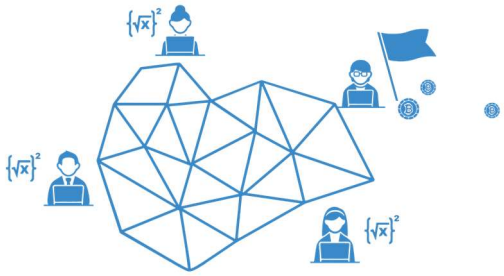


118

Mining a Block

119

Blockchain Basics - Miners



120

Mining Demo

- Mining demo
  - Block Data = “ThisIsMySampleBlockData”
  - Nonce = “24725”
  - Network difficulty: 0000
  - SHA256 hash result of:
  - 00002b1b5e98e4257a504ab55a937ef678de4547fe884d19488927c1e69b173b

121

Mining Demo

- Mining demo
  - Let’s try to cheat...
    - Block Data = “ThisIsMyHackedSampleBlockData”
    - Nonce = “24725”
- SHA256 hash of:
- eae8ad1ce120fb96c790765efa500f81ae633873d3f4069acc9f2957fe3b6a13

122

What is Bitcoin mining?

- Mining is the accounting function to record transactions, a fee-based incentivized system for paying miners to validate a Blockchain transaction
- aka “Proof of Work” Consensus function
- Mining ASICs “discover new blocks”
  - Mining software makes nonce guesses to win the right to record a new block (“discover a block”)
    - At the rate of 2^32 (4 billion) hashes (guesses)/second
  - One machine at random guesses the 32-bit nonce
- Winning machine confirms and records the transactions, and collects the rewards
  - All nodes confirm the transactions and append the new block to their copy of the distributed ledger
- “Wasteful” effort deters malicious players

Fast because ASICs represent the hashing algorithm as hardware

123

Simultaneously Broadcasting Blocks

Since the Blockchain miners are distributed, who gets to make the block?

- Miners are distributed and are in competition with each other
- First to publish/broadcast a block wins
- At the top of the chain multiple miners could create a block at roughly the same time
- Blocks take time to propagate their way round the network
- Different nodes receive blocks at different times
- The network needs a way to decide which block it will use as it's official record of what happened
- Mining doesn't stop while all this is figured out

124

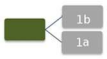
Sequence of Mining Block Mathematical Problem

- Example: the green block is at height 0
- All miners try to solve the next one…
- A miner solves one at height 1

The **height of a block is the **number of blocks in the chain between it and the genesis block**. (Genesis block has height 0.) The height of the block chain is usually taken to be the height of the highest block, in the chain with greatest total difficulty;
i.e. ***the length of the chain minus one***.

125

Sequence of Mining Block Mathematical Problem



- But so does another miner. We don't know which is official.
- Block 1a may contain different transactions from 1b.
- We don't know which is the accepted block yet
- So, mining continues, with half the network working on 2a, half on 2b
- Good idea not to treat any transactions as final yet

126

Sequence of Mining Block Mathematical Problem

- A miner finds 2b
- All miners working on 2a stop work, they must work at the highest height
- All miners work on finding a block at height 3
- Transactions that were only in 1a, are now back to not-being-in-a-block

127

Sequence of Mining Block Mathematical Problem

- A miner solves one and broadcasts to the network
- Other miners abandon their work and start trying to solve a block at height 4

128

Sequence of Mining Block Mathematical Problem

- A miner solves one at height 4, all is well with the world
- All miners try to solve a block at height 5

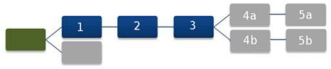
129

Sequence of Mining Block Mathematical Problem

- But, while this is sorting itself out, another miner solves a block at height 4
- We now have a fork at height 4.
- Half the miners will try to solve 5a, half will try 5b

130

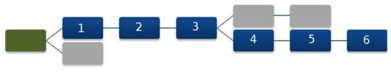
Sequence of Mining Block Mathematical Problem



- We have a race condition, lets pretend that both forks of the chain solve another block at the same time

131

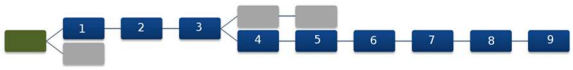
Sequence of Mining Block Mathematical Problem



- The miners working on 5b solve a block first. All miners stop what they're working on, and try to solve for height 7
- Blocks 4a and 5a are now accepted as the longest chain

132

Sequence of Mining Block Mathematical Problem



- Smooth sailing from here on out

133

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

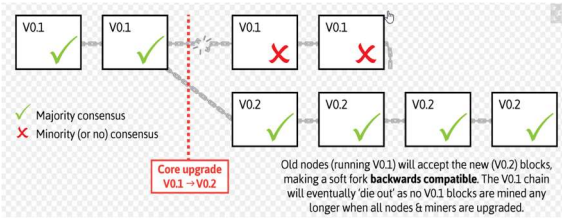
134

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 backwardly compatible, it's a soft fork
- If the upgrade isn't backwardly compatible, it's a hard fork
- Hard forks are much harder and we try to avoid them

135

Blockchain Forks



136

Types of Consensus

137

Three Primary Consensus Algorithms

- POW: Proof of Work (Bitcoin, currently Ethereum)
  - Expensive, not ecological, wasteful computation
- POS: Proof of Stake (Ethereum is moving to POS)
- Next-gen: PBFT: Practical Byzantine Fault Tolerance (DFINITY, Algorand)
  - Law of large numbers: **diversity of participants**
  - For each block of transactions, randomly select a small, one-time group of users in a safe and fair way
  - To protect from attackers, the identities of these users are hidden until the block is confirmed
  - The size of this group remains constant as the network grows

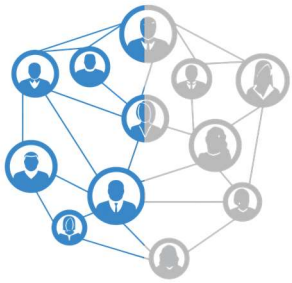
138

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

139

Proof of Work Security Issue – 51% Attack



140

Summary Proof of Work (PoW)

- Proof of Work Consensus
  - When a block is full, each node competes to solve a guessing game problem
    - This problem is non-computational, random guesses are most efficient
    - 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

141

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

142

Proof of Stake (PoS)

- Proof of Stake Consensus
  - How does it work?
    - Let’s pretend there’s a new casino game – Honesty
      - Each hand of Honesty costs $10,000 to join (stake)
      - Every honest player will always win $25 each hand (net gain $25)
      - A winning player keeps their earnings and gets their stake returned
      - Every dishonest player will not only miss out on the $25 winnings, they also loose their stake (net loss of $10,025)
        - Small upside for being honest, large downside for being dishonest

143

Proof of Stake (PoS)

- Proof of Stake Consensus
  - Ok, but how does it really 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

144

Proof of Stake (PoS)

- Proof of Stake Consensus
  - Ok, but how does it really work?
    - 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

145

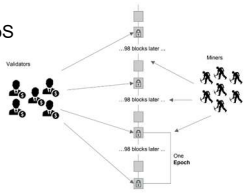
Proof of Stake (PoS)

- 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

146

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



147

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

148

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

149

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

150

Consensus Mechanisms

- Consensus protocols are the key to Blockchain!
  - Blockchain consensus mechanisms are the nuts and bolts of validation. TPS is directly linked to the consensus type.
  - 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.

151

Identity Implementations

Specific Identity Implementations

- Ethereum: A user's identity is an address based on their public key
- Hyperledger: Identity if managed by X.509 certificates
- Corda: Identity is managed by X.509 certificates
  - Public: Certificates published on blockchain
  - Confidential: Certificates only shared with parties involved in transaction

152

Anonymity Implementations

Specific Anonymity Implementations

- Ethereum
  - Ethereum currently does not have any advanced privacy options, but this is planned to change
- Hyperledger
  - Channels: Subsections of the blockchain that make transactions visible only to members
  - Private Transactions: Hashes of private data are stored to publicly verify it on the blockchain
  - Zero-Knowledge Technology: Provers can demonstrate knowledge of a secret without revealing the secret itself
- Corda
  - Parties on the Corda Network can be represented in one of two ways:
    - Party: A public key and name
    - Anonymous Party: Only a public key

153

Blockchain Basics - Recap

Encryption & Hashing

01100
10110
11110

Proof of Work

Network Consensus

154

Blockchain (review)

What is the Blockchain?

- The Blockchain is simply a distributed database.
- Technical definition: The Blockchain is a distributed peer 2 peer ledger
- Every participant has a complete version of the database
- Every Transaction is declared valid only after it has been cleared by a majority of participants in the network
- The Blockchain can transfer any item of value across participants
- The Blockchain is the underlying technology behind Bitcoin
- The Blockchain is NOT Bitcoin

155

Recap: How To Build A Block

- Receive the transaction broadcast
- Verify the crypto in the transaction
- Add it to the unconfirmed pool
- Do some hard maths on all the transactions in the pool (i.e. Mining)
- Broadcast the Block to the network
- The Block is added to the blockchain

156

Key Blockchain Concepts

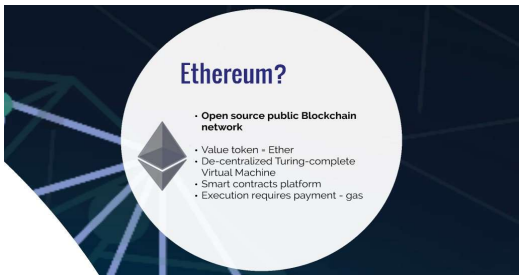
- Public-private networks
  - Trustless vs trusted
- Distributed network
- Consensus algorithms
- Immutability
- Blockchain: trustless, distributed (peer-based), consensus-driven, immutable

157

Blockchain 2.0 and Ethereum

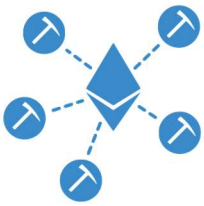
158

Ethereum Overview



159

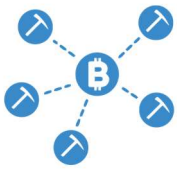
Blockchain - Ethereum



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

160

Blockchain – Current Transactions per Second



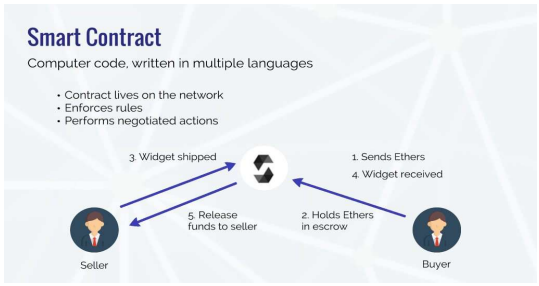
TPS = 7

TPS = 15

Because of global validation (consensus), TPS rate for Blockchain is very slow.
By comparison, Visa CC's can process ~ 24K TPS, and Facebook ~175K TPS !

161

Ethereum Smart Contract

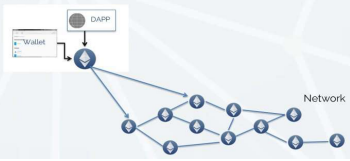


162

Ethereum Smart Contract

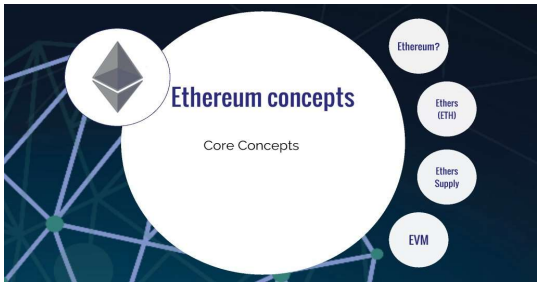
How Does It Work?

- Wallet for managing Ethers
  Smart contracts
- Decentralized Apps (DAPP)
  Interact with contracts on n/w
  Execution is not free



163

Ethereum Concepts

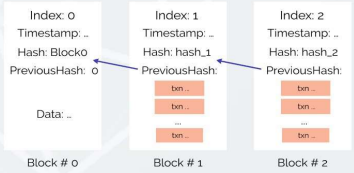


164

Ethereum Overview

Blocks and Chaining

Data added to the ledger CANNOT be updated or deleted



165

Ethers (ETH) Coin

166

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

167

ETH Supply

168

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

169

Ethereum Gas

Gas

- User invoking the transaction pays for the execution

Measures: kWH used

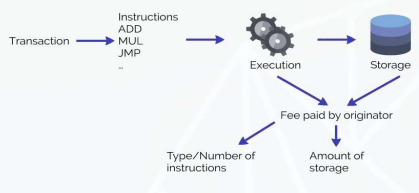
Measures: Gallons of water used

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

170

Ethereum Gas

Gas Calculation



171

Ethereum Gas

Opcodes & Gas

	QUICKSTEP	FASTESTSTEP	FASTSTEP	MIDSTEP	SLOWSTEP	EXTSTEP
Gas cost	2		3	5	8	10	20
	ADDRESS	DUP	MUL	ADDMOD	JUMPI	BLOCKHASH	
	ORIGIN	SWAP	DIV	MULMOD	EXPBASE	BALANCE	
	CALLER	PUSH	MOD	JUMP		EXTCODESIZE	
	CALLVALUE	ADD	SDIV			EXTCODECOPYBASE	
	CALLDATASIZE	SUB	SMOD				
	CODESIZE	LT	SIGNEXTEND				
	GASPRICE	GT					
	COINBASE	SLT					
	TIMESTAMP	SGT					
	NUMBER	EQ					
	DIFFICULTY	AND					
	GASLIMIT	OR					
	POP	XOR					
	PC	NOT					
	MSIZE	BYTE					
	GAS	CALLDATALOAD					
		CALLDATACOPY					
		CODECOPY					
		MLOAD					
		MSTORE					
		MSTORE8					

172

Ethereum Gas

Fee Calculation

gasUsed =
- Instructions executed (summed up gas)

gasPrice =
- User specified in the transaction
- Miners decides the minimal acceptable price

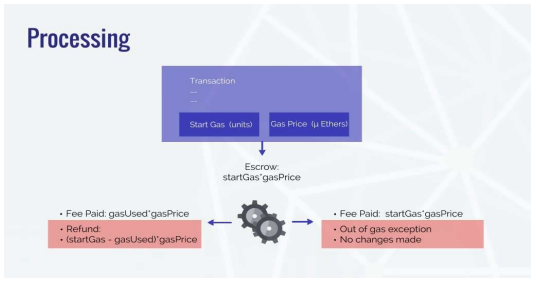
Transaction Fee = gasUsed * gasPrice

173

Ethereum Gas

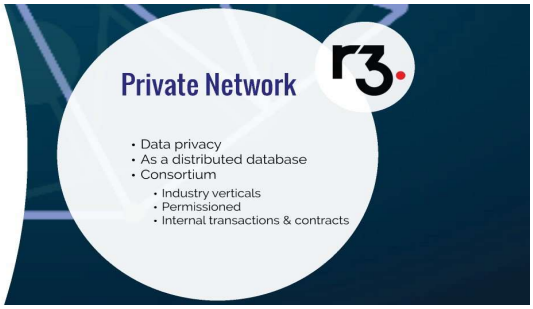
174

Ethereum Gas



175

Private Network - Corda



176

Private Network - Corda

- Corda is officially NOT a Blockchain
- Corda is known as a “Distributed Ledger” technology
- Consensus can be achieved by as few as only two parties agreeing on business terms
- Consensus is determined by digital “Notaries”
- Created specifically for international business transactions
- Corda is being developed by R3, and a consortium of over 200 international banks and other financial institutions
- Corda’s technology is however very similar to Blockchain and is referred to as a Blockchain by many

177

Blockchain Network Nodes
The Nuts and Bolts of Blockchain

178

Blockchain Network of Nodes

Solution – a permissioned, replicated, shared ledger

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

Consensus, Provenance, Immutability, Finality

179

Blockchain Nodes

- A Blockchain Node is generically defined as a “computer connected on a Blockchain Network”, that holds an immutable copy of the complete Blockchain transaction ledger.
- Nodes on the Blockchain each have specific functions

180

Blockchain Use Cases

181

Just a Few Use Cases

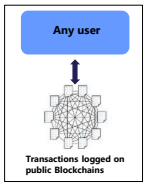
- Background checks: education credentials, criminal records
- Secure document storage: home deed, auto title
- Birth registries
- Land registries
- Financial services: securities clearing, syndicated loans
- Global supply chain: automotive recalls and counterfeit airbags
- Healthcare: EMRs, insurance 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

182

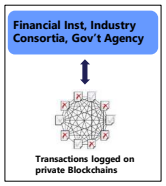
Public and Private Blockchains

- Public: open to anyone ("permissionless")
  - Identity unknown, individuals
    - Ex: Zcash zero-knowledge proofs
  - Open access
- Private: approved users ("permissioned")
  - Identity known, enterprise
    - Approved credentials
  - Controlled access

Examples:
Bitcoin
Ethereum



Examples:
R3
Hyperledger



183

Blockchain Use Cases

184

Four General Classes of Applications

Finance	Property	Contracts	Identity
Trade and settle securities at a fraction of the time and cost.	Permanently record and access real-time property rights.	Self-enforcing contracts based on predefined conditions.	Eliminate invasive identity practices via digital identies.
Money, Payments, Financial Clearing	Smart Property Cryptographic Asset Registries	Smart Contracts IP Registration	Identity Confirmation

185

Store Documents on the Blockchain

- Store Auto Title, Home deed on the blockchain
  - Storj (always-on, do not have login to Dropbox, Google Drive)
- Proof of Existence your Will
  - Proof of Existence

Submissions
Documents registered for certification

Document Digest	Timestamp
0d5851955572c890f2b60eac1e61cd69dc2583f3cd0a2cc57e8fd0245fc3cc46	2017-12-21 01:29:02
26d3c76d8e736cc02a7ccd5350f9b4e4d04cc2e461f59bb221bddb7b4faa7588	2017-12-20 22:48:22

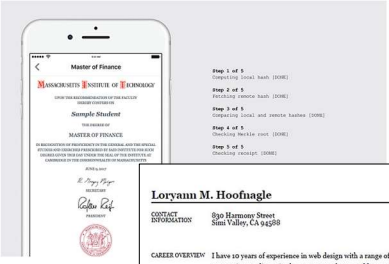
Certifications
Documents confirmed in the blockchain

	Document Digest	Timestamp
✓	de38982cebfd60bc341ec4fbcbeb16cd5ed583338083643fe15949d76eed63de	2017-12-14 08:50:45
✓	162e90df051c9d791886cdc98f976187ab495f66d2915af27ba3a6d86773a8ea	2017-12-11 15:57:11

186

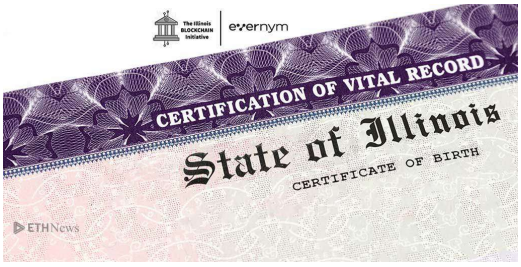
Background Checks

MIT Digital Certificates (diplomas); Criminal Records



187

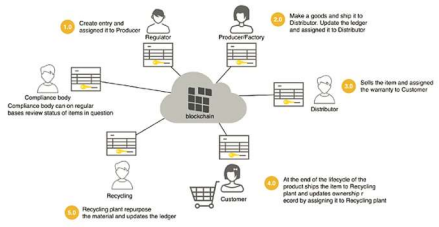
Birth Registry



188

Supply Chain Asset Tracking

- Controlled-use credentials issued to multiple parties in the value chain using single shared blockchain



189

Global Supply Chain

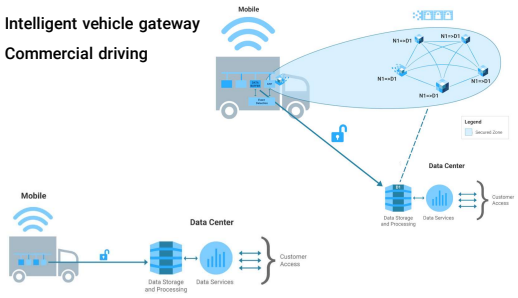
- Automotive Industry Recalls and Counterfeit Airbags
- Business case: 30% global airbags sold and installed are counterfeit
- Solution: Single shared process for airbag registration and lookup

190

Automotive Gateway

Intelligent vehicle gateway

Commercial driving



191

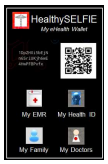
Pharmaceuticals

- Consent
  - Smart Contracts in Managing E-Consent for Patient Privacy On and Off the Blockchain
- Clinical Trials
  - Patient “Life Ledger” Blockchain Platform for Clinical Trials
- Blockchain-based health data marketplaces
  - User-assembled, contributed, remunerated
  - Comprehensive data picture, data security and interoperability
- Regulation and Compliance
  - HL7 and CMS Meaningful Use : Health Level Seven International
  - 21st Century Cures Act (2016)
  - Any US service provider to share on-request electronically with patient CMS: meaningful use Stage 2: Jan 2019

192

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

193

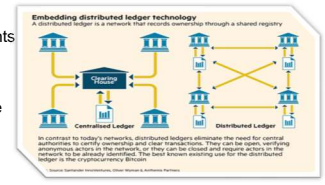
Financial Services

- R3 Corda
- Ethereum Quorum
- IBM Hyperledger Fabric
- Ripple
- Symbiont

194

Financial Services

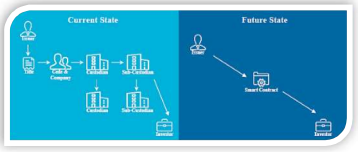
- Clearing and Settlement
- Issuance, Ownership, and Transfer of Financial Instruments
- Servicing of Instruments
- Payments and Remittance
- KYC/AML Compliance
- Regulatory Reporting
- Audit and QA
- Back-office Reconciliation



195

Financial Services – Cap Table

Smart Contracts for Securities
Simplification of capitalization table management for private companies can be enabled by smart contracts, while also reuniting record ownership with beneficial ownership of publicly traded securities, reducing cost, and counterparty risk

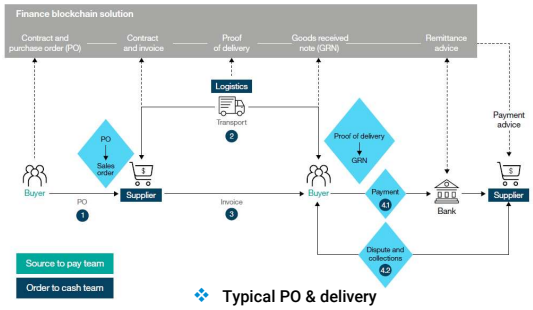


Current Challenges
- Paper-based, manual corporate registration processes
- Companies that fail to keep their corporate
- registrations up-to-date require clean-up and certificate of good standing before issuing securities
- Intermediaries increase cost, counterparty risk and latency

Smart Contract Benefits
- Digitized end-to-end workflows due to securities existing on a distributed ledger
- Trade date plus zero days (T+0) securities settlement cycles
- Facilitates automatic payment of dividends and stock splits, while enabling more accurate proxy voting
- Removes counterparty and operational risks created by intermediaries

196

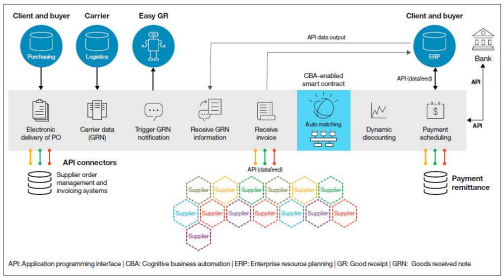
Financial Services - PO



- Typical PO & delivery

197

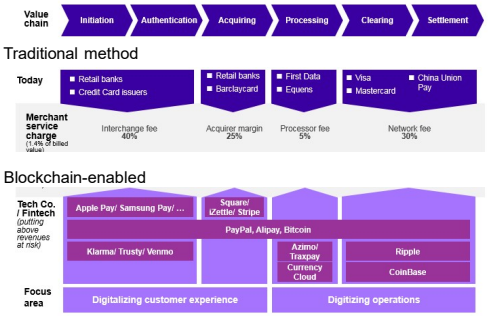
Financial Services – A/P



- Blockchain-enabled A/P process

198

Financial Services – Corporate Payments



199

Airlines

- Registration System (like SABRE)
  - S7 (Russia's largest domestic airline)
- 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

200

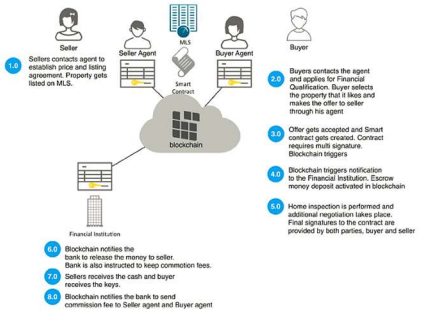
Real Estate Services

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

201

Real Estate Services



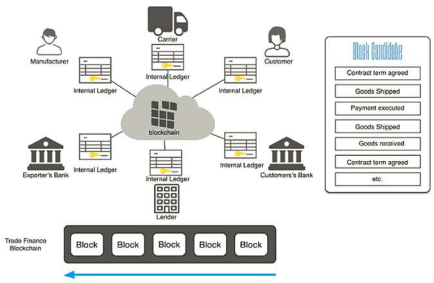
202

Supply Chain

- IBM Hyperledger Fabric
- Ethereum Private Network
- SKUChain
- Provenance
- Sweetbridge

203

Trade Finance



204

Trade Finance

- Transparency—improve credit rating, credit history and risk assessment procedure
- Immutability—No one can change the block (ledger entry) without consensus of participating parties
- Auditability—all history is maintain in the Blockchain
- Safety—as both buyer and seller are on the same infrastructure prevents fraudulent invoices and duplication of invoices.

205

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 (Neighbor.ly)
- Virtual Democracy
  - Instant elections among machine learning models of real voters to address the challenge of ethical decision making

206

BLOCKCHAIN ADOPTION

One of the fastest-moving technology adoptions

207

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

208

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 eliminated.

209

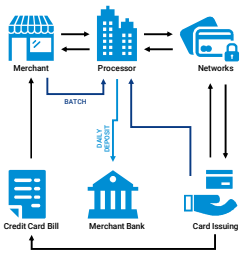
CASH IS PEER TO PEER

Observations:

- No middleman required
- DIY Fraud detection
- Sufficient trust for the value of the transaction
- Anonymous/Private
- Distributed

210

ELECTRONIC MIDDLEMEN



Observations:

- Requires 3rd party trust
- The more complex the flow, the more middlemen required
- Specialized equipment needed (e.g. POS terminal, connection to Txn networks
- Fraud detection by 3rd parties
- Every step adds cost

211

MIDDLEMEN ADDING VALUE

- Provision of infrastructure (Terminals, network connections, etc.)
- Management of commercial relationships between parties (Lots of lawyers)
- Abstraction of complexity
- Fraud detection
- Customer service
- Regulatory compliance KYC, AML, Risk reporting
- Removal of bad-actors from the ecosystem

Until now, this is the best way we've been able to achieve the goal of person-to-person transactions at a distance.

212

BLOCKCHAIN PAYMENT NETWORKS

- **Now:**
- Online banking transaction growth
- SME's/Retail acceptance of electronic transactions
- Online purchases/Commerce
- In-App purchases
- Virtual currencies in games
- International Transaction growth (Commerce and Remittance)
- Value storage cards (loyalty cards, ERP, gift cards, etc., etc.)

- **Future:**
- Internet of Things
- Autonomous Objects
- Programmable money/Finance automation

213

Existing Limitations of Transactions

- Cash is king….but only useful locally and small amounts
- Electronic transactions require Credit/Debit card
  - Fees are high for merchants (Fixed Fee + 1-3%)
  - Settlement is slow (multiple days)
  - Chargebacks shift risk to merchant
  - Micro-transactions are cost prohibitive
- Walled garden/In-country solutions are piecemeal
- International Transfers ITT/Swift
  - Slow, costly, mistake prone
- High onboarding costs/bureaucracy

214

215

BLOCKCHAIN PAYMENT NETWORKS

- **Solved:**
- Return to Peer-to-Peer
- Speed
- Trustless trust
- No special equipment needed
- Fraud
- Minimal Cost
- No chargebacks
- No monthly fees
- Transparency

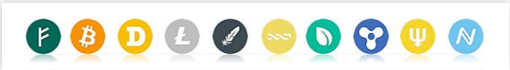
- **Ignored:**
- Policing bad-actors
- KYC/AML
- Insurance
- Onboarding process
- Customer service
- Commercial Relationships

- **Challenges:**
- Technical Complexity
- Regulatory Uncertainty
- Getting the currency in the first place

216

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

217

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

218

PARALLELS TO THE INTERNET

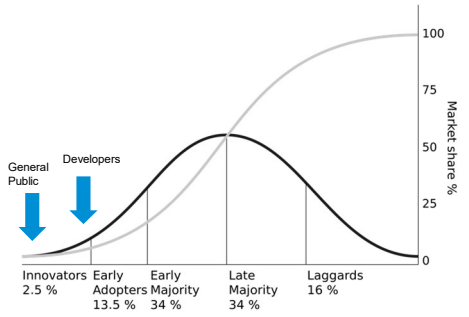
Just as the internet 1.0 revolutionized access to information, Blockchain is doing the same to multiple industrial verticals:

- 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!!

219

WHERE ARE WE NOW?



220

INVESTMENT INTO THE SECTOR

- Reid Hoffman (LinkedIn) Invested US$20M in Blockstream Personally
- Sir Richard Branson backed BitPay (Exchange) in a US$30 Million Round
- 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)
- Billions more invested in 2017 & 2018 by Intl. Banks, corporations.
- 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.

221

EVOLUTION OF THE NETWORKS

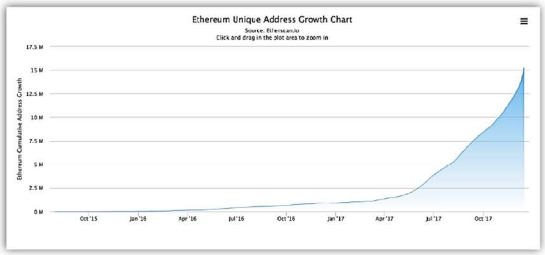
Blockchain 2.0 is currently in a alpha-beta state but is evolving very rapidly and introducing turing-complete functionality

- Ethereum and Codius introduce autonomous applications (recently used by IBM at the core of their new IoT platform - ADEPT)

- Curated blockchains, Private access/Hybrid blockchains, entry/exit points are known & regulated
  - Ripple
  - Tembusu

222

Growth in Crypto Addresses



223

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

224

Web 3.0

225

Internet Technology Progression

226

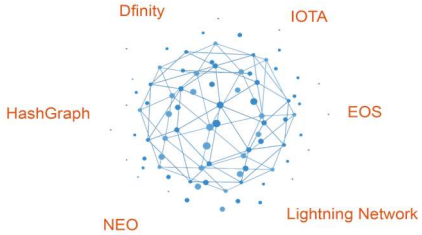
The Future of Blockchain

- **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 eliminated.

227

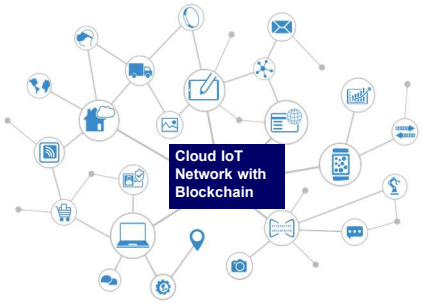
Blockchain – New 3.0 Solutions

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.



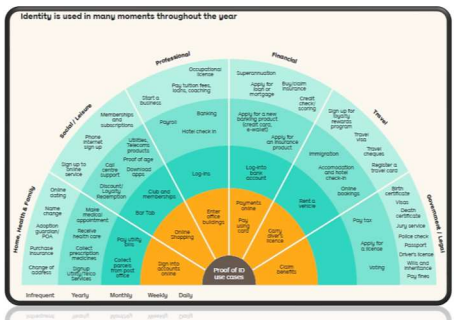
228

Blockchain – Future Internet 3.0



229

Digital Identity Touch Points using Blockchain



230

Blockchain - Global Applications with IoT

231

Blockchain Implementation

232

Top 5 Blockchain Platform Features

Summary of Features of top 5 Blockchain Platforms for Enterprises

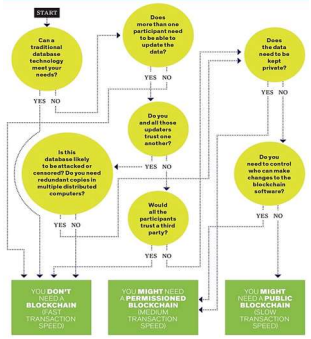
	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry-focus	Cross-Industry	Cross-Industry	Financial Services	Financial Services	Cross-Industry
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum developers & JP Morgan Chase
Ledger type	Permissionless	Permissioned	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

233

When to use Blockchain



234

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

235

When to use Blockchain

- Key question: Why is using a blockchain better than a central database?
  - Still need to secure the endpoints (use cases break down)
- Next-gen EDI/VPM in multi-party business networks
  - Many network points of information and money exchange
  - Information where having a single shared set of trusted information would help in value chain ecosystem?
- Trade-offs and hybrid networks
  - Centralized systems: fast, scalable, adaptable, manage complexity; Blockchain: open-ended, whatever can be secured

236

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

237

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

238