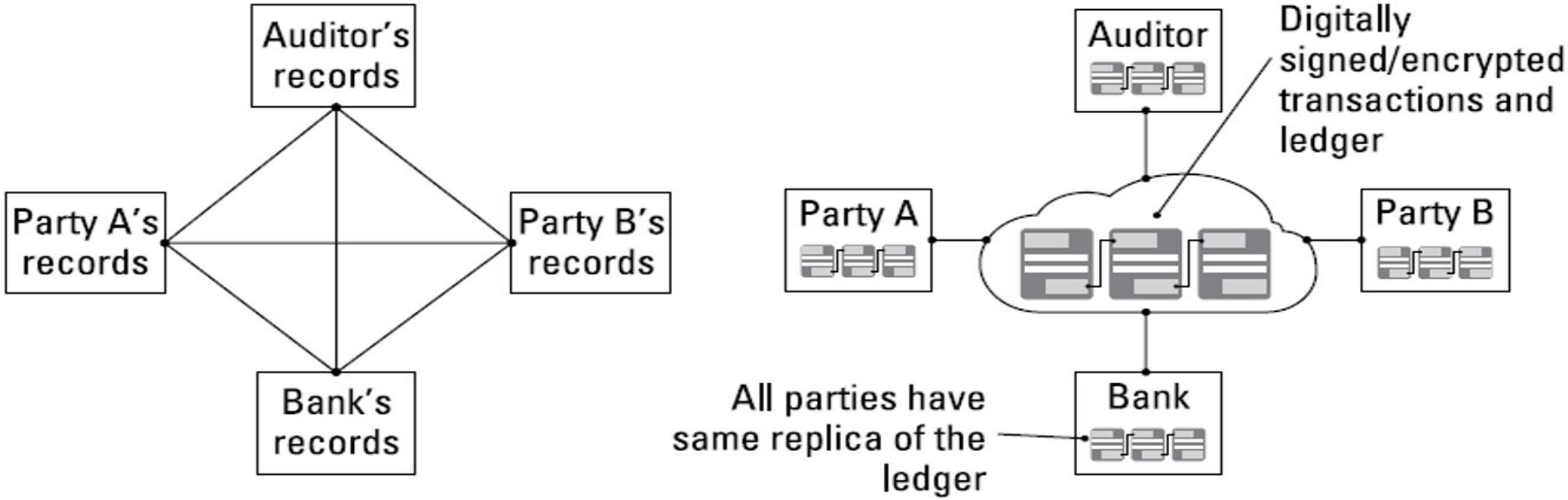
Blockchain Basics

Presented BY: Dr Abdurashid Turgunov

Course name: Blockchain Technology

Tracing Blockchain's Origin

- The shortcomings of current transaction systems
  - During 2000's financial crisis



Bitcoin Whitepaper: 10/31/2008

https://bitcoin.org/bitcoin.pdf

Bitcoin: A Peer-to-Peer Electronic Cash System

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

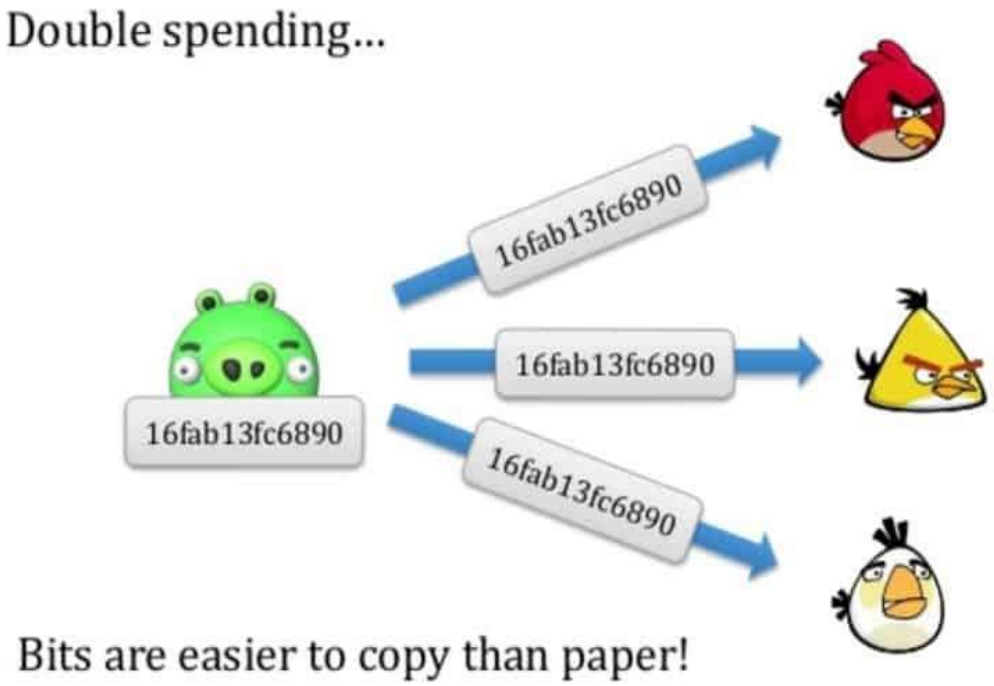
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required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

Digital Currency

- The most successful among lot of efforts: Bitcoin
- Replace cash with numbers and cod
- Advantages
  - Fast
  - International
  - Easy accounting
  - Weighs nothing
  - Cheap
- Problems to be solved

Problems of Digital Currency

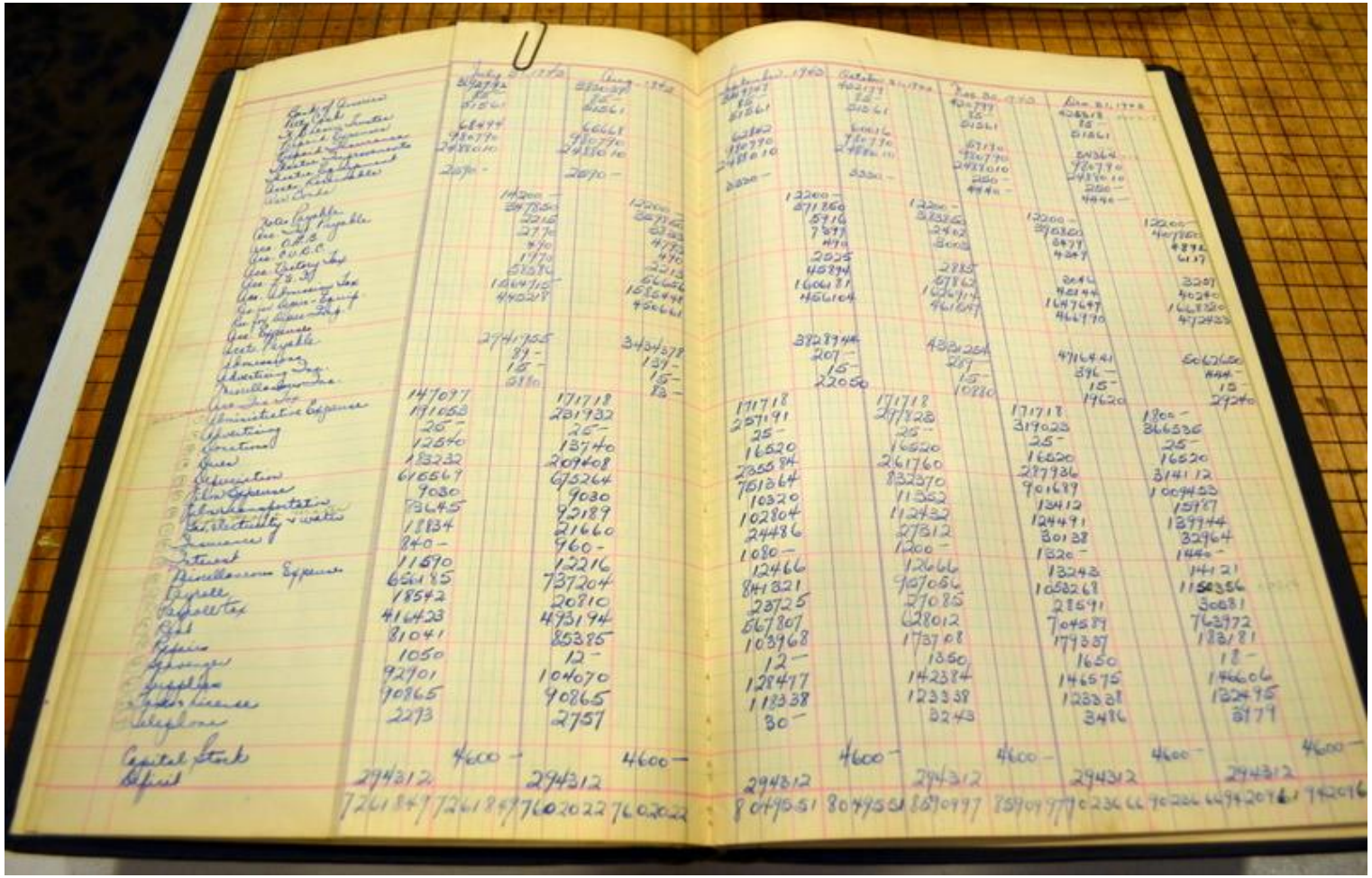
- Perfect Copy
  - Just like downloading attachment fro
  - How to distinguish counterfeits
  - Ownership Problem
- Double Spending
  - Networks are noisy and transmission delay
  - A hacker can capitalize
  - Fraudster Detection Problem



The Long Road to Bitcoin

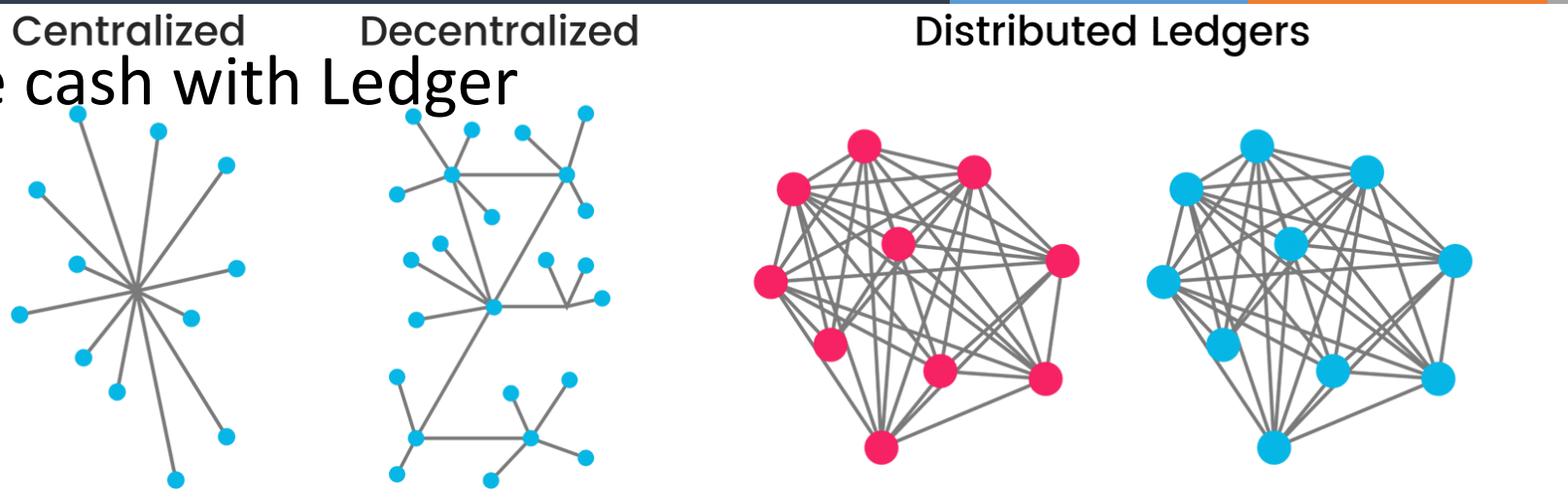
- Centralized Banking: not robust
- Satoshi determined to find the centralized part of banks
  - The ledger
  - “What if I could turn a bank inside out? Instead of one central party controlling the ledger, what if every user were recruited to maintain a constantly updated copy?”
- The strength of the digital was perfect copies, so copy the ledger, everywhere, instantly.
  - Any ledgers with even one common not agreeing with the masses would be discarded, leaving fraudsters powerless
- **Replace cash with Ledger!**

Ledger



Decentralization

- Replace cash with Ledger



The New Networks

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

Public blockchains

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

- Users (●) are anonymous

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

- Users (●) are not anonymous

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

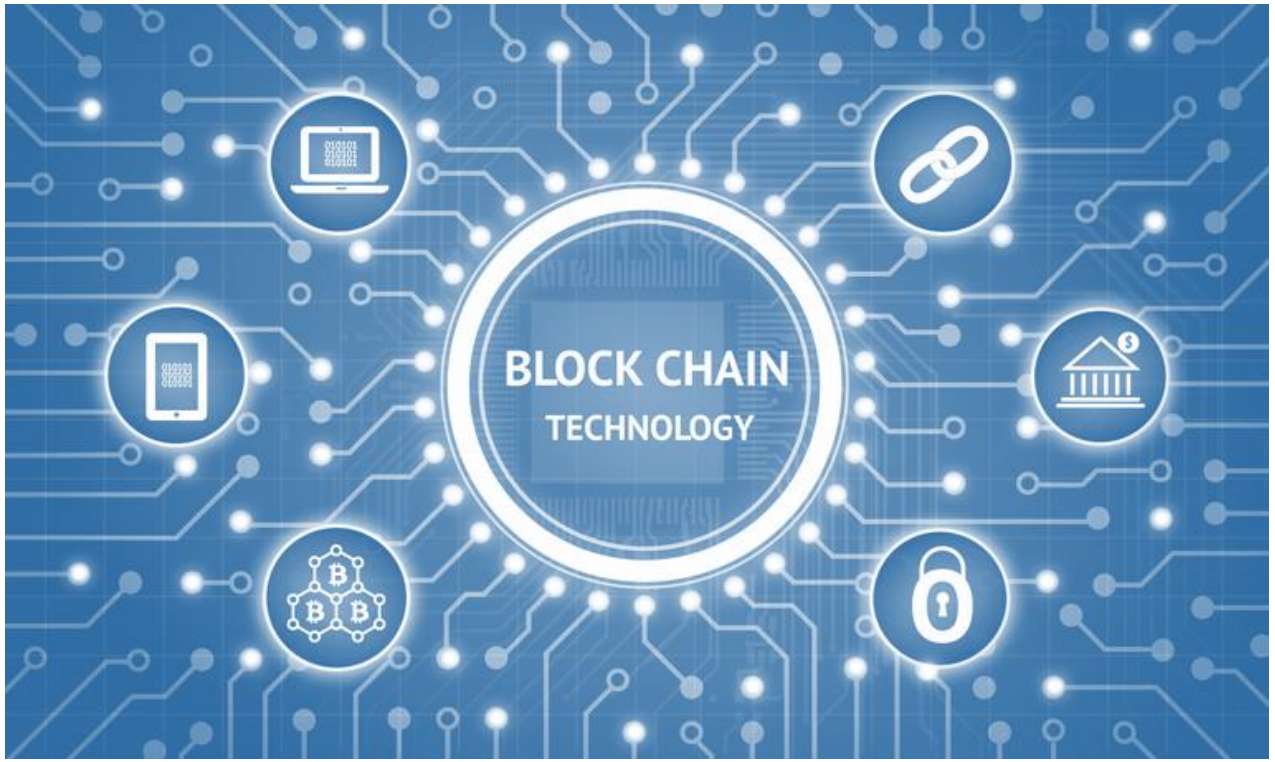
Blockgeeks

The decentralized ledger (Blockchain)

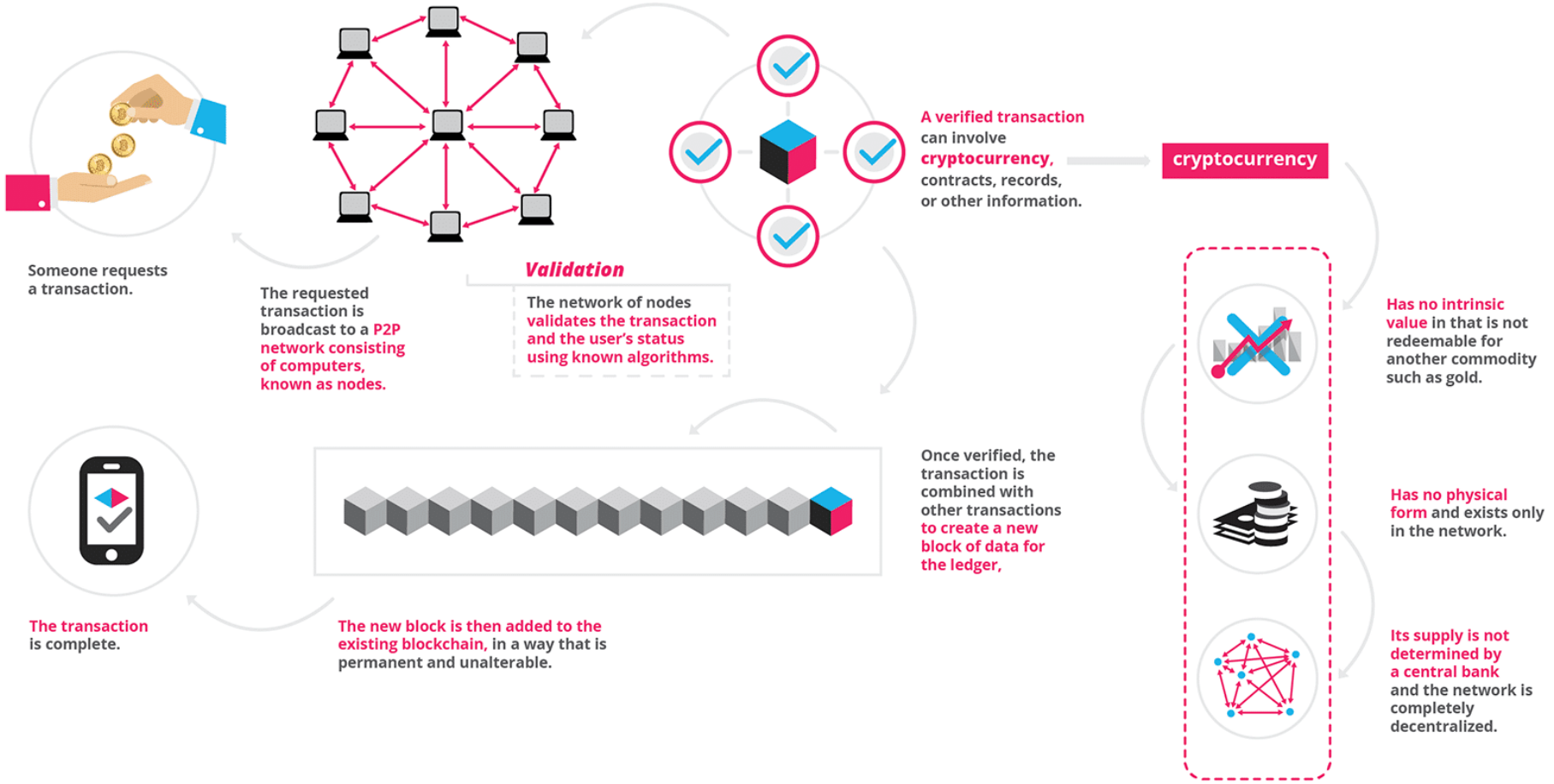
- Decentralization: get rid of the Third Party
- Satoshi paired two main technologies
  - Proof of Work: to solve the double spending problem
  - Elliptic Curves: to solve unique access to the ledger
- Nothing was newer than 2001
  1. 2001: SHA-256 finalized
  2. 1999-present: Byzantine fault tolerance
  3. 1999-present: P2P networks
  4. 1998: Wei Dai, B-money
  5. 1998: Nick Szabo, Bit Gold
  6. 1997: HashCash
  7. 1992-1993: Proof-of-work for spam
  8. 1991: cryptographic timestamp
  9. 1980: public key crypto algorithm

What is Blockchain Technology

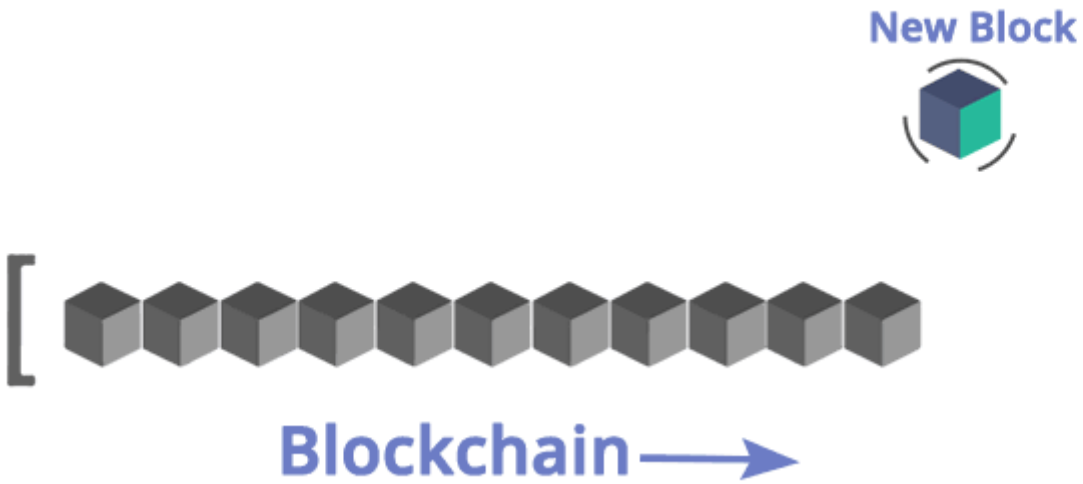
- Bitcoin stores all its transactions onto a public database called as Blockchain



Highlights

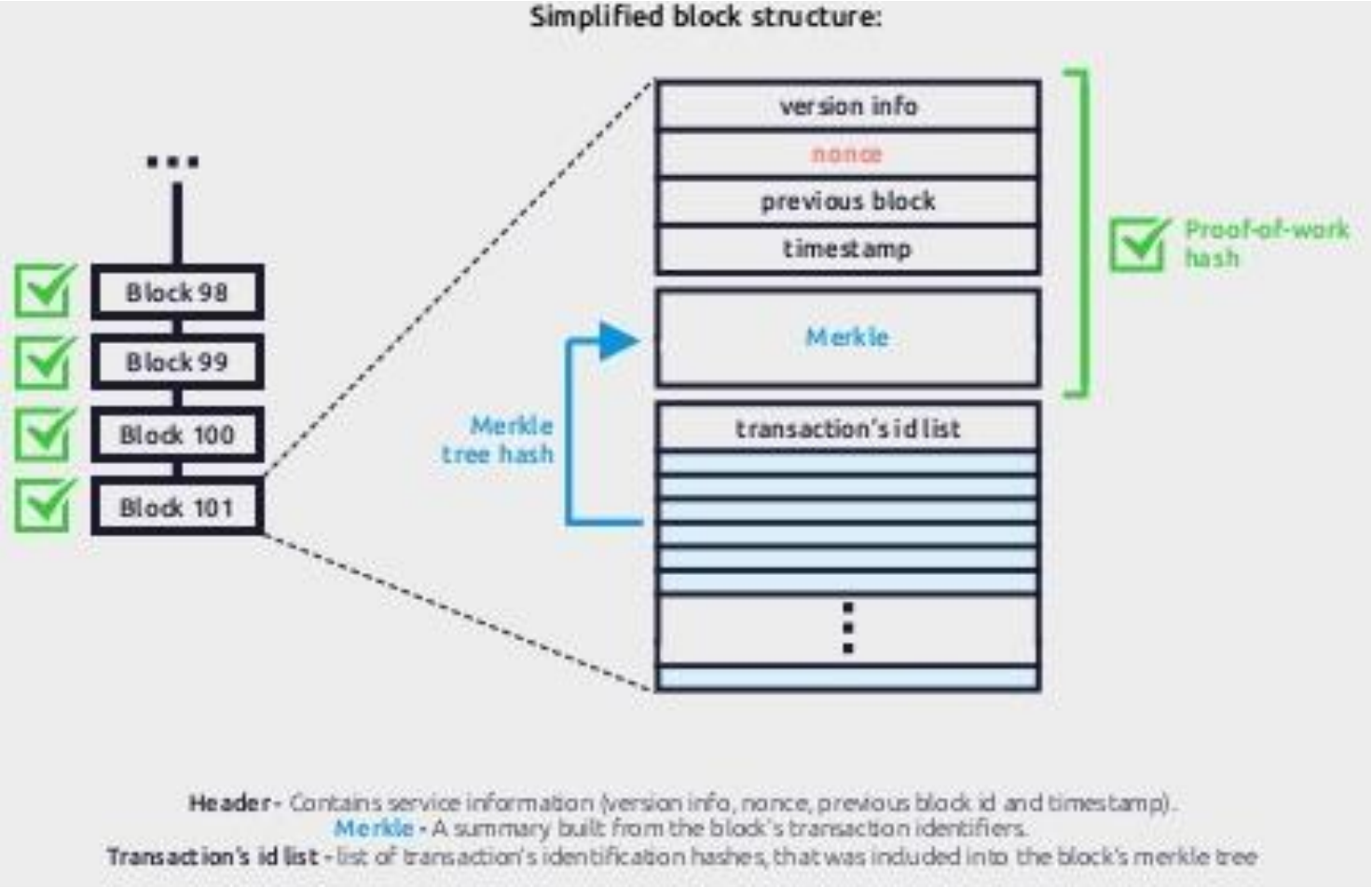

Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
cryptocurrency
Has no intrinsic value in that is not redeemable for another commodity such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Blockchain Structure



Source: https://www.edureka.co/blog/blockchain-tutorial/

What does a block look like?



4 Key Concepts of Blockchain

Distributed shared ledger

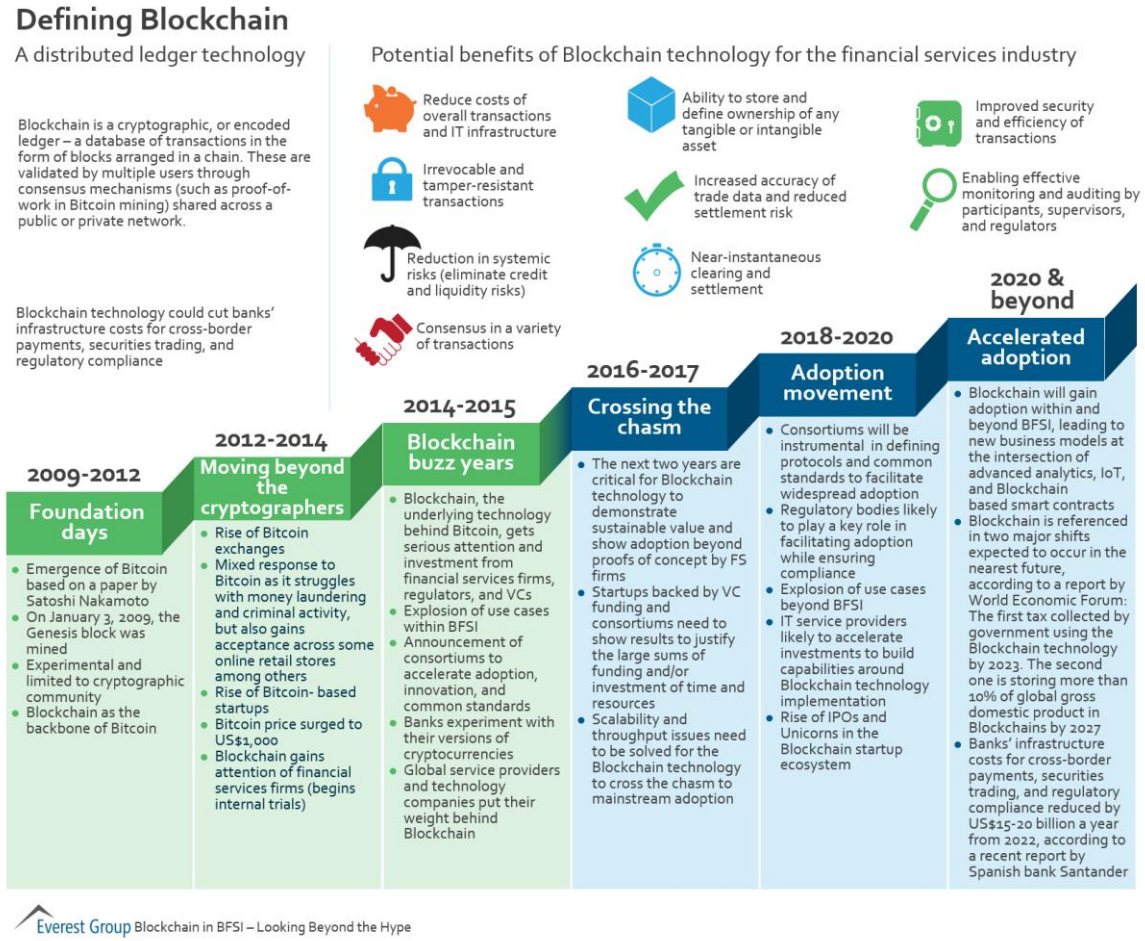
Cryptography

Consensus

Smart contracts

Source: IBM, A new disruption in financial services

Blockchain: Distributed Ledger Technology



Blockchain Architecture

- Revolutionary Technology
  - Protocol
  - TCP/IP, HTTP, Cloud Computation, Big Data, IoT, FinTech…
- Melanie Swan: Blockchain: Blueprint for A New Economy, Jan 2015
  - Blockchain 1.0
    - Bitcoin
    - Programmable Money
  - Blockchain 2.0
    - Ethereum
    - Smart Contract
  - Blockchain 3.0…
    - Non-Financial Uses
- Applications

Bitcoin System vs. Current Banking System

- **Decentralized System**
  - The Blockchain system follows a decentralized approach when compared to banks and financial organizations which are controlled and governed by Central or Federal Authorities.
  - Here, everyone who is involved with the system holds some power.
- **Public Ledgers**
  - The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system.
  - Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous.
- **Verification of Every Individual Transaction**
  - Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes.
  - Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated.
- **Low or No Transaction Fees**
  - These transaction fees are however relatively quite less when compared to the fees implied by banks and other financial organizations.
  - If a transaction needs to be completed on priority then an additional transaction fees can be added by the user so as to have the transaction verified on priority.

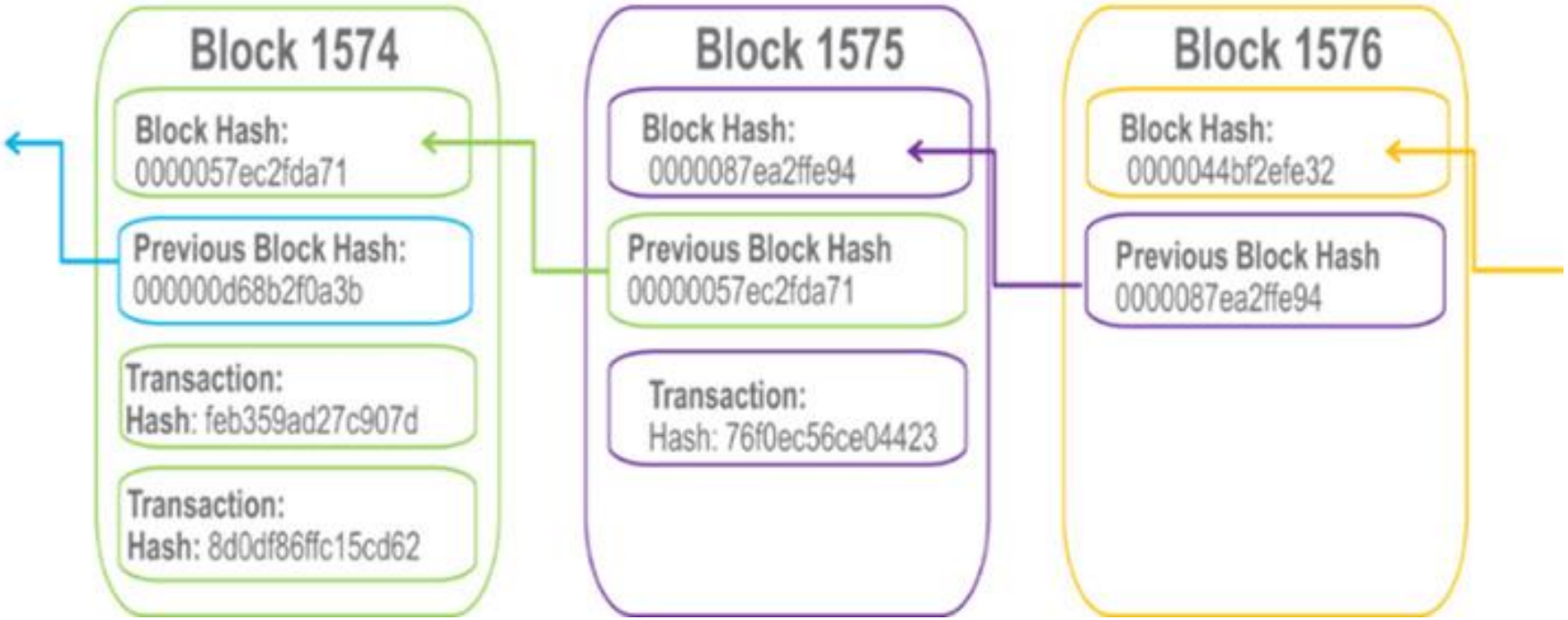
the key business benefits

- **Time savings:**
- **Cost savings:**
- **Tighter security:**
- **Enhanced privacy:**
- **Improved auditability:**
- **Increased operational efficiency:**

Building trust with blockchain

- **Distributed and sustainable:**
- **Secure, private, and indelible:**
- **Transparent and auditable:**
- **Consensus-based and transactional:**
- **Orchestrated and flexible:**

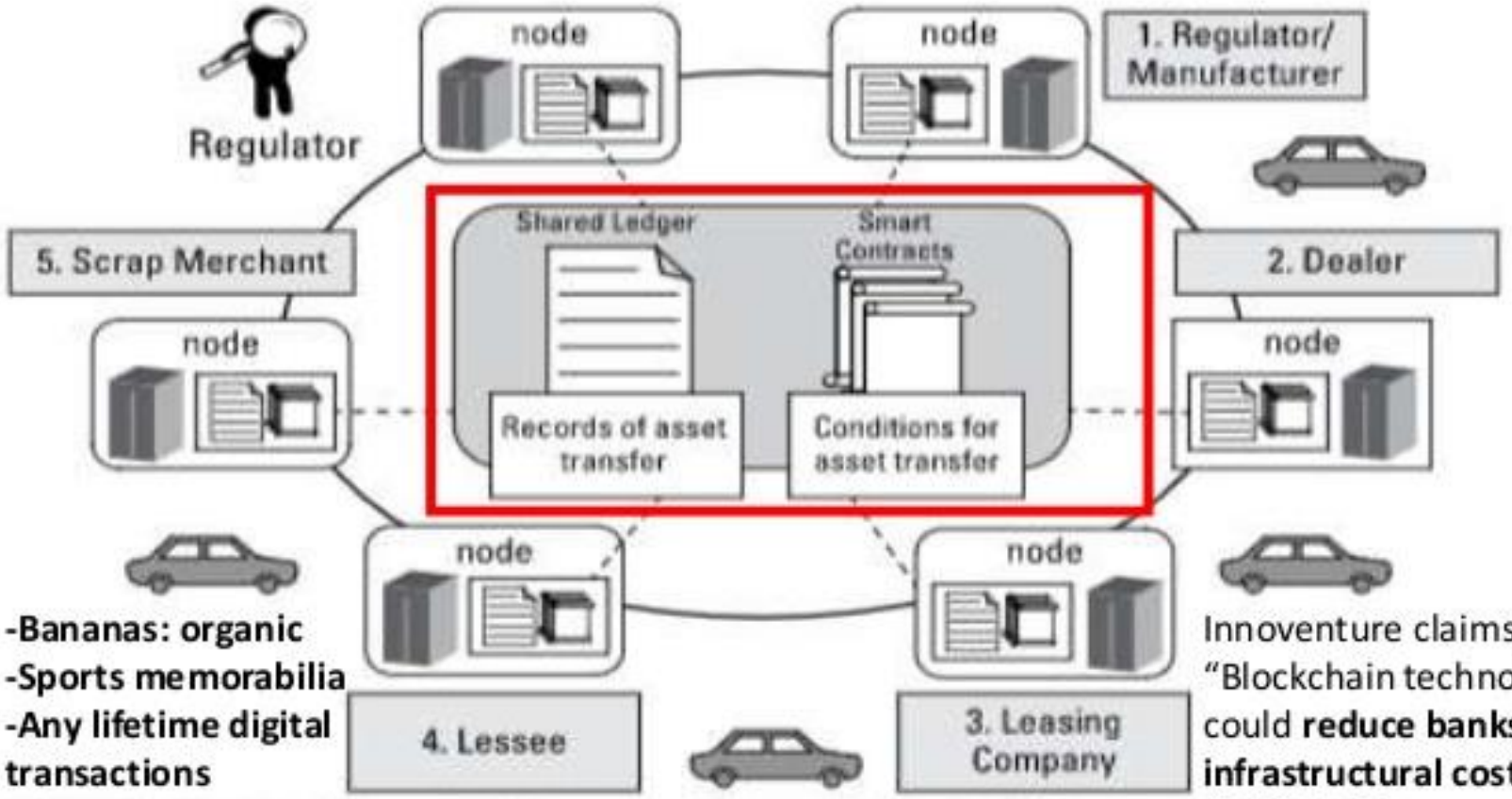
Why It's Called "Blockchain"



Different Players in Implementation

- **Blockchain user**
- **Regulator**
- **Blockchain developer**
- **Blockchain network operator**
- **Traditional processing platforms**
- **Traditional data sources**
- **Certificate authority**

Block Chain usecase (dubai)



-Bananas: organic
-Sports memorabilia
-Any lifetime digital transactions

FIGURE 1-3: Tracking vehicle ownership with blockchain.

Innoventure claims that "Blockchain technology could **reduce banks' infrastructural costs by $1.520 trillion a year by 2022**" [2]

HyperLedger Introduction

Hyperledger Fabric

- The Linux Foundation founded Hyperledger in 2015
- Hyperledger Fabric is a platform for distributed ledger solutions in industrial level.
- A modular architecture - Delivers high degrees of confidentiality, resiliency, flexibility and scalability.
- It is designed to support pluggable implementations of different components, and accommodate the complexity and intricacies that exist across the economic ecosystem.
- Breaks from some other blockchain systems is that it is **private** and **permissioned**

Hyperledger Fabric - Cont.

- Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.
- Ledger data can be stored in multiple formats, consensus mechanisms can be switched in and out.
- Offers the ability to create **channels**, allowing a group of participants to create a separate ledger of transactions.
- Hyperledger is based on blockchain but its not a crypto currency.
- There is no mining, just order system do it.
- Operational power: 0.5 million operations per minute where as other blockchain does only 1000.

In Summary

- Hyperledger Fabric is enterprise grade distributed ledger based on blockchain technologies that uses smart contracts to enforce trust between parties.
- Hyperledger in general do not enforce any requirements about the hardware, network infrastructures, additional software around it, security models etc.
- No concept of computational power.

Advantages of Hyperledger Fabric

- Permissioned membership
- Performance, scalability, and levels of trust
- Data on a need-to-know basis
- Rich queries over an immutable distributed ledger
- Modular architecture supporting plug-in components
- Protection of digital keys and sensitive data

Hyperledger Components

- Fabric CA,
- Peer
- Ordering service
- Channel
- Chaincode

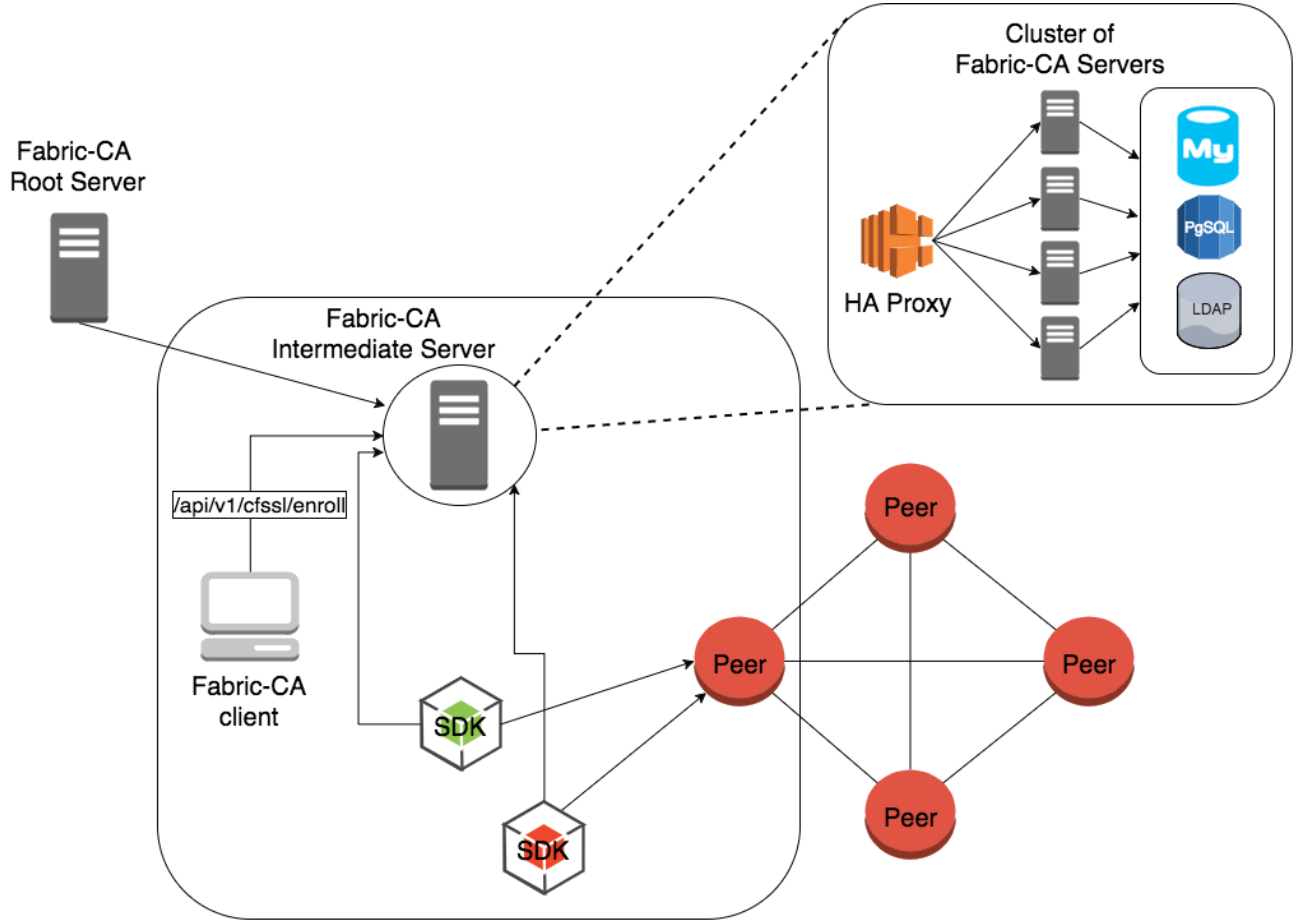
Fabric CA

The Hyperledger Fabric CA is a Certificate Authority (CA) for Hyperledger Fabric.

It provides features such as:

- registration of identities, or connects to LDAP as the user registry
- issuance of Enrollment Certificates (ECerts)
- certificate renewal and revocation
- consists of both a server and a client component.

CA – WorkFlow



Blockchain

CA cont.

- Every single operation that is executed inside hyperledger fabric must be cryptographically signed with this certificate.
- You can add attributes, roles
- Certificates are X.509 standards.
- You can remove the necessity of certificates if you don’t need it.
- Chaincodes read this data and make business decisions.

Peer

- Peer is the place where the ledger and the blockchain data is stored.
- You must have more than one peer in production.
- One peer may be part of many channels.
- Every single channel is inside the peer.
- It endorse any update of the ledger.
- You can create backup of the ledger from the peer

Ordering Service

- Ordering service is actually the heart of consensus algorithm and the heart of hyper ledger fabric.
- Main role is to provide the order of operations.
- before committing anything to ledger it must pass through the ordering service.
- it is responsible for verification, security, policy verification etc.

Channel

- **Channel** is a private “subnet” of communication between two or more specific network members.
- A channel is defined by members (organizations), anchor peers per member, the shared ledger, chaincode application(s) and the ordering service node(s).
- Each peer that joins a channel, has its own identity given by a membership services provider (MSP).

Channel cont.

- channels are completely isolated,
- they have different ledgers, different height of blocks, policies, stories, rules.
- completely isolated instance of hyper ledger fabric.
- never exchange data.
- outside of a channel , one can’t even see that there is a channel.
- you can make a policy who can see the data in the channel and who can make an operation.
- every single party inside a channel must agree about other parties.

Channel configuration properties

- **Versioned**: All elements of the configuration have an associated version which is advanced with every modification. Further, every committed configuration receives a sequence number.
- **Permissioned**: Each element of the configuration has an associated policy which governs whether or not modification to that element is permitted. Anyone with a copy of the previous configtx (and no additional info) may verify the validity of a new config based on these policies.
- **Hierarchical**: A root configuration group contains sub-groups, and each group of the hierarchy has associated values and policies. These policies can take advantage of the hierarchy to derive policies at one level from policies of lower levels.

Chaincode

- A chaincode typically handles business logic agreed to by members of the network, so it similar to a “smart contract”.
- All your business logic is inside the chaincode.
- Its written in Go. Implementation of java and javascript are on the way.
- Chaincode me installed in every peer and channel.
- Policy must be provided.

Hyperledger Composer

- Hyperledger Composer is a set of collaboration tools for building blockchain business networks that make it simple and fast for business owners and developers to create smart contracts and blockchain applications to solve business problems

- Extensive
- Open development toolset and
- Framework to make developing Blockchain applications easier.

Environment setup

Installing the pre-requisites

- Operating Systems: Ubuntu Linux 14.04 / 16.04 LTS (both 64-bit), or Mac OS 10.12
- Docker Engine: Version 17.03 or higher
- Docker-Compose: Version 1.8 or higher
- Node: 6.x (note versions 7 and higher are not supported)
- npm: v3.x or v5.x
- git: 2.9.x or higher
- Python: 2.7.x
- nvm and Apple Xcode (for Mac)
- Hyperledger Composer Extension for VSCode.

Implementation

- http://hyperledger-fabric.readthedocs.io/en/release-1.0/build_network.html

Reference and source

- 1. Bitcoin & Cryptocurrency Technologies: Bitcoin Mining, Blockchain Basics And Cryptocurrency Trading & Investing For Beginners | 7 Books In 1 by Boris Weiser (Author)
- 2. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)
- 3. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World – June 12, 2018 by Don Tapscott (Author), Alex Tapscott (Author)
- 4. Blockchain Technology for IoT Applications (Blockchain Technologies) 1st ed. 2021 Edition
- by Seok-Won Lee (Editor), Irish Singh (Editor), Masoud Mohammadian (Editor)
- 5. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher (Author) Format
- 6. Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond – October 19, 2017 by Chris Burniske (Author), Jack Tatar (Author)