International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-12, Issue-5 September 2024
https://doi.org/10.55524/ijircst.2024.12.5.9
Article ID IRP-1557, Pages 68-72
www.ijircst.org

# Blockchain Voting System- An NFT-Based Approach

**Anshjyot Singh Wadhwa**

B.Tech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India

Correspondence should be addressed to Anshjyot Singh Wadhwa; anshjyotw@gmail.com

Received 27 August 2024; Revised 9 September 2024; Accepted 23 September 2024



**ABSTRACT-** This study introduces an innovative blockchain-based voting system that leverages non-fungible tokens to enhance the integrity, openness, and accessibility of elections. By harnessing the decentralized nature of blockchain and the distinctive characteristics of NFTs, the proposed system aims to address common vulnerabilities in traditional voting methods. The research findings indicate that a blockchain-based voting system utilizing NFTs can substantially improve election integrity. NFTs are employed to authenticate voter identities, bolstering security and mitigating fraudulent activities. Additionally, the public blockchain ledger ensures the permanent recording of votes, promoting transparency and confidence in election outcomes. Furthermore, the internet-enabled voting approach allows participation from any location, reducing barriers to voter engagement and improving accessibility.

This paper examines the technical implementation of the proposed system, including the application of smart contracts and cryptographic methods to protect the voting process. It also explores potential obstacles and areas for future investigation, highlighting the transformative potential of this approach in democratic procedures.

**KEYWORDS-** Blockchain, Non-Fungible Tokens, Smart Contracts, Decentralized Voting, Cryptographic Voting, Immutable Public Ledger.

## I. INTRODUCTION

A distributed ledger system called blockchain makes it possible to securely and decentrally record transactions across numerous computers. A peer-to-peer network known as a blockchain allows every user (or node) to access the complete ledger in contrast to traditional centralized databases that store data in a single location. This decentralized structure makes sure that once information is recorded it cannot be changed without the network's approval. Transactions are grouped into blocks and the term blockchain comes from the way each block is connected to the one before it via cryptographic methods. Blockchains key characteristics security and transparency make it appropriate for a variety of uses from supply chain management to cryptocurrency. Voting systems can benefit greatly from blockchain technology specifically from its capacity to produce an unchangeable publicly verifiable record of transactions. In large-scale or distant elections in particular traditional voting methods are frequently plagued by problems like fraud manipulation and less transparency. These problems can be solved by blockchain technology by nature. A key component of improving the security and operation of a blockchain-based voting system is the use of non-fungible tokens (NFTs), a specialized application of blockchain technology. Unlike crypto currencies Soul bounded non-fungible tokens (NFTs) are distinct digital assets that cannot be split copied or traded one to one. NFTs are ideal for representing individual voter identities in elections because each one has a unique identifier. Since each NFT represents a single authenticated identity we can make sure that no duplicate votes are cast by giving each voter a unique NFT.

Improving the voting process traceability and responsibility can too be fulfilled through the utilization of NFTs in blockchain-based voting frameworks. Each NFT implying an unmistakable voter personality is recorded on the blockchain ensuring that each vote is recorded and that no one can cast a vote for the sake of another person. This makes strides in decision judgment and eases stresses of voter pantomime. Furthermore the voting prepare can be mechanized in a number of ways by joining savvy contracts another basic blockchain innovation include. A keen contract might be utilized in a voting situation to naturally check votes, confirm qualification and make beyond any doubt that the strategy is carried out in agreement with the rules without the requirement for human association. This brings down the plausibility of human mistake and controls upgrading decision security indeed more. Since blockchain voting is conveyed there is no single substance in charge of the preparation making it safe to hack or control. Each hub in the organization has a duplicate of the total record making it about inconceivable for one party to alter the results without the endorsement of the larger part of organized clients. Since the handle is straightforward and irrefutable voters and decision organizers are more likely to have tall levels of belief. Moreover voter protection can be protected through the utilization of zero-knowledge proofs. Without unveiling the genuine data a party can illustrate their information of a specific piece of data (like their vote) through zero-knowledge proofs. This ensures exact and unquestionable vote tallying without compromising the secrecy of the votes.

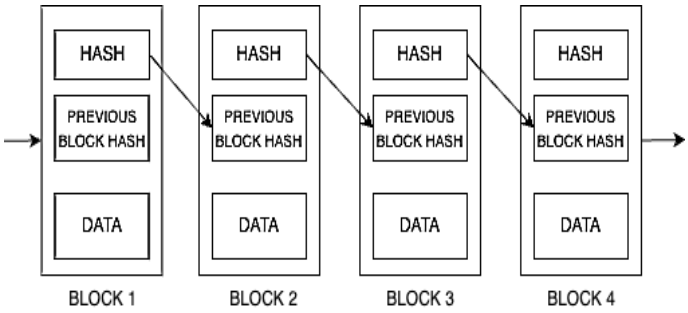


Figure 1: Blockchain Structure

Each square contains a set of exchanges, counting voting information, and a one of a kind cryptographic hash of its substance [1]. This hash incorporates a reference to the past block's hash, guaranteeing that any modification to a piece would require changing all consequent pieces. This structure makes an unchanging and secure chain, making blockchain safe from altering and extortion whereas keeping up straightforwardness and believing in the recorded information, counting voting data as shown in Figure 1.

## II. ISSUES/CHALLENGES IN CURRENT VOTING SYSTEM

In this section, we'll look at the challenges and issues related to the current voting system [2].

### *A. Security*

Considering the growing sophistication of cyber threats, voting machine security is a serious concern in modern elections. Election integrity is compromised by voter fraud, which includes multiple voting and voter impersonation. Election process fairness may be jeopardized by cases where voters vote on behalf of others or vote more than once. Furthermore, hackers and tamperers can manipulate electronic voting systems by taking advantage of flaws in order to change the results or interfere with normal operations. Sensitive voter information is exposed in data breaches, which worsens these problems by raising concerns about privacy violations and eroding public trust in the system. To reduce these dangers and guard against unwanted intervention with the democratic process, it is imperative to have strong security measures in place.

### *B. Accuracy and Reliability*

Accuracy and reliability are essential for preserving public confidence in the democratic process. Voter fraud, whether from technological or human error, can have a big influence on the results of elections. Discrepancies between reported and actual vote totals might arise from malfunctioning voting machines or data input errors. Software problems or other system issues may cause the voting process to be disrupted, delaying the results. These problems show how important it is to have trustworthy and proven voting technology in order to guarantee accurate vote counting and seamless system operation throughout the election.

### *C. Accessibility*

To ensure that all eligible voters may cast ballots in elections, voting methods must be inclusive and accessible. When traditional polling places and apparatus are not made to accommodate people with disabilities, physical accessibility concerns occur. Certain voter groups may be denied the right to vote due to inadequate provisions for wheelchair users or people with visual impairments. These issues are made more difficult by the digital divide since unequal access to technology can limit voters' participation, especially in online voting. In order to assure fair and equal participation, addressing these concerns necessitates building voting methods that are accessible to everyone, regardless of physical ability or technological resources.

### *D. Transparency*

Trust and transparency are essential to an election's legitimacy. Election integrity and fairness may be questioned in the event that there is a lack of openness in the voting process. Voters' and stakeholders' concerns about the electoral process may surface if they are unable to independently confirm the method used to tally votes or produce results. Perceptions of prejudice, corruption, or inefficiency have an impact on the public's confidence in elections. Voter fraud and tampering allegations have the potential to undermine public faith in the electoral process, hence it is critical to establish transparent procedures and make information easily comprehensible about how voting is handled and overseen.

### *E. Cost and Efficiency*

Significant difficulties for election management arise from the expense and effectiveness of voting systems. Election budgets may be strained by the high expenses of deploying and maintaining voting technology, which include buying machines, creating software, and guaranteeing security. In addition, overseeing the intricate and resource-intensive process of managing voting logistics, which includes creating and distributing ballots, running polling places, and tallying results. The aforementioned reasons highlight the necessity of finding economical and effective solutions that strike a balance between technological progress and pragmatic considerations in order to guarantee the smooth and budget-conscious conduct of elections.

## III. METHODOLOGY

To create a successful NFT-based blockchain voting framework, a comprehensive strategy must be taken after, including framework plan, blockchain setup, NFT improvement, voting preparation integration, arrangement, security, and nonstop enhancement.

We start by characterizing the center targets of the voting framework, centering on upgrading security, straightforwardness, and proficiency. Locking in with

partners, counting race specialists and potential voters, permits us to accumulate nitty gritty necessities, guaranteeing that the framework meets their needs. We will plan a high-level design that coordinates the blockchain arrange, NFT issuance, voting components, and client interfacing. Each component, such as savvy contracts and NFT tokens, will be clearly characterized with particular parts and obligations to guarantee a cohesive framework. each quantity in an equation.

For the blockchain arrange, we will select a vigorous stage like Ethereum, which underpins keen contracts and NFT benchmarks such as ERC-721 or ERC-1155. This choice is based on the platform's adaptability, security highlights, and cost-effectiveness. We will arrange, count, set up hubs and choose an agreement component (Confirmation of Stake or Verification of Work) based on our security and execution needs. If a private or consortium blockchain is utilized, we will build up essential authorizations and get to controls to secure the arrangement. We will characterize and execute the NFT guidelines essential for our voting framework. This incorporates creating shrewd contracts for the creation, issuance, and administration of NFTs, guaranteeing that each NFT has an interesting identifier and metadata. These NFTs will be connected to personal voter characters to guarantee that each voter is extraordinarily spoken to and verified. Our execution will incorporate components to confirm NFT genuineness and anticipate the duplication or abuse of votes. Figure 2 shows the function, where users can mint a unique Voter ID (non-transferable NFT) [3].

```
function mintVoterID() external {
 require(whitelist[msg.sender], "");
 require(!hasMinted[msg.sender], "");
 tokenIdCounter++;
 _safeMint(msg.sender, tokenIdCounter);
 hasMinted[msg.sender] = true;
}
```

Figure 2: Code block to define Soulbound NFT minting function

The voting instrument will be coordinated through savvy contracts that handle different perspectives of the voting handle, counting vote accommodation, counting, and result confirmation. We will guarantee that these shrewd contracts are modified to avoid twofold voting and ensure precise vote checking. At the same time, we will create instinctive client interfacing to encourage simple voting by clients. These interfacing will be open by means of both versatile and web stages, and thorough testing will be conducted to guarantee that all components work accurately and safely.

Once the savvy contracts and voting framework are prepared, we will send them to the blockchain organization. This sending will be taken after by the system's dispatch, either for pilot testing or genuine decisions. To guarantee a smooth move, we will give comprehensive back and prepare for clients. Nonstop observing will be executed to address any execution or security issues expeditiously, with standard support to keep the framework operational and compelling. We will execute exacting security measures to defend information and guarantee the judgment of the voting prepare. This incorporates utilizing progressed cryptographic strategies to ensure exchange information and voter personalities. Compliance with lawful and administrative guidelines will be thoroughly upheld to address information security and assurance necessities, guaranteeing that the framework follows all pertinent directions.

One of the key standards in decisions is guaranteeing voter namelessness whereas keeping up vote keenness. The framework will utilize cryptographic strategies such as zero-knowledge proofs (ZKPs) to permit voters to demonstrate they have voted without uncovering their vote's substance. By utilizing ZKPs, we can guarantee that the framework does not uncover individual voting inclinations whereas still affirming that the vote was tallied. Additionally, homomorphic encryption may be connected, permitting for vote counting to happen on scrambled votes, protecting privacy without requiring unscrambling as shown in Figure 3. This guarantees that votes stay private all through the whole preparation whereas guaranteeing straightforwardness in the last count.


Figure 3: Zero Knowledge Proofs

Building voters' belief in the framework is basic for broad selection. The administration of the blockchain framework will guarantee straightforwardness and reasonableness. Decentralized administration instruments will be actualized where voting specialists or trusted partners inside the arrange can propose changes to the framework, but these changes would require a lion's share agreement from the community to be ordered. This decentralization anticipates any single substance from picking up control of the voting handle. Moreover, to build up belief, we will use an open key framework (PKI) to sign and confirm the keenness of each vote, guaranteeing that no vote is altered once casted [4]. In below Table 1 is compare the security mechanisms used in current voting systems versus NFT-Based blockchain voting systems.

Table 1: Current vs. NFT-Based Blockchain Security

| **Security Aspect** | **Current Voting** | **NFT-Based Blockchain Voting** |
|---|---|---|
| Voter Identity | In-person | Verified digital identity through NFTs |
| Vote Tampering Prevention | Manual monitoring | Cryptographic proofs |
| Fraud Detection | Post-election audits | Real-time, transparent transaction verification |
| Data Privacy | Potential risk of leaks | Encrypted data |
| Vote Counting | Manual | Automated |

To build up a secure and unquestionable voting handle, our NFT-based blockchain voting system joins a comprehensive character confirmation instrument. Central to this handle is the issuance of a special, non-transferable NFT that capacities as the voter's advanced character. This approach starts with a thorough Know Your Client (KYC) strategy, where voters must give substantial government-issued IDs, biometric information, or other secure character proofs [5]. Upon effective confirmation, each voter is issued a particular NFT, which is put away in their computerized wallet and speaks to their confirmed voting character as appeared in Figure 4.

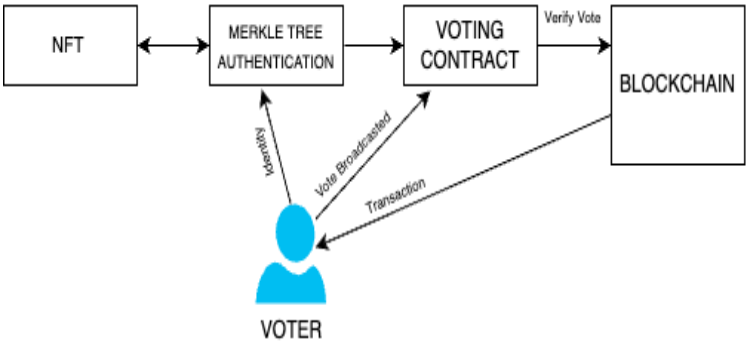


Figure 4: Identity Authentication mechanism

## IV. IMPLEMENTATION

The usage of a blockchain-based voting framework utilizing Non-Fungible Tokens (NFTs) includes different steps, enveloping framework engineering, keen contract advancement, voter confirmation, and the voting handle itself. The arrangement leverages the inalienable properties of blockchain—transparency, permanence, and decentralization—to address common issues in conventional voting frameworks such as extortion, altering, and the need of straightforwardness. Underneath is a point by point depiction of the whole project's usage.

### *A. Framework Architecture*

The design of the NFT-based blockchain voting framework is planned to guarantee security, versatility, and ease of use [6]. The framework is built on the Ethereum blockchain, utilizing savvy contracts and NFTs to speak to interesting voter characters. The design comprises of three primary components:

- Frontend Voting Interface: A web-based interface (DApp) that permits clients to enroll, confirm, and cast their votes. It gives a user-friendly voting encounter and interatomic straightforwardness with the blockchain by means of keen contracts.
- Backend Foundation: The backend handles the creation and administration of NFTs, verification, and interaction with the Ethereum blockchain. It forms the enlistment of voters, stores advanced characters safely, and guarantees smooth execution of the voting process.
- Blockchain Layer: The Ethereum blockchain serves as the decentralized record, putting away all voting exchanges and NFTs. Shrewd contracts sent on this layer oversee the voting rationale, implement security rules, and count votes naturally.

Figure 5 shows the framework architecture of the NFT-based blockchain voting system

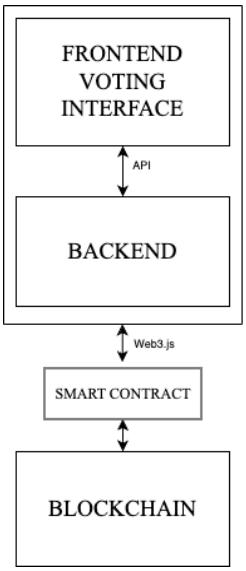


Figure 5: Framework Architecture

### *B. Voter Enlistment and NFT Issuance*

A key component of this system is the utilization of NFTs to speak to voter characters. The voter enrollment handle starts with personality confirmation, where qualified voters are required to confirm their personality utilizing government-issued IDs or biometric information. Once confirmed, the voter is formally enrolled in the framework. Taking after this, an NFT is made for each enrolled voter, with each NFT being interesting and "soulbound," [7] meaning it cannot be exchanged or traded. The NFT contains metadata that joins it specifically to the voter's computerized personality, guaranteeing that as it were one vote can be cast per voter. These NFTs are safely put away on the Ethereum blockchain, and since they are non-transferable, they anticipate any plausibility of numerous votes or personality exchanges. This guarantees a secure and tamper-proof voting preparation.

### *C. Voting Process*

Once enrolled, the voter can take an interest in the race through the secure voting interface fueled by blockchain innovation [8]. On race day, the voter logs into the framework utilizing their accreditations, where their character is verified through their one of a kind NFT, allowing them to cast their vote. After selecting their favored candidate or choice, the vote is scrambled and submitted through the interface. This vote is promptly recorded on the Ethereum blockchain, guaranteeing straightforwardness and permanence. A shrewd contract oversees the whole voting handle, connecting each vote to the voter's NFT, dispensing with any chance of copy voting, whereas moreover dealing with decision due dates and vote counting. Once the vote is finalized on the blockchain, the voter gets affirmation that their vote has been safely recorded and, due to the permanent nature of blockchain, the vote cannot be modified or erased [9].

### *D. Vote Counting and Result Verification*

The vote counting and result confirmation handle in the blockchain-based voting framework is computerized and controlled by keen contracts. As each vote is cast, the keen contract checks the votes in real-time, permitting for persistent checking without uncovering personal voter choices. The utilization of the blockchain as an open record guarantees straightforwardness, as all exchanges, counting votes, are recorded permanently and can be confirmed autonomously by race specialists, screens, or the open. Cryptographic strategies, such as encryption, keep up voter secrecy, whereas still making the by and large preparation unquestionable [10]. After the race concludes, the blockchain record can be inspected to affirm that each vote was precisely checked. Since the blockchain is permanent, any errors in the vote count would be instantly recognizable. Also, zero-knowledge proofs (ZKPs) may be utilized to advance confirmation of the rightness of the vote number without uncovering the subtle elements of personal votes, upgrading both security and straightforwardness [11].

Security is foremost in any voting framework, and the NFT-based blockchain voting framework addresses this comprehensively. It leverages the permanence of blockchain innovation to guarantee that once votes are cast, they cannot be changed or erased, hence disposing of the chance of altering. All votes are scrambled some time recently being included to the blockchain, protecting voter secrecy and anticipating traceability. One of a kind, non-transferable NFTs are utilized for voter confirmation, guaranteeing that as it were qualified people can vote and anticipating copy voting and pantomime. Also, the decentralized nature of the blockchain dispenses with central focuses of disappointment, essentially diminishing the chance of assaults or debasement compared to conventional centralized frameworks [12].

## V. CONCLUSION

The NFT-based blockchain voting framework speaks to a critical headway in discretionary innovation, combining the strength of blockchain with the uniqueness of NFTs to guarantee a secure, straightforward, and tamper-proof voting handle. By leveraging the permanence of blockchain, the framework ensures that once votes are cast, they stay unaltered and irrefutable, subsequently killing dangers related with vote altering and control. Cryptographic encryption encourages guarantees that each voter's choice remains private, securing voter protection. The utilization of non-transferable NFTs for voter verification gives a compelling instrument to anticipate copy voting and pantomime, guaranteeing that as it were, qualified voters take an interest. Also, the decentralized nature of the blockchain organization minimizes the chance of assaults and debasement by expelling central focuses of failure.

Beyond these center highlights, the NFT-based framework moreover encourages real-time following and inspecting of votes, upgrading the straightforwardness of the discretionary prepare. Voters and partners can freely confirm vote tallies and come about, which contributes to a higher level of responsibility. The system's plan too obliges versatility, making it reasonable for races of changing sizes, from nearby submissions to national races. Besides, by coordinating shrewd contracts, the framework can mechanize and streamline different voting methods, lessening authoritative overhead and human blunder. This present day approach not as it addresses conventional voting challenges but moreover sets an unused standard for discretionary keenness and productivity. As the innovation advances and gets to be more

broadly embraced, it has the potential to change the majority rule, cultivating more noteworthy belief and support in decisions around the world.

## VI. FUTURE SCOPE

The NFT-based blockchain voting framework has impressive potential for future progressions that seem to encourage upgrade its viability and selection. One promising zone is making strides interoperability with existing voting frameworks and coordination with other blockchain stages. This would make a more cohesive and versatile voting foundation, encouraging smoother moves and broader acknowledgment. Furthermore, progressing cryptographic strategies, such as zero-knowledge proofs, seem to offer indeed more grounded protection assurances for voters, guaranteeing that their choices stay private and secure. Upgrading client involvement through more instinctive interfacing and user-friendly applications will too be pivotal for expanding availability and empowering broad utilization, especially among people with changing levels of specialized expertise.

As the framework scales to handle bigger decisions, progressing optimization for execution and adaptability will be fundamental to keep up productivity and unwavering quality. Creating comprehensive administrative and legitimate systems will address compliance and lawful concerns, giving a strong establishment for the system's usage. Instructive activities to illuminate the open around the benefits of blockchain-based voting can construct belief and advance appropriation. Investigating synergies with developing innovations, such as fake insights and machine learning, might advance the system's capabilities, counting extortion discovery and prescient analytics. At last, advancing worldwide benchmarks and working towards universal selection can guarantee consistency and encourage cross-border decisions, clearing the way for a more straightforward and comprehensive law based handle. value as well as tutorial expositions and critical reviews of classical subjects and topics of current interest.

## REFERENCES


[1] G. Wood, "Ethereum: a secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014. Available from: https://www.scirp.org/reference/referencespapers?referenceid=3182670

[2] J. U. Aziz, M. J. A. Shukur, Z. "Blockchain for electronic voting system—review and open research challenges," Sensors, vol. 21, no. 17, p. 5874, 2021. Available from: https://doi.org/10.3390/s21175874

[3] VV Bhavani, K Saisri, K Naveen, M Lalitha, "Personalized Secure E-Identity Card," Journal of Advanced Research in Technology and Management Sciences, vol. 03, no. 04, pp. 1-12, July 2021. Available from: http://jartms.org/admin/uploads/j0ctnb.pdf

[4] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkılıç, "Towards Secure E-Voting Using Ethereum Blockchain," Available from: https://www.researchgate.net/publication/323318041_Towards_Secure_E-Voting_Using_Ethereum_Blockchain

[5] R. Zhang, R. Xue, L. Liu, "Security and privacy on blockchain," *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1-12, 2018. Available from: https://doi.org/10.1145/3316481

[6] A. Shukla, D. Mishra, A. Pattnaik, S. R. Salkuti, "Analysis and design on acceptance of blockchain based e-voting system," Indonesian Journal of Electrical Engineering and Computer Science, vol. 33, no. 3, pp. 1793-1801, 2023. Available from: https://doi.org/10.11591/ijeecs.v33.i3.pp1793-1801

[7] S. Reddy, D. S. Kushwaha, "Framework for privacy preserving credential issuance and verification system using soulbound token," *ITM Web of Conferences*, vol. 56, p. 06002, 2023. Available from: https://doi.org/10.1051/itmconf/20235606002

[8] M. Pawlak, A. Poniszewska-Marańda, N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018. Available from: https://doi.org/10.1016/j.procs.2018.10.177

[9] A. Y. Kumar, R. Yang, T. Onginjo, J. See, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," ETRI Journal, vol. 41, no. 1, pp. 1-10, 2019. Available from: https://doi.org/10.4218/etrij.2019-0362

[10] Q. Zhou, H. Huang, Z. Zheng, J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 174104-174121, 2020. Available from: https://doi.org/10.1109/aCCESS.2020.2967218

[11] H. Guo, X. Yu, "A survey on blockchain technology and its security," Blockchain Research and Applications, vol. 100067, 2022. Available from: https://doi.org/10.1016/j.bcra.2022.100067

[12] S. Bhatia, S. S. Tyagi, "Ethereum," in *Handbook of Blockchain, Digital Finance, and Inclusion*, vol. 1, pp. 55-76, 2020. Available from: https://doi.org/10.1002/9781119711063.ch4