Blockchain Technology

Dr. Sudeep Tanwar,
Professor | CSE
Institute of Technology | Nirma University | Ahmedabad, Gujarat

Presentation Outline

Part–I: Introduction of Blockchain Technology

Part-II: Revolution in Blockchain Technology

Part-III: Case study on Cheque clearance system using Blockchain Technology

Part-IV: Case study to demonstrate how to secure EHR in Healthcare 4.0 Using Blockchain Technology

Learning objectives of this talk

Nuts and bolts of Blockchain Technology

History of Blockchain Technology

Open research problems solved through Blockchain Technology

How to frame out case study using Blockchain Technology

Part-1
Introduction to Blockchain Technology

Why you should learn Blockchain?

Reasons To Learn Blockchain

A. Edge Cutting Technology

B. High Demand of Blockchain

C. Money Making

D. Data Security & Digital Identity

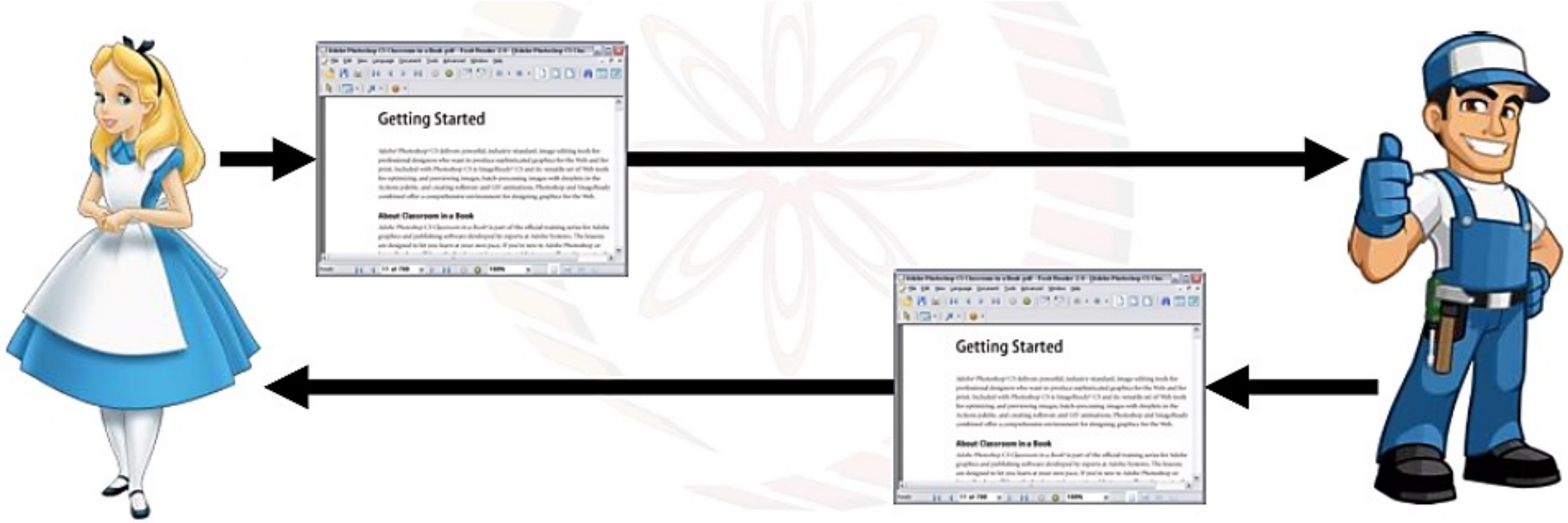
E. Integration With New-Age Technology

F. Benefit For Industries

G. High Job Prospects and Good Pay

Traditional way of document sharing……..

- **Sharing Information using Microsoft Word…..**



- **Both can’t simultaneous update the document ?????**

Image Source: NPTEL

Traditional way of document sharing……..

- **Both users can simultaneously edit the document**

This environment is still centralized……

Does centralized system harm?

If BW is an Issue then you can't upload/work on shared doc

Image Source: NPTEL

A single point failure

If you do not have sufficient bandwidth to load Google doc, You will not be able to edit it.

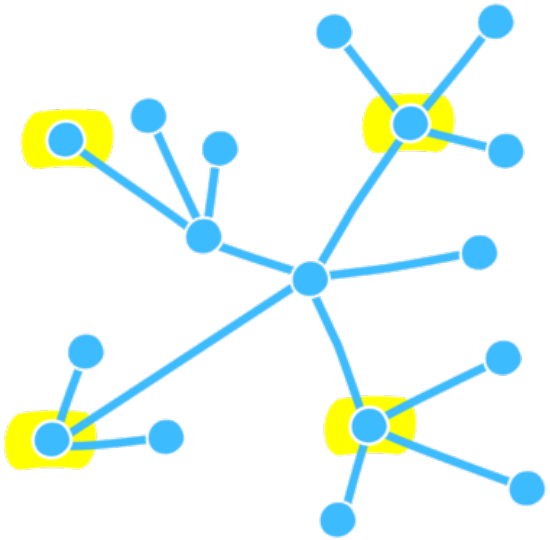
What if server crashes?

Centralized System Problems….

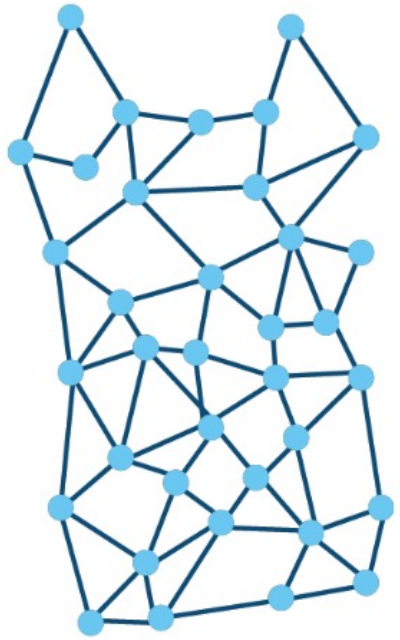
Source: NPTEL

Centralized vs Decentralized vs Distributed

Complete reliance on single point
(Cloud Computing)
If CC fails then all nodes fail
Not scalable

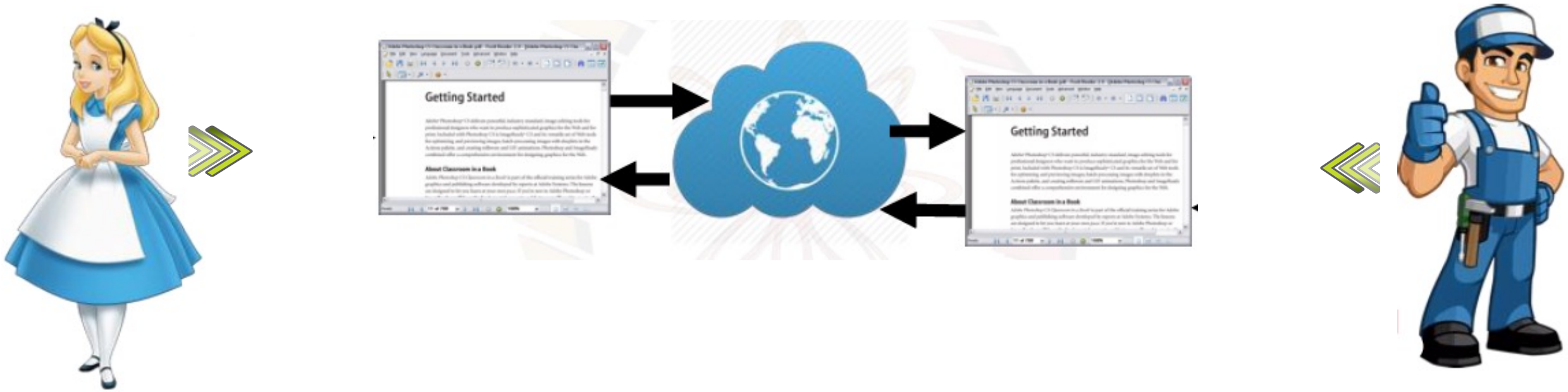


Multiple points of coordination
(Blockchain)



Everyone collectively execute the job
No central controller
Intranets, Internet, WWW, email

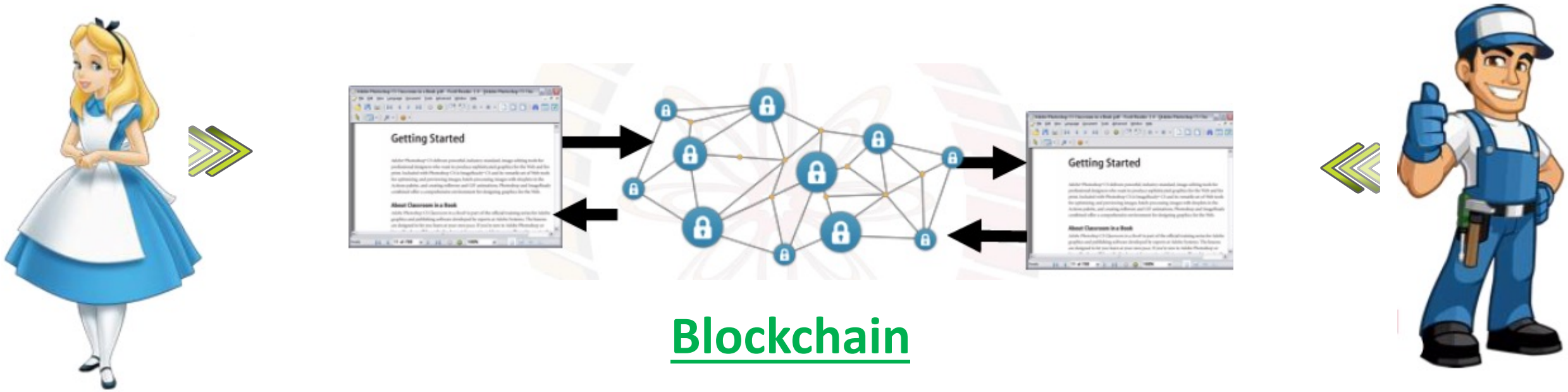
A possible solution……..



- **Everyone can edits on their local copy of the document- the Internet takes care of ensuring information consistency.**
- **Both will see the updated copy**

Image Source: NPTEL

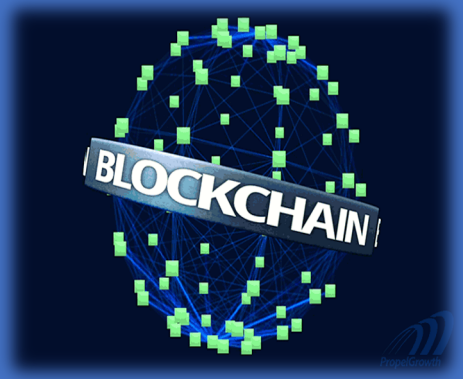
A possible solution…….



Blockchain

A decentralized database with strong consistency support…

Image Source: NPTEL



What is a Blockchain?

- A **decentralized computation and information sharing platform**

- Enables **multiple authoritative domains**, who do not trust each other, to **cooperate**, **coordinate** and **collaborate** in a **rational decision making process**.

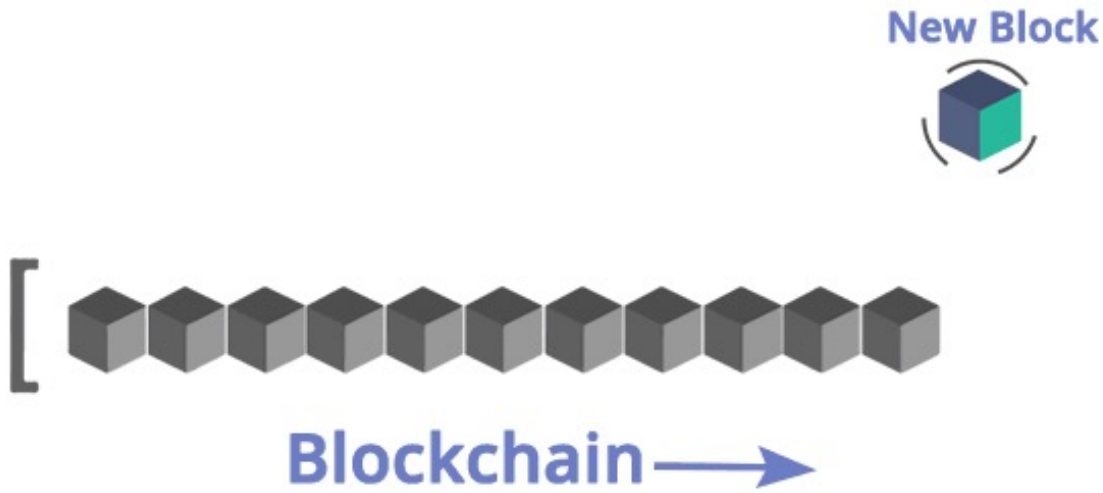
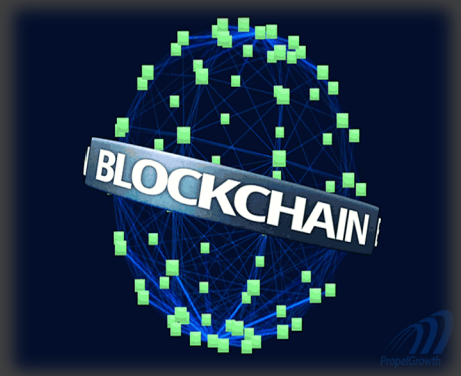


Image Source: https://www.motocms.com/blog/en/blockchain-tutorial-examples/



What is Blockchain?

A blockchain is a growing list of records, called blocks, which are linked using cryptography.

Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

By design, a blockchain is resistant to modification of the data.

Blockchain technology has become a global trend because of bitcoin.

The benefits of blockchain technology in the economy, politics, and legal systems demonstrate its potential to be a revolutionary innovation that reshapes all aspects of society.

The evolution of blockchain can be divided into five stages: 1.0 to 5.0

Example……

Public Ledger of person X

X = $100

X = $100

Public Ledger of person Y

Public Ledger of person P

X = $100

X = $100

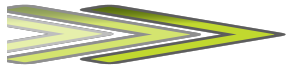
Public Ledger of person Z

Example……

Public Ledger of person X

X = $100

$50



X = $100

Public Ledger of person Y

Public Ledger of person P

X = $100

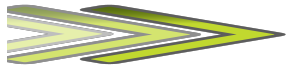
X = $100

Public Ledger of person Z

Example……

Public Ledger of person X

X = $100
X-->Y = $50



$50

X = $100
X-->Y = $50

Public Ledger of person Y

Public Ledger of person P

X = $100
X-->Y = $50

X = $100
X-->Y = $50

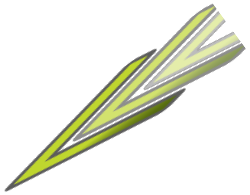
Public Ledger of person Z

Example……

Public Ledger of person X

X = $100
X-->Y = $50

$30



X = $100
X-->Y = $50

Public Ledger of person Y

Public Ledger of person P

X = $100
X-->Y = $50

X = $100
X-->Y = $50

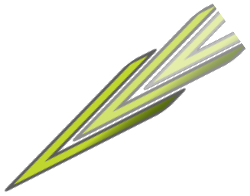
Public Ledger of person Z

Example……

Public Ledger of person X

X = $100
X-->Y = $50
Y-->P = $30

$30



X = $100
X-->Y = $50
Y-->P = $30

Public Ledger of person Y

Public Ledger of person P

X = $100
X-->Y = $50
Y-->P = $30

X = $100
X-->Y = $50
Y-->P = $30

Public Ledger of person Z

Example……

Public Ledger of person X

X = $100
X-->Y = $50
Y-->P = $30

Not valid Transaction (due to insufficient fund)

X = $100
X-->Y = $50
Y-->P = $30

Public Ledger of person Y

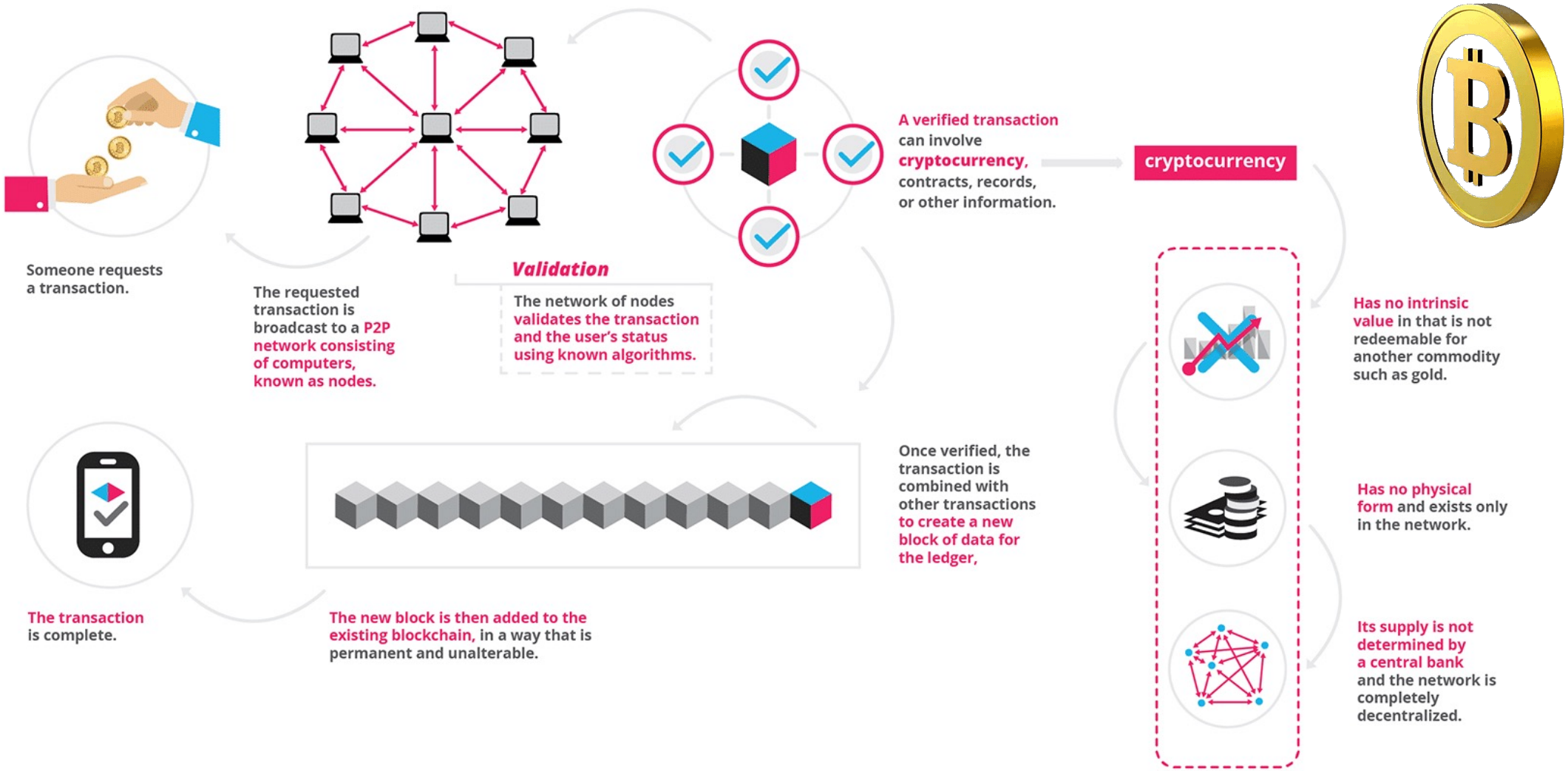
Public Ledger of person P

X = $100
X-->Y = $50
Y-->P = $30

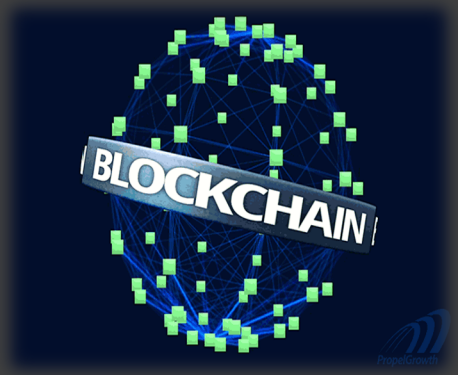
X = $100
X-->Y = $50
Y-->P = $30

Public Ledger of person Z

Transaction Example



https://blockgeeks.com/guides/what-is-blockchain-technology/



Myth about Bitcoin and Blockchain?

People generally think they are the same because **bitcoin was the first ever application of blockchain.**

Bitcoin is a digital currency that can also be called as crypto-currency

Bitoin is used to speedup the cross border transactions, to reduce the govt control over the transactions, and to simplify the whole process without involvement of third party

But, blockchain is a **type of ledger** that records all the transactions and helps in P2P transactions.

Thus, **blockchain acts as a bitcoin ledger and takes care all the transaction of bitcoin.**

Main differences are highlighted in next slide.

Differences between Bitcoin and Blockchain?

Trade

Bitcoin

Bitcoin is limited to trading as a currency.

Blockchain

Blockchain can easily transfer anything from currencies to property rights of stocks.

Scope

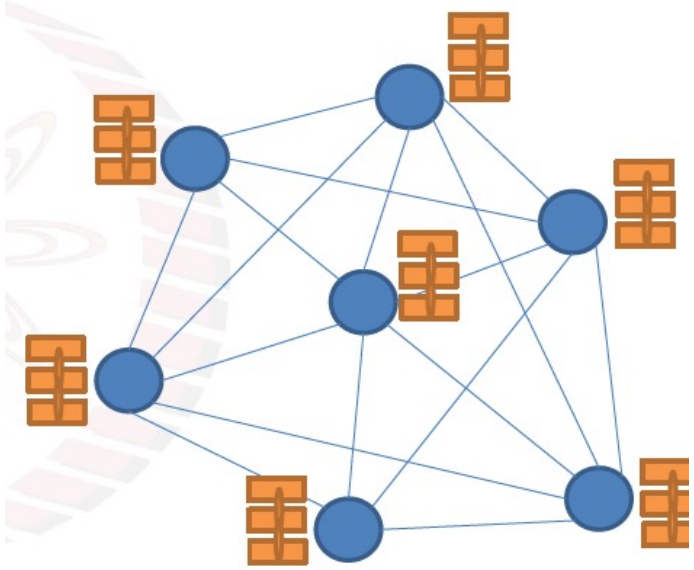
Bitcoin

The scope of bitcoin is limited.

Blockchain

The blockchain is more open to changes and hence has the backing of many top companies.

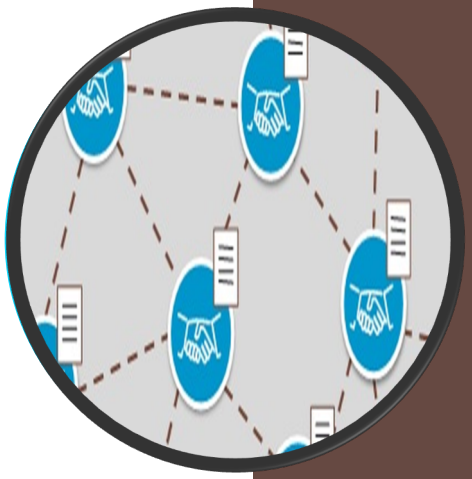
Simplified Blockchain



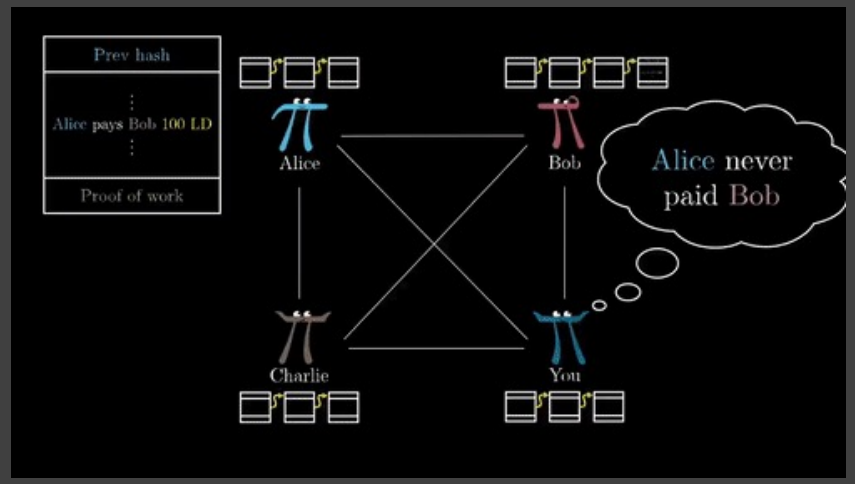
- Every node maintains a local copy of global data-sheets.
- It ensures consistency among local copies:
  - Identical (Similar) local copies at each node.
  - Local copies are always updated based on global information.

Simplified Blockchain

- **We call this a Public Ledger**
  - **Historical information** available to everyone.
  - Historical information may be used for future computation.
- **An example of banking system**
  - Historical information are banking transactions.
  - Old transactions are used to validate new transactions.



Blockchain and Public Ledger



Blockchain works as a public ledger.

It ensures different aspects:

- **Protocols for commitment:** Ensure that every valid transaction from the clients are committed and included in the blockchain with in a finite minute.
- **Consensus:** Ensures that local copies are consistent and updated
- **Security:** Data need to be tamper proof. Note that client may act maliciously or can be compromised.
- **Privacy and Authenticity:** Data or transactions belongs to various clients so privacy and authenticity needs to be ensured.

Formal Blockchain Definition

- A Blockchain is “an open, **distributed ledger** that can record transactions between two parties efficiently and in a verifiable and permanent way”

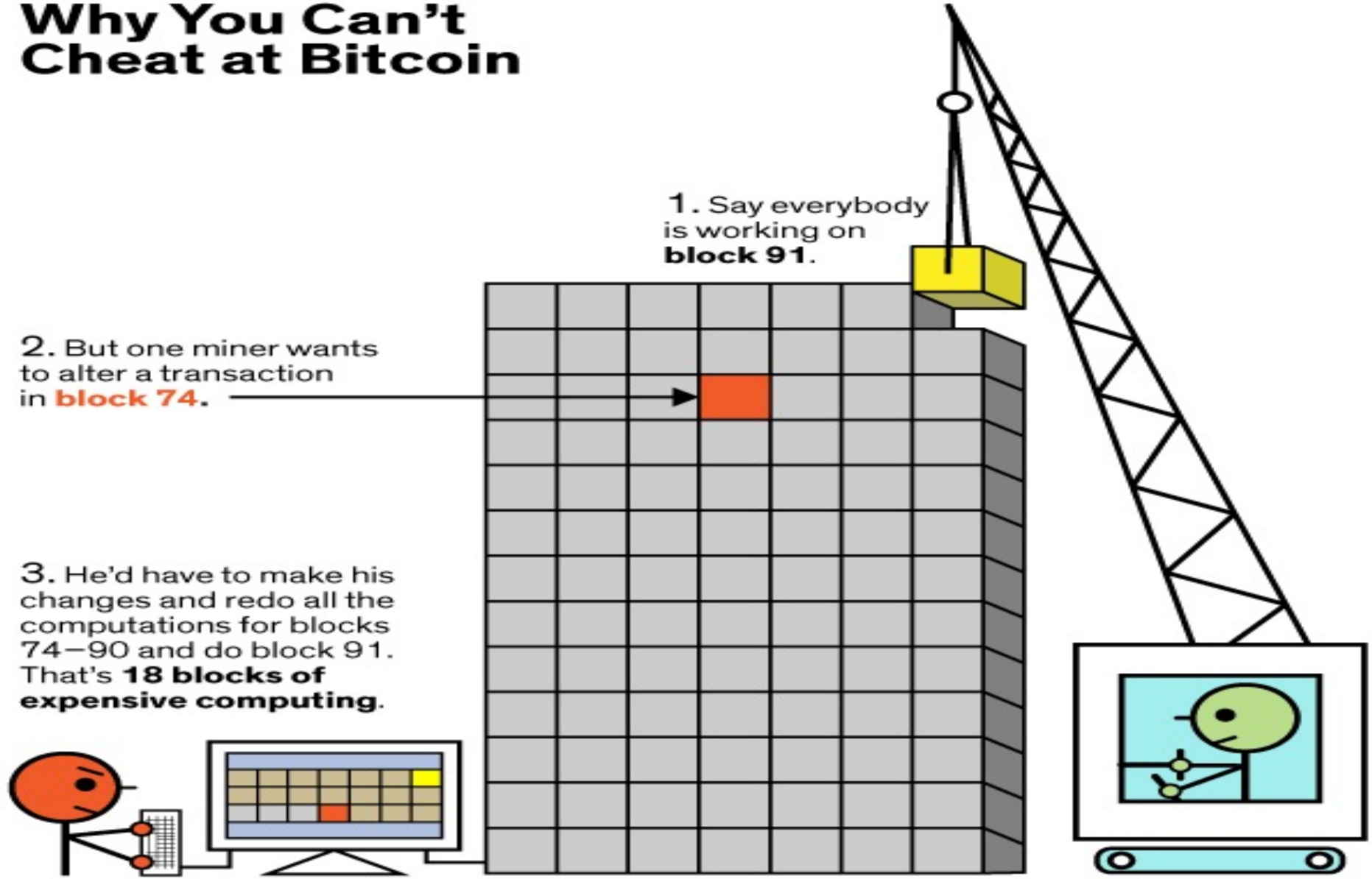
- The keywords:
  - **Open-** Accessible to all users
  - **Distributed or Decentralized:** No single party control
  - **Efficient-** Fast and scalable
  - **Verifiable-** Everyone can check the validity of the information
  - **Permanent-** Information is persistent, means when you entered any information in the blockchain then **no right to change it**.

Why You Can't Cheat at Bitcoin

1. Say everybody is working on **block 91**.

2. But one miner wants to alter a transaction in **block 74**.

3. He'd have to make his changes and redo all the computations for blocks 74–90 and do block 91. That's **18 blocks of expensive computing**.



4. What's worse, he'd have to do it all **before** everybody else in the Bitcoin network finished **just the one block (number 91)** that they're working on.

Blockchain Functions

The **primary function of a blockchain** is to certify the transactions between people.

One of the **greatest advantage of the blockchain** is the high degree of security it guarantees.

Each block in the blockchain consists of a pointer that connects it to the previous block.

A timestamp that certifies the time at which the event and the transaction data actually took place.

Example

Person “X” wants to give $100 to Person “Y”

Without blockchain

- *Person X would send his bank a request to send $100 of his account to his friends’ account. The bank would check a few things like whether Person X actually has the $100. If everything checks out the bank will send Person X $100 to Person B’s account.*

With blockchain

- *Person X creates a transaction of $100 to person Y and sends this transaction over the Internet. This transaction is included in a block. All miners check whether this is a valid transaction. If it is, Person Y has the $100 of Person X.*

With blockchain a centralized third party is no longer needed

The cryptocurrency is built on blockchain so it doesn't need a third 'authority'

Person X
Balance = $100

Person Y
Balance = $0

Types of Blockchain Nodes

1

Miner Node: It is used for authenticating, authorizing and auditing the transactions occurring in the network.

2

Ledger Node: Used to store the history of the transaction at any given instant of time

3

Normal Node: Contains the full copy of the complete blockchain.

Types of Blockchain

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	• Anyone	• Single organization	• Multiple selected organizations
Participants	• Permissionless • Anonymous	• Permissioned • Known identities	• Permissioned • Known identities
Security	• Consensus mechanism • Proof of Work / Proof of Stake	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Transaction Speed	• Slow	• Lighter and faster	• Lighter and faster
	Bitcoin and Ethereum	**Hyperledger**	**Quorum and Corda**

Source: https://blog.xsolus.com/different-types-of-blockchain-networks

Summary of Part 1 – Benefits of Blockchain Technologies

Saves Time
Immutable transaction across parties done at the same time.

Increases Trust
Through shared process and unified Systems of Record. For end consumers it's a System of Proof.

Reduces Risk
Tampering of data, fraud and cyber crime is avoided.

Remove Cost
Overheads on maintaining and synchronizing silos.

Question: Difference between distributed and decentralized systems and whether blockchain is one of them or not.

Reply:

1. A distributed system is one that has multiple interacting components or microservices.
2. These components may be owned and managed by different entities or a single entity.
3. When they are managed by a single entity, it would be a distributed system that is centralized in ownership/control
4. Examples, Like Google search, Facebook are distributed systems that are centrally owned. Of course, a centralized system may have just one component, in which case it won't be a distributed system.
5. When a distributed system is owned and controlled by different entities, it is also referred to as a **decentralized system.**
6. All or many of the nodes in the system can take part in the decision making process. So, by definition, **all decentralized systems are distributed systems.**
7. A good example is BitTorrent(communication protocol for peer-to-peer (P2P) file sharing which is used to distribute data and electronic files over the Internet.). **A blockchain is also a decentralized system.**

Question: Which is better between distributed and decentralized systems?

Reply:

- In any practical system, the term '**better**' can be used if it suits the requirement in a better way.
- Moreover, any decentralized system is a distributed system.
- **For example,** if we want to create a very **basic swarm architecture**, then decentralizing may be enough.
- But if we want something like a **cryptocurrency-based transaction system**, we may need to implement a full-fledged distributed ledger.
- So, the **“betterness” depends on your objective.**

Question: Why all the transactions are visible to all the nodes in the blockchain?

Reply:

- In case of blockchain there are **no central systems** like **banks** which list all the transactions in their ledgers in a centralized manner, instead here decentralized (or distributed) system is used, which involves all the nodes.
- So if you have to store/track/validate a transaction that should be through all these nodes only.
- Therefore, everyone should have the complete knowledge of the system.
- Or in other words, the system needs to be transparent enough,
- So that everyone can see what is happening and can differentiate between the “Good” and the “Bad”.

Question: How the privacy and security are maintained if all the transactions can be viewed by everyone?

Reply:

- In blockchain, the transactions won't involve the names of the users directly. Instead, there will be **encoded id(s)** representing them.
- Hence even though the transaction details would be there still no one will be able to figure out the parties involved.
- A single physical person can have more than one ids as well. So, individual user privacy is always maintained.
- On top of this, all these records are tamper proof hence is highly secure.
- Even if you compare the system with our normal monitory system, this level of information is still available to everyone.
- The distribution of wealth is always public, you know how many percentage of people in a state has what percentage of wealth; but you do not know what is the amount of wealth available to Mr. XYZ.
- The same thing is ensured in Bitcoin. You can see that an id "1BoatSLRHtKNngkdXEeobR76b53LETtpyT" has 20 BTC, but you really cant figure out whether this id belongs to Mr. XYZ or Mrs. UVW.

Question: Who are the miners and who selects them?
Reply:

- No one selects miners.
- If you are a normal Bitcoin user (have a Bitcoin wallet), you can join as a miner as well.
- Miners are simply the nodes with sufficient computation resources so that they can perform the mining process.
- As a miner, its task is just to propose a new block with a proof that the other nodes can verify.

Question: Who validates the transactions?

Reply:

- Every full node in the blockchain network, including the miners validate the transactions.
- Note the term **"full node"** here. A full node is a node that implements full blockchain functionalities (https://bitcoin.org/en/full-node) in Bitcoin.
- A full node Bitcoin wallet is more secure than a client node wallet that implements partial blockchain functionalies.
- A client node wallet with partial implementation just creates the public-private key and initiates the transactions; if they observe the transaction in a valid block, they commit it.
- However such nodes are less secure, typically they rely on more than 50% honest mining power or one or more remote servers to protect them from double-spends and other network attacks (https://en.bitcoin.it/wiki/Clients). Bitcoin always suggests for a full node implementation.

Part-2
Revolution in Blockchain Technology (History)

Blockchain 1.0: Payment Blockchain (2009)

In this generation, the creation of the first cryptocurrencies were introduced.

As a virtual currency system, the total amount of bitcoin is defined by the network consensus protocol.

No individual or institution can freely modify the supply and transaction records therein.

The underlying technology of Bitcoin-the Blockchain is actually an extremely ingenious distributed shared ledger and peer-to-peer value transfer technology that has the potential to affect as much as the financial double entry book Invention.

The main or core concept is payment and its functionality.

Blockchain 2.0: Smart Contract (2014)

Industry create a common technology platform and provide developers with BaaS (Blockchain as service) services.

It greatly improve the transaction speed, reduce resource consumption and support multiple consensus algorithms such as PoW, PoS and make DApp (Decentralized applications, often to refer as smart contracts in ETH blockchain) development easier.

Smart contract and the various financial services started for other application of the blockchain technology around 2010.

The development with etheruem, hyperledger frameworks were introduced

Usage of smart contract in financial services and its assets were started which were force behind the cryptocurrency.

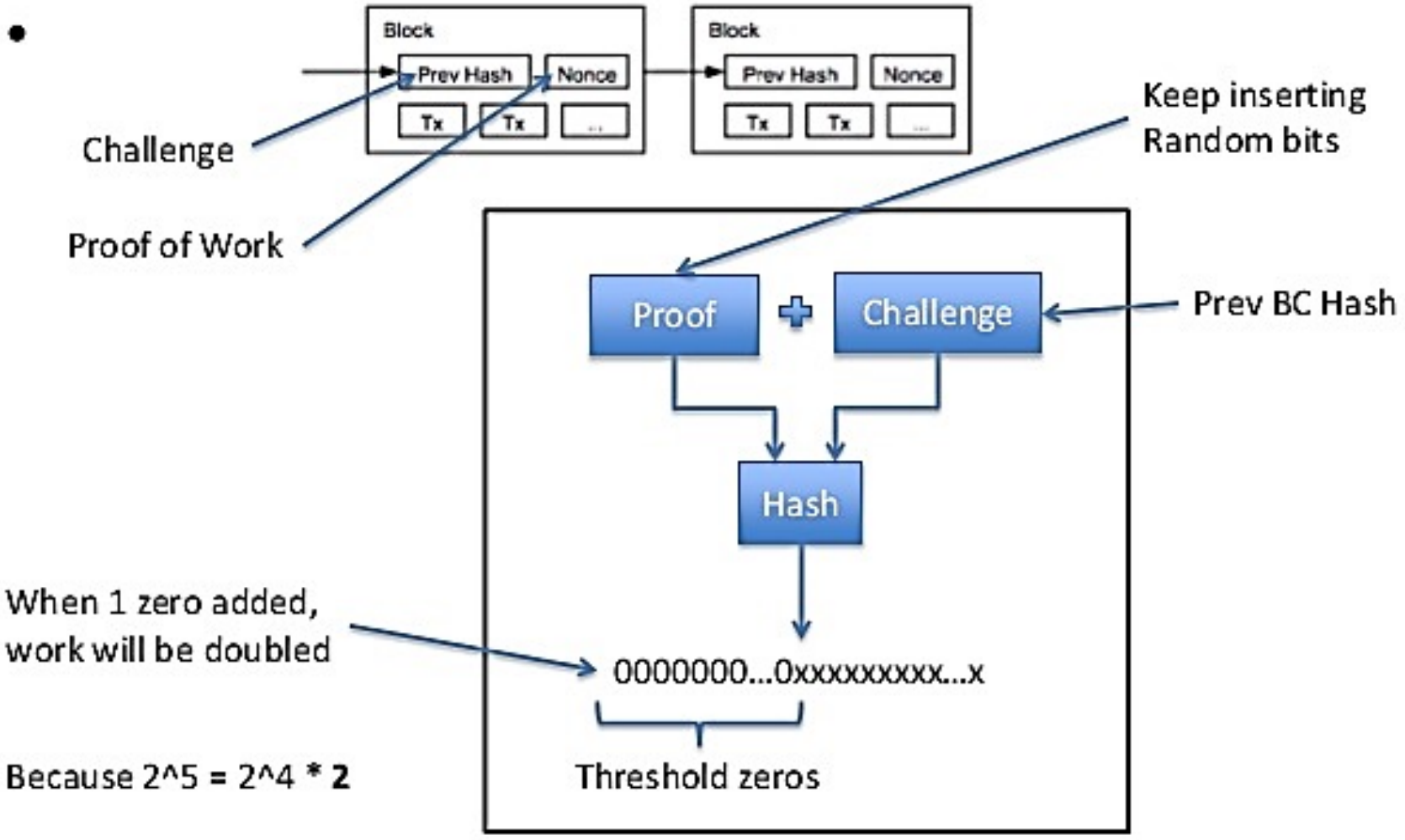
Proof-of-Work (POW)

It requires its users to perform some form of work to participate

The work must be difficult for the client but easy for the server/network to verify.

In Bitcoin and Ethereum, PoW exists in the form of Miner nodes competing to “solve a Block”

Proof-of-Work



https://steemit.com/cryptocurrency/@rrrenaldooo/what-is-hybrid-blockchain-proof-of-work-and-proof-of-stake-explained

Proof-of-Stake (POS)

The purpose is the same of the proof of work, but the process to reach the goal is quite different.

It rewards miners who solve mathematical problems.

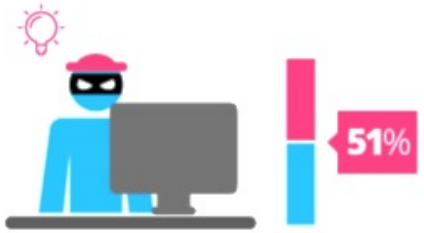
The creator of a new block is chosen in a deterministic way, depending on its wealth

Proof of Work vs Proof of Stake

Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.

Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

Blockchain 3.0: Blockchain of Things (2015)

Blockchain application extension.

Blockchain 3.0 technology based on DAG (Directed acyclic graph is a finite graph with no directed cycle) data structures such as Byteball and IOTA (Unique crypto-currencies).

Blockchain systems are more efficient, scalable, highly interoperable, and have a better user experience than before.

Broader applications such as networking, sharing economy, communications, social management, charity and charity, culture and entertainment.

The convergence towards the decentralized application were introduced.

In this level, **etheruem, hyperledger platforms have the ability to code smart contracts** with different decentralized applications such as health, governance, IoT, supply-chain, business, and smart city.

Blockchain 4.0: Cross-Chain Function (2018)

Based on the HashNet data structure

The consensus algorithm based on the data structure can achieve a qualitative leap in transaction throughput and scalability.

It will **change people's lifestyles** extensively and profoundly.

Cross-Chain Function, the digital economy ecosystem and development trend of various gaming, real estate, entertainment, information, banking, tourism, games, social and other fields

It offers services such as the public ledger and distributed in nature of the database that represents in real time.

It offers seamless integration with the Industry 4.0 and healthcare facility.

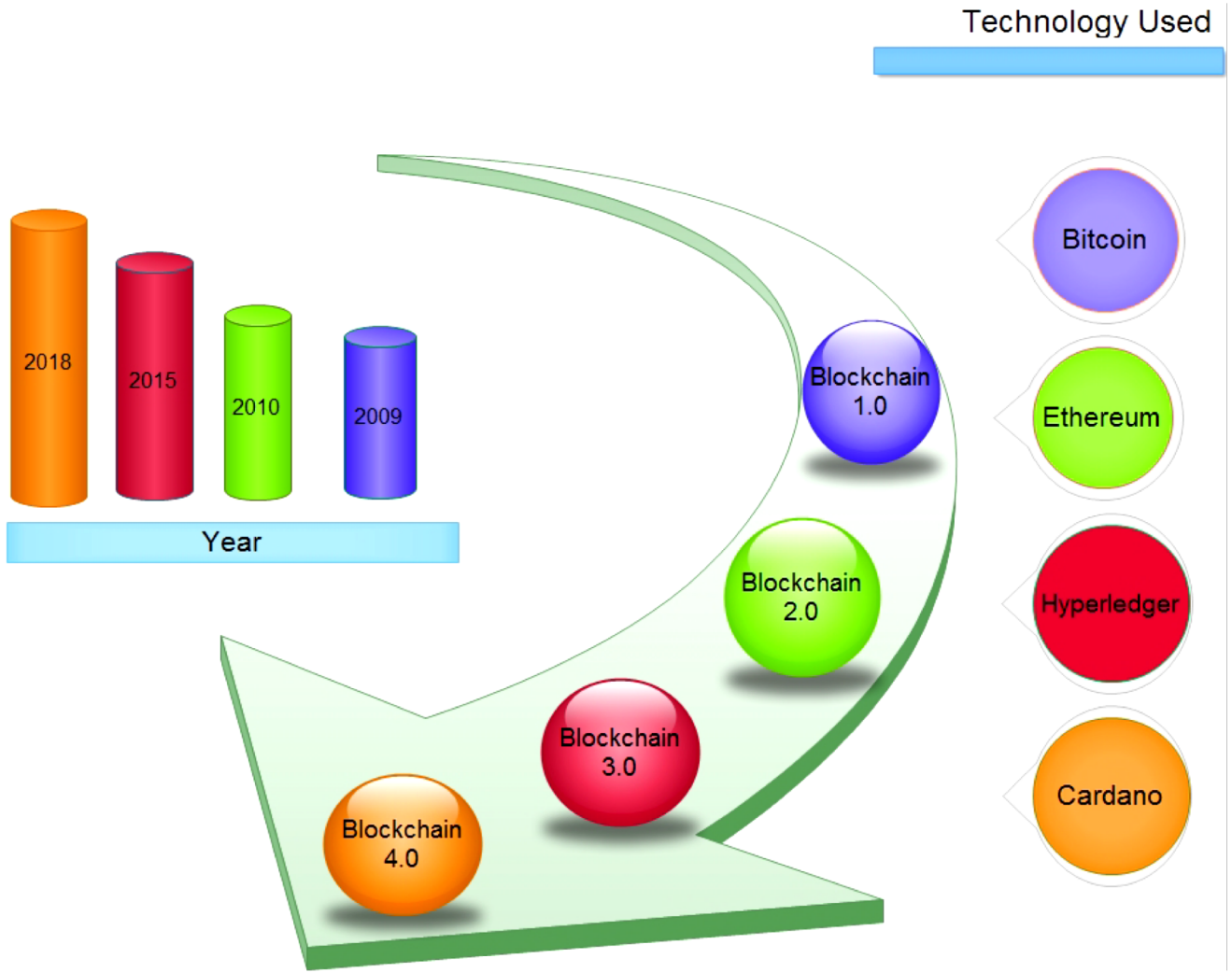
Blockchain 5.0: Unique Tech Blockchain (Present)

It allows users to freely trade in any kind of cryptocurrency in the chain through cross-chain technology, and the transaction process can be completed in just 3 seconds

It has universal smart contract application technology and can integrate the advantages of other chains to develop new sub-chains.

For example, blockchain developers can integrate Ethereum's smart contracts with EOS (blockchain protocol) smart contracts as the underlying application design to develop a new blockchain with faster speed and lesser funding.

Generations of Blockchain



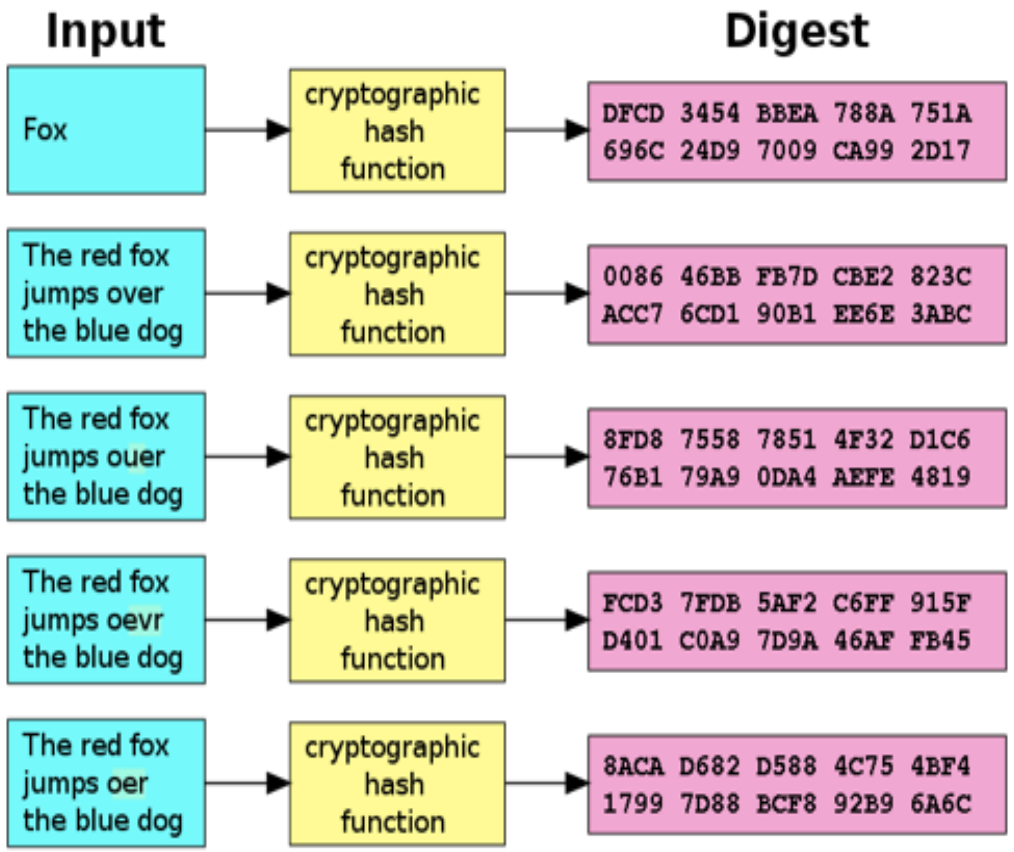
Technologies behind Blockchain

The Fundamentals

- **Cryptographically Secured Hash Functions**
  - ***Hash Functions*:** Map any sized data to a fixed size; Example *H(x) = x % n*, where *x* and *n* are integers and % is the modular (remainder after division by *n*) operations. *x* can be of any arbitrary length, but *H(x)* is within the range *[0,n-1]*.
  - ***Cryptographically Secured:***
    - **One way**, given a *x*, we can compute *H(x)*, but given a *H(x)*, no deterministic algorithm can compute *x*
    - For two different x_1 *and* x_2, $H(x_1)$ and $H(x_2)$ should be different

      (Means Blockchain is a data structure)

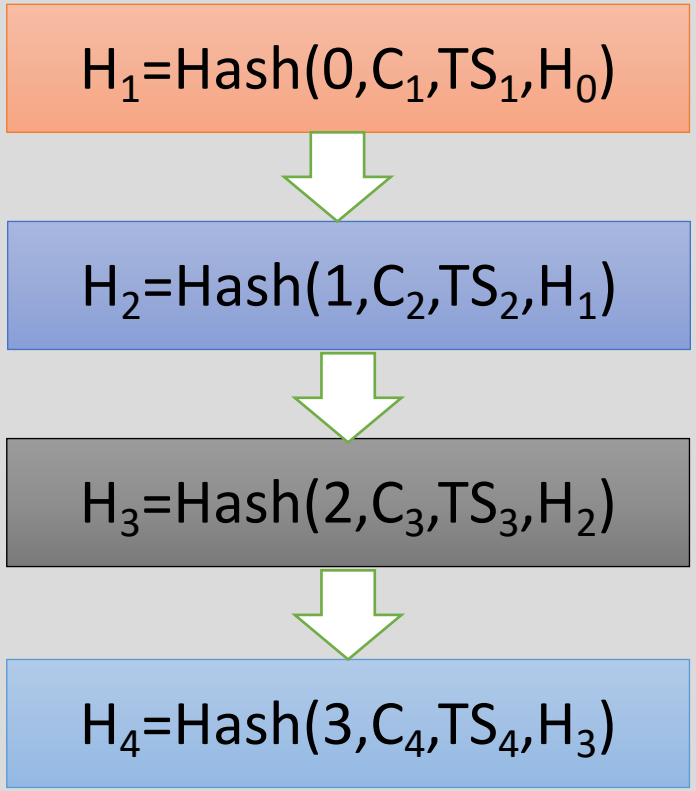
Cryptographic Hash Functions



- Examples: MD5 (Message-digest algo-128 bit hash value), SHA256 (Secure Hash Algorithm designed by NSA USA)
- X is called the **message** and H(X) is called the **message digest**
- A small change in the data results in a significant change in the output – called the **avalanche effect**

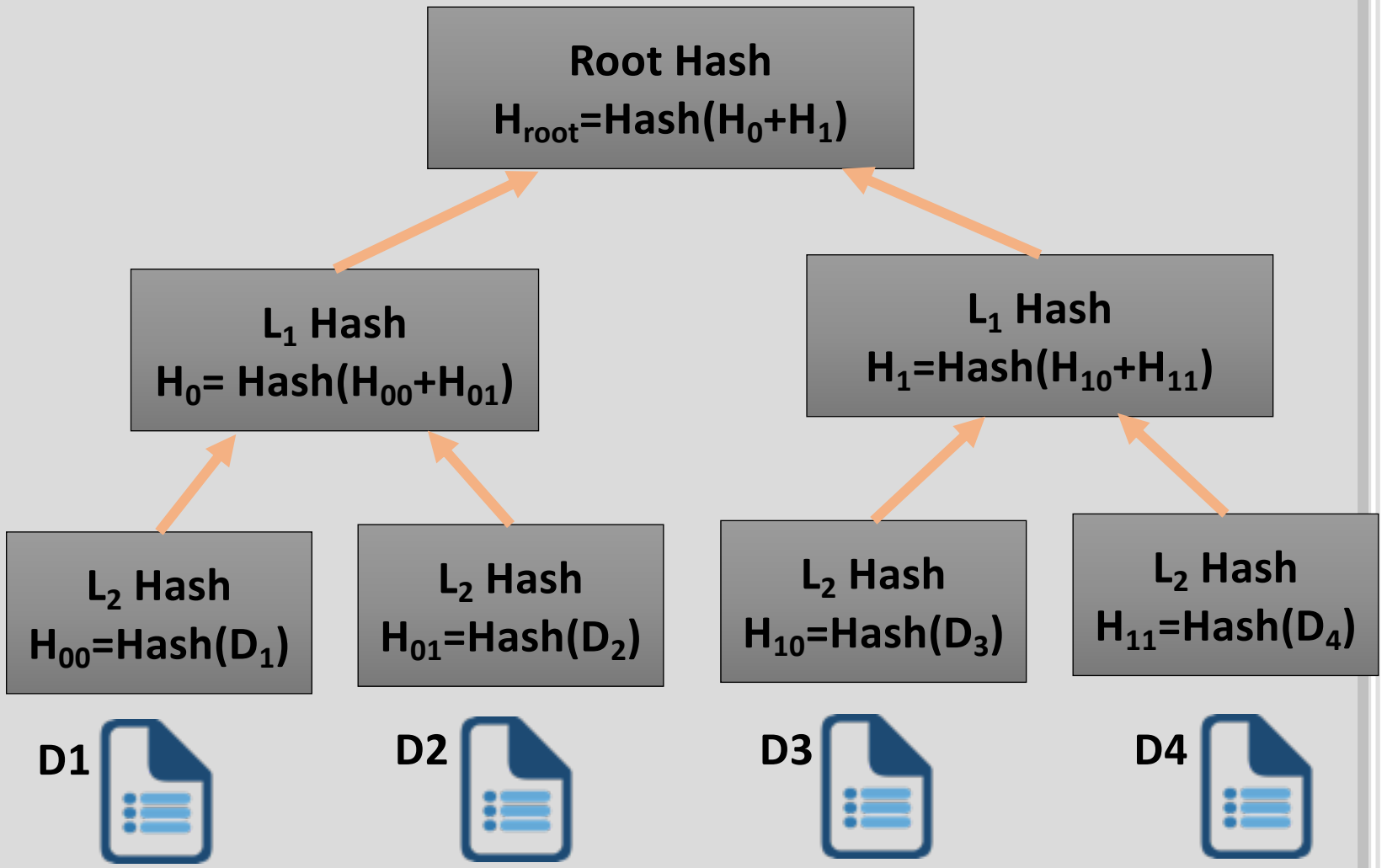
Cryptographically Secured Chain of Blocks

- The first use - **time-stamp a digital document** (*Harber and Stornetta, 1991*)
  - A sequence of timestamps [TS_1, TS_2, TS_3, …] denoting when the document is created or edited.
  - Whenever a client access a document, construct a block consisting of the sequence number of access, **client ID, timestamp, a hash value** from the previous request; and the entire thing is hashed to connect it to the previous blocks.



Merkle Trees

- Also known as **hash tree**
  - ***every leaf node*** is labelled with the hash of a data block
  - ***every non-leaf node*** is labelled with the cryptographic hash of the labels of its child nodes



Use of Merkle Trees

- Bayer, Harber and Stornetta used Merkle Tree in 1992 for timestamping and verifying a digital document - improved the efficiency by combining timestamping of several documents into one block

- Other **uses of Merkle Tree**
  - **Peer to Peer Networks:** Data blocks received in undamaged and unaltered; other peers do not lie about a block
  - **Bitcoin implementation** – shared information are unaltered; no one can lie about a transaction

Bitcoin

Bitcoin in 2014 Is Like Internet in 1994: Weird and Scary

- ***Marc Andreessen***: American entrepreneur, investor, and software engineer. Co-author of Mosaic, cofounder of Netscape

How it began in 2008: a financial system WITHOUT "TRUSTED" THIRD PARTIES

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.

http://satoshinakamoto.me/whitepaper/

Improvements can be proposed by DEVELOPERS AROUND THE WORLD

Bitcoin: A Peer-to-Peer Electronic Cash System

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

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

bitcoin.org/bitcoin.pdf

Number	Title	Owner	Type	Status
1	BIP Purpose and Guidelines	Amir Taaki	Process	Active
2	BIP Status and Comments	Luke Dashjr	Process	Deferred
9	Version bits with timeout and delay	Pieter Wuille, Peter Todd, Greg Maxwell, Rusty Russell	Informational	Draft
10	Multi-Sig Transaction Distribution	Alan Reiner	Informational	Withdrawn
11	M-of-N Standard Transactions	Gavin Andresen	Standard	Final
12	OP_EVAL	Gavin Andresen	Standard	Withdrawn
13	Address Format for pay-to-script-hash	Gavin Andresen	Standard	Final
14	Protocol Version and User Agent	Amir Taaki, Patrick Strateman	Standard	Final
⋮				
141	Segregated Witness (Consensus layer)	Eric Lombrozo, Johnson Lau, Pieter Wuille	Standard	Draft
142	Address Format for Segregated Witness	Johnson Lau	Standard	Deferred
143	Transaction Signature Verification for Version 0 Witness Program	Johnson Lau, Pieter Wuille	Standard	Draft
144	Segregated Witness (Peer Services)	Eric Lombrozo, Pieter Wuille	Standard	Draft
145	getblocktemplate Updates for Segregated Witness	Luke Dashjr	Standard	Draft
151	Peer-to-Peer Communication Encryption	Jonas Schnelli	Standard	Draft

github.com/bitcoin/bips

What is Bitcoin?

- Bitcoin is a **completely decentralized**, **peer-to-peer**, **permission-less** cryptocurrency
  - **Completely decentralized**: no central party for ordering or recording anything
  - **Peer-to-peer**: software that runs on machines of all stakeholders to form the system
  - **Permission-less**: no identity; no need to signup anywhere to use; no access control – anyone can participate in any role

Bitcoin Value Proposition

- The last few years have seen a lot of interest in Bitcoin and cryptocurrencies in general.
- Used as a cross-country, untraceable currency which is not under the control of any government and hence free from regulation.
- Current BTC price **1 BTC = 35,97,448.61** (as of 22nd Feb, 2021 at 12:52 pm)
- The Bitcoin blockchain size as of 22nd Feb, 2021 is approximately **321 GB**.

Source: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

The Technology behind Bitcoin – The Blockchain

A = ₹100

A -> B ₹50

B -> J ₹30

A

₹ 100

₹ 50

B

A = ₹100

A -> B ₹50

B -> J ₹30

₹ 30

J

A = ₹100

A -> B ₹50

B -> J ₹30

P

A = ₹100

A -> B ₹50

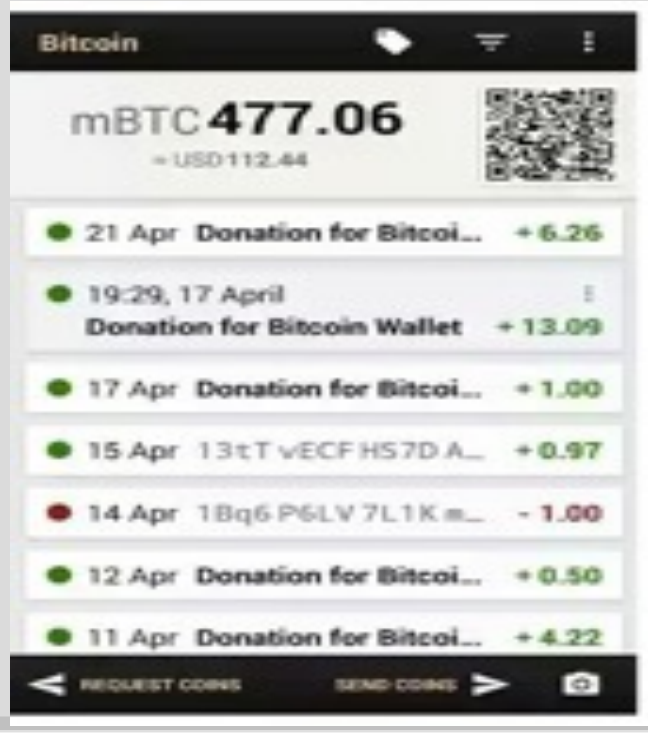
B -> J ₹30

Note: A block may contain multiple transactions

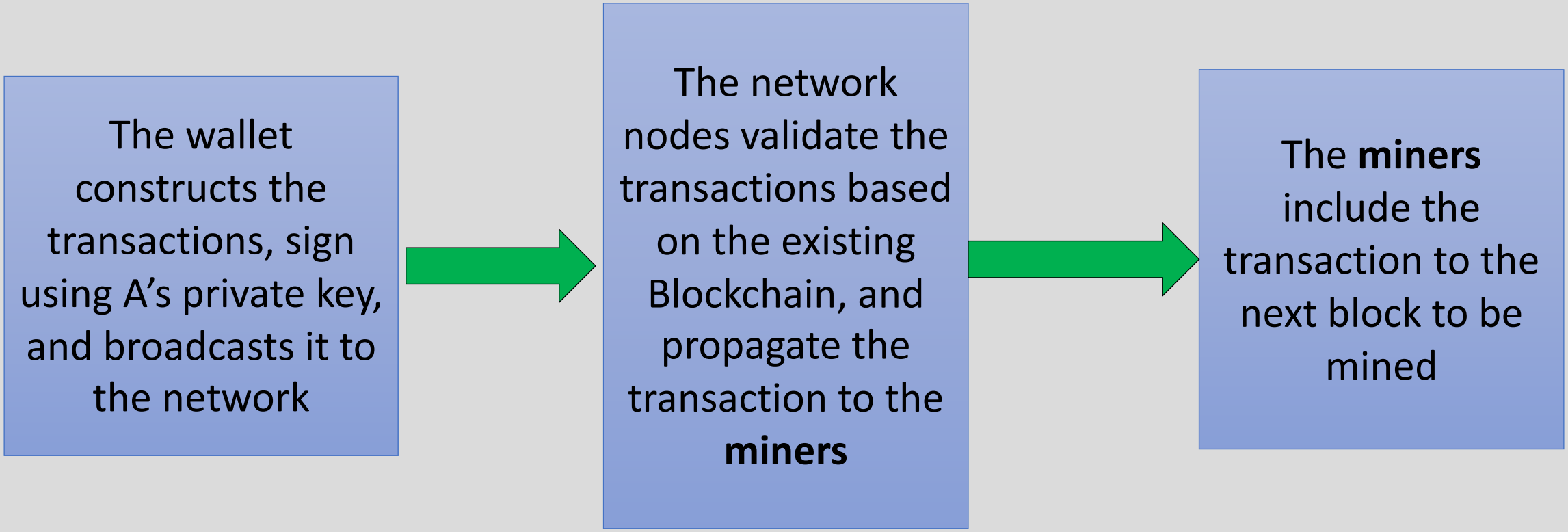
The Bitcoin Transaction Life Cycle – The Sender

"A" opens his Bitcoin Wallet

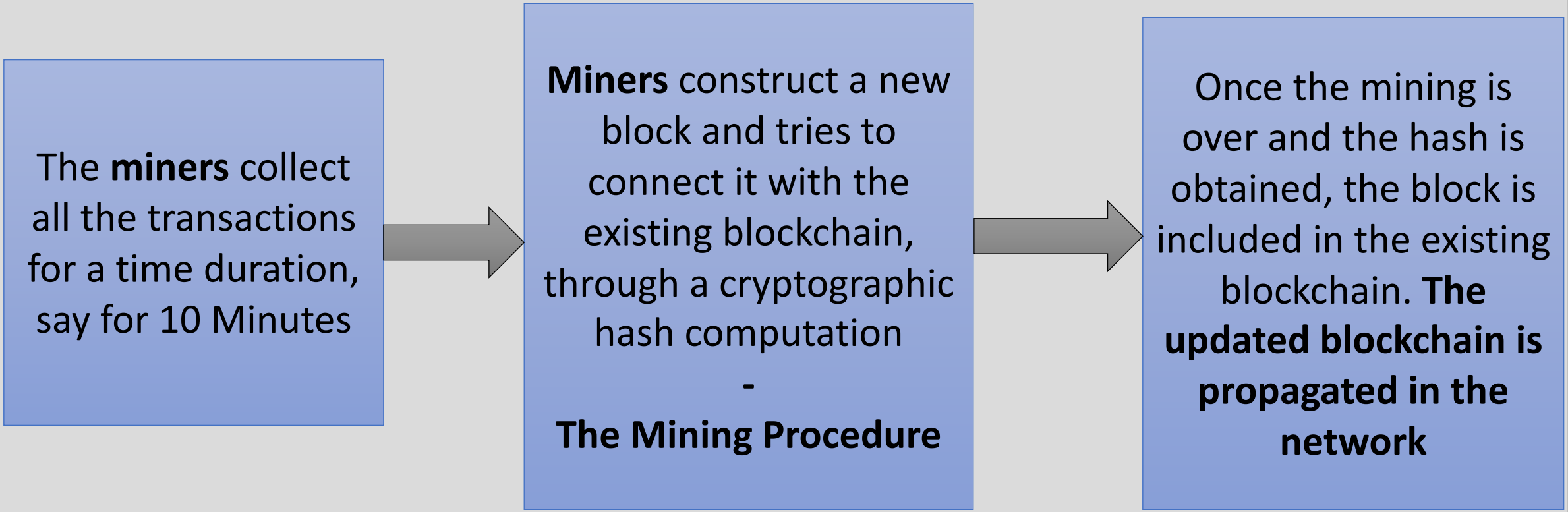
Provides the address of "B" and the amount to transfer, and sends



The Bitcoin Transaction Life Cycle – The Network



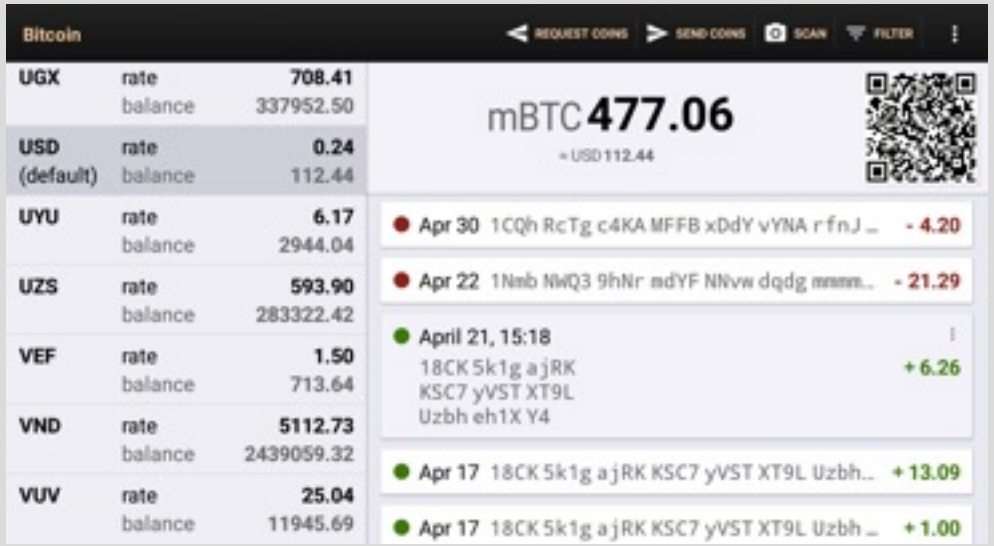
The Bitcoin Transaction Life Cycle – The Network



The Bitcoin Transaction Life Cycle – The Receiver

"B" opens his Bitcoin Wallet and refreshes, the blockchain gets updated

The transaction reflects at B's wallet



What Are Smart Contracts?

Smart Contracts

- The term was coined by Nick Szabo, a computer scientist and cryptographer, in 1996
- Nick claimed that smart contracts can be realized with the help of a public ledger
- Blockchain can be a pioneering technology to realize smart contracts

Smart Contract

- Similar to a contract in the physical world, but it's digital.
- Represented by tiny computer program stored inside a blockchain.
- It stores rules for negotiating the terms of an agreement.
- It automatically verifies fulfilment and then executes the agreed terms.

Smart Contract Example

https://rubygarage.org/blog/guide-to-smart-contracts

Why Trust a Smart Contract?

They’re immutable (Unable to change)

They’re distributed

Smart Contract Benefits for Business

Direct dealing with customers

Resistance to failure

Immutability

Fraud reduction

Cost efficiency

Records keeping

https://rubygarage.org/blog/guide-to-smart-contracts

Contracts in a Centralized Platform – Crowdfunding

World largest funding platform for creating projects

1. You have an interesting project, but do not have sufficient money to execute the project

3. Multiple supporters commit to support the project with small funds

4. The platform ensures that you get the complete money if the project is successful

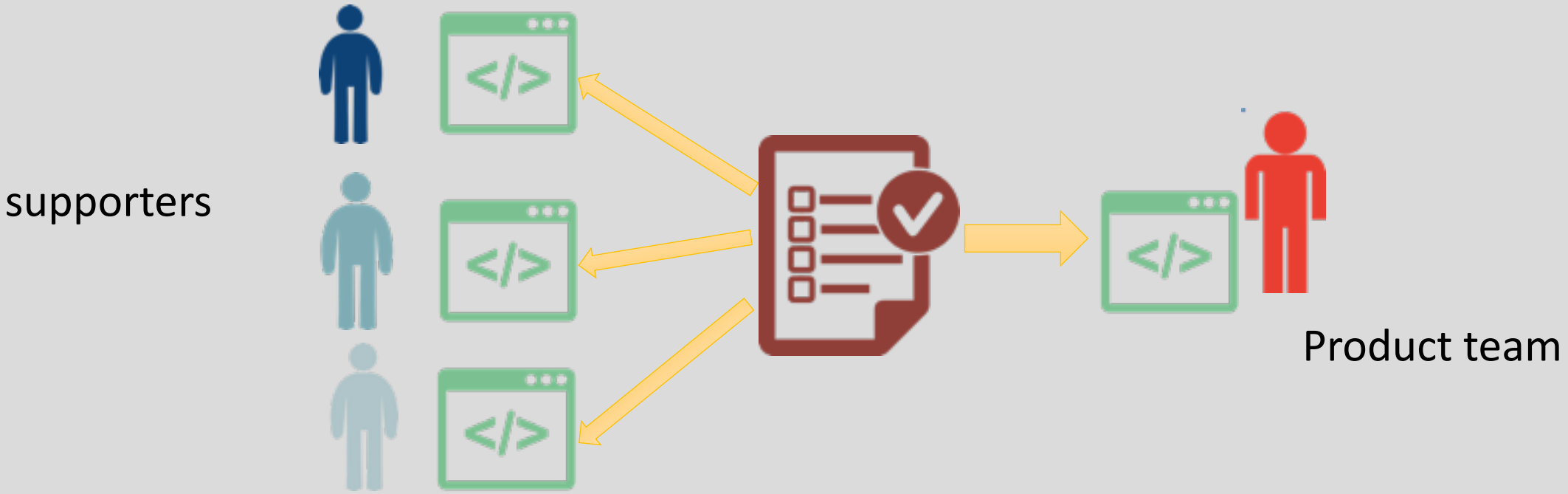
2. Submit the project in a crowdfunding platform

The Crowdfunding Platform

- Both the product team and the supporters need to **trust** the crowdfunding platform
- The product team expects the money to be get paid based on the project progress
- The supporters expect the money to go to the project
- However, the crowdfunding platform, **the middleman, takes significant charge to manage the entire process**

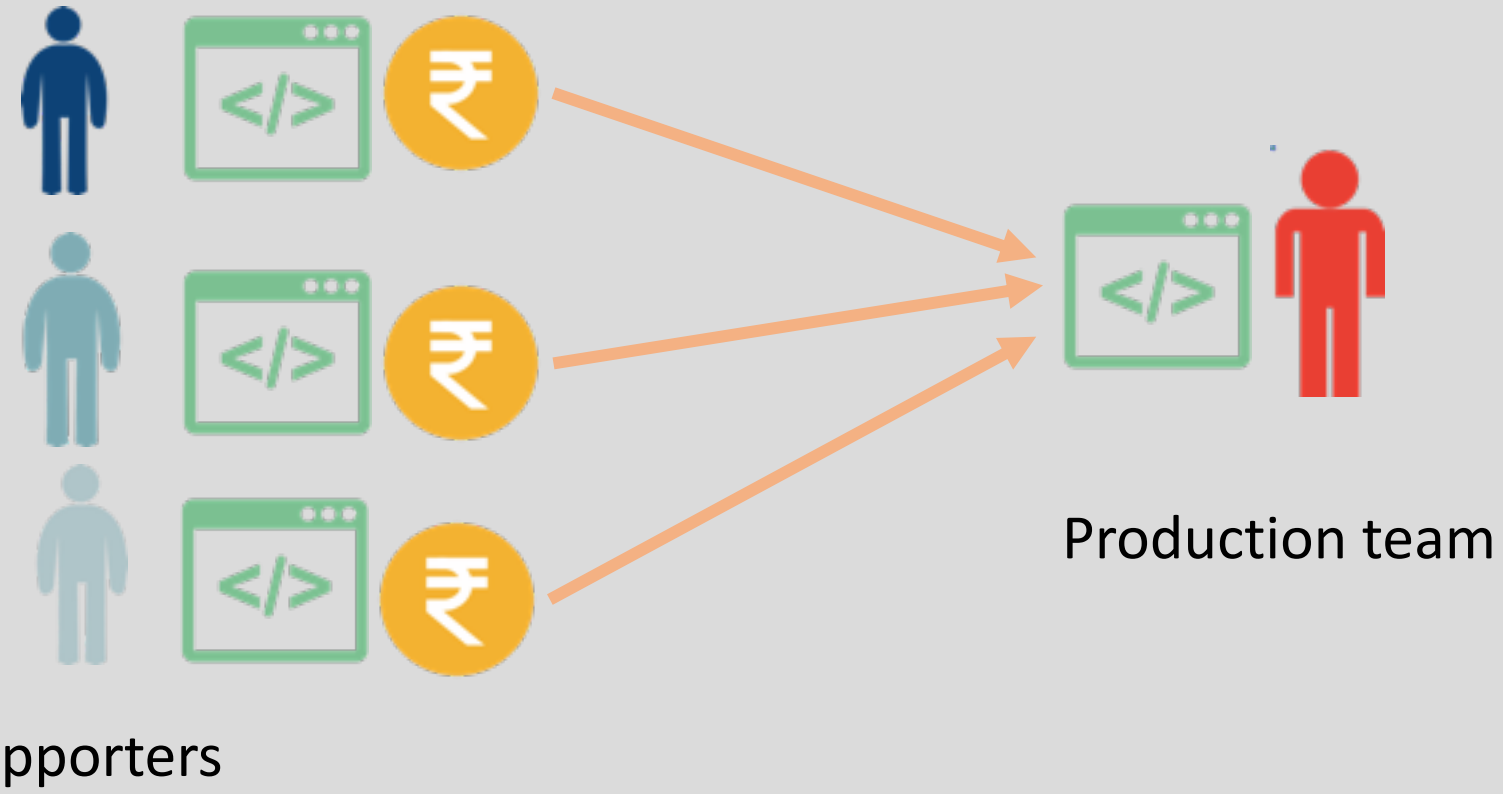
Solution: Crowdfunding Platform using Smart Contracts

- The contract is written in a **code** which is available to all the stakeholders – the supporters and the product team – **Do you see an application of Blockchain here?**

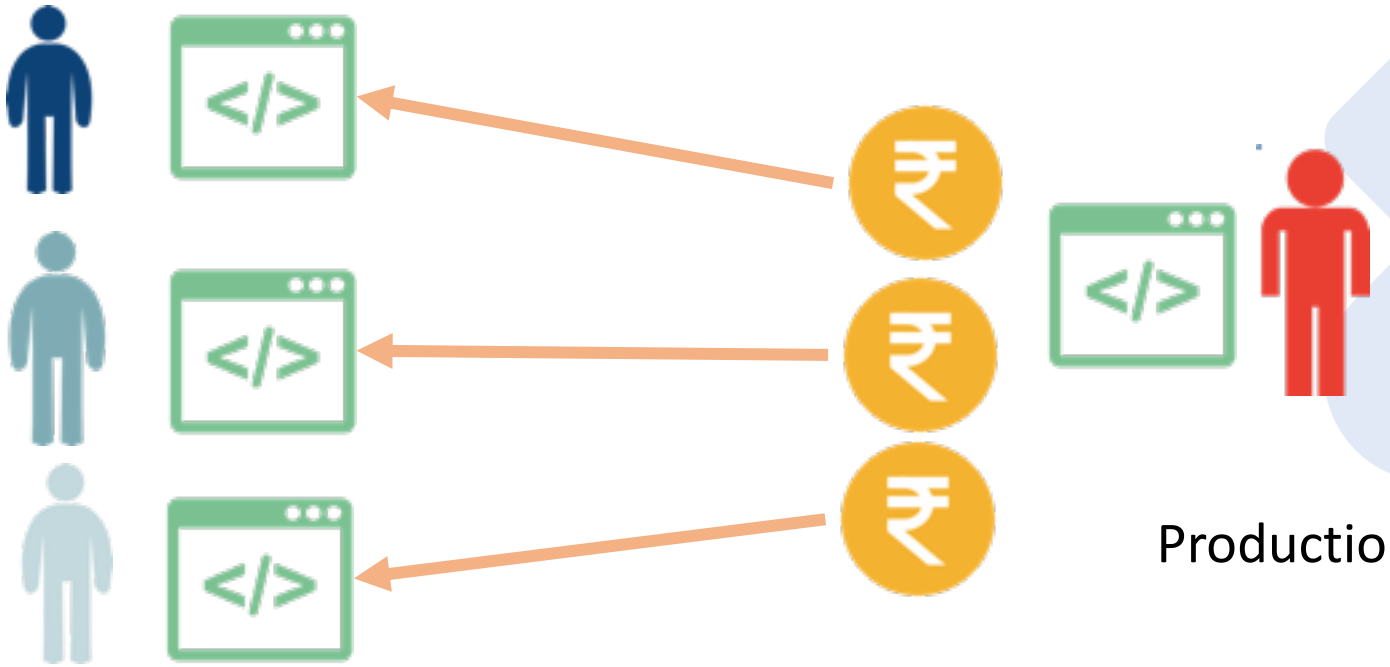


Crowdfunding Platform using Smart Contracts

If certain goals of the project are reached, then the code automatically transfers the money from supporters to the production team



Crowdfunding Platform using Smart Contracts



supporters

Production team

If the project goals (contracts) fail, then the code can transfer the money back to the supporters

Smart Contracts –Advantages

- **Immutable**: No party will be able to change the contract once it is fixed and written to the public ledger (the Blockchain)

- **Distributed:** All the steps of the contract can be validated by every participating party – no one can claim later that the contract was not validated

- **Why Blockchain?**
  - The blocks are immutable
  - The information is open – everyone can check and validate

Smart Contract Platforms

Smart Contract Platforms

	Execution Environment	Language	Turing Completeness	Consensus Mechanism	Permission Type	Cryptocurrency	Cryptocurrency market value	Applications
Etherium	EVM	Solidity	Turing complete	Proof-Of-Work	Public	Ether	US$141.71	Decentralized exchanges, gambling
RSK	RVM (Rootstock Virtual Machine)	Solidity	Turing complete	merge-mining/ federated	Public	SBTC	US$5862.15	Charity, Insurance
EOS	Web Assembly	C++	Turing Complete	BFT-DPOS	Public	EOS Token	USUS$2.56	Profit sharing, copyright security
TRON	Tron Virtual Machine	Solidity	Turing Complete	TRON (DPOS)	Public	Tronix	US$0.013939	Gaming application, currency
Steller	Docker	Net, Scala, C++, GO	Turing Incomplete	Steller Consensus Protocol	Consortium	Lumen	US$0.051458	Universal payment solution, oil trade
Hyperledger Fabric	Docker	Javascript, GO, java	Turing Complete	Custom protocols	Private	None	-	Smart Energy management, supply chain
Nem	JVM	NEM, Java	Turing Incomplete	Proof-Of-Importance (POI)	private/ public	XEM	US$0.035290	Cryptocurrency, liquid assets
Cardano	K-EVM and IELEVM	Plutus, Rust, C, Javascript	Turing-complete	Ouroboros (POS)	Public	Cardano - SL	US$0.036161	Decentralized, security, gambling
Corda	JVM	Java, Kotlin	Turing Incomplete	Raft	Private	Real-World currencies	-	Construction, Healthcare

Summary

Two models of Blockchain network – **Permission-less** (an open environment) and **Permissioned** (a close environment)

Permission-less model is suitable for open control-free financial applications like cryptocurrency

Permissioned model is suitable for business applications like smart contract

Smart Contract for Retail Marketing: A Use Case

Case Study

- Ice-cream Retailing Store (ICRS) is a BC-based store with its own rules and agreements for selling out the various Ice-cream products.
- It has a variety of Ice-creams in its menu with different serving sizes (*small, regular and large*) and additional toppings (*Choco chips, mango slices, pineapple slices, and nuts*).
- In this scenario, we considered both customers and ICRS are on the BC network.
- Customers can order Ice-cream only if he is ordering within the range of 5000m.
- Then, he can make the payment using available options (cash, UPI, credit/debit card, and Internet ng) while placing the order.
- Customer can also add some additional toppings to his order by paying extra for it.
- An ICRS is known for its service, as it claims < 30 mins order delivery, otherwise full amount to be refunded along with the order.

Topping	Price (s)	Topping	Price (s)
Choco Chips	45/-	Mango Slices	35/-
Pineapple Slices	40/-	Nuts	55/-

Item (s)	Small Price (s)	Regular Price (s)	Large Price (s)
Chocolate Icecream	170/-	200/-	230/-
Mango Icecream	120/-	150/-	180/-
Vanilla Icecream	100/-	120/-	140/-
Strawberry Icecream	150/-	180/-	210/-

Parlor on Blockchain Network

ORDER

PAYMENT

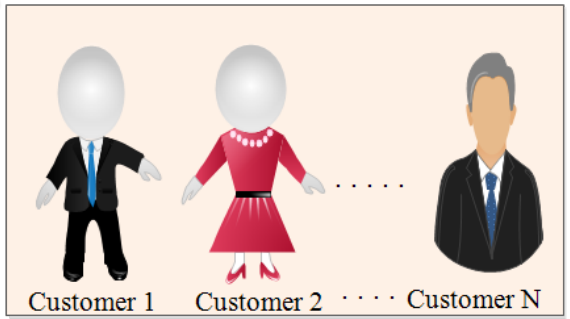
Order Received

Payment Receipt Generated

Order by Customer

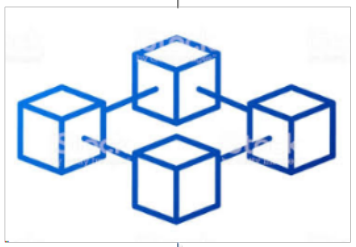
Payment Receipt Received

Customers Making Orders



Customers on Blockchain Network

Smart Contract (SC) [Rules + Agreement]



Artificial Intelligence

SC Acknowledgement

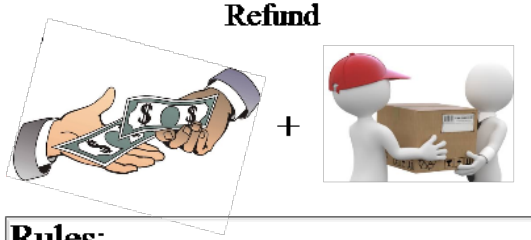
Check Status?

Successful

Unsuccessful

Delivered

Refund



Order: One large chocolate flavoured *Icecream* with extra choco chips for ₹75.

Payment: Cash, Debit/Credit Card, Online, UPI

Agreement:

A1: Ice Cream parlour agree to fulfill the order, once order is received with payment.

A2: Ice Cream parlour and Customer get the acknowledgement on the successfull execution of Subtract(D,T) rules.

A3: In case, the RS = 0 (Unsuccessful), Customer get the Refund.

Rules:

1. Order must be selected from the Menu only.
2. Order should be confirmed only after the payment by the Customer.
3. Customer should reside in the proximity of the Icecream parlor (<5000m)
4. Serving size and extra Toppings must be choosen from given options on payment basis.
5. If (Waiting_Time < 30 mins) then "*Icecream will be delivered to the Customer*" Else "*Refund initiated against the order*"

A sample Smart Contract Algorithm

Acronym	Description
O_t	Customer Order Placing Time in ICRS
O_d	Order Delivery Time by ICRS
R_{menu}	Icecream Parlor Menu Card
R_{id}	Retailer ID on BC Network
C_{id}	Customer ID on BC Network
C_w	Customer Order Waiting Time
C_d	Customer distance from ICRS
P_m	Payment Mode
P_c	Cash Payment
P_{debit}	Payment through Debit Card
P_{credit}	Payment through Credit Card
P_{online}	Payment through Internet banking
P_{upi}	Payment through UPI
R_s	Return Status
T_x	BC Transaction x Data
$C_{balance}$	Customer Balance Amount
O_{id}	Order Identification Number
O_{amount}	Order Amount
$R_{balance}$	Retailer Balance Amount
D_L	Distributed Locations

while $(C_{id} \in BC)$ **do**
  if $C_d < 5000m$ **then**
    BC permits customer to place an order at time O_t.
    if $((O_{id} \rightarrow item) \in R_{menu})$ **then**
      Customer has selected the correct items enlisted in ICRS menu.
    else
      Order will not proceed further for confirmation.
      if $((C_{id} \rightarrow C_{balance}) > O_{amount})$ **then**
        Customer will choose appropriate payment mode (P_c, P_{debit}, P_{online}, P_{upi}).
        $C_{balance} = C_{balance} - O_{amount}$
        $R_{balance} = R_{balance} + O_{amount}$
        Order is Confirmed by the ICRS.
      else
        Insufficient customer balance (Refil Balance before placing the order).
        if $(Subtract(O_t, O_d) < 1800sec)$ **then**
          Order successfully delivered.
        else
          Order successfully delivered and also full refund will initiated against the order as a penalty.
        end if

Part-3

A Case Study to demonstrate how to secure EHR in Healthcare 4.0

Blockchain-based Electronic Healthcare Record System for Healthcare 4.0 Applications

Sudeep Tanwar, Karan Parekh and Richard Evans

***Abstract*—Modern healthcare systems are characterized as being highly complex and costly. However, this can be reduced through improved health record management, utilization of insurance agencies and blockchain technology. Blockchain was first introduced to provide distributed records of money-related exchanges that were not dependent on centralized authorities or financial institutions. Breakthroughs in blockchain technology have led to improved transactions involving medical records, insurance billing, and smart contracts, enabling permanent access to and security of data, as well as providing a distributed database of transactions. One significant advantage of using blockchain technology in the healthcare industry is that it can reform the interoperability of healthcare databases, providing increased access to patient medical records, device tracking, prescription databases, and hospital assets, including the complete life cycle of a device within the blockchain infrastructure. Access to patients' medical histories is essential to correctly prescribe medication, with blockchain being able to dramatically enhance the healthcare services framework. In this paper, several solutions for improving current limitations in healthcare systems using blockchain technology are explored, including frameworks and tools to measure the performance of such systems, e.g., Hyperledger Fabric, Composer, Docker Container, Hyperledger Caliper, and the Wireshark capture engine. Further, this paper proposes an Access Control Policy Algorithm for improving data accessibility for healthcare providers, assisting in the simulation of environments to implement the Hyperledger-based EHR sharing system that uses the concept of a chaincode. Performance metrics in blockchain networks, such as latency, throughput, Round Trip Time (RTT) etc. have also been optimized for achieving enhanced results. Compared to traditional EHR systems, which use client-server architecture, the proposed system uses blockchain for improving efficiency and security.**

***Index Terms*—Blockchain, Healthcare Systems, Security, Chaincode, Electronic Healthcare Records.**

the use of blockchain technology, transparency and communication between patients and healthcare providers is also enhanced.

This section introduces the relevant concepts related to smart technologies in the healthcare industry. We examine the development of smart technologies, and the necessary security requirements for implementation into the healthcare industry. An overview of blockchain technology is provided, including its benefits and how it can be applied to healthcare systems. Since the introduction of healthcare provision in the 1970s, the emergence of modular IT systems has been observed. This period is known as Healthcare 1.0. In this era, healthcare systems were limited and not coordinated with digital systems due to lack of resources. Similarly, bio-medical machines were not yet developed and did not integrate into networked electronic devices. During this period, paper-based prescriptions and reports were widely used in healthcare organizations which led to increased costs and time.

The Healthcare 2.0 era was observed from 1991-2005. During this period, health and information technologies were combined to create healthcare systems, as we know them today. During the Healthcare 2.0 phase, digital tracking was introduced, providing doctors with imaging systems for analyzing patients' health. At the same time, new user-enabled technologies began to emerge in the healthcare industry, surfacing alongside the introduction of social media. Healthcare providers began to create online communities for information and knowledge sharing, store information on cloud servers, and provide access to documents and patient records via mobile devices, enabling ubiquitous access for both the provider and patient. During this period,

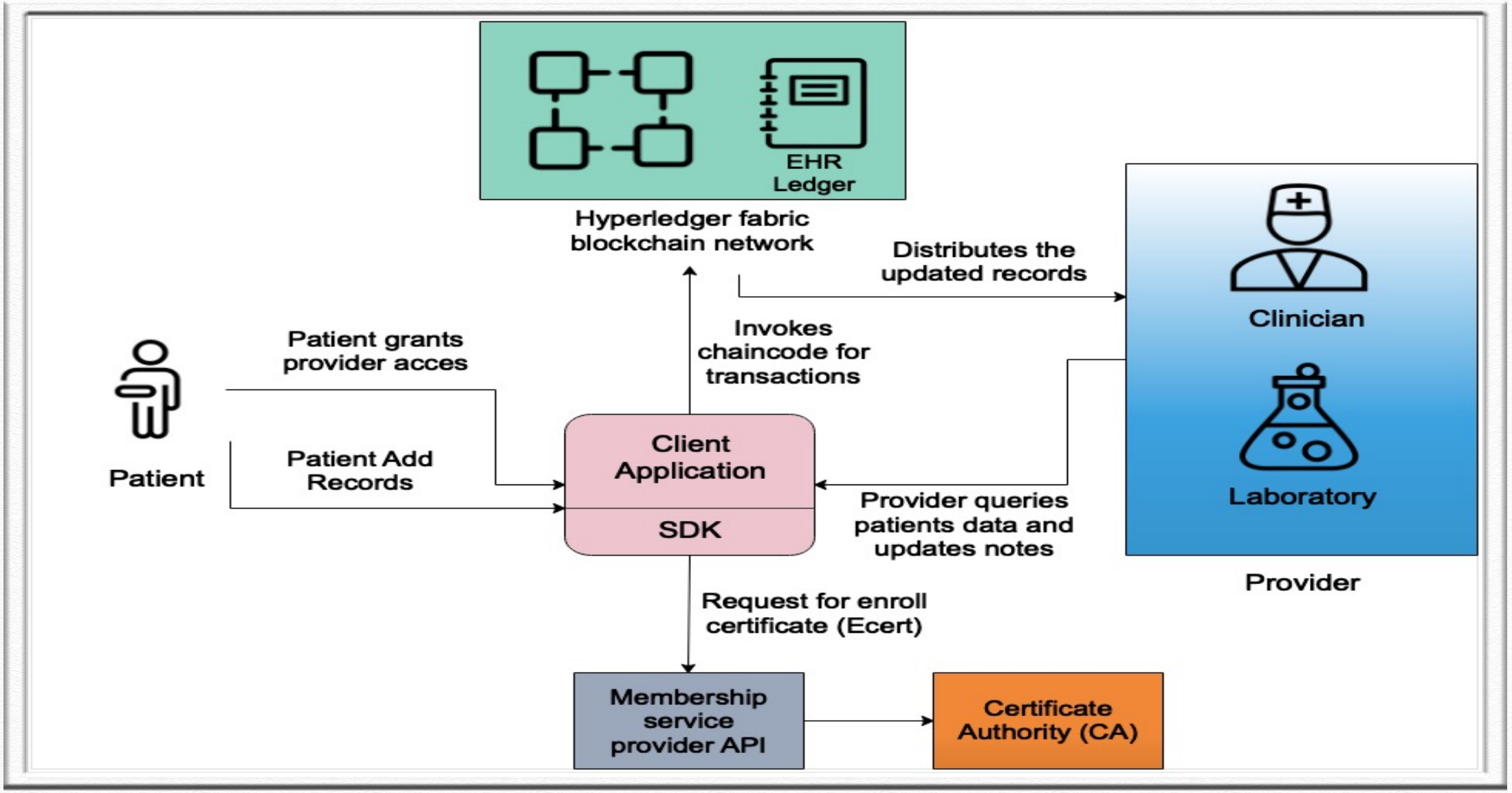
Objective

To develop EHR management system

that enables the user to give healthcare professionals access to their personal health related data

in auditable, transparent and secure way on system using distributed ledger.

System Architecture



System Evaluation

Simulation Settings :

Hyperledger Fabric - Permissioned, Consortium-managed blockchain

Hyperledger Composer - Smart contract by using fabric network

Docker Container - Operating system level virtualization

IBM Blockchain Platform - For production of Dapp

Data structure of EHR system

Patient	
Field	**Data type**
PatientID	String

Clinician	
Field	**Data type**
ClinicianId	String

MedicalRecord (Asset)	
Field	**Data type**
RecordId	String

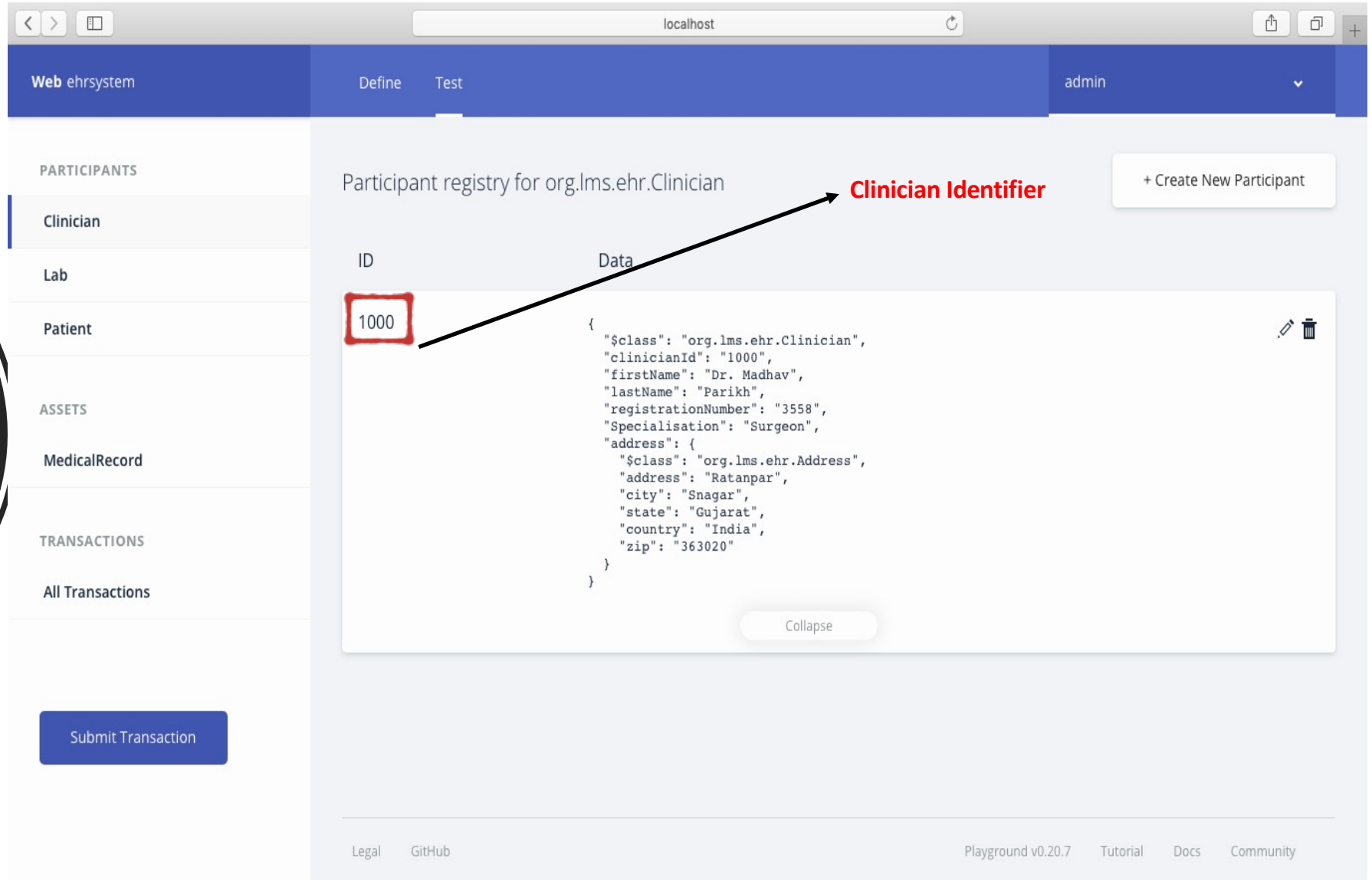
Access Control List (ACL)

Participant	Access Control
Admin	Having full access to user resources
Patients	Write EHRs, Able to search clinician/lab over the network
	String
Clinician / Lab	Read/Write on Permissioned EHRs

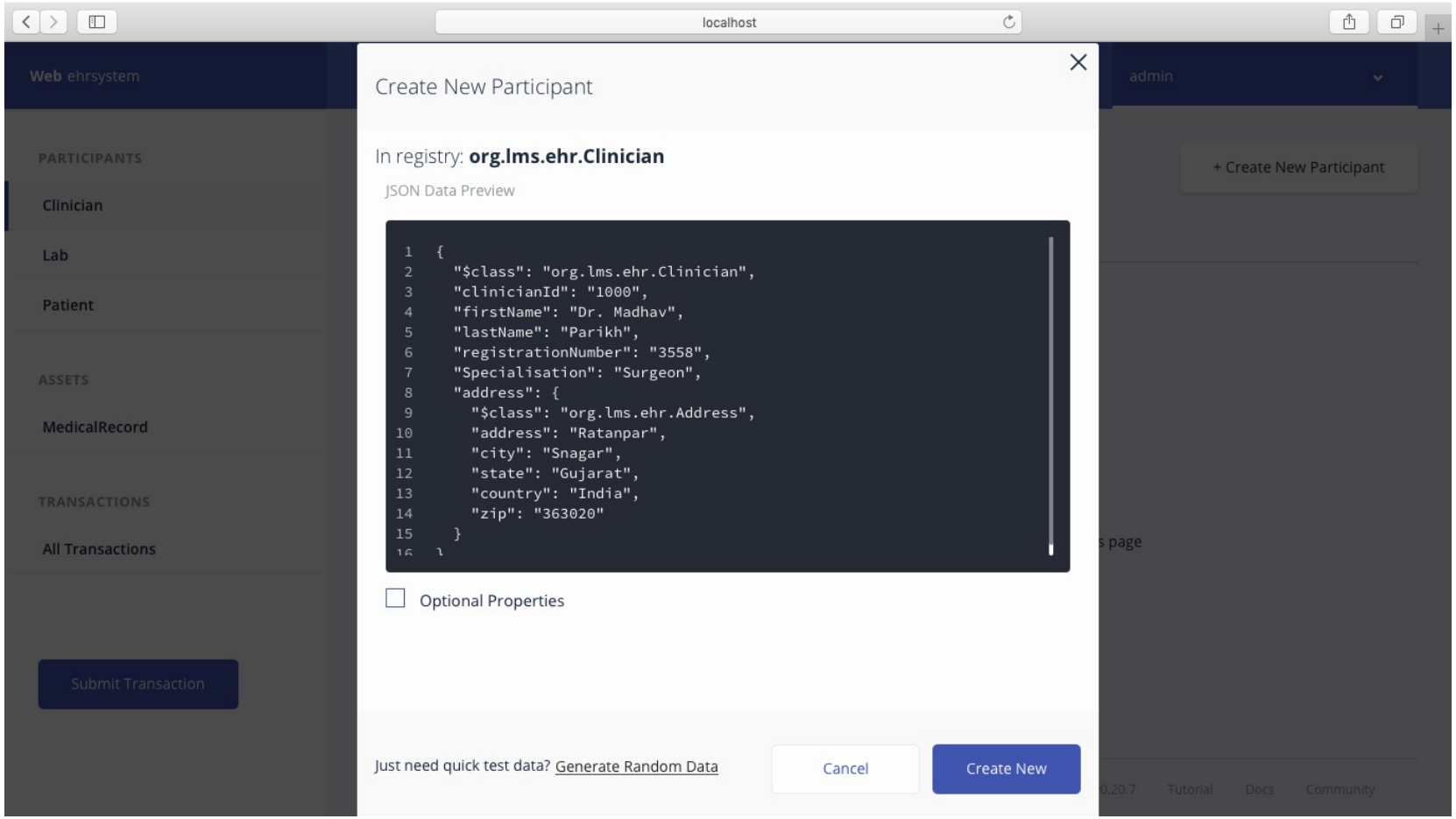
Smart contract (Logic)

- Create MedicalRecord
- GrantAccess
- GrantAccessToLab
- RevokeAccess
- RevokeAccessToLab

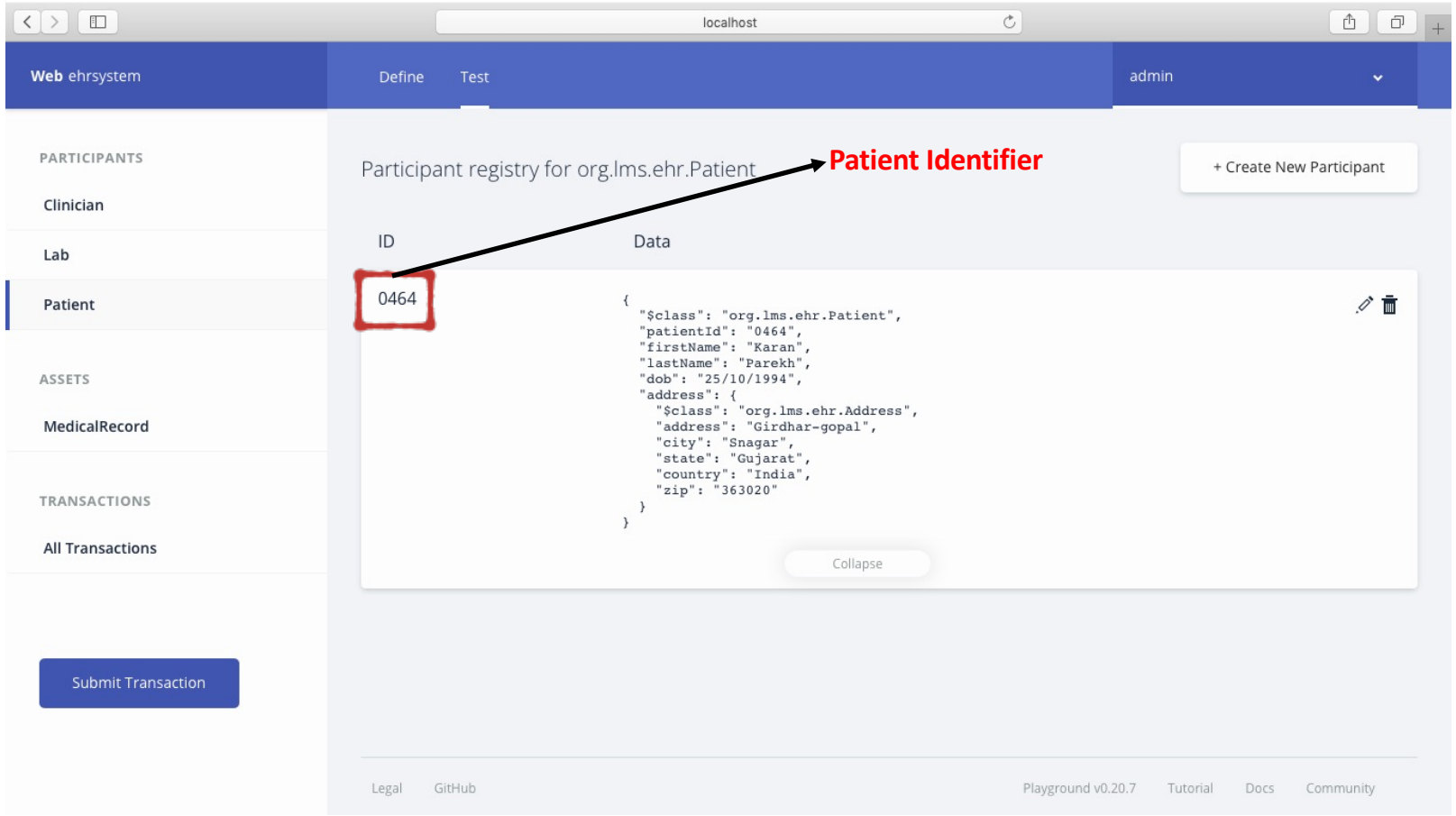
Dashboard for Clinician



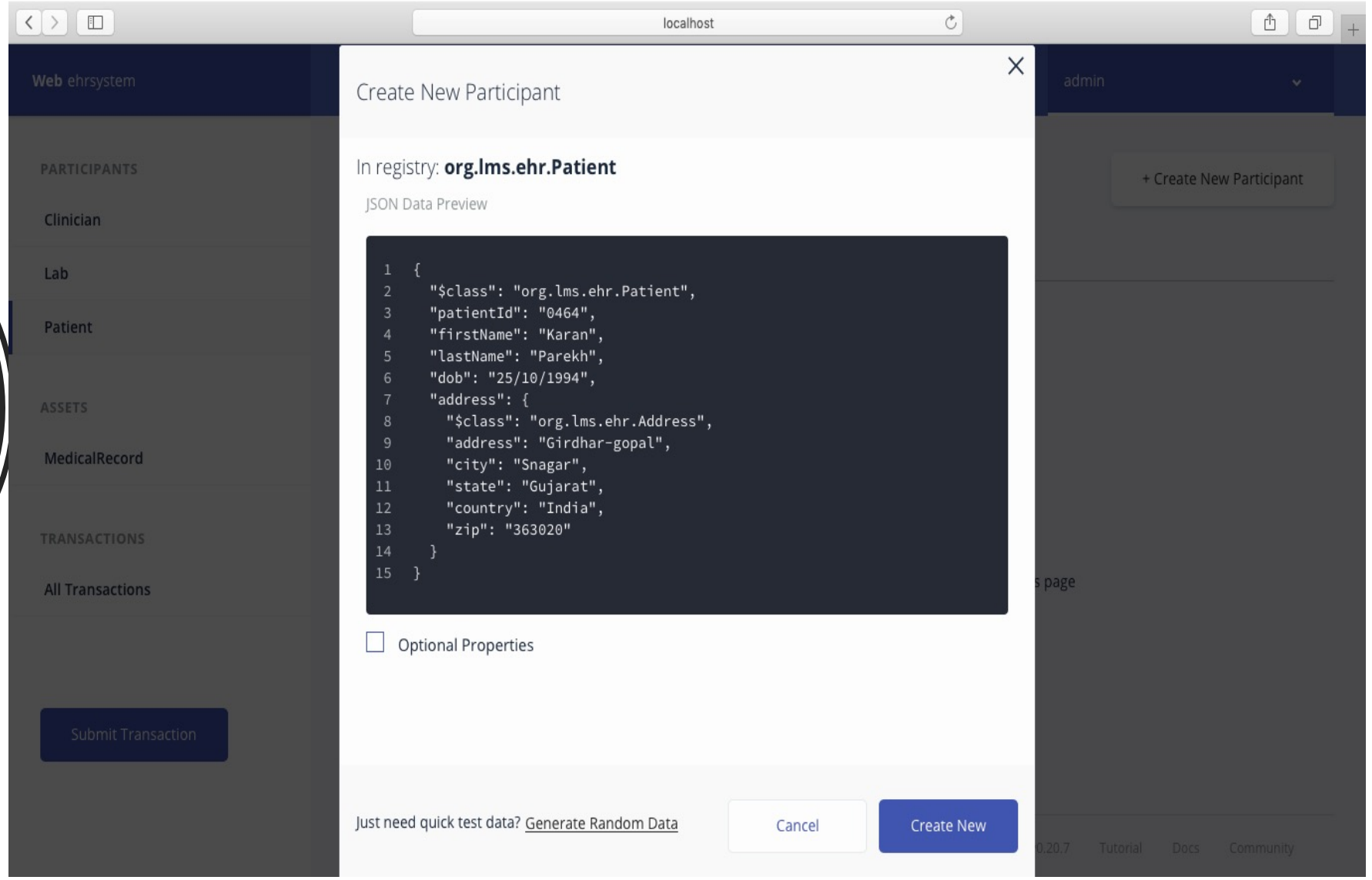
Create new clinician



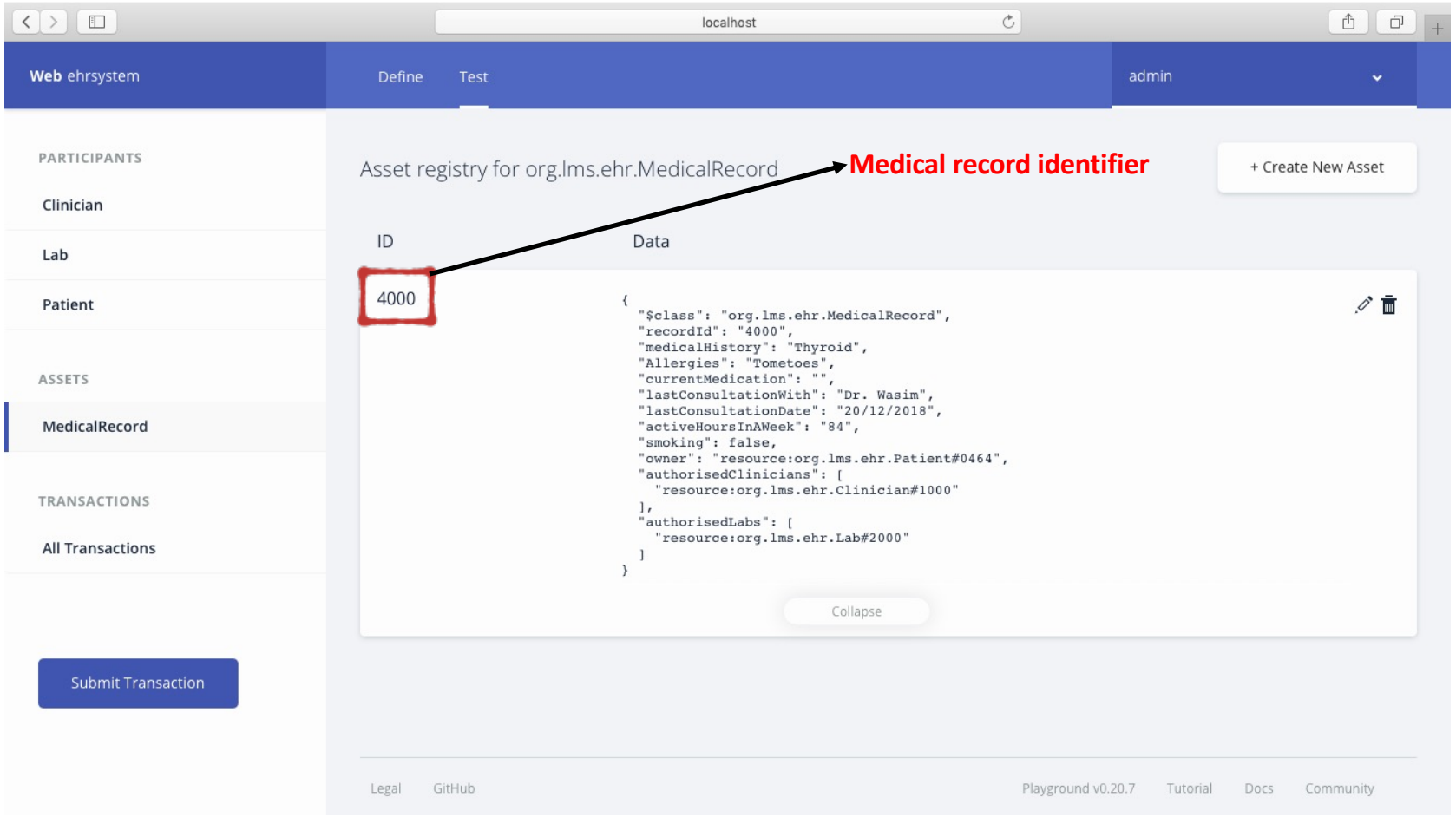
Dashboard for patient



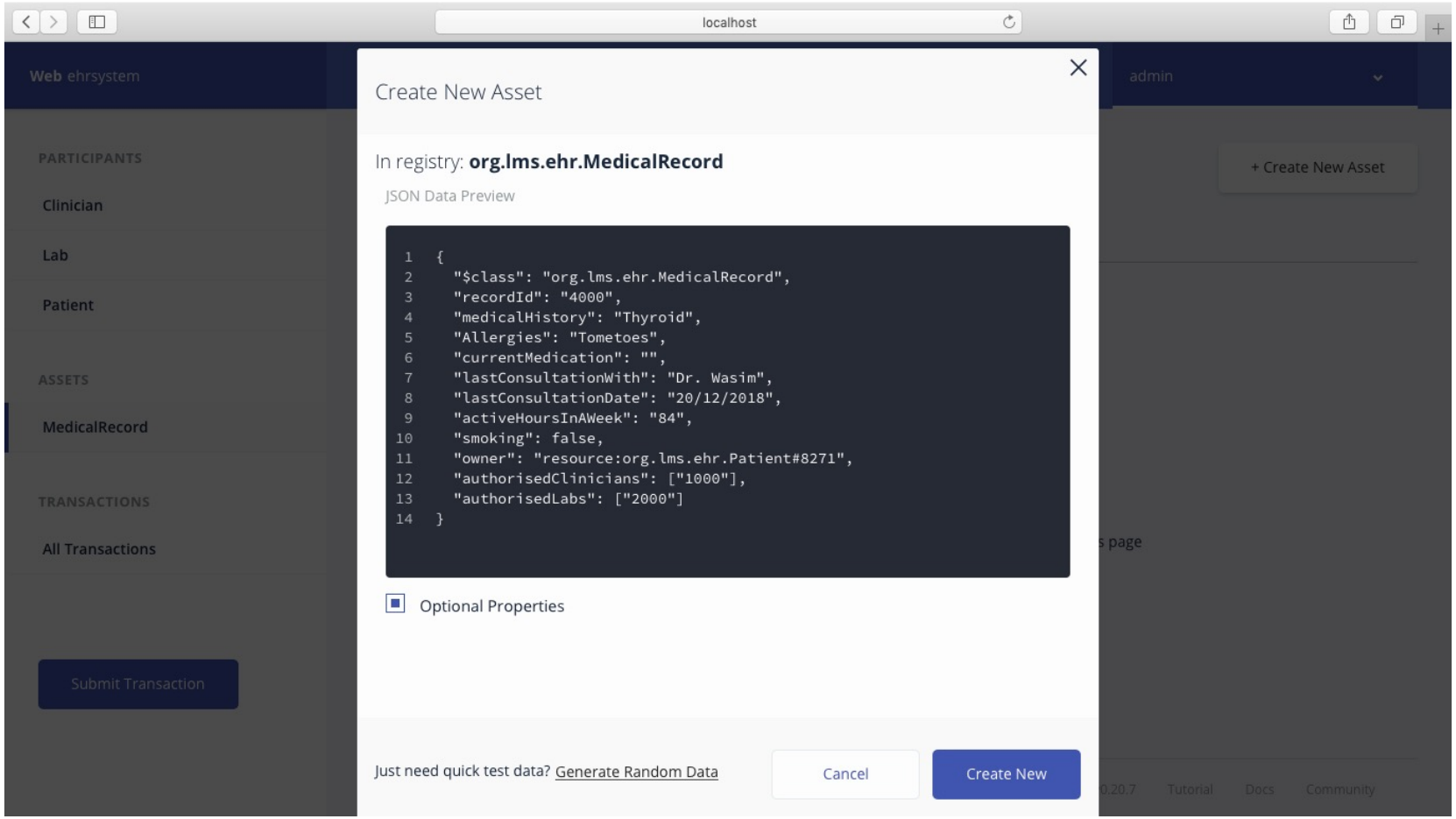
Create new patient



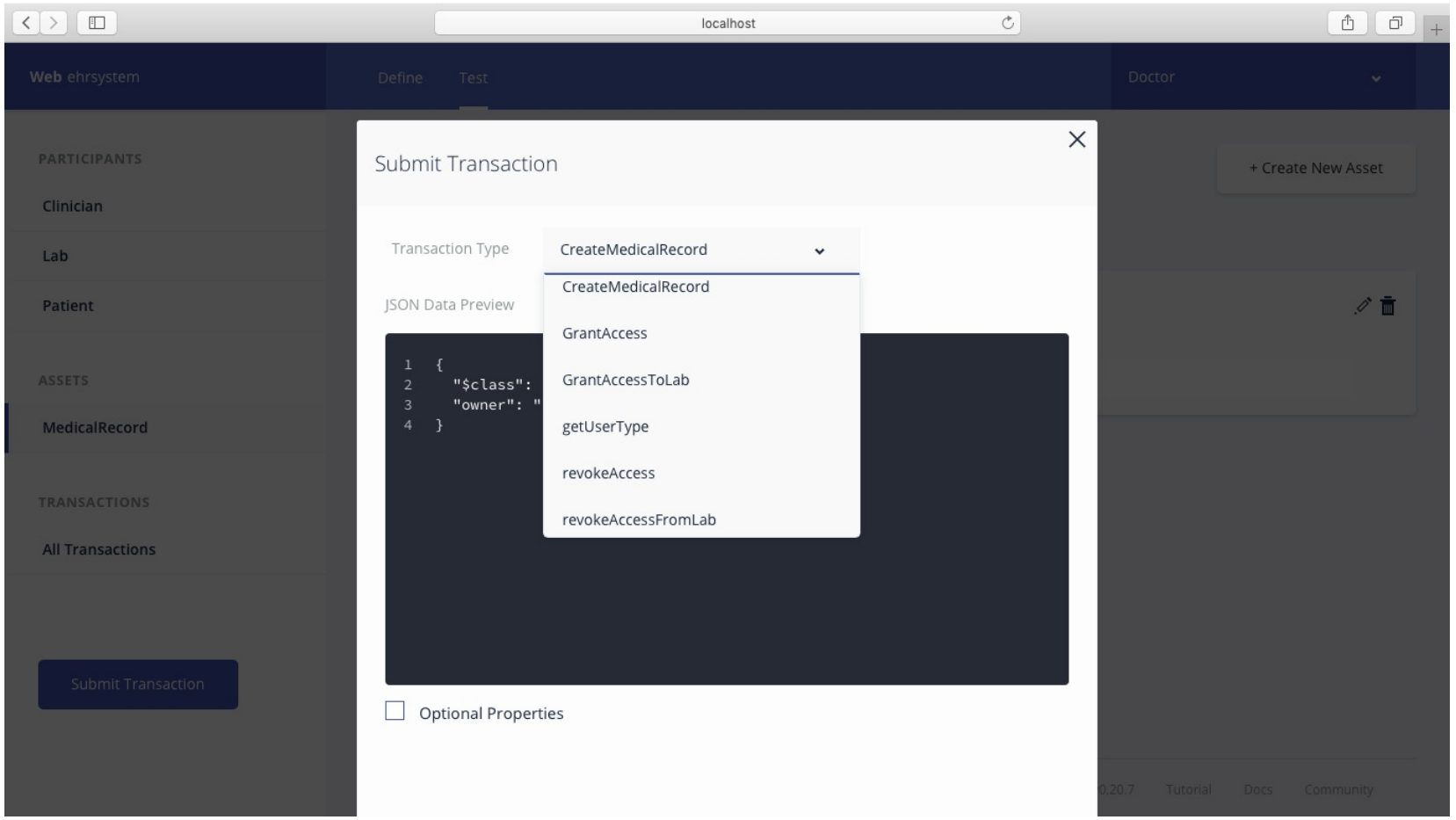
Dashboard for Medical Record



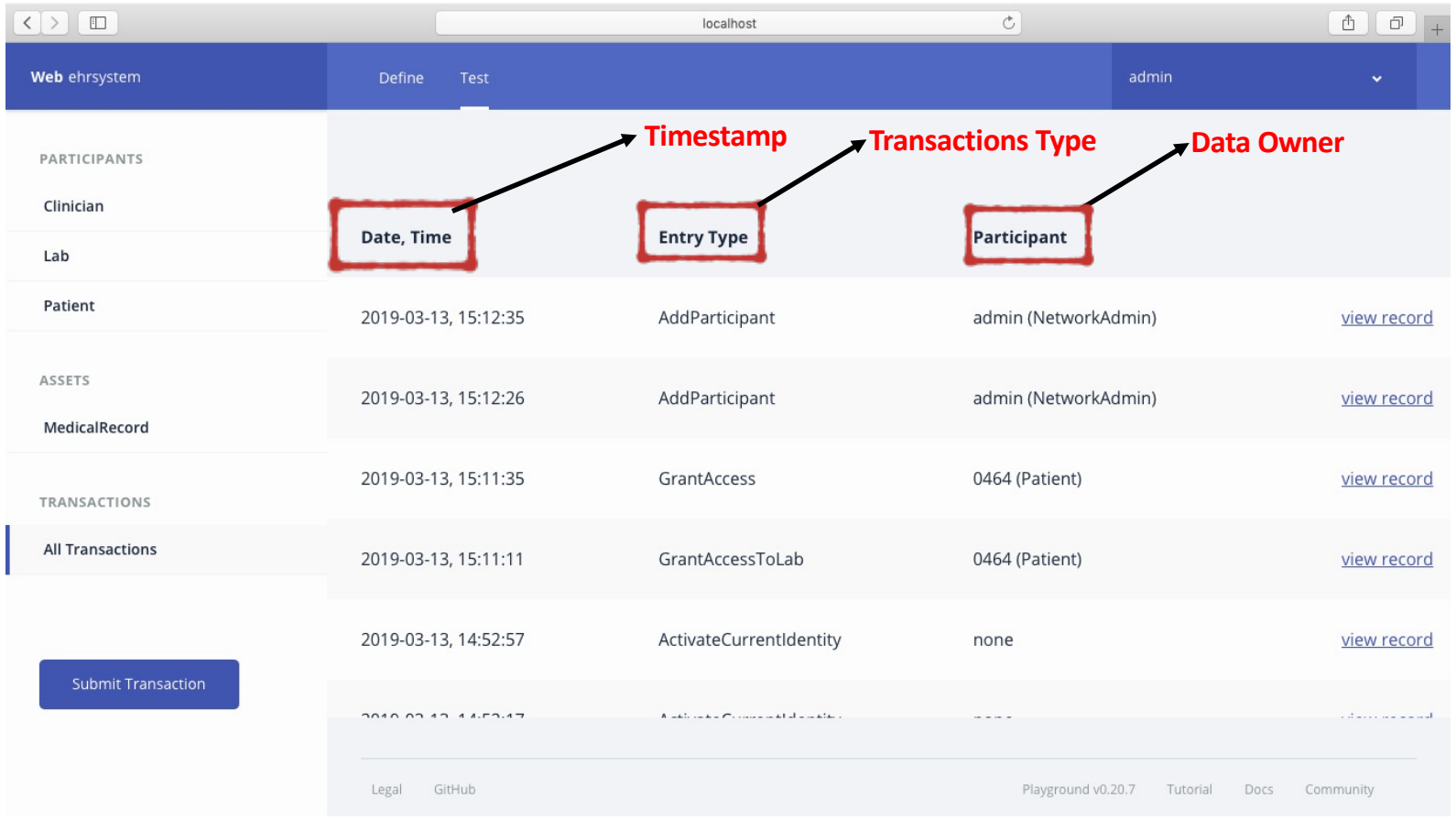
Create new medical record



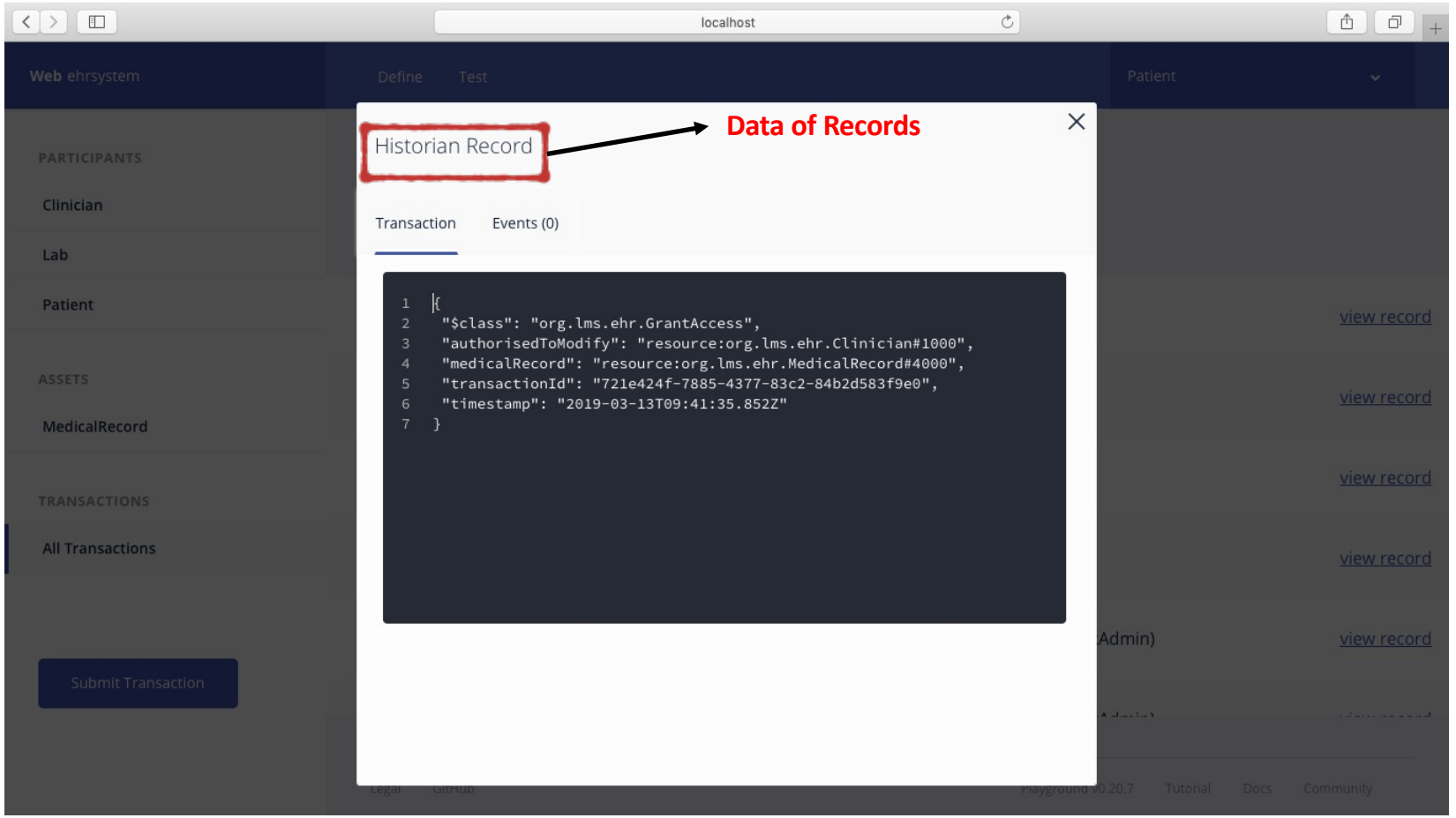
For submitting transactions



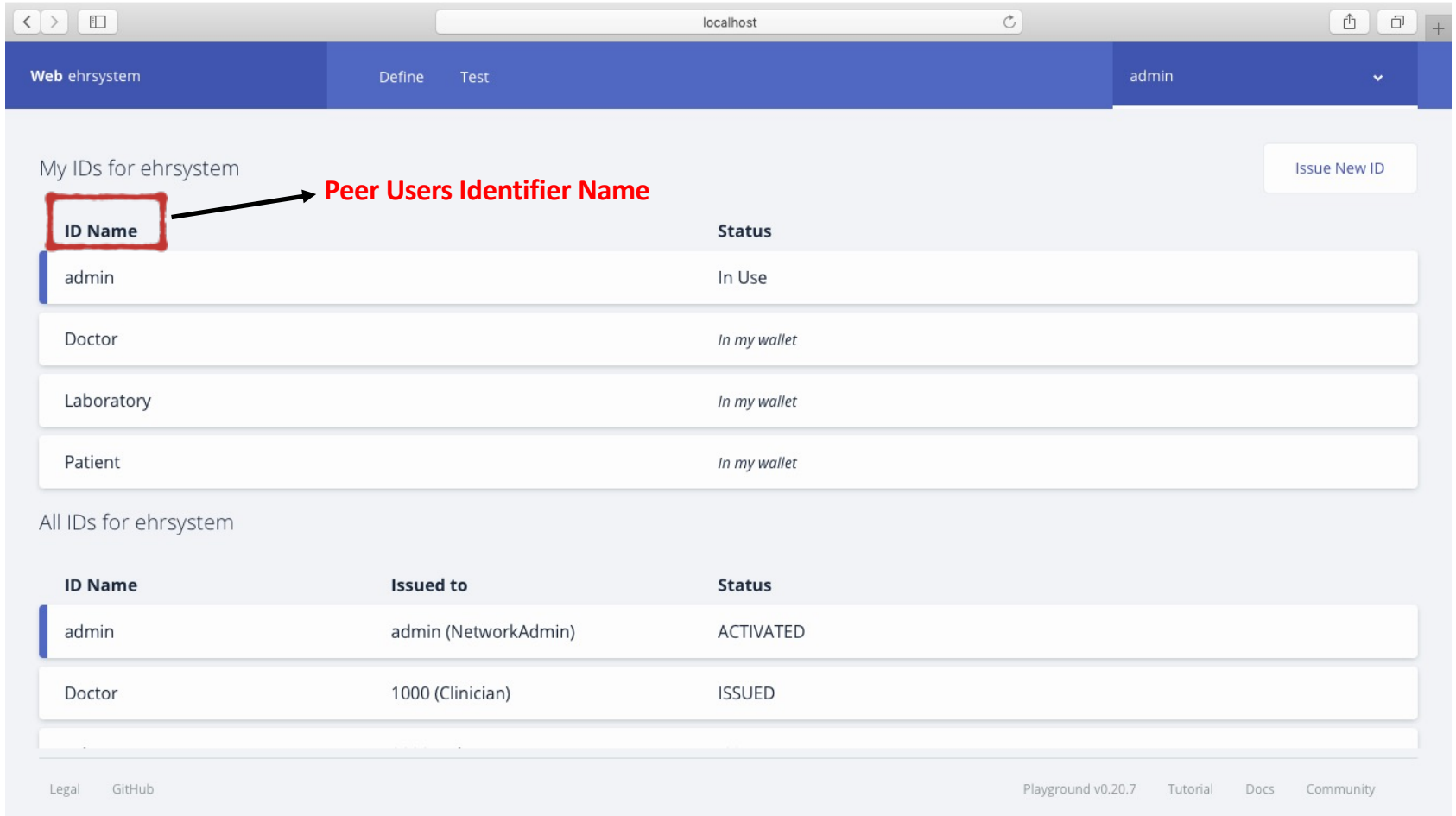
Immutable Ledger - cannot be modified or deleted



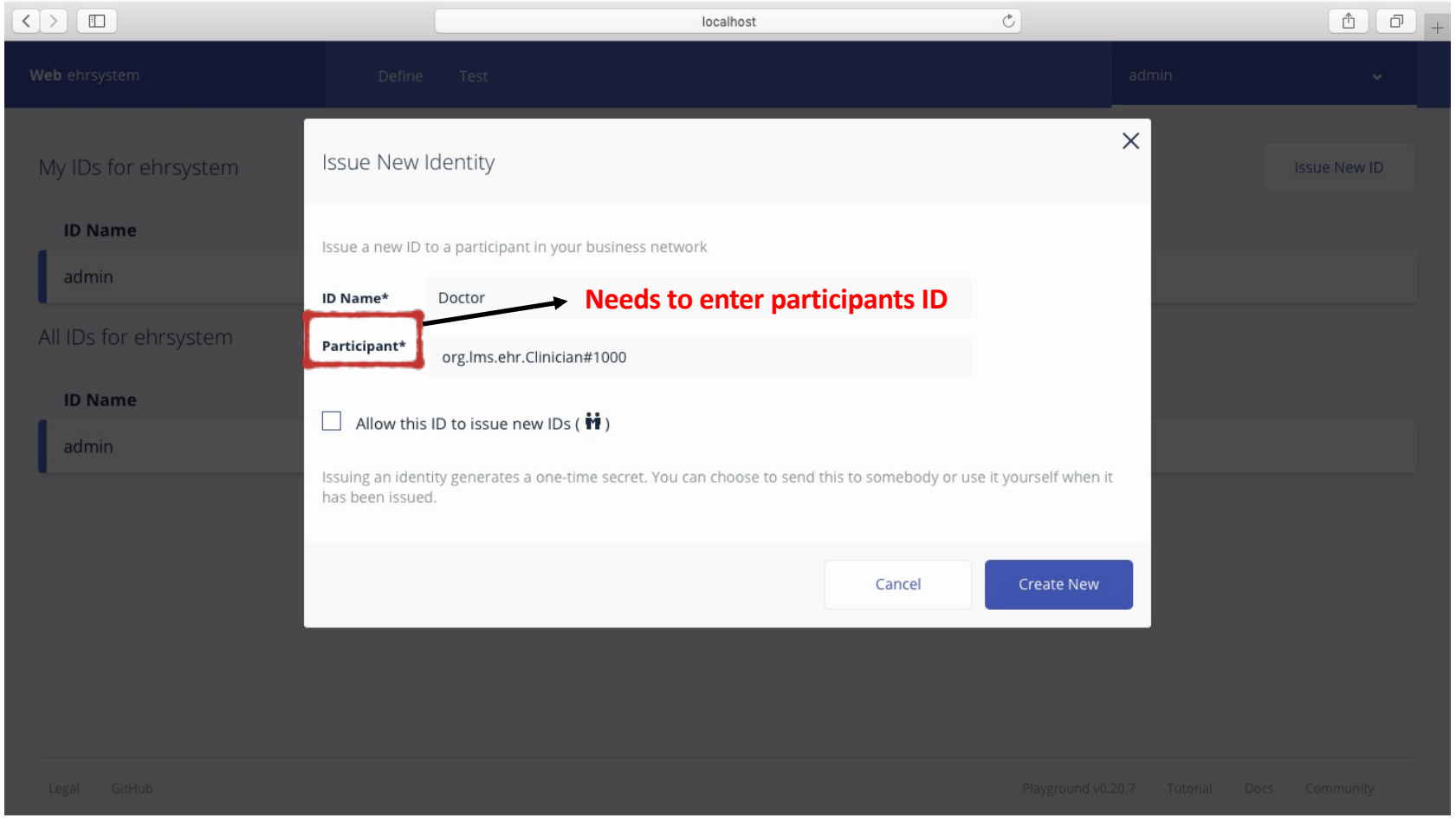
Details of records



Dashboard for Admin



Issue new ID


localhost
Web ehrsystem
Define
Test
admin
My IDs for ehrsystem
Issue New ID
ID Name
admin
All IDs for ehrsystem
ID Name
admin
Issue New Identity
Issue a new ID to a participant in your business network
ID Name*
Doctor
Needs to enter participants ID
Participant*
org.lms.ehr.Clinician#1000
Allow this ID to issue new IDs ( )
Issuing an identity generates a one-time secret. You can choose to send this to somebody or use it yourself when it has been issued.
Cancel
Create New
Legal
GitHub
Playground v0.20.7
Tutorial
Docs
Community

Blockchain in Healthcare……

Blockchain in Healthcare

Blockchain is one of the greatest inventions of this decade.

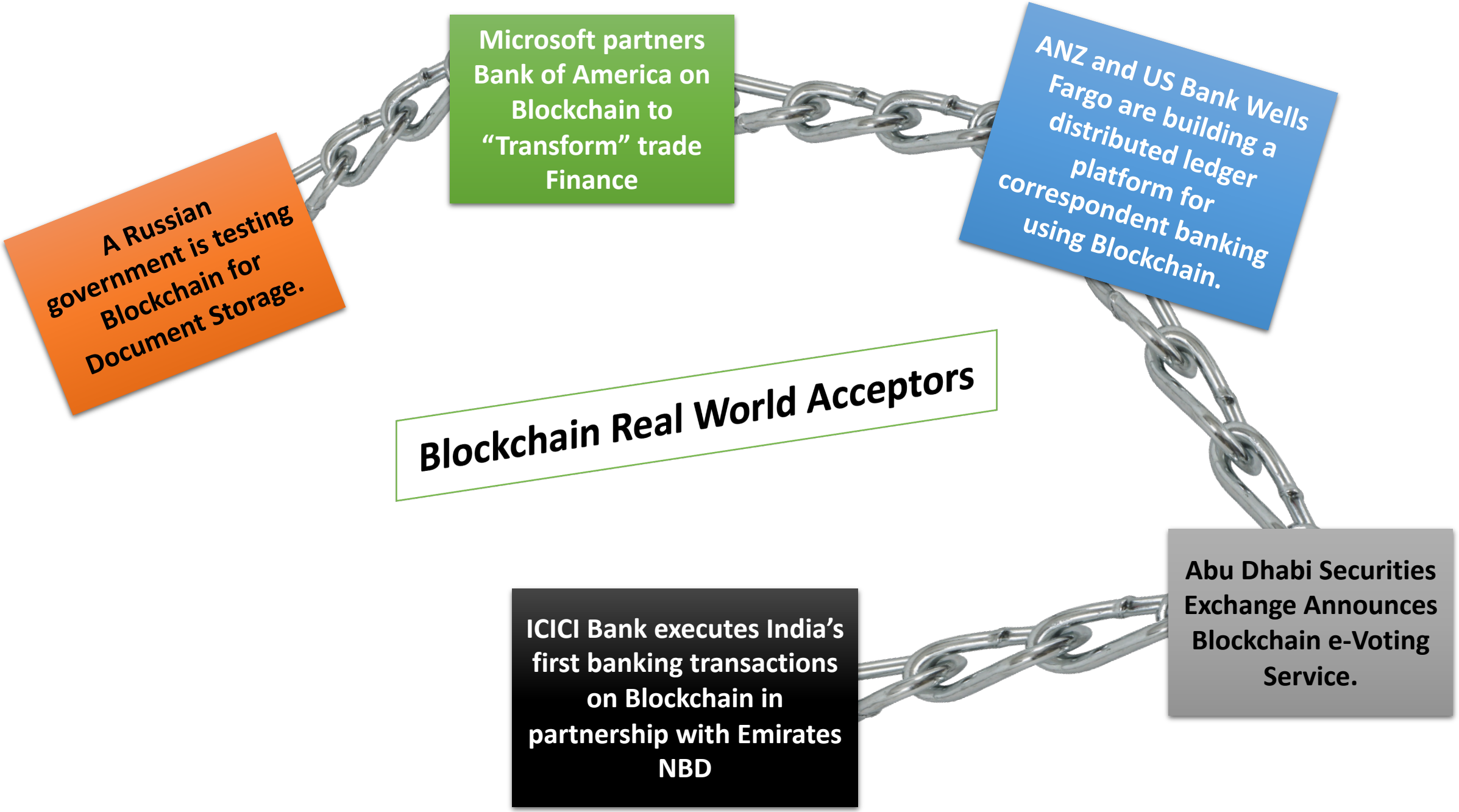
Overtaken by all the sectors including banking, industrial, healthcare etc.

Technology to solve healthcare looming solutions.

Provides security to healthcare EHR data.

Customer reaction when healthcare data breaches?

Source: https://www.accenture.com/au-en/insight-accenture-health-2017-consumer-survey


Microsoft partners Bank of America on Blockchain to "Transform" trade Finance
ANZ and US Bank Wells Fargo are building a distributed ledger platform for correspondent banking using Blockchain.
A Russian government is testing Blockchain for Document Storage.
Blockchain Real World Acceptors
Abu Dhabi Securities Exchange Announces Blockchain e-Voting Service.
ICICI Bank executes India's first banking transactions on Blockchain in partnership with Emirates NBD

HIPAA (Health Insurance Portability and Accountability Act)

COBIT (Control Objectives for Information and Related Technologies)

HITRUST (The Health Information Trust Alliance)

ISO2799 (Health informatics)

NIST CSF (Cybersecurity Framework)

DoD 8500 (Information Assurance)

NIST RMF (Risk Management Framework)

DISHA (Digital Information Security in Healthcare)

IOMT (Internet of Medical Things)

Worldwide Healthcare Security Standards

Healthcare- How does Blockchain fit?

Healthcare Industry Challenge	Blockchain Opportunities
Fragmented Data	• Decentralized storage using computer networks for patient data • Shared data across the network and nodes • Decentralized source of Internet of Things (IoT) data
Timely Access to Patient Data	• Distributed, secure access to patient health data across the distributed ledger • Shared data enables real-time updates across the networks
System Interoperability	• Decentralized Internet and computer networks across geographies • Enables authenticity (system authentication)

Healthcare Industry Challenge	Blockchain Opportunities
Data Security	• Digitizing data security of transactions – digital identity protects patient privacy
Patient Generated Data	• Data from wearable devices (IoT) aggregated to provide holistic patient care
Access and Data Inconsistency	• Smart Contracts create a consistent and rule-based method for accessing and analyzing patient data that can be permissioned to selected health organizations
Cost Effectiveness	• Reduced transaction costs and real-time processing to make the system more efficient • Elimination of third-party applications removes time lag in data access

Blockchain Answers to common Healthcare Industry Challenges

Source: "Blockchain- A healthcare Industry View by Capgemini

Challenges in Blockchain

Challenge	Blockchain Solution
-Time to access patients data **-Critical for lifesaving of critically ill patient** **-Data fetching plays an important role**	-Distributed and secure access to patients EHR across the distributed ledger -Real-time updates on shared data across the network
-Interoperability **(Exchange /Make use of EHR among nodes such as Dr.,/Nurses/etc…)**	-Decentralized Internet and CN across geographies -Authentication system-which enables authenticity
-Data Security **EHR of patients**	-Digital Identity of patients protects them against privacy
-Patient generated data **(How, where, control)**	Data collected from wearable IoT aggregated to provide proper patient care
-Access Mechanism, Data Inconsistency **(Who access what, when etc.)-Rights**	-Smart contract creates consistent and rule-based method to access and analysed patient-data
-Cost effectiveness	-Reduce transaction costs and real-time processing to make system efficient -Elimination of third-party applications -Remove timeline in data access
-Scalability	-By storing small records and hashes on Blockchain

Part-4

A Case study on Cheque clearance system through blockchain

Future Generation Computer Systems 102 (2020) 574–587

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions

Naman Kabra [a], Pronaya Bhattacharya [a], Sudeep Tanwar [a,*], Sudhanshu Tyagi [b]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[b] Department of ECE, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India

ARTICLE INFO

Article history:
Received 30 April 2019
Received in revised form 12 August 2019
Accepted 31 August 2019
Available online 9 September 2019

Keywords:
Blockchain
QR code
Two-factor authentication
Cheque clearance
Hyperledger fabric

ABSTRACT

Currently, the burden on the cheque clearing houses in financial institutions is increasing day-by-day, which necessitates the upgrading of the existing cheque truncation system (CTS). It is a manual process which uses Magnetic Ink Character Recognition (MICR), where cheques have been scanned and sent to the clearing house for further processing. The limitations of existing CTS are — illegal duplication of cheque images, invisible ink usage, visibility issues in beneficiary name, and amount on the cheque. To handle the aforementioned issues of the existing CTS, blockchain has emerged as a new technology which is a distributed ledger that is timestamped and immutable. Being immutable, forgeries related to images of cheques during clearance cycles are not allowed. This provides trust and consensus among all participating entities in the network. Motivated by the above discussion, in this paper, we propose a framework named *MudraChain* for automated cheque clearance, where clearance operations are handled by the blockchain network, instead of existing CTS. It includes: (i) A multi-level authentication scheme to make the blockchain-based framework secure and tamper-proof among participating financial stakeholders, (ii) A quick-response (QR) code generation algorithm which performs digital signing of a cheque, and (iii) A novel two-factor authentication protocol to generate a time based one-time password (TOTP) for secure funds transfer. The obtained results are examined against state-of-the-art approaches to indicate the supremacy of the proposed framework. Thus, *MudraChain* allows a seamless flow of clearance operation via blockchain for the payer and the payee without any intermediaries. Finally, it addresses the requirements of building a secure application for cheque clearance in view of decentralized blockchain 4.0 applications.

Background

Financial institutions are shifted towards digital wallets and payments, hence ***Trade*** becomes a critical factor.

Background

Financial institutions are shifted towards digital wallets and payments, hence ***Trade*** becomes a critical factor.

Existing ***Cheque Truncation System (CTS)*** use magnetic ink character recognition (***MICR)*** to scan cheques and sent to the clearing house for further processing.

Background

Financial institutions are shifted towards digital wallets and payments, hence ***Trade*** becomes a critical factor.

Existing ***Cheque Truncation System (CTS)*** use ***MICR*** to scan cheques and sent to the clearing house for further processing.

MICR system focuses on Watermarks, UV Light and other microscopic features to scan a cheque.

Problem with traditional CTS….

Problem with traditional CTS….

- CTS has limited functionality.
- It checks only the greyscale image of cheque which reduces the visibility of MICR features.
- Features can be duplicated with photo editing software and forged cheque can be created.
- Leads to wrong payment by the bank to the malicious user.

Problem with traditional CTS….

Problem with traditional CTS….

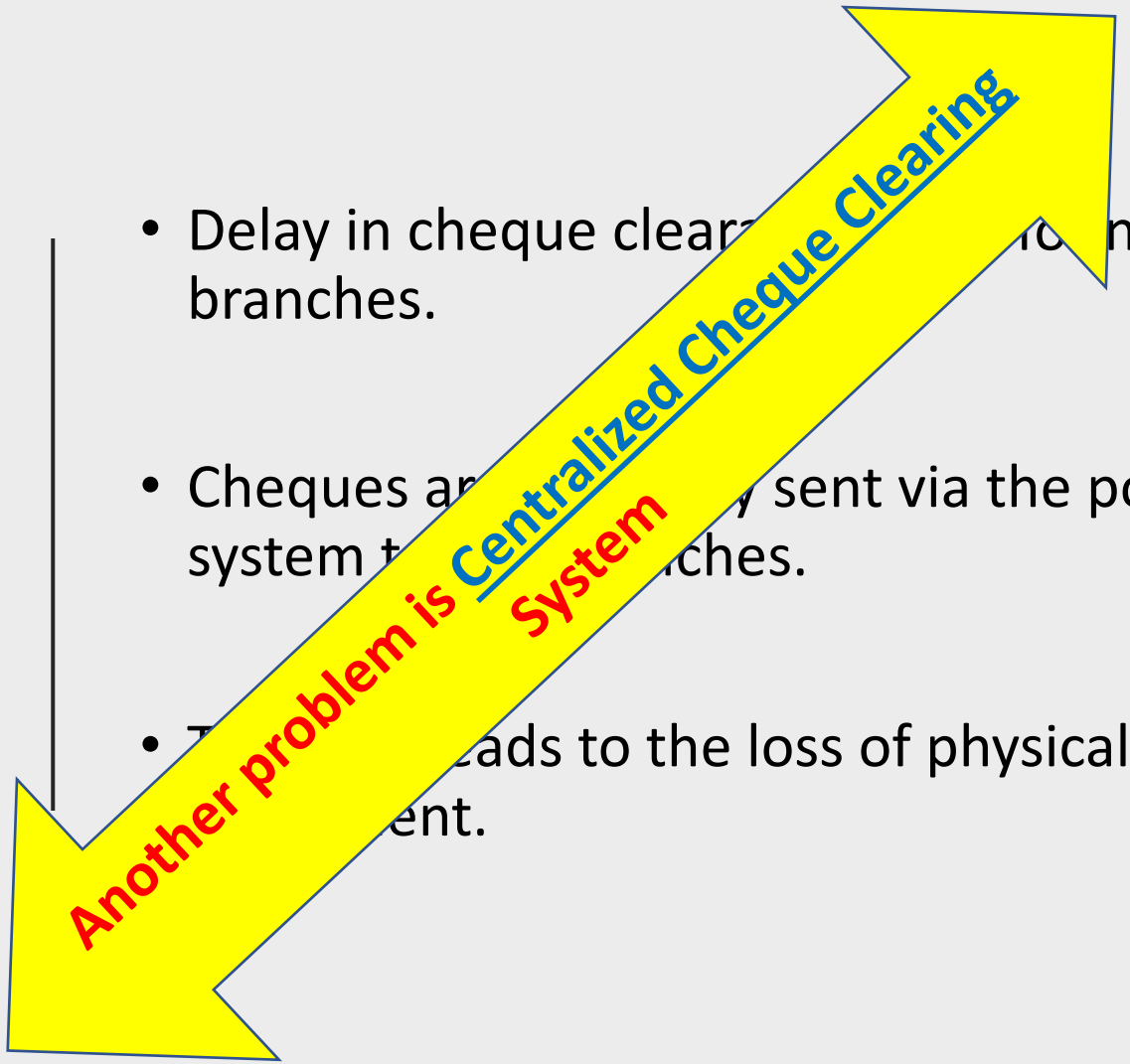
- Possible security frauds with traditional CTS

  ✓*Duplication of cheque images*
  ✓*Invisible ink usage*
  ✓*Visibility issues in beneficiary name*
  ✓*Visibility issues with amount on the cheque*

Problem with traditional CTS….

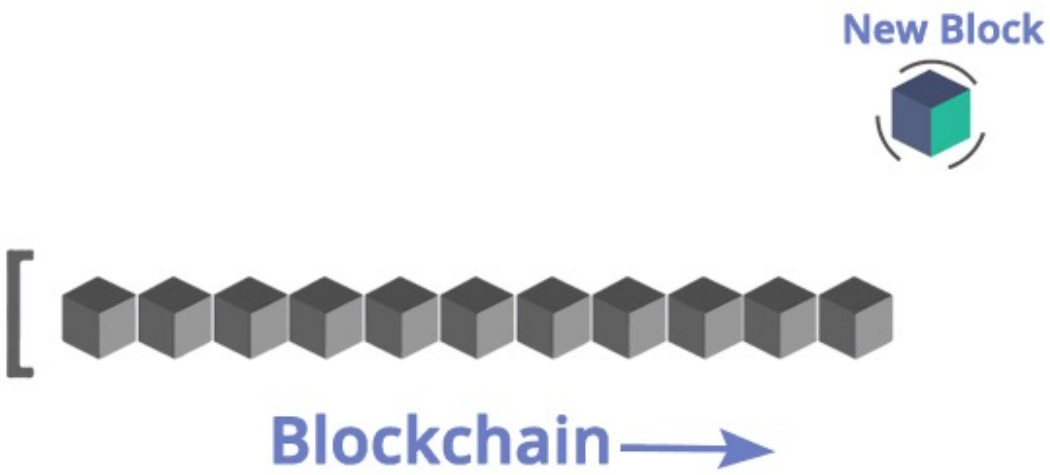
Problem with traditional CTS….

- Delay in cheque clear… …non-CTS branches.
- Cheques ar… …y sent via the postal system t… …ches.
- T… …eads to the loss of physical …ent.

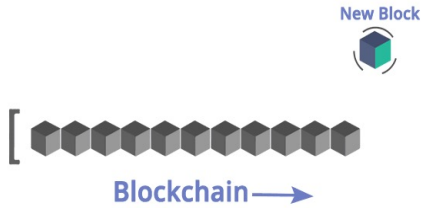


All these limitations of traditional CTS creates the need for secure and automated system

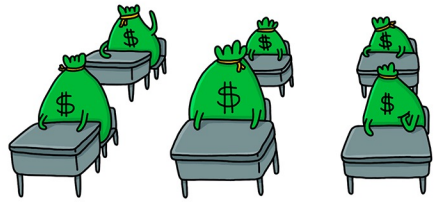
Possible Solution…



Possible Solution….

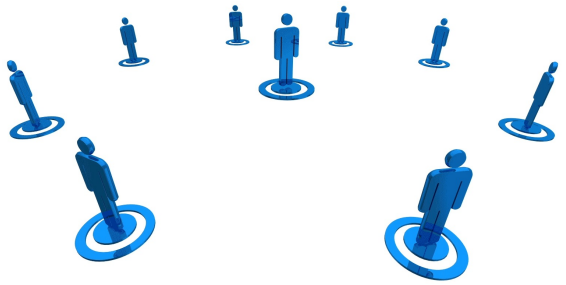


Integration of Blockchain in clearing process.



Distributed and immutable.

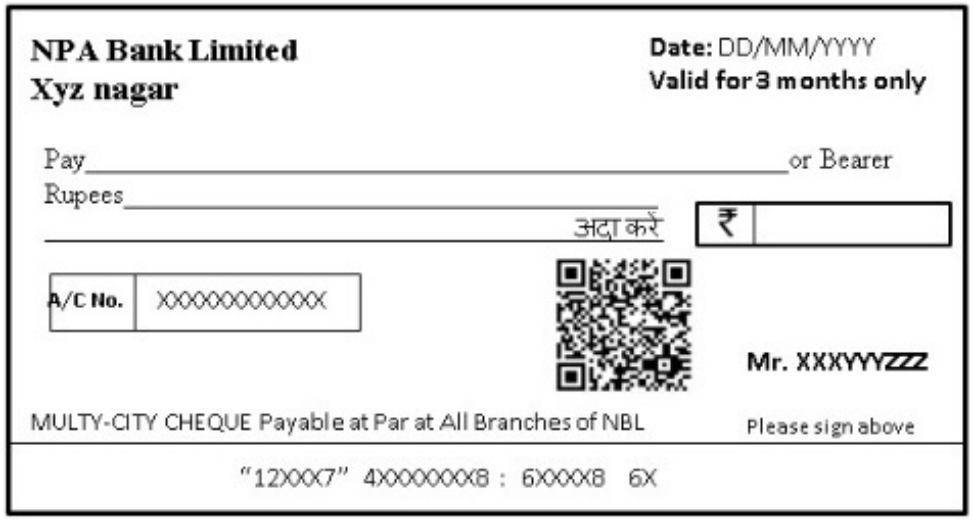
Leads to transparency.



Increases the efficiency of cheque clearing

Blockchain Enabled Cheque

- Blockchain enabled cheque will be presented to the users of the bank which can operate in ***Consortium*** mode.
- Cheque is embedded with a QR code.
- QR code is generated by encrypting bits with the issuer private key *K*.



Blockchain Enabled Cheque

The wallet operates in ***Consortium*** mode and is accessible to only the beneficiary.

Blockchain Enabled Cheque

The wallet operates in ***Consortium*** mode and is accessible to only the beneficiary.

It is developed in Hyperledger Fabric which mainly uses ***Practical Byzantine Fault Tolerance (PBFT)***.

Blockchain Enabled Cheque

The wallet operates in ***Consortium*** mode and is accessible to only the beneficiary.

It is developed in Hyperledger Fabric which mainly uses ***Practical Byzantine Fault Tolerance (PBFT)***.

PBFT provides a mechanism for the files to communicate even after one of the files is corrupted.

Blockchain Enabled Cheque

A blockchain cheque runs smart contracts called ***Chaincode*** in ***Hyperledger Fabric***.

Chaincode are written in programming languages such as ***Go or Node***.

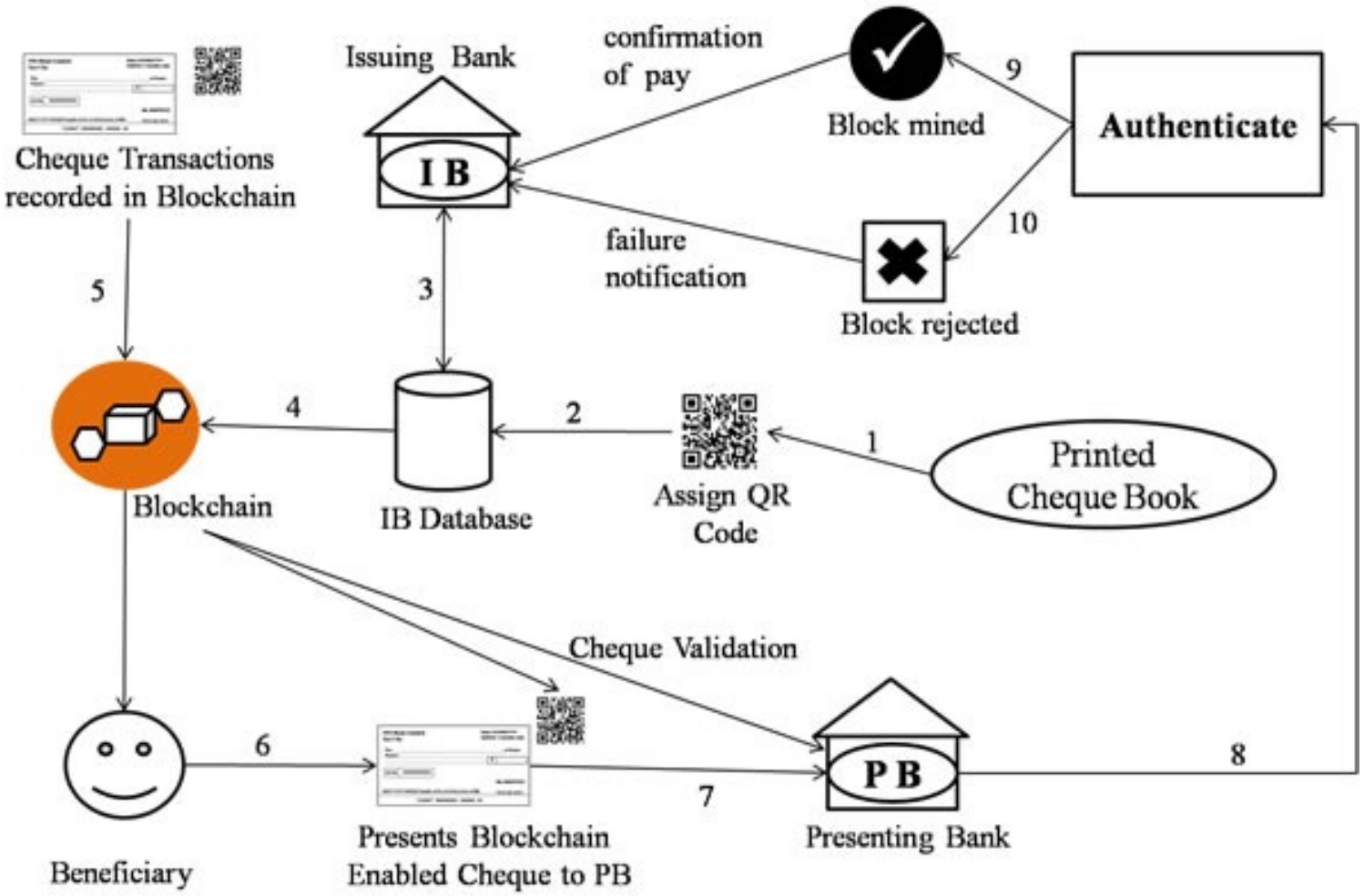
Chaincode separates various entities participating in a financial transaction.

Log of encrypted transaction is ***untraceable*** for normal parties in the chain.

Comparison of Traditional Wallet (Bitcoin) Vs Blockchain Cheque System

Features	Traditional Wallet (Bitcoin)	Blockchain cheque	Description
Nature	Public	Consortium	Service-oriented and flexible anonymous transaction system.
Smart Contracts	No	Yes	Programming Languages like Cotlin/NodeJs/Python/Solidity
Encryption	Single	Multiple	Public Source Addresses and Destination Addresses, or even anonymous accounts.
Identity Authentication	No	Yes	Permissioned chain
Verification Time	10 milliseconds	10 microseconds	GPU based parallel computational models available

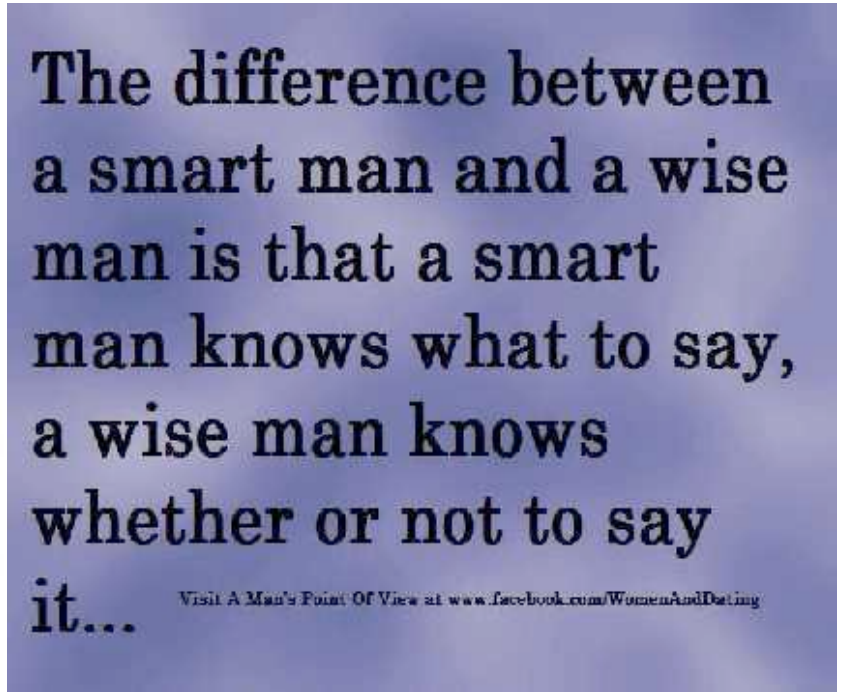
Possible System with Blockchain



Enhancing Security of Blockchain enabled Cheque Clearance System

- Generation of QR Codes.
- Two-Factor authentication of the Blockchain Enabled Cheque.
- Auto-Verification of OTP and transfer of Funds.

Smart vs. Intelligent



If you had a graph in which the x axis represented situations and the y axis the outcome, the graph of the wise person would be high overall, and the graph of the smart person would have high peaks.


Q
&
A