Real state Registration system based on Permissioned Blockchain

By

Ehab Ibrahim Gomaa

9 Jan 2024

Internal Seminar For : Computer Science Dept.

Agenda

- What is Blockchain.
- Blockchain Use Cases.
- Problem Definition.
- Literature review.
- Work Plan.
- Proposed Model
- References

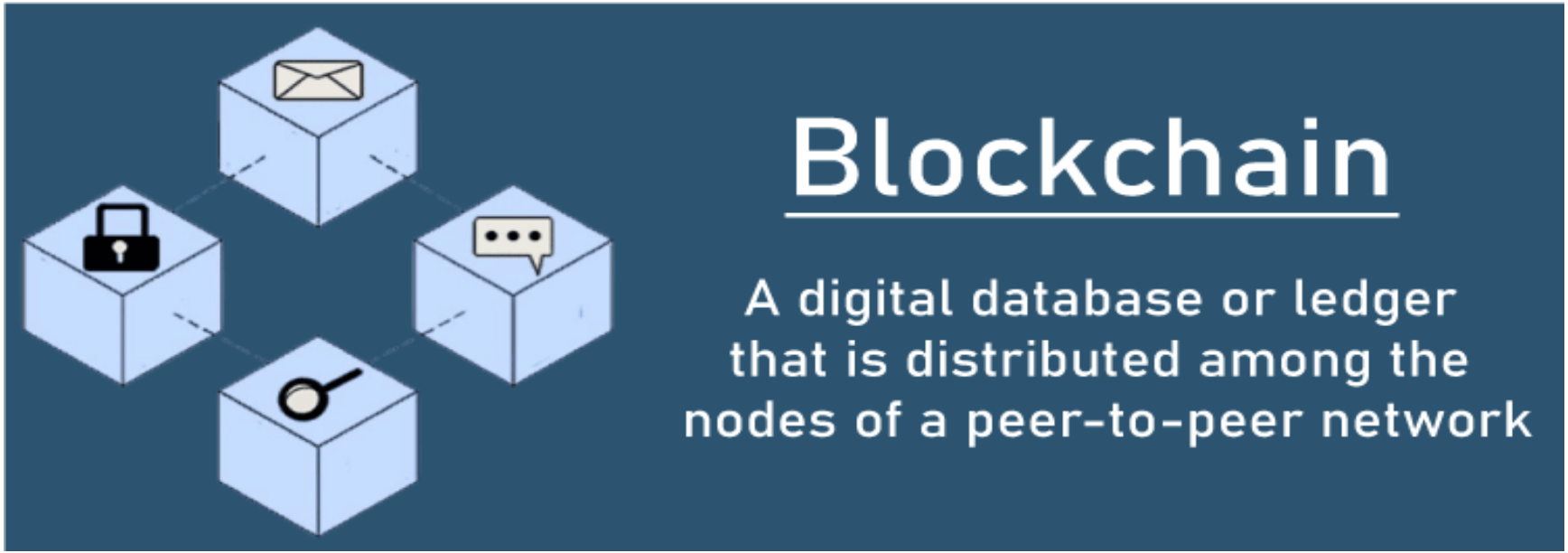
What is Blockchain

What

Why

- Are Blockchain Technologies ?
- Is it relevant for our business ?

Definition


Blockchain
A digital database or ledger that is distributed among the nodes of a peer-to-peer network

Definition

At a technical level, a blockchain can be defined as an immutable ledger for recording transactions, maintained within a distributed network of mutually untrusting peers.

Every peer maintains a copy of the ledger. The peers execute a consensus protocol to validate transactions, group them into blocks, and build a hash chain over the blocks.

This process forms the ledger by ordering the transactions as is necessary for consistency

Transferring Assets, building Value (what)

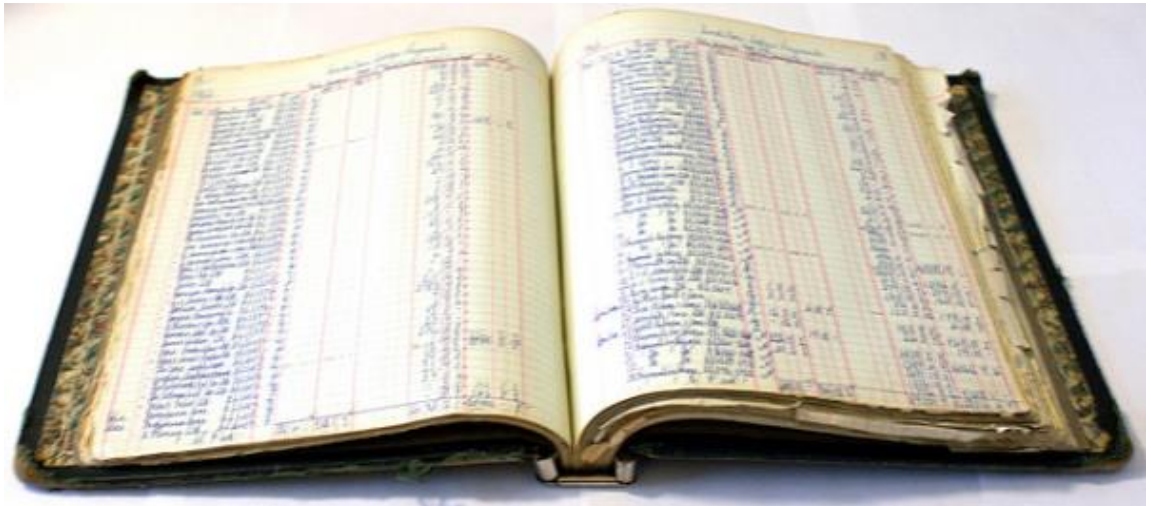
- Anything that is capable of being owned or controlled to produce value, is an asset

- Two fundamental types of asset
  - Tangible, e.g. a house
  - Intangible e.g. a mortgage
- Intangible assets subdivide
  - Financial
  - Intellectual e.g. patents
  - Digital e.g. music
- Cash is also an asset

Ledgers are Important(what)

- Ledger 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.



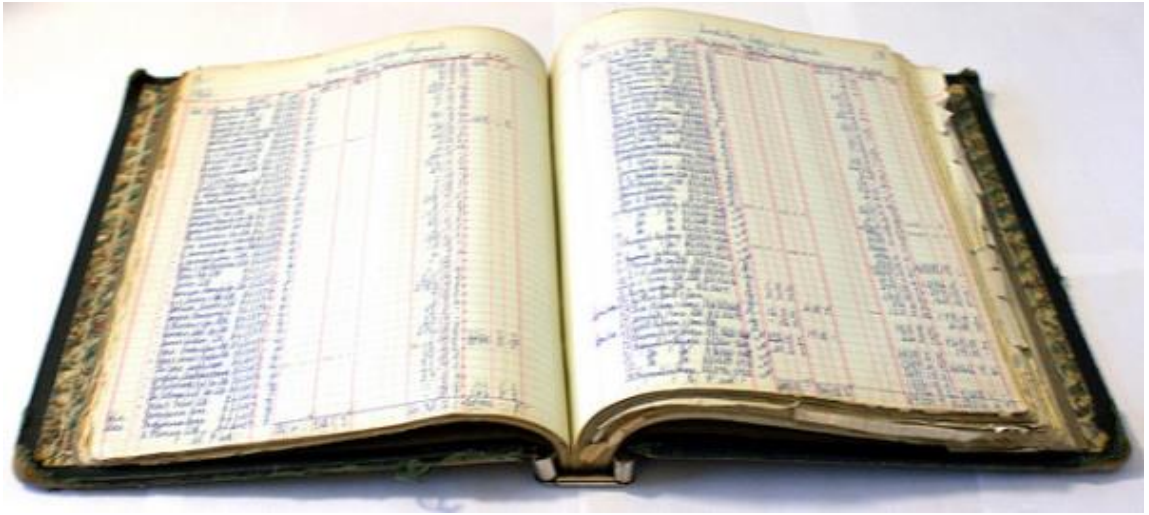
Participants, Transactions & Contracts(what)

- Participants - members of a business network
  - Customer, Supplier, Government, Regulator
  - Usually resides in an organization
  - Has specific identities and roles
- Transaction - an asset transfer
  - John gives a car to Anthony (simple)
- Contract - conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony
  - If car won't start, funds do not pass to John

Participants, Transactions & Contracts(what)

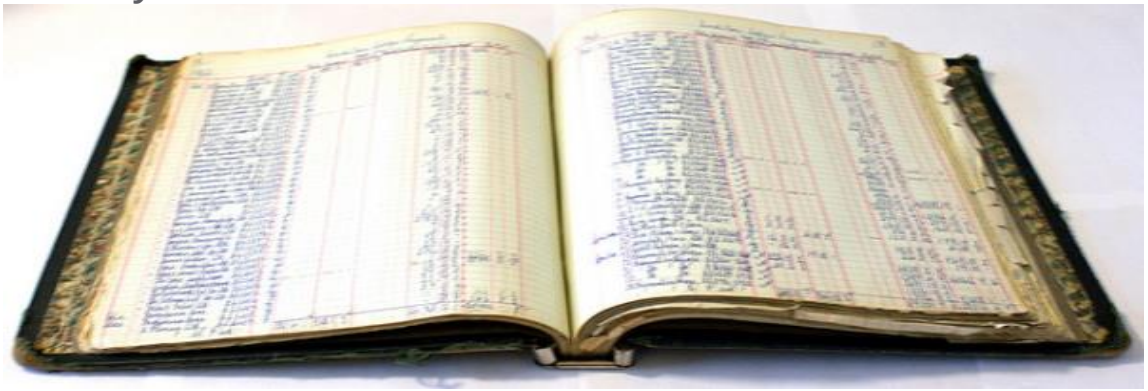
Introducing Blockchain(what)

- *A shared ledger technology allowing any participant in the business network to see THE system of record (ledger)*

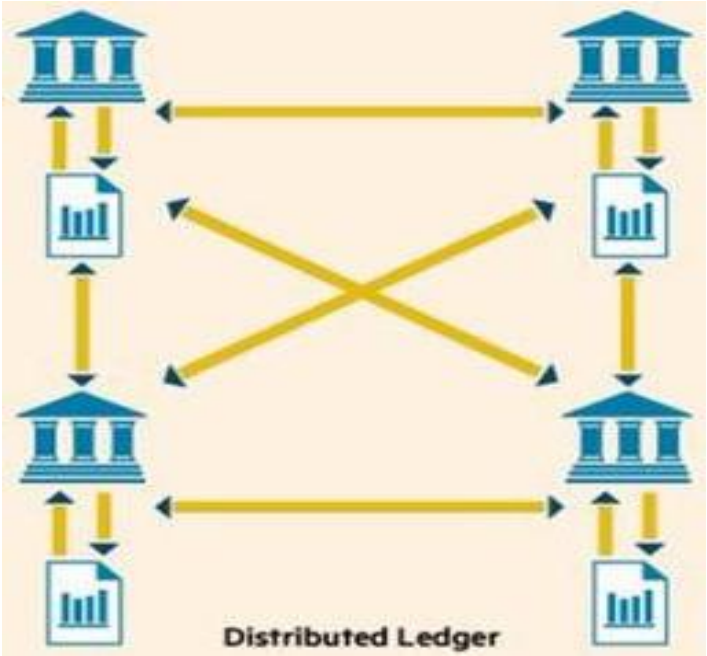


Shared Ledger(what)

- 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



Shared Ledger(what)



Smart Contract(what)

- Blockchains may execute arbitrary, programmable transaction logic in the form of smart contracts.
- A "smart contract" is simply a program that runs on blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the blockchain

Privacy(what)

- Ledger is shared, but participants require privacy
- Participants need:
  - Transactions to be private
  - Identity not linked to a transaction
- Transactions need to be authenticated
- Cryptography central to these processes

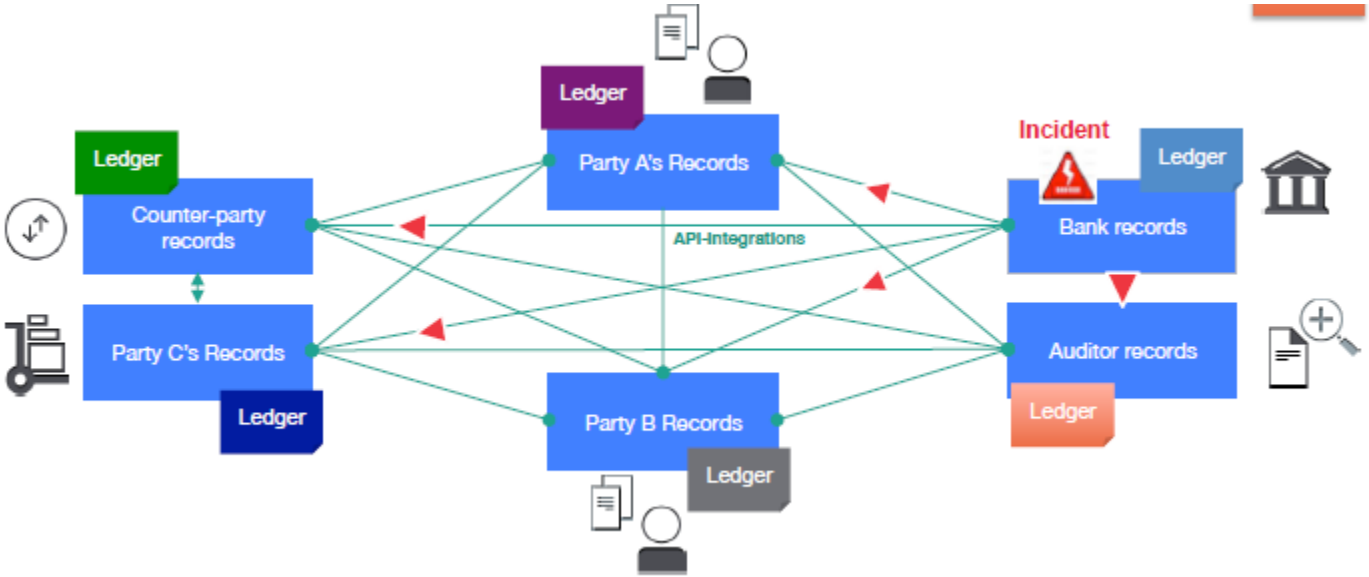
Validation(what)

- Transaction verification & commitment

- When participants are anonymous
  - Commitment is expensive
- When participants are known & trusted
  - Commitment possible at low cost
- Multiple alternatives
  - proof of stake where fraudulent transactions cost validators (e.g. transaction bond)
  - multi-signature (e.g. 3 out of 5 participants agree)

Problem(what)

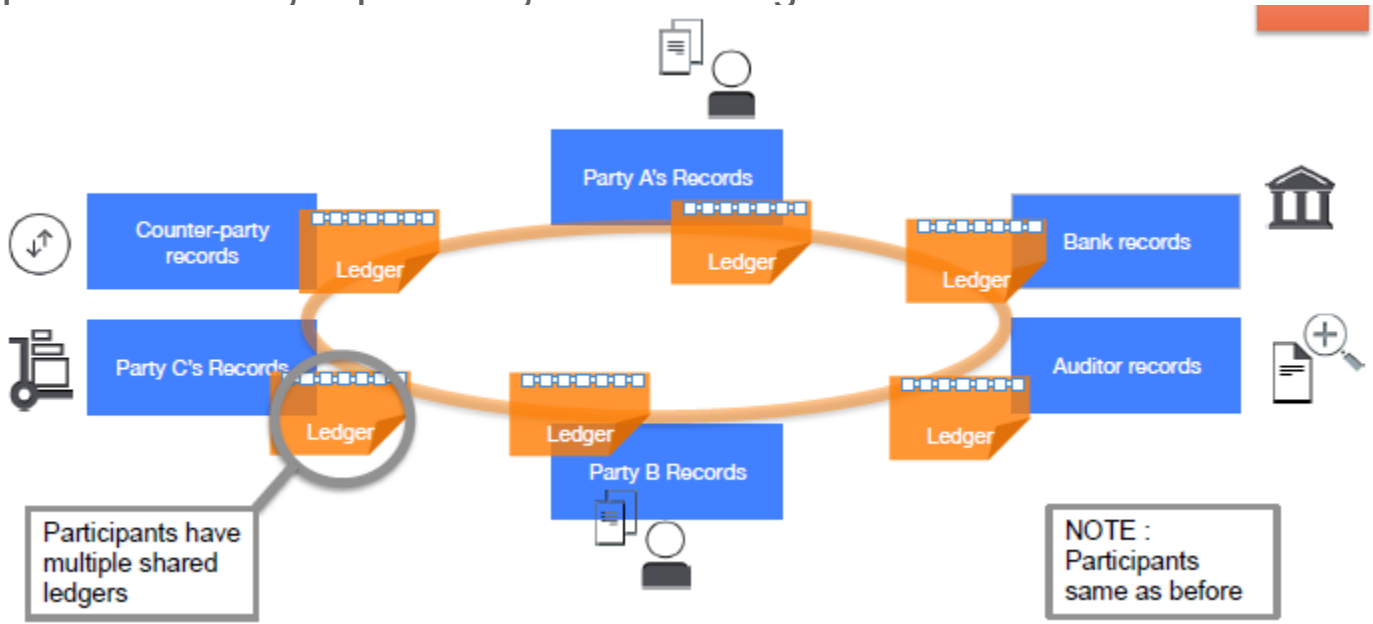
- Difficult to monitor asset ownership and transfers in a trusted business network



Inefficient, expensive, vulnerable

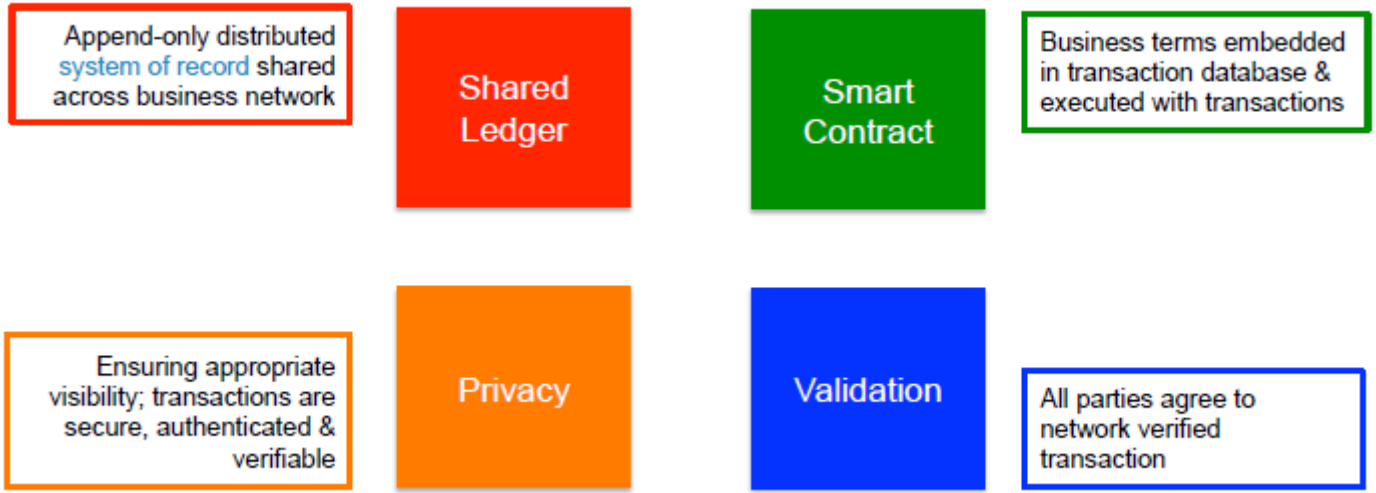
Solution(what)

- a permissioned, replicated, shared ledger



Consensus, **provenance**, **immutability**, **finality**

Blockchain for Business(what)



Broader participation, lower cost, increased efficiency

Industrial Blockchain Benefits(why)

Reduce costs and complexity

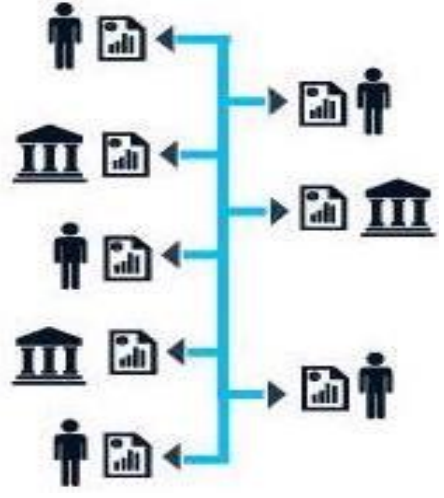
Improve discoverability

Trusted recordkeeping

Shared trusted processes

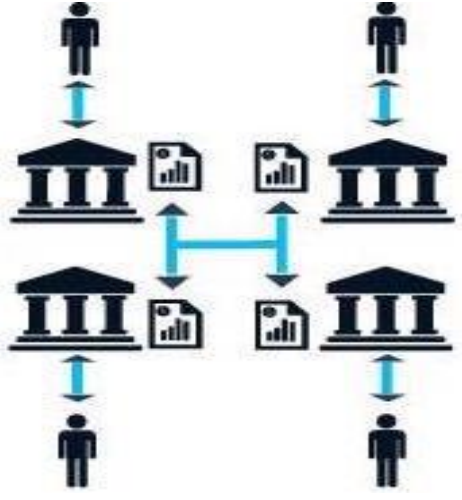
Blockchain Types

- Public blockchain (e.g. Bitcoin)
  - Open P2P network
  - Participants can join and leave without notification
  - Anonymous, untrusted participants
  - Large-scale distributed ledger



Blockchain Types (cont.)

- Private (Permissioned) blockchain
  - Closed permissioned network
  - Identified, trusted participants
  - Regulated control
  - Small to medium-scale distributed ledger



Permissioned blockchains have membership services that manage confidentiality and auditability within the system

Use Case – Bitcoin

- A Peer-to-Peer Electronic Cash System
  - Satoshi Nakamoto (pseudo), Oct. 31, 2008
  - Cryptocurrency and payment system

  Since then
  - Many blockchains: Ethereum in 2013, Ripple in 2014, etc.
  - Increasing use for high-risk investment
    - ✓ Initial Coin Offerings

Brief history of Bitcoin

- In 2010, Laszlo Hanyecz bought two pizzas for 10,000 bitcoins.
- Bitcoin had low value then, so it was seen as a novelty.
- *Rising value:*
  - ✓ Bitcoin’s value increased significantly.
  - ✓ In 2013, it reached over $1,000 per Bitcoin.
- *Price crash:*
  - ✓ In late 2013, Bitcoin’s price crashed.
  - ✓ It lost more than 80% of its value.
  - ✓ Reasons included the Mt. Gox exchange collapse and regulatory concerns.

Brief history of Bitcoin

Current status:

- ✓ Today, thousands of businesses accept Bitcoin.
- ✓ The total value of all cryptocurrencies is over $2 trillion.
- ✓ Bitcoin experienced a significant surge in October 2023, rising from $27,967.51 to approximately $35,000.

Historical Bitcoin Price Trends

- In 2009-2010, Bitcoin had negligible value, and its first real-world transaction involved 10,000 BTC exchanged for two pizzas.
- The year 2011 witnessed a notable spike to $29.6, accompanied by a significant crash.
- Subsequent to this, 2012 marked a period of steady growth, characterized by a gradual increase in the price of Bitcoin.
- The year 2013 was pivotal for Bitcoin, experiencing exponential growth and reaching a value exceeding $1,000. However, this period was also marked by extreme volatility.

https://www.blockchain-council.org/cryptocurrency/how-many-bitcoins-are-left/

Historical Bitcoin Price Trends

- The years 2014-2015 were challenging for Bitcoin due to regulatory hurdles and the infamous Mt. Gox scandal, both impacting its price dynamics.
- In 2016, Bitcoin followed a gradual uptrend, concluding just below $1,000.
- The year 2017 emerged as a landmark period, witnessing an unprecedented surge in price, reaching nearly $20,000.
- However, 2018 marked a correction phase with a substantial 73% price drop.
- Throughout 2019, Bitcoin's price displayed signs of stabilization, fluctuating within the range of $3,000 to $4,000

https://www.blockchain-council.org/cryptocurrency/how-many-bitcoins-are-left/

Historical Bitcoin Price Trends

- The year 2020 saw a temporary dip in price caused by the pandemic, but it rebounded, closing the year around $29,000. In 2021, Bitcoin achieved record highs but also encountered heightened volatility.
- The year 2022 faced a “crypto winter” characterized by a significant price decline influenced by various economic factors and regulatory actions.
- In 2023, Bitcoin started to recover, with a trading value over $38,000 as of November. This recovery indicated renewed investor confidence and interest in the cryptocurrency.

https://www.blockchain-council.org/cryptocurrency/how-many-bitcoins-are-left/

What exactly is the situation with Bitcoin's supply?

- Satoshi used a method in the source code to impose a hard cap, or maximum limit, on Bitcoin production of 21 million.
- The supply of bitcoins is replenished at a set rate of one block every ten minutes.
- The system design reduces the number of new bitcoins in each block by half every four years.
- There are only about 2 million bitcoins left. Experts predict that the last bitcoins will be mined by 2140.

Important Question

Why should you know how many bitcoins exist and how many are left to mine?

- Limited Supply: Bitcoin has a maximum supply of 21 million coins, and as of March 2023, more than 19 million have been mined.
- Remaining bitcoins: There are approximately 2 million bitcoins left to be mined.
- Impact on Value: Knowing this matters because it affects Bitcoin’s value and future price. When fewer bitcoins are available, demand can rise, increasing the price.
- Volatility: Decreased supply can lead to price volatility, but if demand doesn’t grow, prices may stay the same or drop.
- Security: Understanding the mining process is crucial for the security of the Bitcoin network.

Why is Bitcoin supply limited to 21 million?

- As discussed earlier, Bitcoin has a maximum supply of 21 million. This was hard-coded into its protocol by Satoshi Nakamoto.
- This limit ensures that Bitcoin is scarce and cannot be manipulated like traditional currencies.
- The reason behind the 21 million Bitcoin limit lies in the concept of scarcity, which is a fundamental principle of economics.
- By limiting the supply of bitcoins, the value of each individual Bitcoin is theoretically increased. This is because as demand for Bitcoin increases, but the supply remains fixed, the price of Bitcoin is likely to increase as well.
- This is known as the law of supply and demand.

Why is Bitcoin supply limited to 21 million?

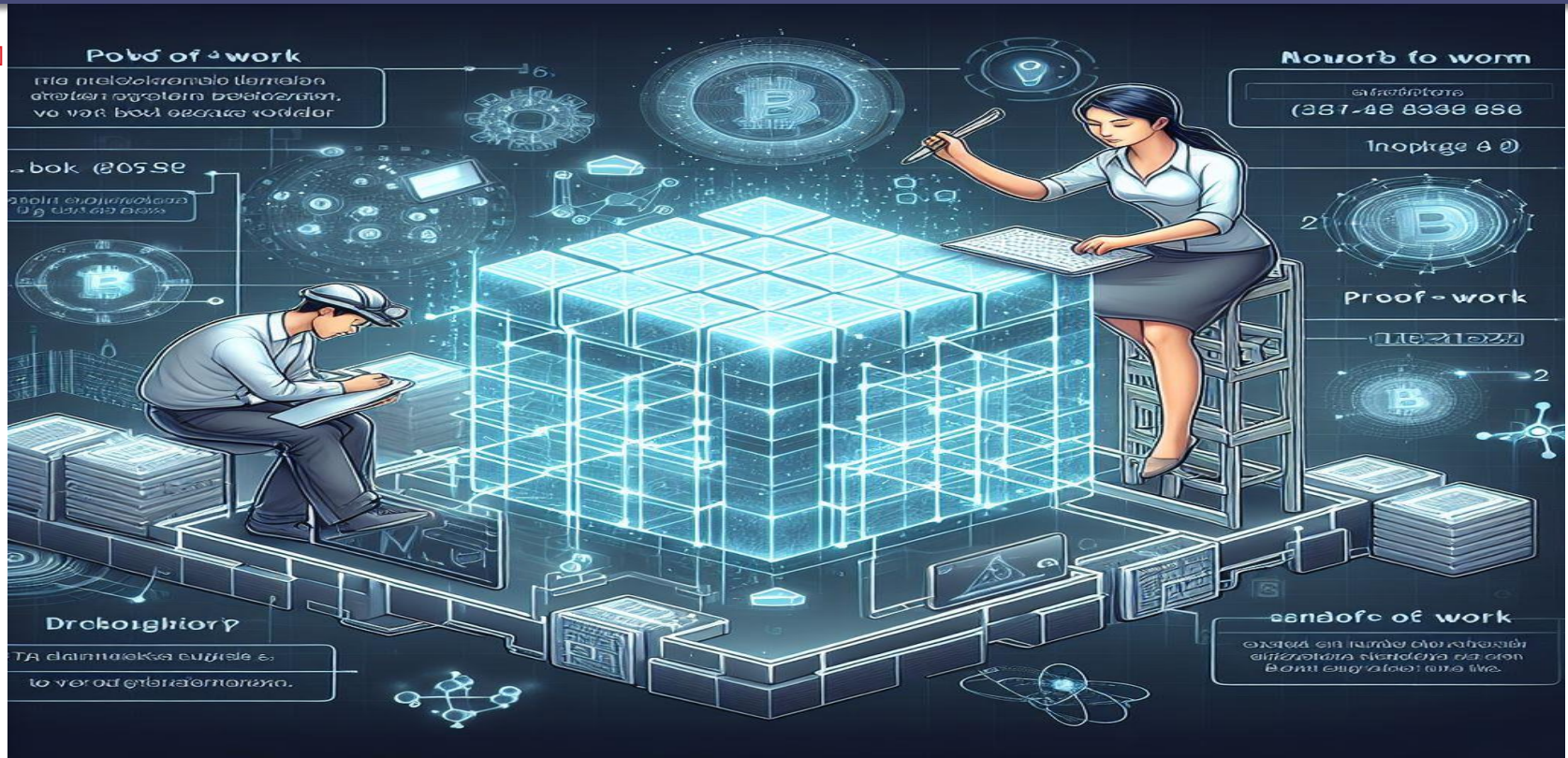
- The limit of 21 million bitcoins also ensures that there is no risk of inflation. Inflation is the decrease in the purchasing power of a currency due to an increase in its supply.
- Governments can manipulate traditional currencies by printing more money, leading to inflation. But with Bitcoin, the supply is fixed, which makes it immune to inflationary pressures.
- Bitcoin’s maximum supply of 21 million is also due to the mathematical rules set in the code. This limit is hardcoded into the protocol, meaning it cannot be changed by anyone, including the developers or miners.

Bitcoin mining

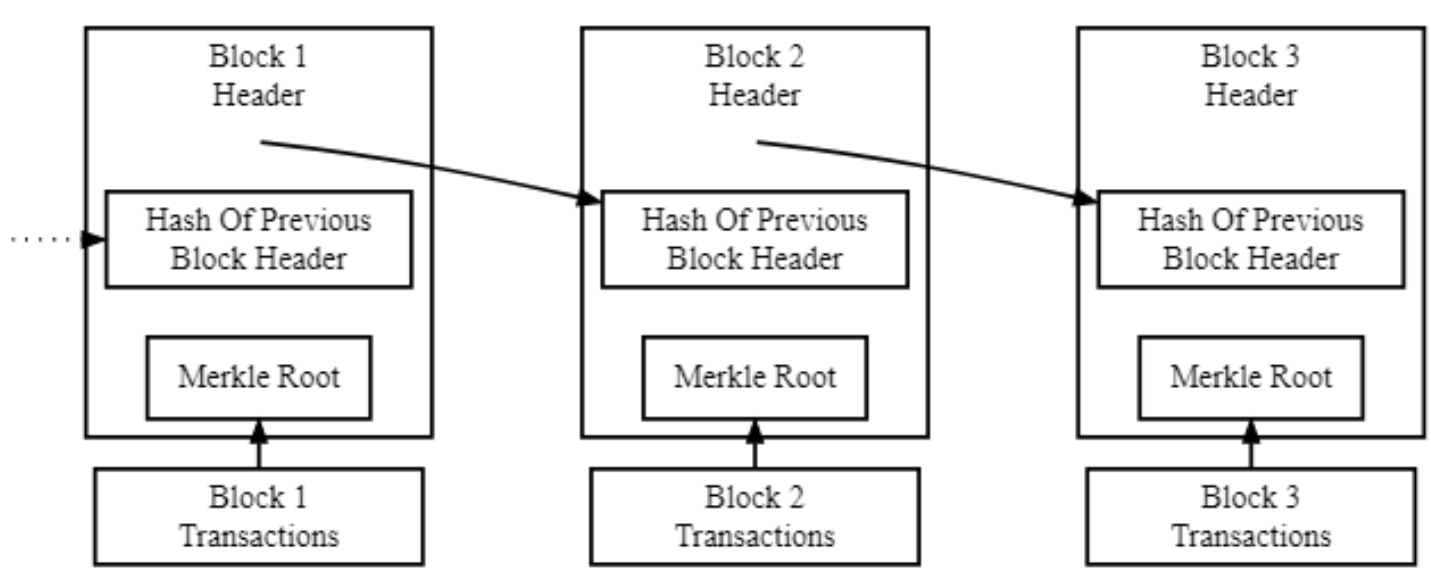
Bitcoin mining

- Bitcoin mining is the process by which new bitcoins are created and added to the Blockchain, which is a decentralized ledger that records all Bitcoin transactions.
- As more bitcoins are mined, the rate at which new bitcoins are created is gradually reduced. This is because the Bitcoin protocol is designed to halve the mining reward every 210,000 blocks.
- The initial reward was 50 bitcoins per block, but this has been halved several times and is currently at 6.25 bitcoins per block.
- The reward will continue to be halved until it eventually reaches zero, at which point no more new bitcoins can be created.

Proof-of-work



Bitcoin Design



Simplified Bitcoin Block Chain

Use Case – Letter of Credit

What?

- Bank handling letters of credit (LOC) wants to offer them to a wider range of clients including startups
- Currently constrained by costs & the time to execute

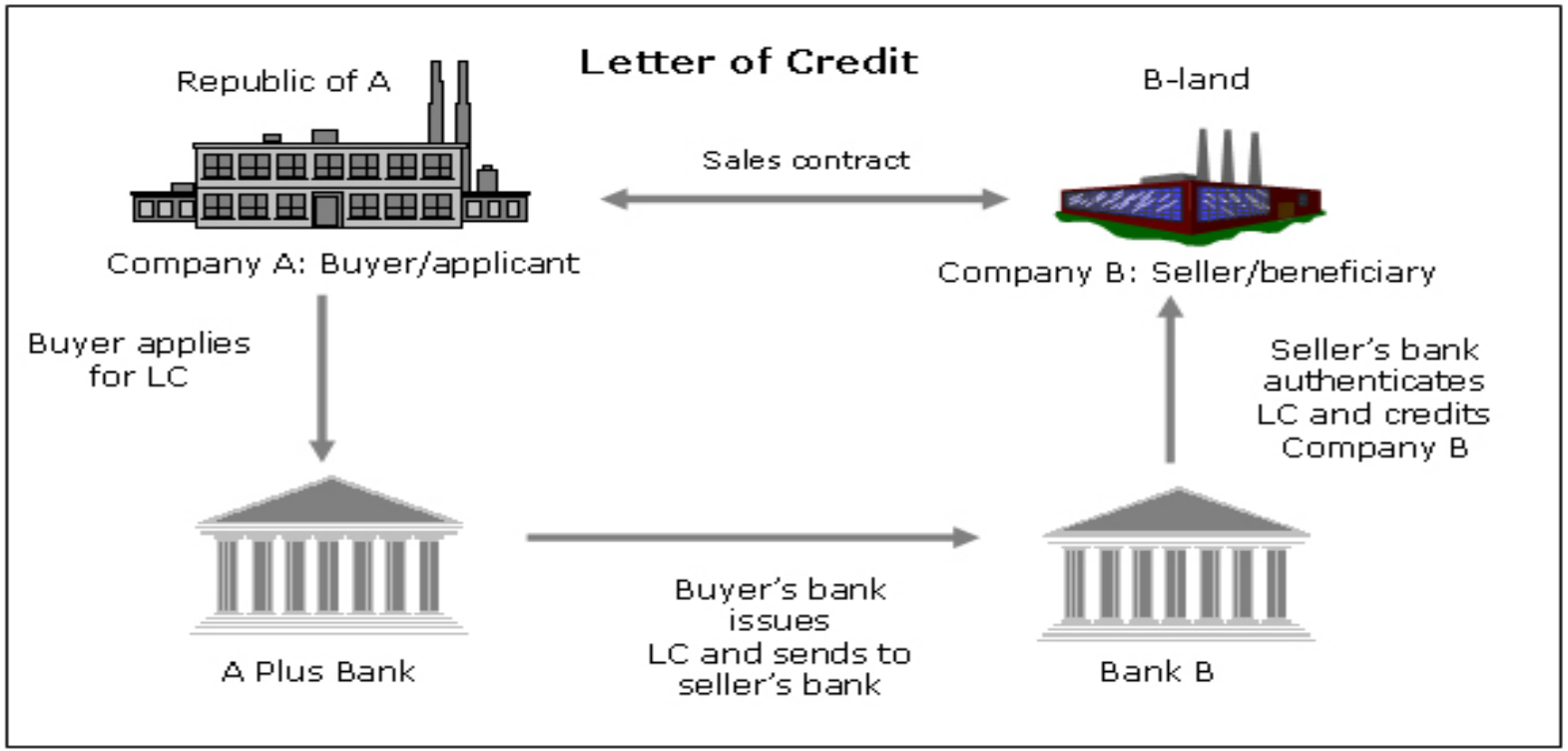
How?

- Blockchain provides common ledger for letters of credit
- Allows bank and counter-parties to have the same validated record of transaction and fulfillment

Benefits

- Increased trust
- Vastly reduced cost

Use Case – Letter of Credit



Problem Definition

Imagine you are a small farmer and your local land registry office is destroyed by a natural disaster.

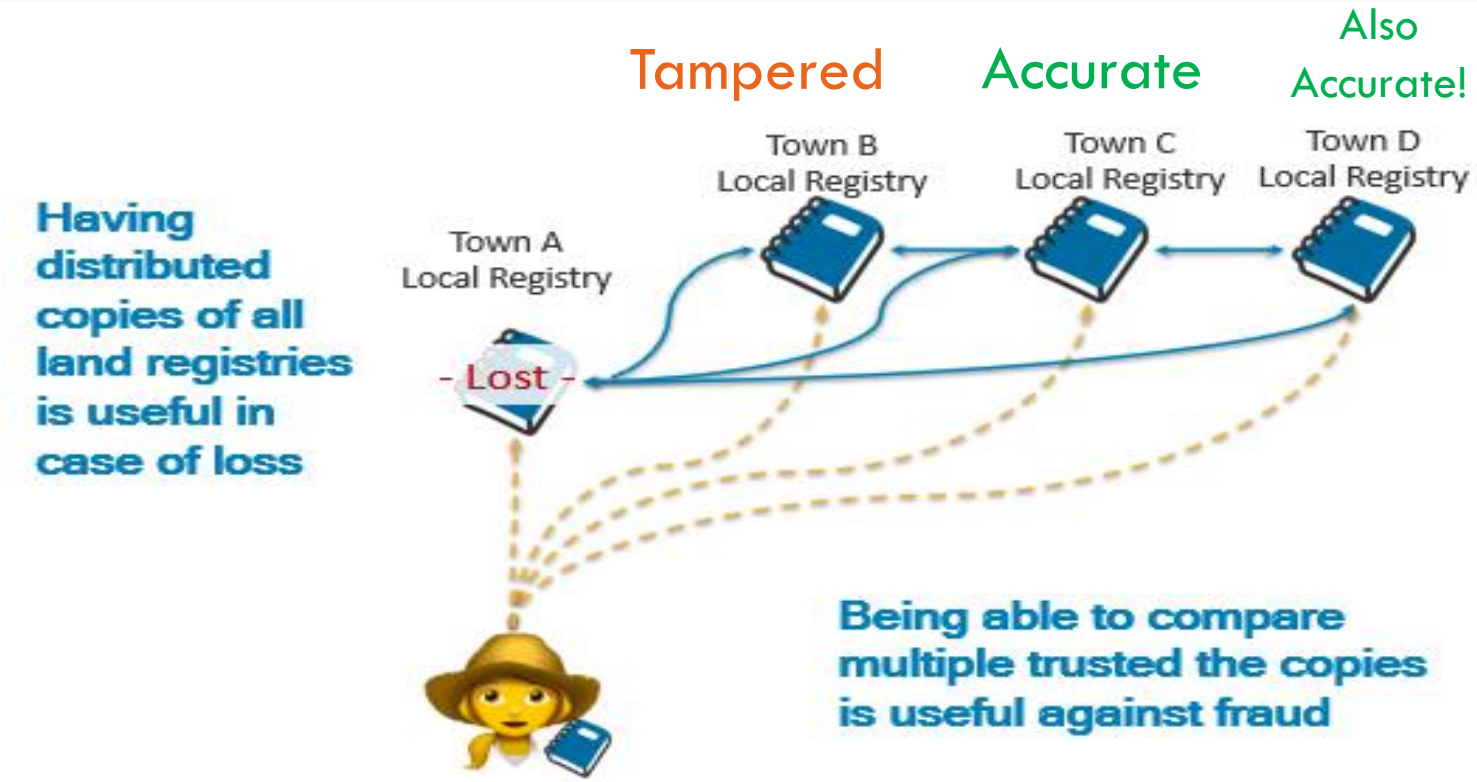
Problems with the existing land registry systems

- The process of land registry and transferring of a land is currently manual.

Even though, some of the processes and records are digitized, however it still has many problems, such as

- It is developed on a centralized system.
- It cannot maintain the complete history of the land
- It does not have a built-in mechanism for record tempering detection

How could we prepare against this risk?



Literature review

Reference	Contribution
1st Toqeer Ali ,2nd Adnan Nadeem , Ali Alzahrani 3rd and 4th Salman Jan "A Transparent and Trusted Property Registration System on Permissioned Blockchain" 2022 IEEE.	This study contributes to providing a transparent and decentralized real estate registration system over Blockchain for Saudi Arabia as a use-case. Initially, the study investigates various processes involved in property registration in Saudi Arabia, i.e. property transfer, buying, selling, etc. The study undergoes understanding the complete automated process of the Ministry of Housing in Saudi Arabia

Literature review

Reference	Contribution
Alketbi, A.; Nasir, Q.; Abu Talib, M. Novel blockchain reference model for government services: Dubai government case study. Int. J. Syst. Assur. Eng. Manag. 2021, 11, 1170–1191.	This study contributes to providing a Housing rental system over Blockchain for Dubai as a use-case. Initially, the study investigates various processes involved in property registration in Dubai, i.e. property transfer, buying, selling, etc.

Literature review

Reference	Contribution
Nguyen, N.H.; Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards Blockchainizing Land Valuation Certificate Management Procedures in Vietnam. In Proceedings of the International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 14–15 October 2020; pp. 1–6.	This study contributes to providing a Land Management e-gov application framework in Vietnam as a use-case.

Literature review (cont.)

Reference	Contribution
I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the blockchain smart contract: a use case for real estate," Journal of Information Security, vol. 9, no. 03, p. 177, 2019.	This study utilize the concept of smart-contract for real estate. They provided an overall design of smart contract make use of the same for examining renting buildings including the real smart cities. The smart contracts are designed and implemented in Solidity. The contracts are compiled for generating binary while the deployment is carried out over the Ethereum. For interaction with the smart contract, a front end web based application is developed

Literature review (cont.)

Reference	Contribution
Sara Ayele, “BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL LAND RECORDS Case of Addis Ababa City Administration” March 2021	This study contributes to providing a transparent and decentralized real estate registration system over Blockchain for Addis Ababa City as a use-case . It uses Ethereum blockchain to provide the users to call the smart contract and read/write information , IPFS which is a tamper-proof storage used to store and read records from the network . React Js which provide an interface to the clients who use a blockchain enabled browser with Ethereum wallet.

Work Plans/Research Objectives

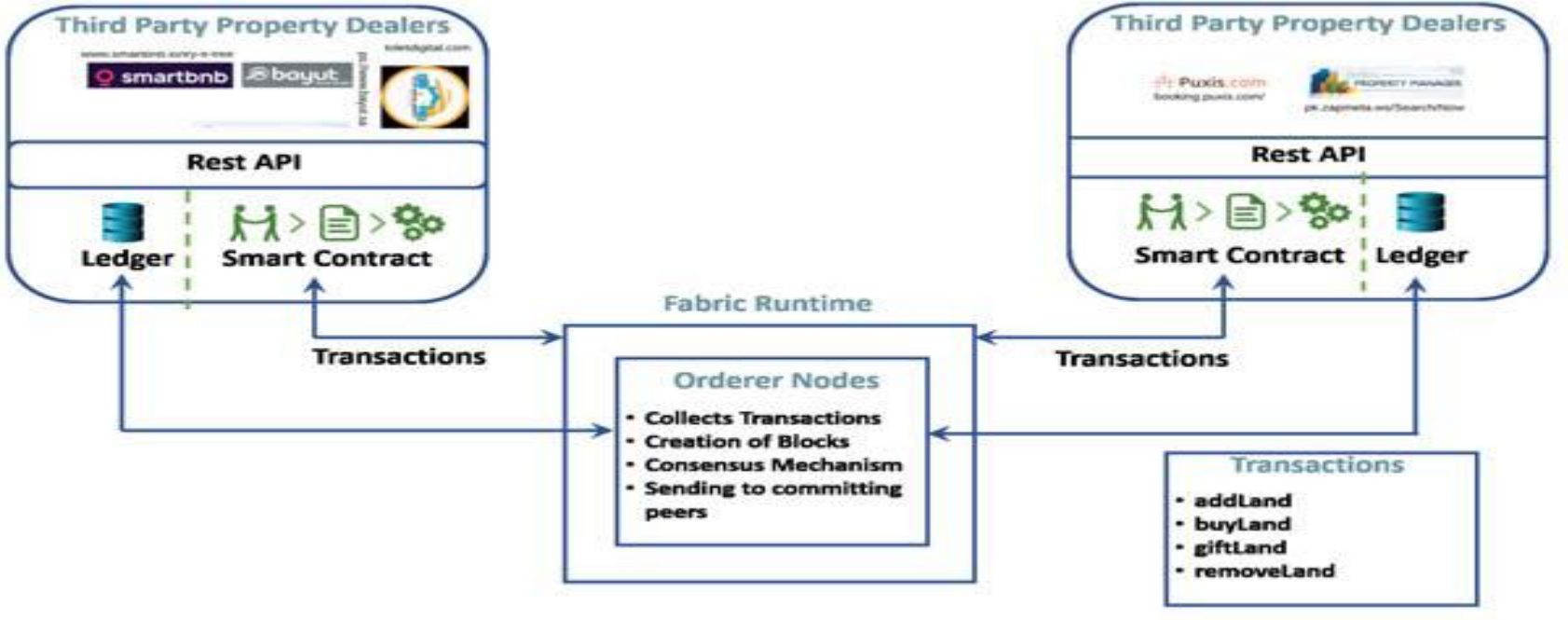
- The proposed model that will be introduced in this Thesis will imply the following steps:

1. Study the related work in land and real estate registration and acquisition approaches (Real estate Agency).
2. Suggest and introduce a solution that guarantee keeping the privacy, security and integrity of the real estate registration system.
3. Build a user friendly system to be applied in the real life (Beni-Suef as a use case).

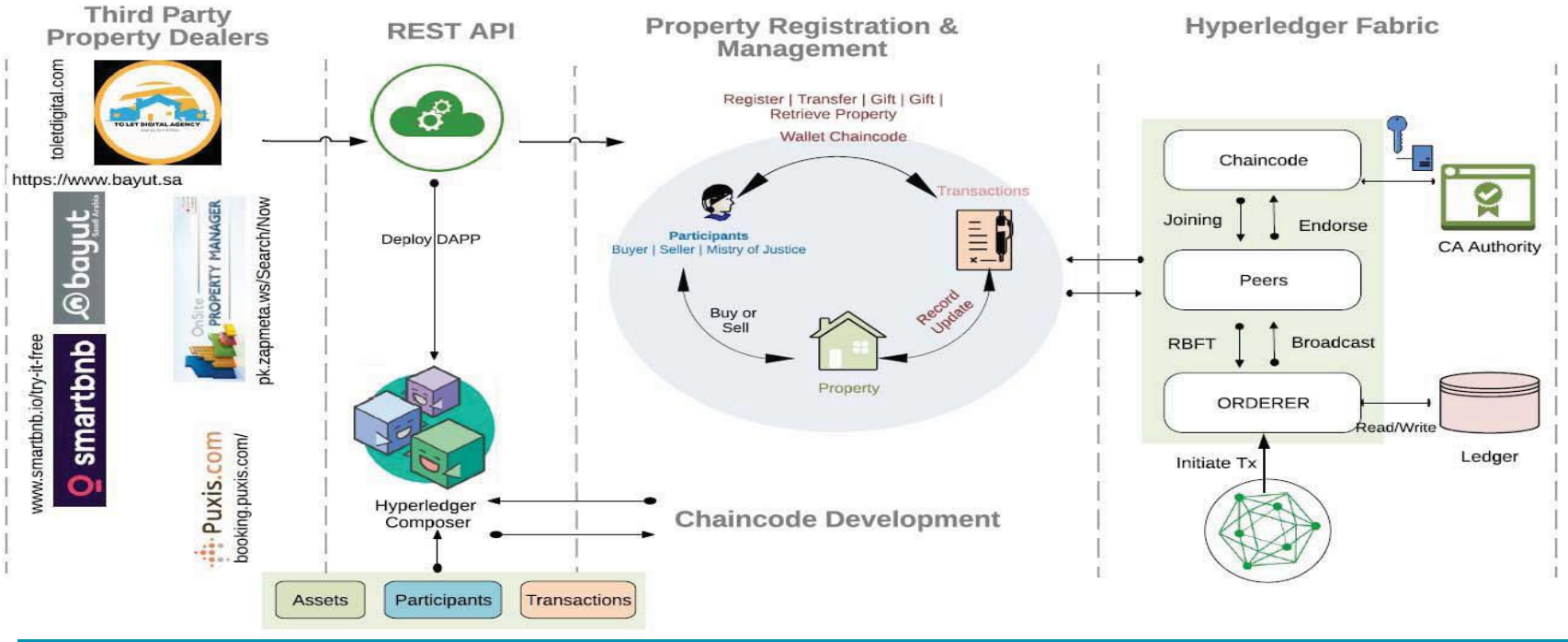
Work Plans/Research Objectives

4. Apply a membership Service so the identity will be verified by the national identity.
5. Conduct a performance analysis of Proposed Model with the existing ones.
6. Testing the system against cheating and altering attempts.

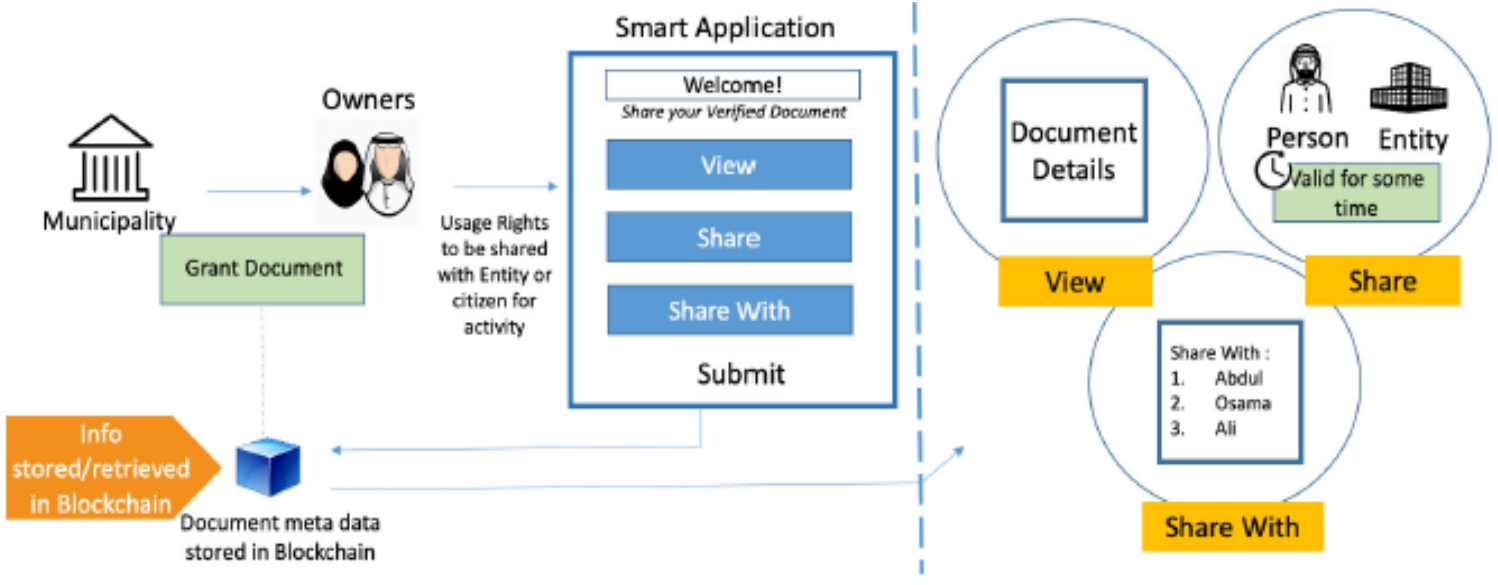
Proposed Model



Proposed Model



Data Flow


Smart Application
Welcome!
Share your Verified Document
View
Share
Share With
Submit
Owners
Municipality
Grant Document
Usage Rights to be shared with Entity or citizen for activity
Info stored/retrieved in Blockchain
Document meta data stored in Blockchain
Document Details
Person
Entity
Valid for some time
View
Share
Share With :
1. Abdul
2. Osama
3. Ali
Share With

References

[1] 1st Toqeer Ali ,2nd Adnan Nadeem , Ali Alzahrani 3rd and 4th Salman Jan "A Transparent and Trusted Property Registration System on Permissioned Blockchain" 2020 IEEE.

[2] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the blockchain smart contract: a use case for real estate," Journal of Information Security, vol. 9, no. 03, p. 177, 2018.

[3] Sara Ayele, "BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL LAND RECORDS Case of Addis Ababa City Administration" March 2021

[4] Balaji S. Asst Professor, Department of Computer Science and Engineering, Ranippettai Engineering College, India "Blockchain based Secure Smart Property Registration Management System and Smart Property Cards" June 2019

References

[5] Karamitsos, Ioannis & Papadaki, Maria & Barghuthi, Nedaa. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security. 09. 177-190. 10.4236/jis.2018.93013.

[6] Ameyaw, P.D.; de Vries, W.T. Toward Smart Land Management: Land Acquisition and the Associated Challenges in Ghana. A Look into a Blockchain Digital Land Registry for Prospects. Land 2021, 10, 239. https://doi.org/ 10.3390/land10030239

[7] Making Blockchain Real for Business Explained v2.09 19 Jan 2016

[8] Nguyen, N.H.; Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards Blockchainizing Land Valuation Certificate Management Procedures in Vietnam. In Proceedings of the International Conference on Computing and Communication Technologies (RIVF),

Thanks