Incentivized Decentralized Voting

Mohammad Ahmad, *University of Maryland College Park*

Abstract

In a time of escalating concerns over data privacy and security breaches, the integration of blockchain technology offers a promising avenue for reimagining traditional loyalty programs. This abstract explores the concept of Incentivized Anonymous Voting, a novel approach that leverages blockchain and Zero-Knowledge Proofs (ZKPs) to safeguard user anonymity while incentivizing active engagement. By shielding personal data behind unique identifiers (UIDs) and employing ZKPs to authenticate eligibility without compromising privacy, the proposed system addresses the vulnerabilities inherent in traditional loyalty programs. Through decentralized transaction recording and transparent reward distribution facilitated by smart contracts, the Incentivized Anonymous Voting system leads the way to a process of new loyalty programs where security, privacy, and real-world utility converge to redefine user engagement.

1. Background

Blockchain technology has become increasingly significant in various industries due to its ability to provide security and transparency. Essentially, it functions as a digital ledger, recording transactions securely and immutably (Yue). In finance and technology, it plays a crucial role in ensuring trust and integrity. Loyalty programs have been a staple in customer engagement strategies for companies for a number of years. These programs incentivize customer loyalty by offering rewards or benefits for repeat business or engagement. However, traditional loyalty programs often collect extensive personal information, raising concerns about privacy and security. Recognizing these challenges, innovative approaches have emerged, seeking to integrate blockchain technology with loyalty programs. One such concept is the Incentivized Anonymous Voting system. While the name may sound complex, its aim is straightforward: to enhance the security and privacy of loyalty programs while maintaining user engagement. By leveraging blockchain's decentralized structure and cryptographic security features, along with techniques like Zero-Knowledge Proofs, this system aims to protect user privacy while ensuring the integrity of transactions. In simpler terms, it keeps personal information safe while still allowing users to participate in loyalty programs and receive rewards. In essence, the Incentivized Anonymous Voting system represents a significant advancement in the evolution of loyalty programs. It offers a balanced solution that addresses concerns about privacy and security while preserving the benefits of customer engagement and reward incentives.

2. Proposals

At the start of this project, we brainstormed five ideas for our final deliverable. Two concepts stood out: a decentralized voting system and a blockchain-based loyalty program, both raising Professor Miers' interest.

2.1. Decentralized Voting Application

The core idea behind the decentralized voting system is to utilize blockchain technology to create a secure and transparent environment for casting and recording votes (Healy). Blockchain's inherent properties (decentralization, immutability, and transparency) make it an excellent choice for this purpose. In traditional voting systems, especially those online, concerns about security, voter fraud, and transparency persist. By leveraging blockchain, each vote can be recorded as a transaction on the blockchain, ensuring that it is securely logged and cannot be altered once submitted. This tamper-proof nature is crucial for maintaining the integrity of the voting process. Smart contracts, self-executing contracts with the terms of the agreement directly written into lines of code, play a vital role in this system. They can be used to automate the voting process, ensuring that votes are counted and confirmed according to predefined rules. Smart contracts can also help preserve voter anonymity while providing a verifiable way for all participants to check that their vote was counted without being altered.

2.2. Blockchain Based Loyalty Program

On the other hand, a blockchain-based loyalty program focuses on enhancing customer engagement through a reward system that is transparent, secure, and flexible. Traditional loyalty programs often suffer from issues such as lack of transparency, slow reward accumulation, and difficulties in redemption. Blockchain can address these challenges by providing a decentralized ledger that tracks all transactions and rewards in a transparent way (Santos). In such a system, customers earn tokens for their purchases or interactions with a brand. These tokens can be stored in a digital wallet and can be used like traditional loyalty points to redeem rewards, discounts, or even exclusive products. However, unlike traditional points, blockchain tokens can be designed to be transferable, allowing them to be traded or sold, which adds a layer of flexibility and value for the consumer.

2.3. Integrating The Two Together

Initially I had planned to move forward with just the primary idea of a decentralized voting application, however after moving forward with the project it was determined that the project required more to be interesting. In order to balance this, I opted to create a project integrating both proposal ideas mentioned before. The integration of these two systems (decentralized voting and a loyalty program) creates a dynamic platform where engagement and rewards go hand in hand. In this combined system, consumers are not just passive recipients of tokens; they actively participate in the decision-making processes of the brand or entity through voting. For instance, a company could issue polls or surveys about new products, services, or initiatives. Participation in these polls not only gives consumers a voice in the company's direction but also rewards them with tokens. This not only incentivizes engagement but also creates a deeper connection between the brand and its customers. The potential applications of such a system are numerous. A music streaming service could allow users to vote on playlists or upcoming features, or a city council could engage local citizens in decision-making about community projects. These are just a couple of examples of some applications a system like this could be used for.

3. Problems

While we continue to increase in our dependency on all things digital, the collection and analysis of personal data have become widespread especially within the framework of customer loyalty programs and accounts in general. These programs that are designed to incentivize repeat business by rewarding customers for their purchases, are common in today's retail environment. However, they come with significant privacy and security challenges that are becoming more critical as data breaches and privacy concerns increase.

3.1. Privacy Concerns

One of the primary concerns is the extensive amount of personal data these programs collect. This includes not only basic information such as names and addresses but also more detailed data on purchase history and consumer preferences. Such information can be highly sensitive. For example, a notable incident involved Target, which managed to infer that a teenage girl was pregnant before her family was aware, simply based on her purchasing patterns (Hill). This case came to light in 2012 and highlighted the sophisticated data analysis capabilities that retailers possess and the potential for such data to be used in ways consumers might not expect or approve of. The information tracking was severe enough to detail a pregnancy before one knew about it themselves.

3.2. Data Security

Moreover, loyalty programs typically rely on a centralized data management system where all consumer information is stored in a single database. This centralized approach makes the stored data a lucrative target for cyberattacks. If hackers gain access to this database, they can potentially obtain a wealth of personal data from a large number of users. Centralized databases also pose risks of insider threats, where individuals within a company might access data inappropriately for personal gain or malicious purposes. Data breaches involving customer loyalty programs are not just hypothetical scenarios; they have occurred and have affected millions of consumers. For example, in recent years, there have been several high-profile breaches where customer data associated with loyalty programs was compromised. One such breach was as recent this year with the banking giant JP Morgan, in which the sensitive information of at least 451,000 retirement plan members were compromised (Almazora). These breaches not only lead to the exposure of personal data but also to financial losses and damage to the company’s reputation.

3.3. Fraud

The issue of fraud in loyalty programs is significant as well. Customers can exploit vulnerabilities in the program to create multiple accounts or use other dishonest methods to accumulate rewards. This not only leads to financial losses for the company but also undermines the integrity of the program and can lead to higher costs for other consumers.

3.4. Lack of Transparency

There is a lack of transparency in how companies use the data collected through loyalty programs. Consumers often do not have a clear understanding of how their information is being used, who it is being shared with, or how it is being protected. This lack of transparency can contribute to a distrust of such programs and concerns over personal privacy. The challenges associated with traditional loyalty programs point to a need for a more secure and privacy-preserving approach.

4. Solution

The use of blockchain technology and Zero-Knowledge Proofs (ZKPs) provides an innovative solution to the privacy and security issues traditionally associated with loyalty programs. This

combination addresses the core concerns of data privacy, security, fraud, and transparency in several ways.

4.1. Enhanced Privacy through Anonymity

Blockchain combined with ZKPs allows for a system where consumers' identities remain confidential while participating in the loyalty program. Consumers are represented on the blockchain by a unique identifier (UID) rather than by personally identifiable information. This setup ensures that the privacy of users is maintained, as their real identities are not exposed or stored on the blockchain.
Zero-Knowledge Proofs further enhance this by enabling consumers to prove their eligibility for certain rewards or promotions without revealing underlying personal data (Lu). For instance, a consumer can prove they are over a certain age to qualify for a promotion without showing their exact birth date.

4.2. Security through Decentralization

Blockchain's decentralized nature means that data isn't stored in a single location or controlled by a single entity, which mitigates the risks of centralized data breaches. Instead, data is distributed across a network of nodes, each maintaining a copy of the entire ledger. This not only makes tampering with transaction records extremely difficult but also ensures that the system is not vulnerable to single points of failure. Each transaction recorded on the blockchain is cryptographically secured, providing a robust layer of protection against unauthorized data manipulation.

4.3. Tamper-resistant Transaction Records

The integrity of transactions in a blockchain-based loyalty program is inherently protected by the technology's design. Once a transaction, such as the issuance of a reward or redemption of points, is recorded on the blockchain, it cannot be altered retroactively (Healy). This immutable record-keeping is crucial for maintaining trust between consumers and the loyalty program, as participants can be confident that their earned rewards and transactions are accurately recorded and secure from tampering.

4.4. Automation and Reduced Fraud with Smart Contracts

Smart contracts automate the process of reward distribution based on predefined rules encoded into the blockchain. This automation reduces the administrative overhead and the potential for human error or manipulation. Additionally, because eligibility and transactions are verified through cryptographic means and governed by the immutable logic of smart contracts, the potential for fraud is significantly diminished (Healy). Users cannot claim rewards dishonestly, as the system requires cryptographic proof of transactions and eligibility, validated by the network.

4.5. Improved Transparency and Trust

The transparency inherent in blockchain technology allows consumers to see exactly how their data is being used and how rewards are calculated and distributed without revealing their personal information. This transparency, coupled with the security and privacy features of the technology, helps rebuild trust that might have been lost from the practices of traditional loyalty programs.

In summary, integrating blockchain and Zero-Knowledge Proofs into loyalty programs addresses the significant challenges of traditional systems by ensuring privacy, enhancing security, reducing the possibility of fraud, and increasing transparency. This approach not only protects consumers but also builds a stronger foundation for loyalty programs that can lead to more sustainable and beneficial relationships between consumers and businesses.

5. Development Framework

This is a comprehensive framework built on Ethereum, utilizing smart contracts to manage various aspects of corporate operations, including loyalty programs, user management, and governance. The proposed system leverages the inherent benefits of blockchain technology to enhance the effectiveness and trustworthiness of corporate processes.

5.1. Goals of the Blockchain Implementation

Decentralized Management: By utilizing smart contracts, the system decentralizes management functions, reducing the reliance on central administrative authorities. This approach helps mitigate the risks associated with centralized control, such as data tampering and single points of failure.

Enhanced Security and Privacy: Through cryptographic techniques and secure contract protocols, sensitive data and transactions within the corporation are protected against unauthorized access and breaches. Privacy is further increased by advanced concepts like Zero-Knowledge Proofs, ensuring that user data remains confidential while facilitating verifiable transactions.

Increased Transparency and Accountability: Blockchain provides an auditable and transparent ledger of all transactions and interactions. This

visibility ensures that all actions within the corporate structure are traceable and accountable, fostering a culture of trust and integrity among stakeholders.

Automation of Corporate Processes: The system employs smart contracts to automate various operations, from managing loyalty programs to conducting polls and surveys. This automation not only simplifies processes but also eliminates human errors and reduces administrative costs.

Interoperability and Standardization: Adhering to established standards such as ERC20 for token management ensures that the system is compatible with other blockchain-based services and applications. This creates easy and seamless interactions across different platforms and enhances user experience.

6. Implementation

The implementation of this project is a collection of five contracts working with one another.

6.1. CompanyMaster.sol

This smart contract is designed to orchestrate the interaction and administration of various subsidiary contracts, which handle specific functional aspects within the corporate structure. Its implementation ensures a streamlined, secure, and efficient management process that leverages the decentralized capabilities of blockchain technology.

6.1.1. Purpose and Strategic Importance

CompanyMaster.sol is fundamentally designed to centralize the administrative control within a decentralized environment. This role is crucial for maintaining order and governance across various decentralized processes in the corporate blockchain ecosystem. The contract effectively bridges the gap between decentralized operations and centralized governance requirements, ensuring that all other contracts under it operate in harmony and in accordance with corporate policies and security standards.

6.1.2. Core Functionalities

Role Management through AccessControl: The contract utilizes the AccessControl mechanism to define and manage different roles within the corporate structure, such as poll manager, token manager, and user manager. This feature is importantly for restricting access to various functionalities, ensuring that only authorized personnel can execute certain operations. Role-based access control is critical for maintaining the security and integrity of the system. Deployment and Linkage of Subsidiary Contracts: CompanyMaster.sol has the capability to deploy and establish connections between other smart contracts, namely LoyaltyToken, UserContract, and PollContract. This functionality enables a modular system where each component can be independently managed yet integrated together. The deployment and linkage are controlled by the master contract to avoid redundant deployments and ensure consistent inter-contract communication. Exclusive Owner Privileges: The contract ensures that critical actions, such as deploying new contracts or updating the system, are exclusively performed by the owner (the original deployer of the CompanyMaster.sol). This safeguard is crucial for preventing unauthorized modifications to the system, thereby protecting the corporate structure from potential security risks posed by external threats or internal breaches. Audit Trail and Event Logging: CompanyMaster.sol provides comprehensive event logs for key actions performed within the system. This functionality is essential for creating an immutable audit trail that enhances transparency and accountability. The event logs help in tracking the history of operations, providing clear evidence of all transactions and changes, which is invaluable for audit purposes and compliance monitoring.

6.1.3. Impact on Corporate Operations

The implementation of CompanyMaster.sol as the central management hub significantly enhances the operational efficiency and security of the corporate blockchain system. By centralizing the control of decentralized components, it ensures that the entire ecosystem functions cohesively and adheres to the predetermined governance framework. Moreover, the robust security measures and comprehensive logging capabilities foster a trustworthy environment, encouraging stakeholder confidence and facilitating smoother regulatory compliance.

6.2. PollContract.sol

The primary role is to facilitate the creation, execution, and analysis of polls, making it a vital tool for governance and decision-making. This contract leverages the security and transparency of blockchain technology to ensure that all polling activities are conducted fairly and efficiently.

6.2.1.Purpose and Strategic Importance

The ability to gather and analyze stakeholder opinions is crucial for any organization aiming to be responsive to its community. PollContract.sol serves this need by providing a platform for conducting polls and surveys. In the context of a blockchain-based system, this contract ensures that all responses are securely recorded and that the integrity of the polling process is maintained, thereby

supporting informed decision-making and enhancing stakeholder engagement.

6.2.2 Core Functionalities:

Creation of Polls: The contract allows authorized users (such as poll managers) to create polls with multiple questions and multiple-choice options. This flexibility supports various types of inquiries, from simple yes/no questions to more complex surveys that require nuanced responses. Each poll can be customized to meet specific informational needs, making it a versatile tool for gathering insights. Unique Response Recording: To ensure the accuracy and fairness of the poll results, PollContract.sol records each user's response while ensuring that no user can respond more than once to the same poll. This is achieved through a combination of user authentication and response tracking, which prevents duplicate submissions and potential manipulation of the polling process. Transparency in Poll Results: The contract provides functionalities to fetch and display poll results and detailed data, allowing all stakeholders to access this information. The transparency not only fosters trust in the polling process but also enables all participants to engage with the results constructively. Access to poll data encourages an informed discussion among stakeholders, which is essential for collective decision-making processes. Security and Data Integrity: By utilizing blockchain technology, PollContract.sol ensures that all data related to polls is cryptographically secured and immutable once recorded. This security measure protects the data from tampering and unauthorized alterations, thereby maintaining the credibility of the poll results.

6.2.3. Impact on Corporate Governance

This contract enhances corporate governance by providing a transparent and secure platform for stakeholder engagement. Through effective management of polls and surveys, the contract helps organizations capture and understand the opinions and preferences of their stakeholders, which can inform strategic decisions and policy formulations. The reliable and tamper-proof nature of the polling process, enabled by blockchain technology, ensures that the decision-making process is based on accurate and verified stakeholder feedback.

6.3 LoyaltyToken.sol

This contract enables the issuance, management, and utilization of digital tokens as rewards within the corporate ecosystem, thereby fostering user engagement and loyalty through the use of ERC20 standard tokens.

6.3.1. Purpose and Strategic Importance

Tokens serve as a powerful tool for incentivization and engagement in various corporate activities, including shopping, participating in polls, and other interactive engagements. The LoyaltyToken.sol contract uses these tokens to create a tangible sense of value and reward for the participants, enhancing their involvement and loyalty to the organization. This system not only motivates continued engagement but also builds a closer relationship between the corporation and its stakeholders.

6.3.2. Core Functionalities

Token Issuance and Burning: The contract allows for the minting (issuance) and burning (destruction) of tokens. Minting tokens can be triggered by certain user actions, such as making purchases or participating in surveys and polls, thus directly rewarding engagement. Burning tokens, on the other hand, can be used to manage the token supply or allow users to redeem tokens for goods, services, or privileges, maintaining the economic balance within the loyalty program.

Integration with Other Contracts: LoyaltyToken.sol is designed to work seamlessly with other contracts within the corporate blockchain system, such as PollContract.sol and UserContract.sol. This integration ensures that tokens can be awarded automatically based on specific interactions or behaviors tracked by these contracts, such as completing a survey or reaching a purchase milestone. Adherence to the ERC20 Standard: By complying with the ERC20 standard, the LoyaltyToken.sol ensures compatibility with a wide range of wallets and other smart contracts within the Ethereum ecosystem. This standardization is crucial for the usability and liquidity of the tokens, as it allows them to be easily transferred, exchanged, and utilized across various platforms and applications.

6.3.3. Impact on Consumer and Stakeholder Relations

The implementation of LoyaltyToken.sol significantly enhances the dynamics of consumer and stakeholder relationships. The tokenized rewards system not only incentivizes participation and engagement but also provides a measurable and flexible means of rewarding loyalty and contribution. This approach aligns the interests of the stakeholders with those of the corporation, creating a mutually beneficial environment where engaged behavior is tangibly rewarded. The use of blockchain technology ensures that all token transactions are transparent and immutable, enhancing trust in the fairness and reliability of the loyalty program. Stakeholders can see the direct correlation between their actions and

the rewards they receive, which reinforces their trust and commitment to the organization.

6.4. UserContract.sol

This contract plays a crucial role in handling the registration, authentication, and overall management of user data, ensuring a secure and efficient user experience across the corporate system.

6.4.1. Purpose and Strategic Importance

User management is fundamental to the functioning of any corporate system, particularly in environments that handle sensitive or personal data. UserContract.sol is strategically designed to centralize the user management process while maintaining the high standards of data privacy and security that blockchain technology offers. This contract ensures that user interactions within the ecosystem are smooth, secure, and compliant with data protection regulations, thereby supporting the integrity and reliability of the entire system.

6.4.2. Core Functionalities

User Authentication and Authorization: The contract is responsible for authenticating users and granting authorization based on predefined criteria. This process is vital for ensuring that access to sensitive functions and data is strictly controlled and limited to verified users. By implementing robust authentication mechanisms, UserContract.sol helps prevent unauthorized access and protects the system from potential security breaches. Management of User-Specific Data: UserContract.sol handles the storage and management of critical user-specific information, such as user profiles, voting records, and accumulated loyalty points. This data is kept private and secure, accessible only to the user it pertains to and authorized system administrators. The contract ensures that all personal data is handled in compliance with privacy standards, with encryption and other security measures applied to protect user information. Data Privacy and Security: In addition to managing user data, the contract also ensures that all information is stored with a high degree of security. Blockchain technology offers the advantage of decentralized storage, reducing the risks associated with centralized data breaches. Furthermore, the immutability of blockchain ensures that once data is recorded, it cannot be altered without a consensus, thereby providing an additional layer of security and trust.

6.4.3. Impact on User Experience and System Integrity

The UserContract.sol enhances the user experience by providing a seamless and secure method for managing user interactions and personal data. Users can trust that their information is handled responsibly and that their interactions with the system are secure. This trust is crucial for user retention and satisfaction, as it directly impacts the perceived reliability and integrity of the corporate system. By centralizing user management in a secure and controlled environment, the contract significantly reduces the risks of data leaks and unauthorized access. The rigorous authentication and authorization processes ensure that only eligible users can access sensitive functions, safeguarding the system against potential security threats.

6.5. VotingContract.sol

This contract is designed specifically to manage and oversee the voting processes on various polls and initiatives within the system. This smart contract is integral to maintaining the democratic aspects of corporate governance, enabling transparent and secure voting mechanisms that reflect the true intent of the stakeholders.

6.5.1. Purpose and Strategic Importance

Voting is a fundamental aspect of participatory decision-making, allowing stakeholders to express their opinions and influence the direction of the organization. The VotingContract.sol facilitates this process within a blockchain environment, ensuring that each vote is not only recorded accurately but is also verifiable and secure against tampering. This capability is crucial for maintaining trust in the corporate governance process and for ensuring that all decisions made are legitimate and representative of the stakeholder's will.

6.5.2. Core Functionalities

Accurate and Secure Vote Management: The contract ensures that each vote cast in various polls is recorded accurately and securely. Leveraging blockchain technology, the voting process is made tamper-resistant, as each vote is cryptographically sealed and immutably recorded on the blockchain. This not only prevents any alteration of votes but also provides a transparent audit trail that can be reviewed if disputes arise. Access Control for Voting: To ensure that only authorized and eligible users can participate in the voting process, the contract implements strict access control measures. This functionality is critical for maintaining the integrity of the voting process, preventing unauthorized access and ensuring that each vote cast is legitimate. Integration with LoyaltyToken Contract: The contract is designed to work in tandem with the LoyaltyToken.sol contract to reward users for their participation in the voting process. This integration motivates stakeholders to engage actively in

corporate governance, fostering a more dynamic and participatory community. Rewards for voting can help increase turnout and participation, which is beneficial for achieving a more representative outcome in decision-making processes. Verification of Voting Status: The contract provides functionalities that allow users to check whether they have already voted, preventing duplicate votes and ensuring the uniqueness of each vote. This feature is essential for upholding the one-person-one-vote principle that is foundational to fair voting practices.

6.5.3. Impact on Corporate Governance and Stakeholder Engagement

The implementation of VotingContract.sol enhances the transparency and integrity of the voting processes within the organization. By ensuring that all votes are securely recorded and that only authorized users can participate, the contract upholds the democratic values essential to fair corporate governance. The ability to incentivize participation through token rewards not only enhances stakeholder engagement but also aligns the interests of the users with the long-term goals of the organization. This strategic alignment helps ensure that decisions made through voting are both reflective of the collective will and supportive of the organization's objectives.

7. Issues and Backlogs

In the development of my blockchain-based corporate system, one of my ambitious goals was the integration of ZKPs to enhance privacy and security. My intention was to leverage this technology to allow users to verify transactions or claims without revealing any underlying data, thereby preserving user privacy and data integrity.

7.1. Efforts and Approaches

I undertook significant efforts to integrate ZKPs into my system, exploring various frameworks and tools known for their robust capabilities in supporting ZKP implementations. Among these were:

Circom and SnarkJS: I attempted to use Circom to create zero-knowledge circuits, with SnarkJS to generate and verify zero-knowledge proofs. Circom is particularly suited for defining complex arithmetic circuits that can prove general computational statements. However, the complexity of constructing these circuits and the intensive computational power required posed substantial challenges.

ZoKrates: Another tool I explored was ZoKrates, a toolbox for zkSNARKs on Ethereum, which is designed to help developers write, compile, and deploy proofs. ZoKrates aims to abstract some of the complexities involved in writing zero-knowledge proofs by providing a higher-level language and a standard toolbox. Integrating these proofs into my existing system's architecture required a deep and often intricate understanding of both the theoretical and practical aspects of zkSNARKs.

7.2. Challenges Encountered

The integration of ZKPs proved to be exceptionally challenging due to several factors:

Technical Complexity: The theoretical underpinnings of zero-knowledge proofs involve advanced concepts from algebraic geometry and number theory. The steep learning curve required for effective implementation can be a significant barrier, even with the use of abstraction tools like ZoKrates.

System Compatibility: Ensuring that the ZKP components interacted seamlessly with other blockchain components, such as smart contracts managed by CompanyMaster.sol, added another layer of complexity. Each integration point required meticulous attention to ensure that data integrity and security were maintained without compromising system performance.

7.3. Moving Forward

Despite these challenges, my efforts to integrate ZKPs underscore my commitment to enhancing privacy and security within my blockchain solution. While I was not able to fully implement ZKPs in the current phase of the project, the groundwork laid by my development efforts provides a strong foundation for future advancements. Moving forward, I plan to continue my research and development in this area, seeking more efficient and scalable solutions, and potentially collaborating with academic and industry experts to overcome the technical hurdles I encountered.

References

Abba, Abdullahi Lawal, et al. “Security analysis of current voting systems.” 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), 21 Nov. 2017, https://doi.org/10.1109/icecta.2017.8252006.

Almazora, Leo. “JP Morgan Data Breach Hits 451,000 Retirement Plan Members.” InvestmentNews, 1 May 2024, www.investmentnews.com/regulation-and-legislation/news/jp-morgan-data-breach-hits-451000-retirement-plan-members-252872.

D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 2018, pp. 1-6, doi:10.1109/IMCET.2018.8603050

Healy, John J. (2023) "Veto the Black-Box Politics: How Implementing Blockchain Technology into the United States Voting System Will Give Our World the Transparency We Deserve," Hofstra Law Review: Vol. 52: Iss. 1, Article 5.

Hill, Kashmir. “How Target Figured out a Teen Girl Was Pregnant before Her Father Did.” Forbes, Forbes Magazine, 20 Feb. 2024, www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=72520f7e6668.

Lu Zhou, Abebe Diro, Akanksha Saini, Shahriar Kaisar, Pham Cong Hiep, Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities, Journal of Information Security and Applications, Volume 80, 2024, 103678, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2023.103678.

OpenZeppelin. "AccessControl." GitHub, GitHub, Inc., https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/access/AccessControl.sol

Santos AF, Marinho J, Bernardino J. Blockchain-Based Loyalty Management System. Future Internet. 2023; 15(5):161. https://doi.org/10.3390/fi15050161

Yue Liu, Qinghua Lu, Guangsheng Yu, Hye-Young Paik, Liming Zhu, Defining blockchain governance principles: A comprehensive framework, Information Systems, Volume 109, 2022, 102090, ISSN 0306-4379, https://doi.org/10.1016/j.is.2022.102090.