ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal
Bi-monthly
Open Access

DESIGN AND DEVELOPMENT OF A BLOCKCHAIN-BASED DIGITAL IDENTITY ECOSYSTEM USING CRYPTOGRAPHIC AND CONSENSUS ALGORITHMS

Jitendra B. Kapade[1], Rakesh S. Deore[2]
[1,2] Research Scholar, Department of Computer Science, S.S.V.P.S'sL.K. Dr. P.R. Ghogrey Science College, Dhule, Maharashtra, India.
Email: jitendra.kapade@gmail.com[1], rakeshsdeore@gmail.com[2]

Abstract
An immutable ledger that is kept in a dispersed network of peers that are not trusting one another is known as a blockchain. It is used to record transactions in a verifiable and permanent manner. A copy of the ledger is kept by each peers. To validate transactions, the peers use a consensus mechanism. They then organise the transactions into blocks and create a hash chain over the blocks. As required for consistency, this procedure arranges the transactions to create the ledger. For his well-known creation of digital cash, or crypto currency, such as Bitcoin, Satoshi Nakamoto (presumed pseudonymous person or persons) developed Blockchain technology. Bitcoin's double spending issue was resolved by Nakamoto using Blockchain technology, but this innovative technology quickly found use in a wide range of other applications.The blockchain-based digital identity system employs well-established cryptographic and consensus algorithms such as RSA, SHA-256, RSA-SHA256, and Proof of Authority to ensure security, integrity, confidentiality, and decentralization. These algorithms collectively provide a robust foundation for trustworthy digital identity management. In this paper we discuss various algorithms for Digital Identity using Blockchain Teachnology

Keywords: Blockchain, Smart Contract, Techniques, Consensus Algorithms.

► *Corresponding Author: Jitendra B. Kapade*

I. Introduction

Blockchain is essentially a series of blocks that together form a public ledger that records all committed transactions(Salah K. 2019). When fresh blocks are added to the chain, it keeps growing. A number of fundamental technologies, including distributed consensus methods, digital signatures, and cryptographic hashes, enable the decentralised environment in which blockchain operates. Since all of the transactions take place in a decentralised fashion, no middlemen are needed to validate and verify the transactions (Litke, D. Anagnostopoulos and T. Varvarigou 2019). Key features of blockchain include auditability, immutability, transparency, and decentralisation(Kouhizadeh and J. Sarkis 2018).

Services, Industry 4.0, share trading, and smart cities. Instead of depending on a single controlling authority, it uses a distributed ledger system in which digital data is synchronized, shared, and copied across multiple servers. This distributed structure guarantees more security, dependability, and transparency in data management. In basic terms, every block in a blockchain is a digital record made up of three crucial parts: the transaction data itself, a cryptographic hash connecting

the current block to the one before it, and a timestamp marking the time the transaction took place. Transactions between parties can be permanently and verifiably recorded thanks to this structure, which creates a safe, unchangeable chain of records.

Nodes (computers) in the peer-to-peer system that manage the blockchain network communicate information and verify transactions using a consensus process. A transaction is considered immutable once it has been confirmed and added to the blockchain. In order to change its content, all previous blocks in the chain would need to be recalculated and changed, which would take an enormous amount of processing power and make such tampering nearly impossible. Blockchain is special because of a few important features. Since it is fully decentralized, no one entity or person has authority over the network. Immutability strengthens security and trust by ensuring that a transaction cannot be removed or altered once it has been recorded. Users may create Blockchain addresses for transactions using pseudo-anonymity without disclosing their true identities. When suitable steps are taken, it is impossible to link an address to a specific person. Because of these features, Blockchain is a trustless system, meaning that users can conduct transactions without having to trust one another. Rather, the technology itself is trusted since its design and procedures ensure that private data is transferred securely over an unidentified network of participants. Because of this, Blockchain is a potent instrument to boost openness, decrease fraud, and enable safe digital transactions across a range of sectors.

II. Structure of Blockchain

Bitcoin is one of the most well-known examples of blockchain technology. It was first established in 2008 as a cryptocurrency and payment system(Bitcoin 2008). When a seller or payer makes a transaction, digital assets like bitcoin are transferred within a blockchain(P. 2016) as shown in figure A.

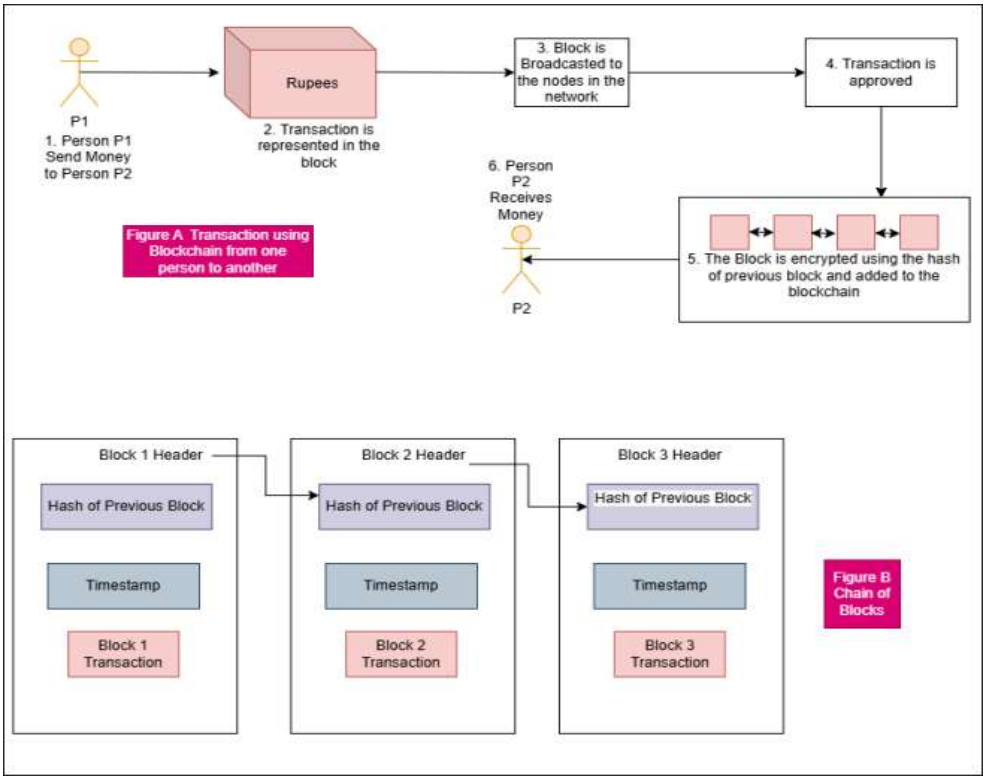
Every peer linked to the blockchain network receives these transactions, and clients known as miners use a cryptographic procedure to verify the transaction. The two main issues with digital currency exchange that were previously resolved by this validation are making sure the digital asset is real and hasn't been used up. If a miner determines that a transaction is well-formed (the input and output only contain the fields specified in the protocol) and that the outputs it seeks to transmit are there, the transaction is considered legitimate.

Anyone who offers to invest their resources can be a miner; they are not required to be certified. Bitcoin, which is created and given to miners for each block of transactions that are verified, serves as an incentive for miners. The necessary software is easy to use and may be downloaded for free. A block containing the details of confirmed transactions, a time stamp, and a cryptographic hash—a mathematically produced string of alphanumeric characters—is created once a transaction has been verified by a predetermined number of clients.

After adding the block with the transaction details to the blockchain's end, the receiving party receives the transferred assets. An essential component of the blockchain is the one-way cryptographic hash, which is generated using the hash of the block before it to create a unique digital signature exclusive to the current block of data as shown in figure B.Malicious alterations to the blockchain record are avoided since each block is safely connected to the block that came before it via the hash. One of the main characteristics of blockchain is its immutability.

This method differs from typical transaction processing in a number of useful ways. For instance, a merchant's payment processor confirms the availability of money when a credit card transaction is started, and after a few days, the funds are authorised and sent to the merchant. By creating a digital trust that promotes more effective transaction processing, blockchain as a digital ledger

seeks to eliminate these middlemen. In a blockchain setting, the network itself secures the transaction history, verifies the transaction, and permits direct asset transfers between participants after it has been digitally verified.



III. Cryptographic and Consensus Algorithms

Using Cryptographic and Consensus Algorithms we are able to design a Digital Identity using Blockchain. Here are some of the Algorithms used for digital identity management using blockchain:

1. Asymmetric Key Generation Algorithm (RSA)

RSA (Rivest–Shamir–Adleman) Algorithm:

The RSA algorithm is used for generating a public–private key pair for each identity owner. The public key is shared for encryption and signature verification, while the private key is securely stored by the user for signing and decryption operations.

Role in System:

RSA ensures secure identity ownership, authentication, and confidentiality. It prevents unauthorized users from impersonating identity holders.

2. Cryptographic Hashing Algorithm (SHA-256)

SHA-256 (Secure Hash Algorithm – 256 bit):

SHA-256 is a one-way cryptographic hash function that converts identity data into a fixed-length hash value. Any change in input results in a completely different output hash.

Role in System:

SHA-256 is used to generate identity fingerprints that are stored on the blockchain instead of raw personal data, ensuring privacy and integrity.

3. Digital Signature Algorithm (RSA-SHA256)

RSA Digital Signature Algorithm with SHA-256:

The RSA-SHA256 algorithm combines RSA asymmetric encryption with SHA-256 hashing to create digital signatures. The identity owner signs the identity hash using their private key, and the signature is verified using the corresponding public key.

Role in System:

This algorithm provides authentication, non-repudiation, and integrity verification of identity data.

4. Data Encryption Algorithm (RSA-OAEP)

RSA-OAEP (Optimal Asymmetric Encryption Padding):

RSA-OAEP is used to encrypt identity information using the public key of the recipient. It introduces randomness into encryption, making it secure against chosen-plaintext attacks.

Role in System:

RSA-OAEP ensures confidentiality of identity data shared between users, validators, and service providers.

5. Smart Contract Execution Algorithm (Deterministic State Machine)

Ethereum Smart Contract State Transition Algorithm:

Smart contracts operate as deterministic finite state machines. Given the same input and initial state, every blockchain node produces the same output state.

Role in System:

This algorithm guarantees consistent identity registration and verification across all blockchain nodes without centralized control.

6. Blockchain Consensus Algorithm

- **Proof of Authority (PoA)** – Private Ethereum Testnet
- **Proof of Stake (PoS)** – Public Ethereum Network

The consensus algorithm validates transactions and ensures agreement among distributed nodes before adding blocks to the blockchain.

Consensus algorithms maintain ledger integrity, fault tolerance, and immutability of identity records.

7. Identity Verification Algorithm (Hash & Signature Matching)

Hash Comparison and Digital Signature Verification Algorithm:

The verification process recomputes the SHA-256 hash of decrypted identity data and compares it with the hash stored on the blockchain. The RSA-SHA256 signature is then verified using the public key.

Role in System:

This algorithm ensures that identity data is authentic, untampered, and owner-authorized.

8. Access Control Algorithm (Owner-Based Authorization)

Role-Based / Owner-Based Access Control Algorithm:

Access control is enforced within the smart contract by verifying the caller's blockchain address against the registered identity owner.

Role in System:

This algorithm prevents unauthorized access and ensures user-centric control of digital identities.

9. End-to-End Algorithm Integration

Decentralized Identity Management Workflow Algorithm:

This algorithm integrates cryptographic operations, blockchain transactions, and smart contract execution into a single secure workflow.

Role in System:
It enables secure, decentralized, and privacy-preserving identity creation, storage, and verification.

IV. Conclusion

The blockchain-based digital identity system employs well-established cryptographic and consensus algorithms such as RSA, SHA-256, RSA-SHA256, and Proof of Authority to ensure security, integrity, confidentiality, and decentralization. These algorithms collectively provide a robust foundation for trustworthy digital identity management.

To sum up, blockchain-based digital identity management offers a viable route to a user-controlled, privacy-focused, and safer identity ecosystem. To improve these ideas and create standardised frameworks for broad adoption, cooperation between governments, businesses, and researchers will be crucial.

V. References

1. A.S.Konoplev, A.V. Chekhov , A.V. Bogatov. “"A Blockchain Decentralized Public Key Infrastructure Model".” (Researchgate) 2018.
2. Agbo C.C., Mahmoud Q.H. & Eklund J. M. *"Blockchain Technology in healthcare : A Systematic review"*. Multidisciplinary Digital Publishing Institute, 2019.
3. Agora. *"Agora: Bringing our voting systems into the 21st Century*. Agora, 2017.
4. Bakre, Akshay, Nikita Patil, and Gupta Sakshul Vaneet . “Implementing Decentralized Digital Identity Using Blockchainb.” *International Journal of Engineering and Technology Science and Research*. Hyderabad, Oct. 2017. 8.
5. Bitcoin, Nakamoto S. “A Peer-to-Peer Electronic Cash System.” 2008.
6. Bodell, William E. *"Farm Share : Blockchain Community-supported Agriculture*. White Paper, 2015.
7. El Haddouti, S. & El Kettani, M.D.EC. “"Analysis of Identity Management System using Blockchain Technology".” 2019. 1-7.
8. Kouhizadeh, M., and J. Sarkis. “Blockchain practices, potentials, and perspectives in.” *Sustainability* 10 (2018): 3562.
9. Litke, A., D. Anagnostopoulos, and T. Varvarigou. “Blockchains for supply chain: Architectural elements and challenges towards a global scale deployment.” *Logistics*, 2019: 5.
10. Meng Han, Zhigang Li, Jing (Selena) He, Dalei Wu, Ying Xie, nad Asif Baba. “"A Novel Blockchain -Based education records verification solution.” *19th Annual SIG Conference on Information Technology Education*. 2018. 178-183.
11. Mengelkamp E., Garttner J. ,Rock K, Kessler S, Orsini L & Weinhardt C. “"Designing microgrid energy markets: A Case study ".” *I*. The Brooklyn Microgrid. Applied Energy , 2018. 870-880.
12. Mettler, M. “"Blockchain Technology in Healthcare : The revolution starts here".” IEEE, 2016. 1-3.
13. Naik N., Jenkis P. “"Self-Sovereign Identity Specifications : Govern your Identity through your digital wallet using blockchian technology".” IEEE, 2020. 90-95.
14. Nikos Fotiou, Iakovos Pittaras, Vasilios A. Siris, Spyros Voulgaris, George C. Polyzos. “OAuth 2.0 Authorization Using Blockchain-Based Token".” *arXiv preprint arXiv :2001.10461*, 2020.
15. P., Forrest. *"Blockchain and Non Financial services use cases*. linkedin, 2016.
16. Patrick McCorry, Siamak F. Shahandashti, and Feng Hao. *"A Smart Contract for Boardroom Voting with Maximum Voter Privacy"*. IACR, 2017.

17. Popper, N. *Business giants to announce creation of a computing system based on Ethereum.* The New York Times, 2017.
18. Salah K., Rehman, M. H. U., Nizamuddin N., Al-Fuqaha A. “Blockchain for ai : Review and open research challenges.” *IEEE Access*, 2019: 10 127-10 149.
19. Tasfia Rahman, Sumaiya Islam Mouno, Arunangshu Mojumder Raatul, Abul Kalam Al Azad, Nafees Mansoor. “"Verifi- Chain : A credential Verifier using Bklockchain and IPFS".” *arXiv preprint , arXiv :2307.05797*, 2023.
20. Wolfond, Grerg. “ A Blockchain Ecosystem for Digital Identity Improving Service Delivery in Canada’s Public and Private Sectors.” *timereview.ca.* Technology innovation management Review, Oct. 2017. 7.
21. Xiaohui Yang, WenjieLi. *A Zero Knowledge Proof Based Digital Identity Management Scheme in Blockchain.* Elsevier, 2021.