Emerging issues in Computer Science

Week 5:Blockchain Technology and Crypto currencies

Lecturer: Ikwap Flavia Agatha

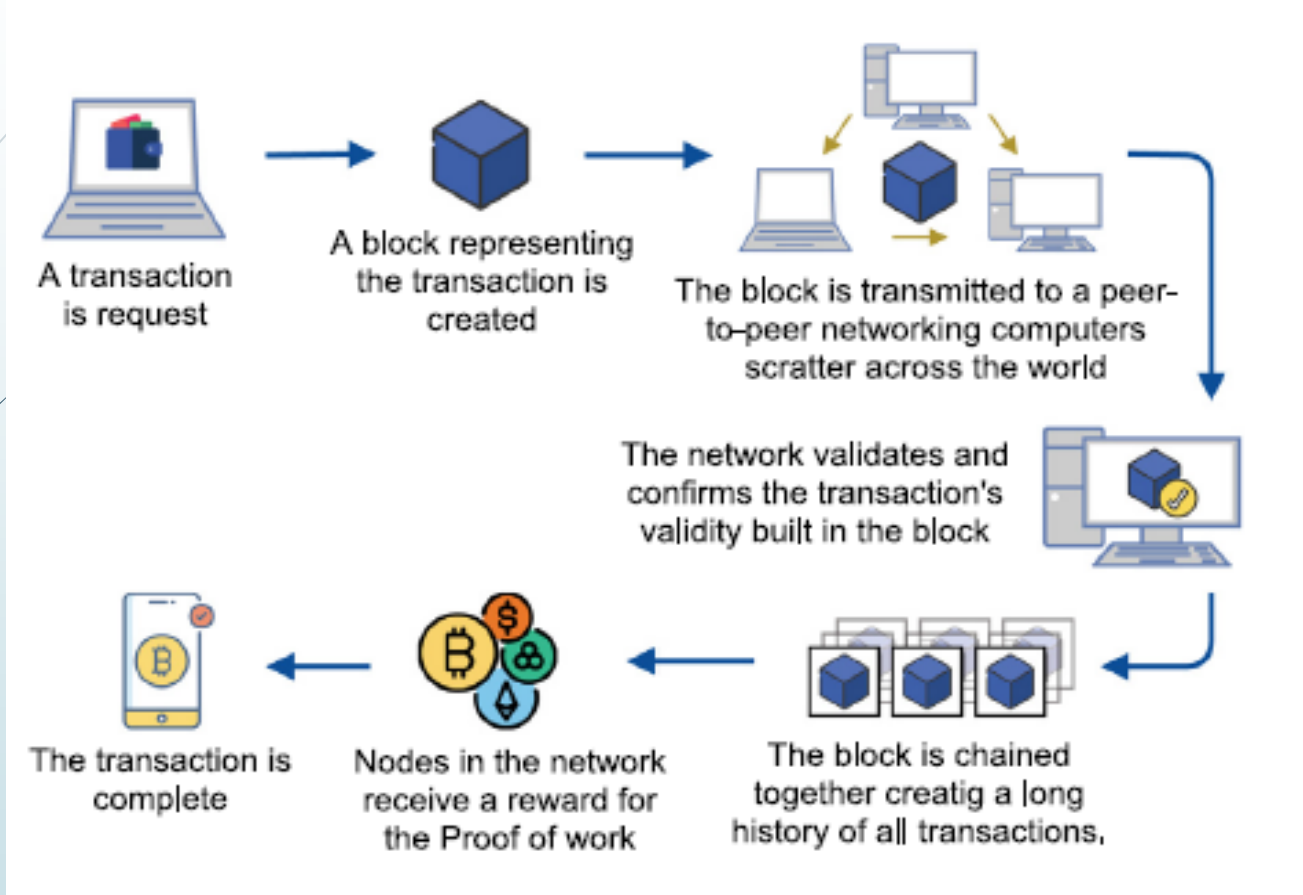
Lecture Out come

- Understanding Block Chain technology
- Understanding How Block chain Works
- Understanding the various technologies used in block chain
- Understanding Applications of Block Chain
- Understanding Crypto currencies and the different types of Crypto currencies

Basics of Block chain

- Block chain is a decentralized, distributed, shared, and immutable (data cannot be erased or altered) database ledger where block data contain a list of all transactions and a hash to the previous block, block chain has a full history of all transactions and provides global trust

Basics of Block chain



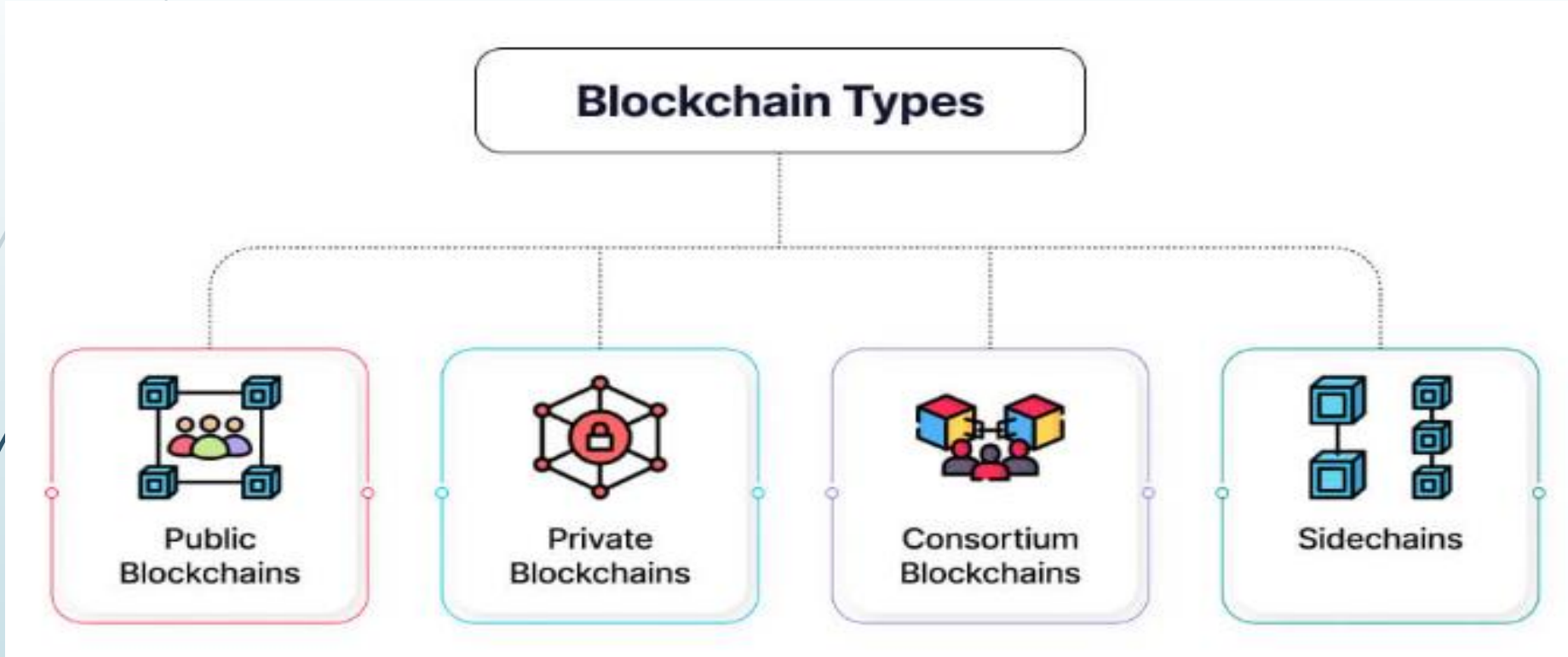
- (Huynh-The, 2023)

Elements of Block chain

- **Blocks**: Data (such as transaction details) is grouped together in "blocks." Each block contains a timestamp, a unique identifier (called a hash), and the hash of the previous block, which links it to the next.
- **Chain**: The blocks are linked together in chronological order, forming a "chain." This structure ensures that each block is connected to its predecessor, making it difficult to alter any data in a block without changing all subsequent blocks.
- **Decentralization**: Unlike traditional centralized databases, block-chain operates on a peer-to-peer network of computers (nodes). Each participant in the network has a copy of the block-chain, which helps prevent fraud and ensures transparency. There is no single point of failure.

- **Consensus Mechanisms**: For a new block to be added to the chain, the majority of participants must agree that it is valid. Different consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) are used to achieve this agreement.
- **Security and Immutability**: Once data is added to the blockchain, it is cryptographically secured and extremely difficult to change. This makes blockchain technology highly resistant to hacking and fraud.

Types of Block chain



- https://www.solulab.com/beginners-guide-to-understand-blockchain-technology/

Public block chain

- A public block chain network is totally open, and anybody can take part in the network by joining it. The network normally has a reward system to urge more members to join the network. Everyone can check the transaction and confirm it and can likewise take part the way toward getting consensus. Bit coin and Ethereum are both public block chain.

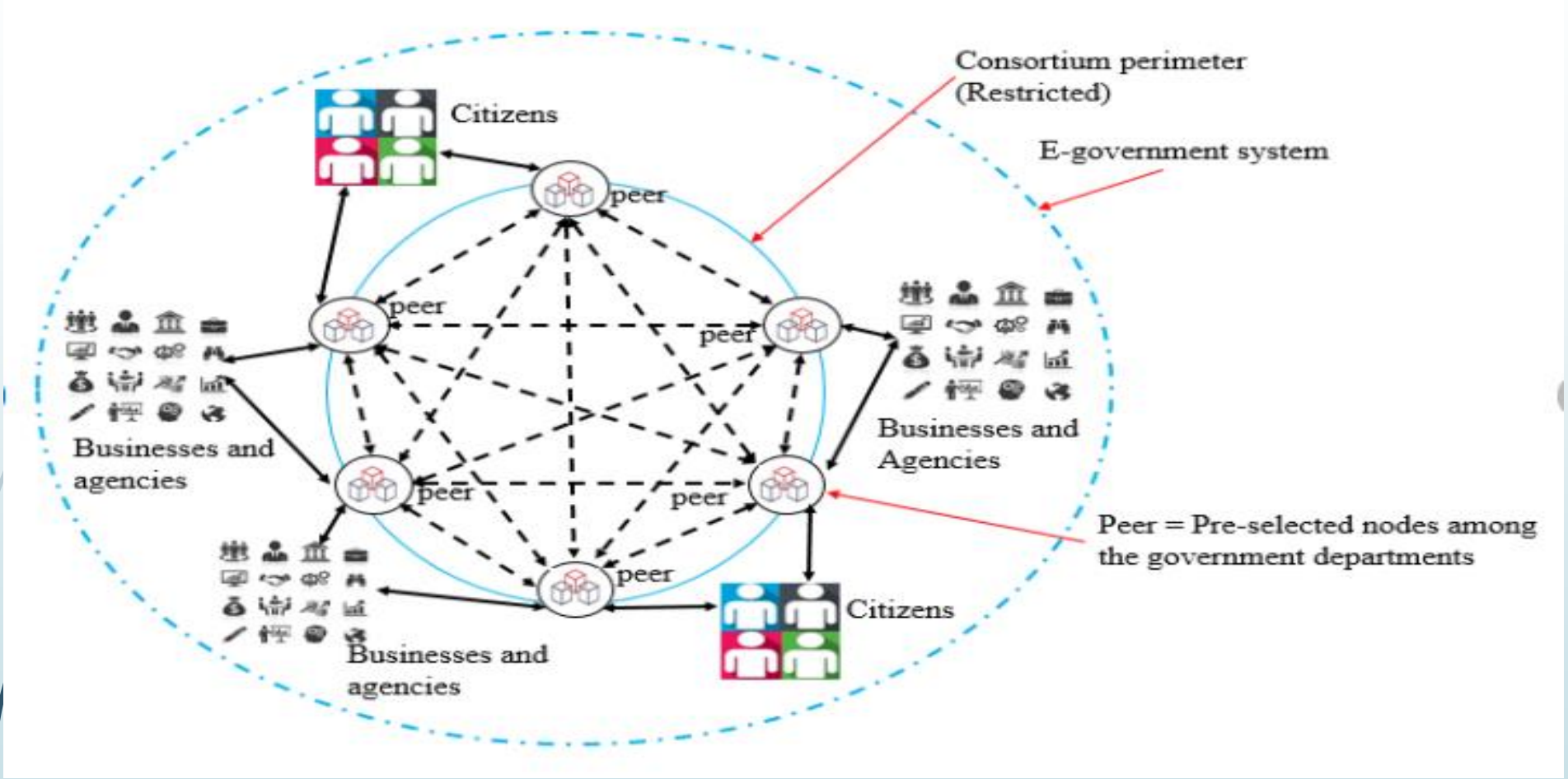
Advantages of public block-chains

- **Trust:** From the outset, public block chains have aimed to remove intermediaries of any kind and, more importantly, to eliminate the need for trust in them. Participants don't need to trust each other for transactions to be processed and verified. Public block chains are considered trustless because everyone is incentivized to act in the best interest of the network's improvement.
- **Transparency and Openness:** All transaction data is publicly accessible for anyone to verify. The transparency of public block chains is a key feature that attracts a wide range of use cases, including voting and financial transactions. Additionally, the authenticity of transactions and data can be verified by anyone within the network.
- **Security:** The security of a block chain increases with more active participants and greater decentralization. As the number of nodes grows, it becomes much harder for hackers to compromise the system. In a public block chain, anyone can become a full node or miner, contributing to the system's security. It is virtually impossible for hackers to conspire and control the consensus process.

Consortium block chain

- Consortium block-chains differ from public block-chains because they are permissioned, meaning only authorized users can access them. Control of the block-chain is shared among a group of approved participants, rather than being controlled by one entity. These participants are usually pre-approved nodes on the network. As a result, consortium block-chains combine the security features of public block-chains with more control over the network.

Consortium block chain



- https://www.researchgate.net/figure/The-consortium-blockchain-based-e-government-network-Network-Layer-The-main-function_fig2_339441749

Private Block Chain

- A private block-chain network requires a request that must be approved either by the network originator or according to the rules established by the originator. Organizations that create a private block-block chain will have a permissioned network, which restricts who can participate and which transactions they can execute. To join, members must receive an invitation or authorization. The access control system can vary: existing members might select new participants, an administrative authority may grant participation licenses, or a consortium could make the decisions. Once a node joins the network, it helps maintain the block-chain in a decentralized manner. While all nodes contribute to data transfer, only certain nodes will have special permissions, such as the ability to write on the block-chain.

Advantages of private block chain

- **Faster**: Private block chains can process a higher number of transactions per second (TPS) compared to public block chains. This is because the presence of a limited number of authorized members reduces the time needed to reach consensus on the network, allowing more transactions to be processed per block. Private block chains can handle thousands, or even millions, of TPS.
- **Scalable**: The network is capable of supporting and processing a significantly higher volume of transactions. Unlike decentralized systems, where achieving consensus can be time-consuming, decision-making in a private network is more centralized, resulting in much faster processes.

Disadvantages of private block chains

- The consensus algorithm is hardcoded into the system, and transaction validation relies on a trust-based model. This limits the network's scalability after deployment, and since validation depends on trust between nodes, it increases the potential for internal attacks within the network.
- The use of non-standard programming languages for creating smart contracts makes adoption challenging. This leads to confusion and errors among developers. Additionally, the open-source community supporting Hyper-ledger is still small, and the available documentation is insufficient.
- Hyper-ledger only supports deterministic transactions, which hinders the broader adoption of the technology.

Demonstrating the Block chain Process

- **Problem: Centralized Control by a Single Authority**

  In traditional systems, a single entity, such as a bank, controls transactions and regulatory compliance, which can create dependency on a central authority.

- **Solution: Decentralized Book-keeping**

  The solution is a decentralized system where anyone can participate as a bookkeeper. All participants maintain identical records, ensuring no one has control over the transactions. This decentralized setup provides resilience, as bookkeepers act as checks and balances to prevent manipulation.

Demonstrating the Block chain Process

- **Problem: Transaction ordering**

  With multiple bookkeepers, each might have a different view on the order of transactions, causing inconsistencies across the network

- **Solution: Blocks**

  Transactions are grouped into blocks, which are processed less frequently than individual transactions. This helps synchronize the order of transactions across bookkeepers. Once transactions are included in a block, they are considered confirmed and become more secure as additional blocks are added on top.

Demonstrating the Block chain Process

- **Problem: Who Can Create Blocks, and How Often?**

  Centralized control over block creation is undesirable. A decentralized, secure method for assigning block creators is needed.

- **Solution: Proof-of-Work**

  In Bitcoin, miners solve cryptographic puzzles (proof-of-work) to create blocks. The process ensures fairness, as the miner must find a valid hash, using a nonce to alter the block's data until they meet the target. This decentralizes the control of block creation.

Demonstrating the Block chain Process

- **Problem: Incentivizing Block Creators**

  Block creation requires significant resources (computing power, electricity, etc.), so a system is needed to motivate miners to participate.

- **Solution: Transaction Fees**

  Instead of relying on external payments, an internal system of transaction fees incentivizes miners. Each block creator receives a small fee for processing transactions, keeping the system decentralized and avoiding third-party interference.

Demonstrating the Block chain Process

- **Problem: How to Bootstrap?**

  During the early stages or periods of low transaction activity, miners may be discouraged from continuing due to high costs.

- **Solution: Block Rewards**

  Block creators receive a "block reward" for each block mined, providing additional incentive to continue mining. Over time, as the system matures, block rewards can decrease, with transaction fees taking over as the primary incentive.

Demonstrating the Block chain Process

- **Problem: Faster Hashing, Faster Blocks, and Increased Monetary Supply**

  If miners can increase their hashing power, they can create blocks faster, leading to rapid BTC creation and potential devaluation.

- **Solution: Difficulty Adjustment**

  The network adjusts the difficulty of finding valid blocks based on the speed of block creation. If blocks are created too quickly, the difficulty increases, slowing down block creation. This self-correcting mechanism maintains stability in the system

Demonstrating the Block chain Process

- **Problem: Block Ordering**

  Miners may attempt to mine blocks out of sequence, disrupting the order and structure of the block chain.

- **Solution: A Block chain**

  Each block refers to the previous block's hash, which means miners must mine blocks in sequence. This ensures blocks are linked securely in the correct order, preventing miners from skipping ahead or disrupting the chain.

Demonstrating the Block chain Process

- **Problem: Block Clashes / Consensus**

  Miners may simultaneously create valid blocks, creating confusion about which block should be accepted.

- **Solution: Longest Chain Rule**

  The network follows the longest chain rule, where the longest chain is considered the valid one. The shorter chain becomes an orphan, and its transactions are reprocessed in future blocks.

Demonstrating the Block chain Process

- **Problem: Double Spend**

  A malicious miner could exploit the longest chain rule to create two transactions with the same bit-coins, leading to double spending.

- **Solution: Wait for Six Blocks**

  To prevent double spending, it’s recommended to wait until a transaction is confirmed by six additional blocks. This makes it extremely difficult for a malicious actor to rewrite the blockchain, ensuring the transaction is secure and irreversible.

Block Chain Process

- The block chain process, from initiation to transaction completion, involves several key steps:
- **User Initiates a Transaction**: The user starts by submitting a transaction request through a wallet or app, specifying details like the recipient, amount, and any conditions. The transaction is digitally signed using the user's private key for authentication.
- **Transaction Broadcast to the Network**: The transaction is broadcast to the block chain network and placed in a pool of unconfirmed transactions, waiting for validation by network nodes.

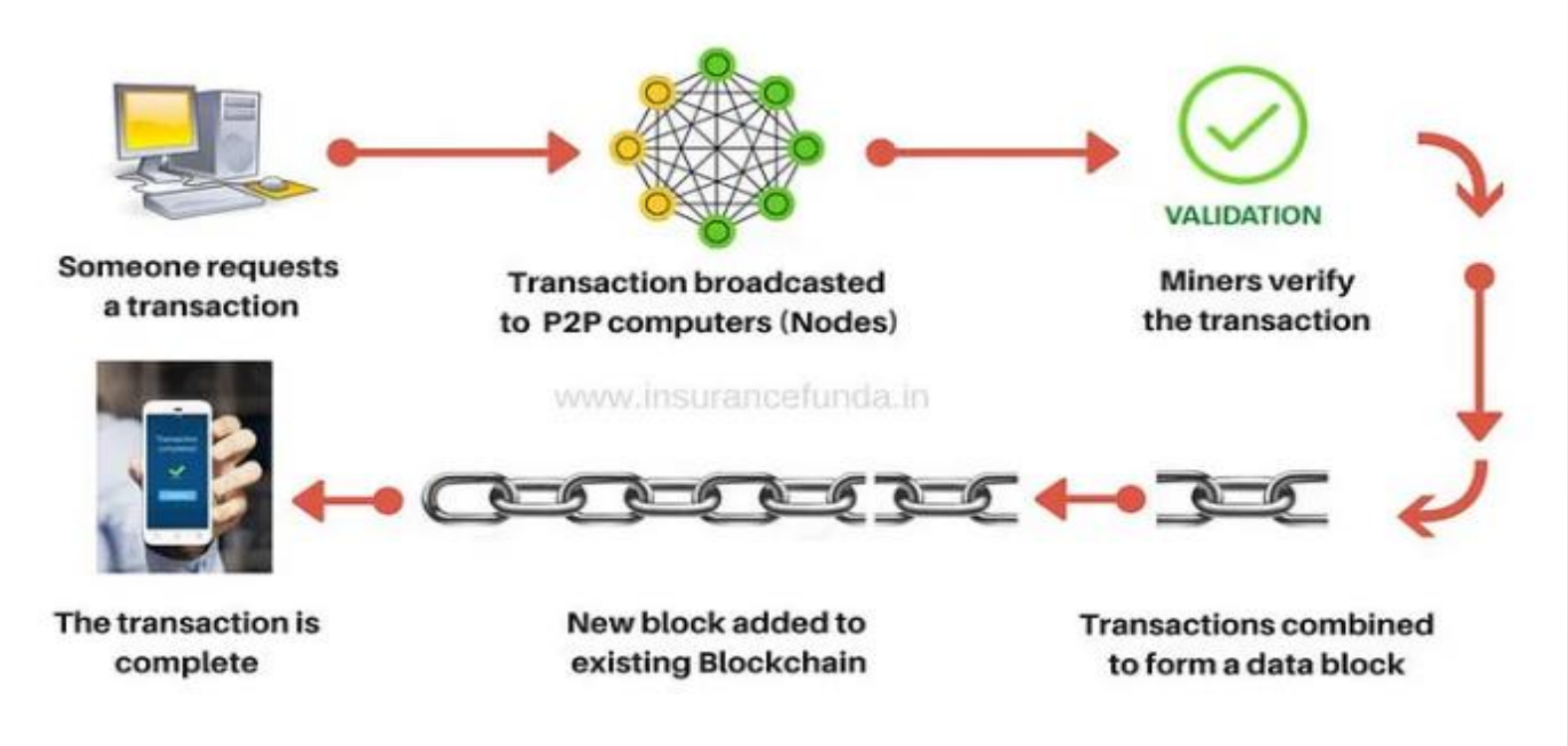
Block Chain Process

- **Transaction Validation (Consensus Mechanism)**: Validators or nodes check the transaction’s validity, ensuring the digital signature is correct, the sender has sufficient funds, and the transaction follows the block chain's rules. A consensus mechanism (like Proof of Work or Proof of Stake) helps confirm its validity and prevent fraud.
- **Transaction Included in a Block**: Once validated, the transaction is grouped with others into a new block, which is linked to the existing block chain, maintaining its continuous, immutable nature.
- **Broadcasting the Block to the Network**: The new block is broadcast to the network. Nodes validate the block, and if the majority agree on its validity, the block is added to their copy of the block chain.

Block Chain Process

- **Transaction Confirmation**: After the block is added, the transaction is confirmed. Some block chains require additional blocks for confirmation (e.g., Bitcoin needs six confirmations), ensuring the transaction is secure and irreversible.
- **Transaction Complete**: The transaction is final, and the recipient's wallet balance is updated. The transaction is recorded on the block chain, reflecting the changes made.

Block Chain Process



- https://itnext.io/pulling-the-blockchain-apart-the-transaction-life-cycle-381b76842c6

Technologies Involved In Block Chain
Cryptography: Hash Functions

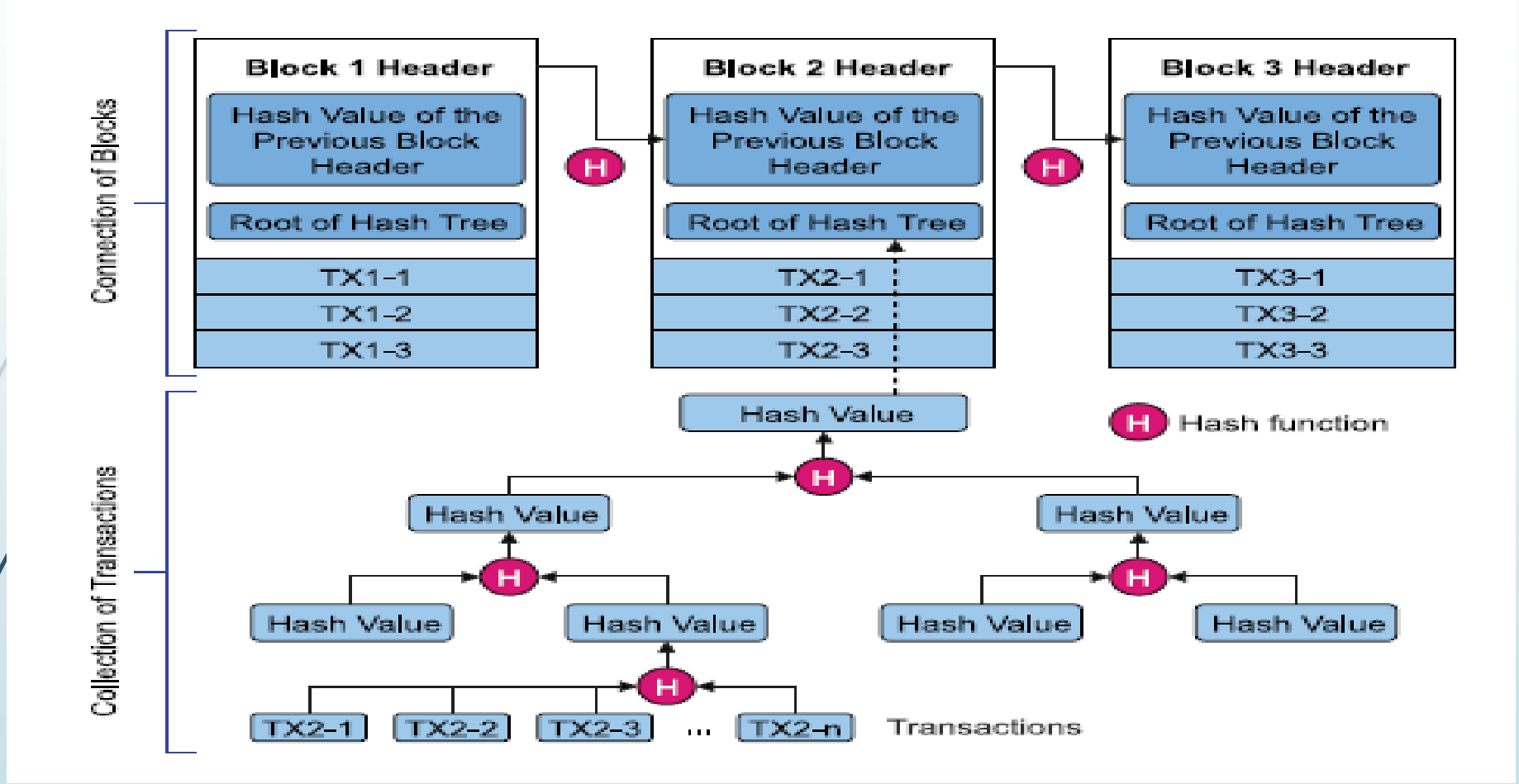
- **Basic Hash Function**

  A hash function is a mathematical process that transforms input data into a fixed-size output, known as a hash, fingerprint, or digest. For example, a basic hash function might take the first character of the input string, so for "What time is it?", the output would be 'W'. This function is deterministic, meaning the same input always produces the same output.

- **Cryptographic Hash Functions**

  Cryptographic hash functions are a more advanced version used in blockchains. They produce a fixed-length output and are designed to ensure data integrity. Even a small change in the input results in a drastically different hash. SHA-256, used by Bitcoin, is one well-known cryptographic hash function.

Cryptography: Hash Functions

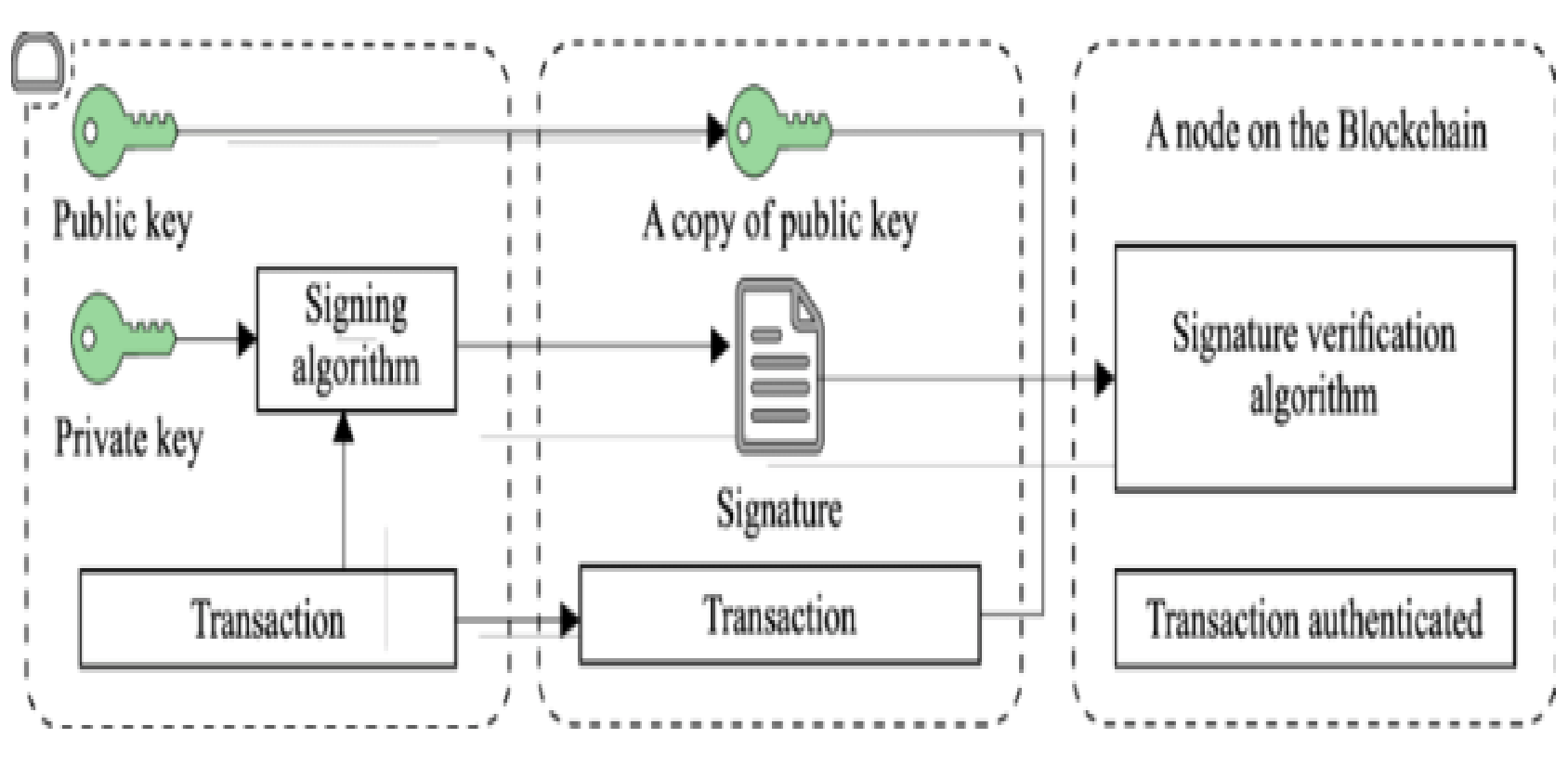


- (Huynh-The, 2023)

Public Key Infrastructure (PKI)

- **Public Key Infrastructure (PKI)**
  PKI uses a pair of public and private keys to ensure secure transactions. The private key signs transactions, while the public key is used to verify them, providing users with control over their block chain assets securely.
- **Solution: Use Public Keys as Account Numbers**
  In Bit coin and most crypto currencies, account numbers are derived from public keys, known as addresses. You can share your Bit coin address to receive payments, but only you, with your private key, can spend from it. You can generate as many addresses as needed, with wallet software managing them for you.
- The public/private keypair system also solves the authentication issue. Instead of logging in with a username and password, you digitally sign transactions with your private key. This signature proves your identity to the system.

Public Key Infrastructure (PKI)

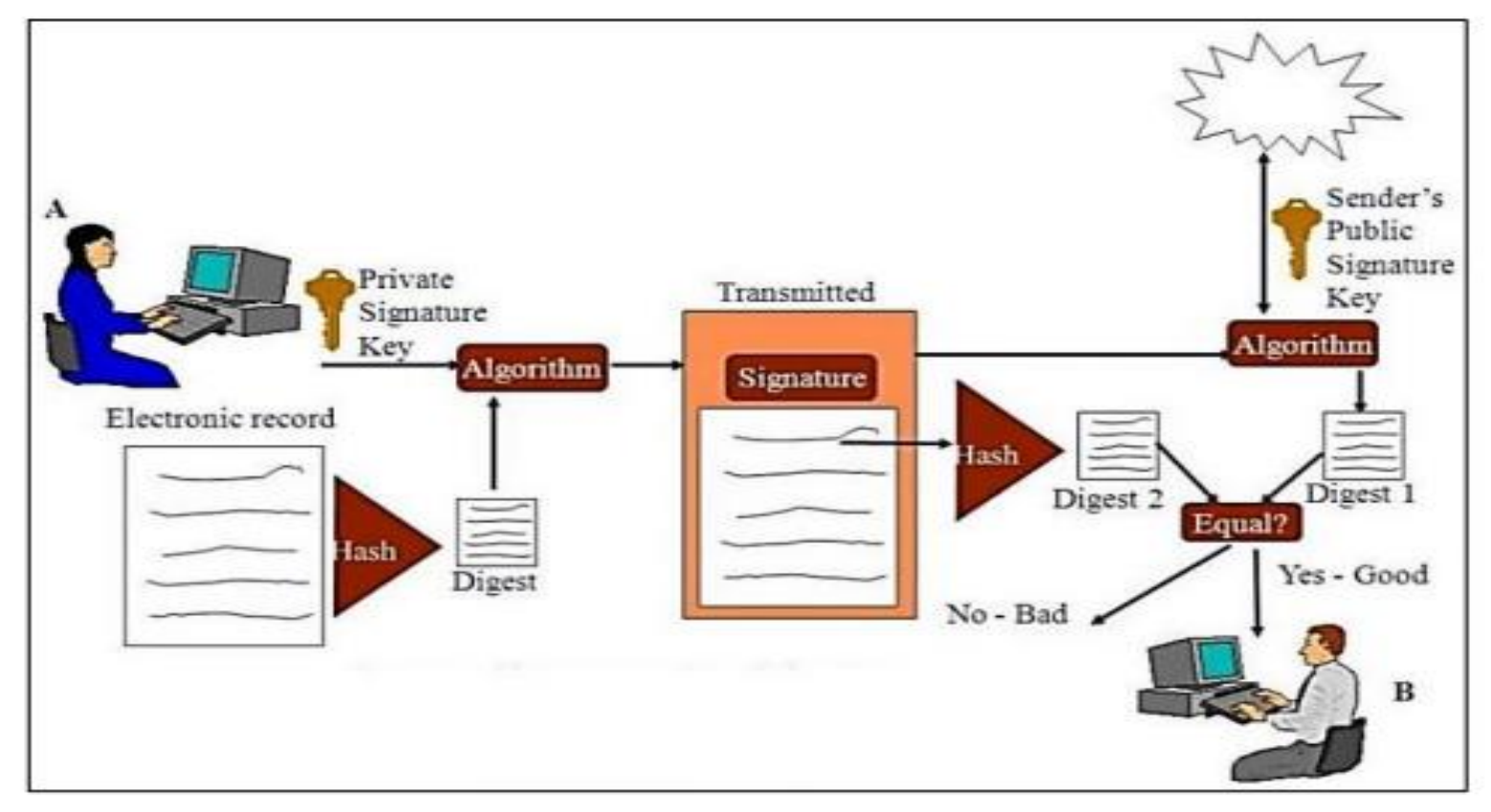


- https://www.researchgate.net/figure/Asymmetric-key-cryptography_fig3_334097375

Digital Signatures

- Digital signatures ensure both authentication and data integrity, confirming that transactions are initiated by the rightful holder of the private key.
- **Digital Signatures in Block chain:** In Bit coin and other block chains, digital signatures play a key role in creating valid transactions by "signing" transaction messages that transfer coins from one account to another. From a cryptographic perspective, digital signatures are a specific type of electronic signature, which can come in various forms.

Digital Signatures



- (Chandrashekhara, 2021)

Decentralized Network And Consensus Mechanisms

- **Peer-to-Peer (P2P) Networks:** Block chain operates on a decentralized, peer-to-peer network where all participants (nodes) possess a complete copy of the block chain. This removes the need for a central authority and minimizes the risk of a single point of failure.
- **Consensus Mechanisms:** These are algorithms that ensure all nodes in the network agree on the block chain's state. Some examples include:
  - **Proof of Work (PoW):** Miners solve complex puzzles to validate transactions and add blocks to the chain. This method is energy-intensive and is used by Bitcoin.

- **Proof of Stake (PoS):** Validators are selected based on the amount of crypto currency they "stake" as collateral. It’s more energy-efficient and is used by Ethereum (after Ethereum 2.0).
- **Delegated Proof of Stake (DPoS):** A variant where delegates are chosen to validate transactions and maintain the block chain.
- **Practical Byzantine Fault Tolerance (PBFT):** A consensus mechanism designed to address issues caused by faulty or malicious nodes within the block chain network.
- **Smart Contracts:**

  Smart contracts are self-executing agreements with the terms directly written into code. Once specific conditions are met, they automatically execute the agreed actions. Ethereum is a major block chain platform that supports smart contracts.

- **Distributed Ledger Technology (DLT):**

  Block chain is a form of Distributed Ledger Technology (DLT), where the database is distributed across multiple nodes. Each node maintains a complete copy of the ledger, ensuring data synchronization and immutability.

- **Tokenization and Crypto currencies:**

- **Crypto currencies** like Bit coin and Ethereum use block chain to securely record transactions and prevent counterfeiting.

- **Tokens** are digital assets created on a blockchain, representing ownership, rights, or access to services (often seen in ICOs).

Block chain Platforms and Frameworks: Ethereum

- A widely-used platform for smart contracts and decentralized applications (DApps).
- **Hyper ledger:** A suite of open-source block chain frameworks, including Hyper ledger Fabric and Sawtooth, designed for business and private block chains.
- **Solana:** A high-performance block chain known for speed and scalability, mainly for decentralized finance (DeFi).
- **Ripple (XRP):** A block chain focused on cross-border payments and remittances.

Block chain Interoperability:

Interoperability solutions like Polkadot and Cosmos enable different block chain networks to communicate and share data with each other.

- **Off-Chain and On-Chain Storage:**
- **On-Chain:** Storing data directly on the blockchain, offering security and immutability but with high costs and inefficiency for large data.
- **Off-Chain:** Storing data outside the blockchain, which is more scalable and cost-effective, but requires trust in the external provider (e.g., IPFS for decentralized file storage).
- **Consensus Algorithms:**
- **Proof of Work (PoW):** Used by Bitcoin and others, where miners solve cryptographic puzzles to validate transactions.
- **Proof of Stake (PoS):** A more energy-efficient algorithm where validators are chosen based on the cryptocurrency they stake as collateral.
- **Proof of Authority (PoA):** Trusted validators validate transactions, typically used in private blockchains.

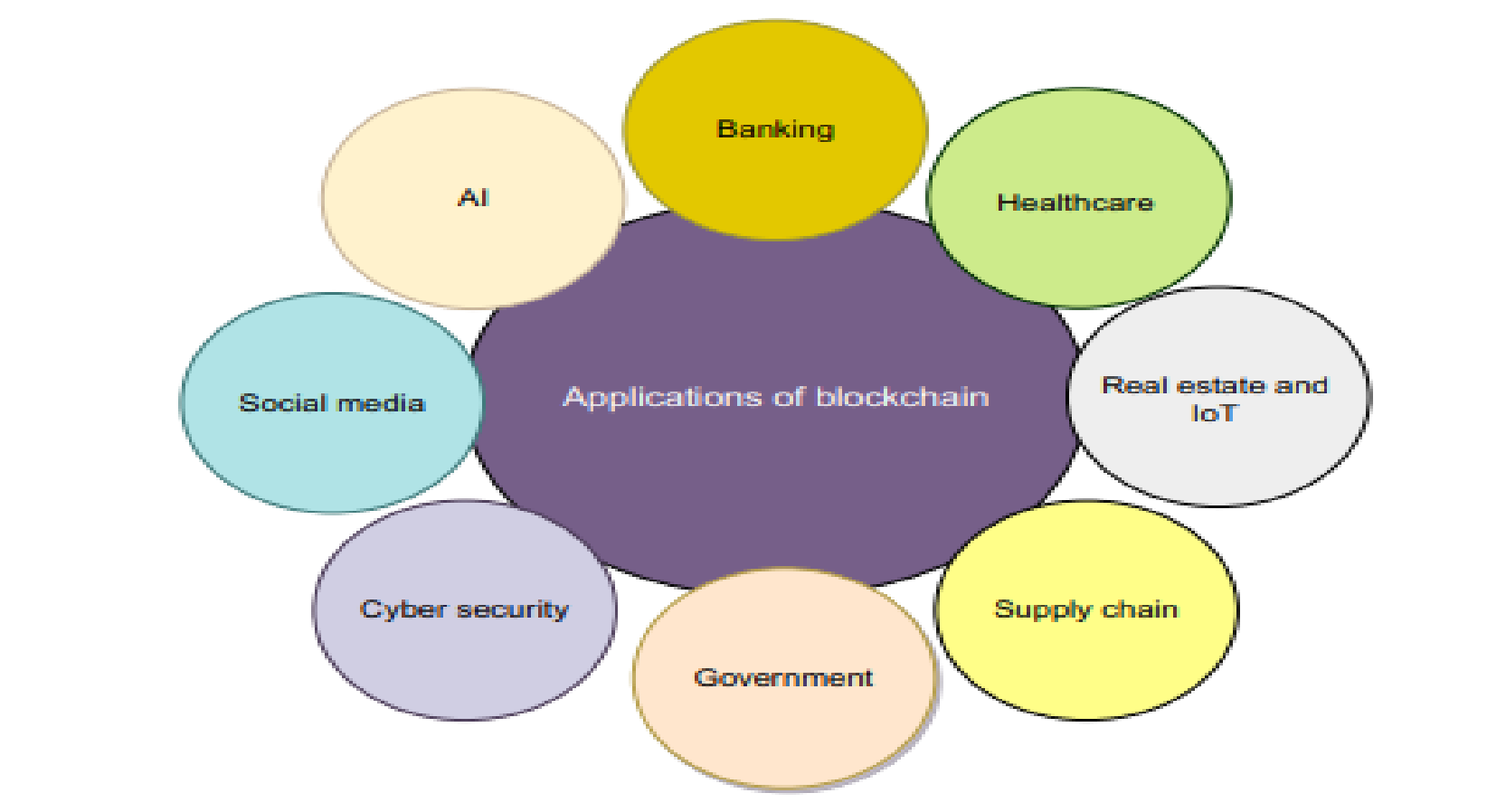
- **Side chains:**

  Sidechains are secondary block chains connected to the main block chain, allowing independent operation but maintaining interoperability. They help with scalability and testing new features without disrupting the main block chain.

- **Oracles:**

  Oracles are external data sources that provide real-world information to block chains, enabling smart contracts to react to events outside the block chain (e.g., weather data for insurance contracts).

Application of block chain



- (Krishnan, 2020)

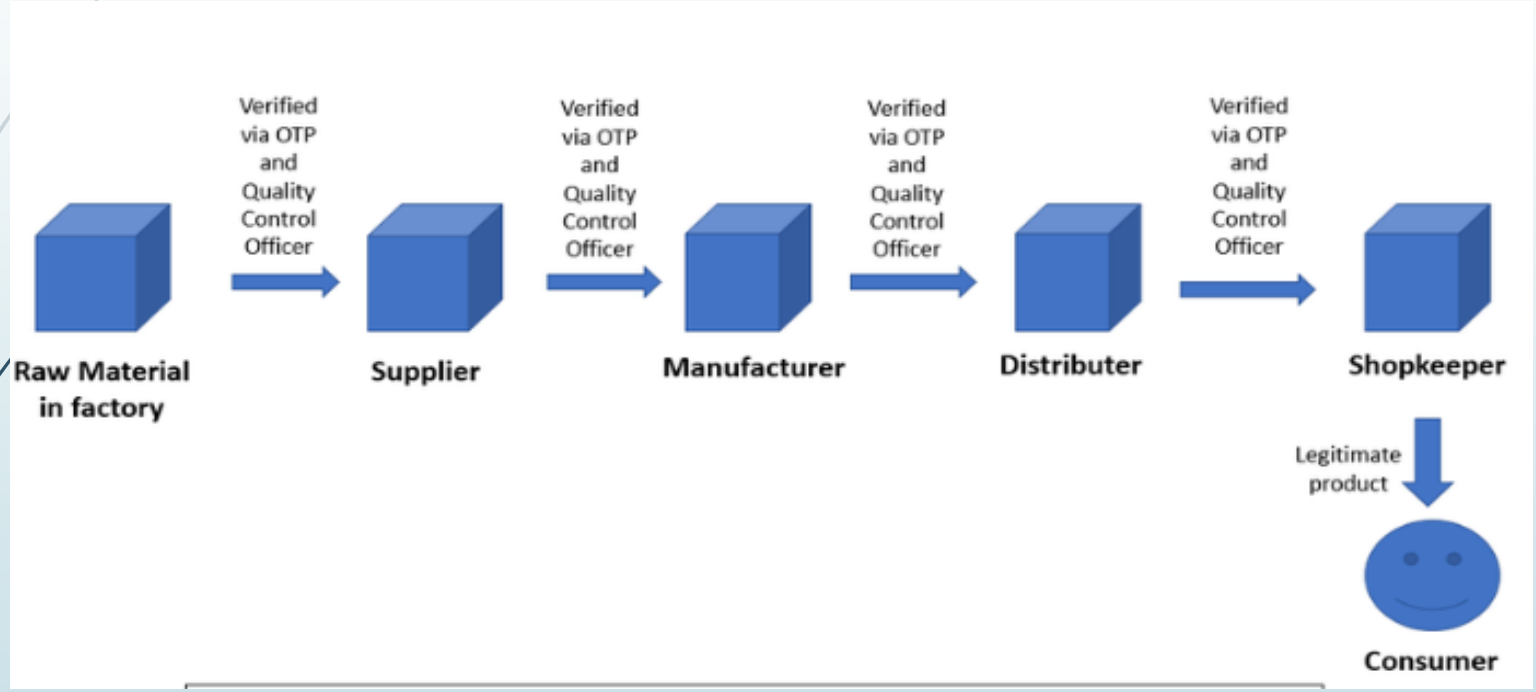
- **Block-chain in Financial Services:**
  Block-chain technology (BCT) has numerous applications in banking and financial services, offering benefits like automating transactions without intermediaries. Some key uses include:
- **Cross-border Transactions**: Block-chain enables fast and inexpensive cross-border transactions, bypassing the slow, costly processes of traditional banking systems.
- **Smart Bonds**: These are bond contracts that use block-chain for registration and enable instant settlements.
- **Point of Sales Systems**: BCT facilitates crypto currency payments at merchants, cutting down fees associated with traditional payment systems.
- **Bookkeeping and Auditing**: Block-chain allows real-time audits, making financial records verifiable and accurate through immutable data and hash strings.

- **Block chain in Insurance:**
  Block chain is transforming the insurance sector by streamlining processes and enhancing security and transparency. Key applications include:
- **Auto Insurance**: Block chain reduces paperwork and improves claims processing for vehicle insurance.
- **Travel Insurance**: Block chain offers more efficient claims processing for travel insurance, especially in cases like flight delays.
- **Block chain in Healthcare:**
  Block chain technology can significantly improve the healthcare sector by enhancing interoperability, data storage, security, and cost-efficiency. Benefits include:

- **Interoperability**: Enables seamless data sharing across healthcare systems for better services.
- **Data Storage & Analytics**: Block chain provides secure, immutable storage for patient data and allows for better data analytics.
- **Block chain Applications in Voting:**
  Block chain can enhance voting systems by eliminating central control and reducing manipulation risks. Notable projects include:
- **Block chain in Real Estate:**
  Block chain is revolutionizing the real estate industry by enabling secure, cost-effective transactions between buyers and sellers. It lowers transaction fees, eliminates intermediaries, and simplifies property ownership and rental processes through smart contracts.

Block chain in Supply Chain Management

Block chain is improving supply chain management by offering better provenance tracking, inventory management, identity verification, and shipping logistics. Key use cases include



https://www.researchgate.net/figure/The-proposed-system-model-for-block-chain-based-supply-management_fig2_353971876

- **Block chain in the Music Industry:**

  Block-chain transforms the music industry by enabling direct artist-to-fan interactions and transparent revenue sharing. Key use cases include:

- **Revenue Sharing**:
- **Tokenized Fandom**:
- **Media Ecosystems**:
- **Block-chain in Identity Management:**

  Block-chain is used to enhance data accuracy, security, and accessibility in identity management. Key use cases include:

- **Data Collection & Analysis**:
- **E-Residency**:

Benefits of Block chain Technology

- **Transparency:** Block-chain provides a transparent network where all participants can observe ongoing transactions, ensuring accountability and reducing discrepancies. The distributed ledger makes it easy for everyone to track transactions in real-time.
- **Security:** Block chain offers robust security by using a system where each block is interconnected through hashes. Altering one block spoils the entire chain, making it nearly impossible to hack. The cost and time required to breach the system make it highly secure, and hacking becomes futile.
- **Cost-effectiveness:** Block-chain eliminates the need for physical offices and reduces the high fees typically associated with traditional financial transactions. Without intermediaries, financial services become more affordable for users.
- **Secure Platform for Intellectual Property:** Block-chain creates a secure digital platform that guarantees intellectual property protection. For example, artists can register their work with a digital signature, ensuring they receive fair payment and recognition for their creations, preventing their work from being lost or exploited.

Benefits of Block chain Technology

- **Better Contribution Economy:** Block-chain fosters a trusted network for buyers and sellers to trade directly without third parties. This creates a more efficient marketplace, lowering costs for traders and allowing them to earn more profit, thereby boosting the economy.
- **Prevention of Payment Scams:** Block-chain helps prevent fraud by using smart contracts to ensure that once a coin is spent, it cannot be used again. This eliminates the possibility of corruption or discrepancies in payments. Additionally, transactions are secured with digital signatures from both parties, providing further protection against fraud.
- **Faster Transactions:** Block-chain enables rapid money transfers and document exchanges, saving time. Traditional payment systems often involve lengthy processes with third-party intermediaries, leading to delays in transactions. Block-chain reduces these inefficiencies by enabling instant transactions.

Cryto currencies

- The concept of block chain originated from a white paper published by Nakamoto Satoshi in 2008. Block chain, also known as a distributed ledger, consists of consecutive blocks linked together using the hash value of the previous block's header.
- Crypto currencies are digital or virtual assets that use cryptography to secure transactions. These currencies operate on decentralized networks, typically powered by block chain technology, which serves as a public ledger to document all transactions across a distributed network of computers. This decentralized structure helps prevent fraud, manipulation, and interference from central authorities like banks or governments

Key features of crypto currencies include

- **Decentralization**: Most crypto currencies function on decentralized networks where no central authority controls them. Transactions are verified and recorded by a global network of computers (nodes).
- **Block chain**: Block chain technology underpins most crypto currencies. It acts as a public ledger that records all transactions in "blocks," ensuring both transparency and security.
- **Cryptography**: Cryptographic methods are used to secure transactions, regulate the creation of new units, and confirm the transfer of assets, making crypto currencies highly secure.

Key features of crypto currencies include

- **Anonymity and Pseudonymity**: Crypto currencies offer more anonymity compared to traditional financial systems. While transaction histories are recorded on the block chain, the identities of the parties involved can remain private.
- **Ownership**: Users control their funds through private keys, which are essentially passwords granting access to their crypto currency wallets. Losing the private key means losing access to the funds.

Examples of crypto currencies

- **Bit coin (BTC)**: The first and most recognized crypto currency, created in 2009 by the pseudonymous Satoshi Nakamoto.
- **Ethereum (ETH)**: Known for enabling smart contracts and decentralized applications (dApps) alongside its role as a digital currency.
- **Ripple (XRP), Litecoin (LTC),** and **Cardano (ADA)** are other notable crypto currencies.

Risks of Investing in Bit coin:

- **Market Volatility**: Bit coin's price is highly unpredictable, with significant fluctuations. For instance, on November 6, 2018, Bit coin was valued at $6,461.01. To mitigate losses, it's recommended to make small, long-term investments.
- **Cybertheft**: Being technology-based, Bit coin is susceptible to hacking. There have been instances where mining or exchange platforms have been targeted, and even wallet applications, despite security measures, are at risk.
- **Fraud**: In addition to hacking, fraudulent activities in Bitcoin trading can occur, especially with fake exchanges. The lack of robust security systems increases risks for large investors.

Risks of Investing in Bit coin:

- **Lack of Regulation**: The Bit coin market operates without clear government regulations, and there is no specific stance on crypto currency. The absence of taxation can make it appealing for some investors, but the market's future is uncertain.
- **Technology Dependence**: Bit coin relies entirely on digital platforms for mining, exchange, and storage. Unlike traditional assets like gold or real estate, it has no physical backing or collateral.
- **Limited Acceptance**: While Bit coin represents a new form of monetary exchange, only a limited number of businesses currently accept it, restricting its practical use.

Risks of Investing in Bit coin

- **Financial Loss**: Bit coin investments are prone to creating speculative bubbles. When these bubbles burst, the value of Bit coin may drop significantly, resulting in financial losses for those holding the crypto currency.

References

1. Chandrashekhara, J. (2021). A Comprehensive Study on Digital Signature. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, 1-5.
2. Huynh-The, T. (2023). Block-chain for the metaverse: A Review. *Future Generation Computer Systems*, 1-19.
3. Krishnan, S. (2020). *Handbook of Research on block chain technology.* Chennai, India: Mara Conner.