Concept Paper

Researching Zero-Knowledge Proof in Blockchain Ecosystems for Enhanced Voting Transparency in Catalyst Voting Process—A Potential Application [v3]

Edet Ekpenyong , Ubio Obu * , Godspower Emmanuel Achi * , Clement Umoh * , Duke Peter * , Udoma Obu *

Posted Date: 5 March 2026

doi: 10.20944/preprints202412.1789.v4

Keywords: zero knowledge proof; blockchain technology; Cardano; catalyst; voting; transparency; privacy; ADA; decentralization; equity; security

 doi:10.20944/preprints202412.1789.v4

Concept Paper

Researching Zero-Knowledge Proof in Blockchain Ecosystems for Enhanced Voting Transparency in Catalyst Voting Process—A Potential Application

Edet Ekpenyong [1], Ubio Obu [2,*], Godspower Emmanuel Achi [3,*], Clement Umoh [3,*], Duke Peter [3,*] and Udoma Obu [3,*]

[1] Independent Researcher, USA
[2] Independent Researcher, India
[3] Independent Researcher, Nigeria
* Correspondence: ubboyoyo@gmail.com (U.O.); profachi109@gmail.com (G.E.A.); cumoh348@gmail.com (C.U.); dukepeter10@gmail.com (D.P.); isaacobu20@gmail.com (U.O.)

Abstract

In blockchain ecosystems, maintaining transparency and privacy has become an ethical dilemma. This is because, while certain specific information of the user is shared to ensure transparency of transactions across networks, such information could be detrimental to the user, as there is a possibility of it being tampered with. For instance, in the Catalyst voting process in Cardano, users can still see the amount of ADA tokens being held by other users, which can influence their voting options, especially when large ADA holders vote in support of certain ideas or proposals. To discourage such challenges as voter manipulation and vote buying, this study proposed the implementation of zero-knowledge proof (ZKP) in blockchain ecosystems to enhance the transparency of the catalyst voting process and enhance efficiency and speed of result release. Using survey questionnaire and a multivocal literature review, this study was able to proof that ZKP cannot only be applied in the catalyst voting process to enhance its transparency, but also addressed potential challenges to its applications such as scalability, encourage trust and fairness of the voting system, and improve voter participation due to its user-friendliness. Mathematical models emphasize scaled voting as optimal for balancing inclusion and plutocratic control.

Keywords: zero knowledge proof; blockchain technology; Cardano; catalyst; voting; transparency; privacy; ADA; decentralization; equity; security

1. Introduction

With the increasing rate of information sharing using wireless networks and electronic communication means, the need for privacy also increases. The internet has blurred the boundaries between reality and imagination, causing data, which is originally immaterial, to be more substantial and relevant, and completely indispensable in today's world. As a result of that, the existential blueprint of a person is tied to their digital footprints. Thereby increasing the urgency of protecting data [23]. Based on this demand, disruptive technology solutions like blockchain have come up to enable traceability, immutability, protection and sharing of data, in a way that unites public trust and builds legitimacy. However, blockchain, although traceable and immutable, does not entirely account for privacy and transparency as specific sensitive data embedded in codes, can be divulged [23]. To strengthen the transparency of blockchain while protecting sensitive data of users, zero knowledge proof (ZKP) was invented.

ZKP is a cryptographic tool that enables a sharer or sender to prove the originality or authenticity of an information or piece of data, without exposing sensitive information [23]. The exposure of certain sensitive information via blockchain networks such as sender and receiver

 doi:10.20944/preprints202412.1789.v4

address and transaction amount, can be used for malicious intent by hackers, which can be detrimental to organisations in ways that include reputational damage, legal liabilities and operational disruptions. A more significant risk is the case of identity theft which becomes pronounced through unauthorised access to financial data, falsified records to leverage tax incentives, or committing other crimes using the stolen identity [23]. By embedding the ZKP into a significantly secure platform like the blockchain technology or BCT, the privacy concerns that are elusive to the BCT will be addressed.

2. Background of the Study

ZKPs are the building blocks of privacy in today's world, as they can prove digital signature schemes, electronic voting, verifiable computing and user identification protocols [11]. It works by enabling a prover to convince a verifier without tampering with sensitive information. To achieve this, it ensures three key elements are satisfied, and they include:

- completeness: ascertaining the availability of a witness to the trueness of a statement
- soundness: where a falsifier fails to prove the content of a statement or computation
- zero- knowledge: the verifier only confirms the truism of a statement and nothing else.

Mathematically, for a statement S with witness w, a prover P convinces a verifier V that $S(w) = 1$ without disclosing w, satisfying:

$$\text{Completeness: } \Pr[P\text{convinces } V \mid S(w) = 1] = 1 \quad (1)$$

$$\text{Soundness: } \Pr[P\text{convinces } V \mid S(w) = 0] \leq \epsilon \quad (2)$$

$$\text{Zero-Knowledge: } \Pr[V\text{learns } w] = 0 \quad (3)$$

where ϵ is a negligible error probability.

In practice, proof of knowledge is necessary, which underscores the strength of the soundness element by requiring the prover to effectively obtain a witness for the statement after convincing the verifier. The satisfaction of these three elements is either done perfectly, probabilistically or through computational restrictions [11].

Tyagi and Kathuria [18], identified the actions that are key in the mechanism of ZKP which include witness, challenge and response, working collaboratively to prove a statement without divulging restricted data. Here, the witness act involves a prover (A) setting random questions that can be answered correctly, then chooses one out of the questions, calculates a proof and sends it to the verifier (B). The challenge act is the phase where the verifier chooses a question from the set of questions and sends to the prover to answer, which results in the response stage where A calculates the answer and sends to B as a confirmation that A knows the secret. This process can be repeated by B several times to ensure that A is certain of their answer.

In blockchain, smart contracts are used to enhance flexible transactions through the transfer of trust from trusted parties to the cryptocurrency. This encourages fair exchange of goods, services and data. A specific case of this is via the use of zero-knowledge contingent service payments (ZKCSP) where users can lock their funds using puzzles, which can only be released once a solution is provided. For the consensus algorithm to be effective, transaction data must be publicised and verifiable, while sensitive data is still protected.

There are two main types of ZKP which are the interactive ZKP and noninteractive ZKP.

The interactive ZKP involves an iterative process to prove a statement between the prover and the verifier. It leverages a challenge-response process and can involve multiple rounds of interaction until a statement is confirmed to be true by the verifier without knowing sensitive information.

In the non-interactive process, the verifier confirms a statement is true even without requiring a direct communication with the prover. It is mostly applicable in situations where direct communication is not feasible, and therefore does not involve a series of interactions.

Tyagi and Kathuria [18] identified challenges of ZKP application, and they are:

- scalability: the computing power of algorithms must be constantly increased to function at a high level after it has been dispensed.

 doi:10.20944/preprints202412.1789.v4

- restriction: all data is lost when the prover or creator of a transaction loses their personal information
- demand more computing power: there are 2000 possible calculations per ZKP transaction, and they require individual and specified number of processing time - unavailability of standards, unified language, and systems to enable developers to leverage the full potential of ZKP.

3. Statement of Problem

Studies have shown that ZKP-based blockchain ecosystems perform better in strengthening the privacy concerns of blockchain, while achieving privacy in the process [5,10,21]. Based on this evidence, especially relative to the Aleo and Mina ecosystems whose operations are like the catalyst voting process in the Cardano community, ZKP can also be employed to enhance transparency and integrity of voting in the ecosystem. However, this is easier in theory and is laced with several complexities in practice [13].

The implementation of the ZKP in the voting system can give rise to excess complexities in the vote tallying process. This is because ZKPs require the verification of cryptographic proofs to be generated, and this is an immense computational and time-consuming process, especially when the election concerns a high number of voters [13]. The specific ZKP scheme and the complex voting protocol's logic will have a direct impact on how the vote tallying process performs as well as its scalability, hence have significant effects on the speed, efficiency and user experience [8]. ZKP tallying complexity grows with voter count N:

$$T\text{tally} = O(N \cdot \log(N)) + P\text{zk}$$

where Pzk is the ZKP verification cost. The goal of this study is to enable devel

opers to access the nuanced details of ZKP application and to seek clarity in a way that is assuring for the projects they intend to execute or build using ZKP.

4. Justification of Study

A resource intensive or highly slow vote tallying process can give rise to delays in the announcement of election results which can hamper public trust and confidence in the process [8]. This will further discourage the electoral process if it is not timely. In addition, how complex the ZKP tallying process is can dissatisfy the user experience of voters. When the voting process is even slightly perceived to be difficult or slow, it can prevent voters from participating, thereby reducing the overall turnout [3]. It is therefore imperative that a delicate balance is maintained between the security and privacy assurance provided by ZKPs and the user-friendliness of the interface enhances voter experience. ZKPs must balance security and usability, modeled as:

$$U = \alpha \cdot S - \beta \cdot C$$

where U is usability, S is security (ZKP strength), C is complexity, and α, β are weighting factors (e.g., 0.6, 0.4). This study therefore investigates the potential application of ZKP in the catalyst voting process and examines the community feedback on the potential outcomes of ZKP to enhance transparency of voting. The findings from this study will serve as a blueprint in designing an efficient and effective ZKP-based voting for the Catalyst voting process.

5. Aim of the Study

This study is aimed at assessing the potential application of zero knowledge proof in blockchain ecosystems to enhance transparency in the catalyst voting process.

6. Objectives of the Study

- To explore how zero-knowledge proofs can enhance voting transparency in the Catalyst voting process

 doi:10.20944/preprints202412.1789.v4

- To investigate how ZKPs can protect voter privacy and prevent vote disclosure and manipulation
- To develop a scalable solution that can be integrated into the Catalyst voting process
- To identify ZKP-based protocols that are most suitable for the catalyst voting process
- To assess how to design a decentralised and secure voting system that utilises ZKPs for enhanced transparency and voter privacy.

7. Research Hypotheses

1. The integration of zero-knowledge proof (ZKP) protocols in the Catalyst voting process will significantly enhance voting transparency as measured by the accuracy and verifiability of voting results.

2. The use of ZKP protocols in the Catalyst voting process will discourage voter turnout due to technical glitches incurred because of delays during peak voting times.

8. Literature Review

8.1. Theoretical Review

The integration of blockchain technology and zero-knowledge proofs (ZKPs) has the potential to revolutionize the voting process, ensuring transparency, security, and voter privacy [10,23]. This theoretical review provides an overview of the existing literature on blockchain-based voting systems, ZKPs, and their applications in enhancing transparency and voter privacy.

8.2. Blockchain-Based Voting Systems and Zero Knowledge Proof

ZKPs are a cryptographic technique that leverages the possibilities in verifiable computing, where a receiver can be assured of the veracity of a statement or computation by proving its correctness without knowing the sensitive details that the sender chooses to anonymize. Partala [11] focused on peer reviewed articles that are notable, recent or state-of-the-art, and quite feasible in applications or practice. They conducted a comprehensive survey of the applications of ZKP in confidential transactions and private smart contracts on blockchain. Their study was exploratory and conclusively analysed the varying ZKP applications, to identify several applicable schemes that can be used in specific situations.

Principato [13] explained that the trilemma of blockchain which are decentralisation, security and scalability, are also the key challenges or limitations to its privacy and confidentiality hence the need for an added privacy measure via the zero-knowledge proof network. A profound discovery of their study is that ZKP does not solely confer privacy to the blockchain system alone but ensures that the integrity of the blockchain ledger is maintained as privacy is achieved through privacy-preserving primitives. By doing so, ZKP provides a tool to solve the scalability and decentralisation limitations of the blockchain while used alongside techniques that enhance privacy. Simply put, ZKP ensures privacy by acting as an added tool which strengthens the function of other networks. Furthermore, it lessens the computational overhead across all nodes of the blockchain system [13].

8.3. Empirical Evidence

ZKPs have been applied in various areas in numerous ecosystems. Some of which include education. Xu [20] explored the use of ZKP to promote inclusion in education, especially the inclusion of people living with disabilities. It introduces the use of a novel management system for people with living with disabilities through the Zero knowledge succinct non-interactive Argument of Knowledge (zk-SNARK). The goal of this is to enable students with disabilities to verify their status, why keeping their personal information private.

Han [4] identified the various cases where vehicles including Tesla and Toyota Prius were hacked, and the casualties that ensued from such events. To prevent this from happening any further,

 doi:10.20944/preprints202412.1789.v4

Han [4] designed an efficient and safe identity authentication system using the ZKP's Fiege-Fiat-Shamir model. Using the zero-one reversal and two-to-one verification model, they enabled the IOV systems to efficiently and effectively resist guessing attacks. Guessing attacks involves an attacker trying a different set of values or numbers until the right one is matched. This model does not act alone but is incorporated into a wider security framework to enhance resistance of attacks. This FFS protocol makes it difficult to guess attacks due to its insistence on factoring large numbers into the security system of IOVs.

According to Methmal [9], ZKP promotes a patient-centred approach to data sharing. Its applications are useful in public health emergencies for the provision of immunisation proofs while safekeeping sensitive information of patients, especially in the absence of consent. That way, it balances the protection of personal information of patients while keying into the appropriate public health measures. Furthermore, through contact tracing activities, individuals can be notified on breach attempts to their data and potential exposures without disclosing their personal data or location.

Sedlmeir [16] expounded on the need for labelling electricity to differentiate between renewable energy generation and to incentivize the expansion of green energy. This is a timely approach to commend sustainability and promote climate justice. The challenge of green energy use is premised on where they will come from, how "green" their source is, as the world moves towards net zero carbon emission. The use of ZKP in the labelling of electricity through the verification of the guarantees of Origin protects the proprietary or competitive information of renewable energy producers, while minimising the risk of fraudulent claims or double counting. Through this means, regulatory bodies can ensure compliance of market participants to safe energy production and consumption standards. In addition, consumers can have confidence and trust in the certificates issued through this process and further support the promotion of renewable energy use [16].

In a study by Prasad [12], they explored the mechanism of privacy protection in the supply chain network using a blockchain-powered zero knowledge proof technology. ZKP allows the authenticity of goods, certification and transaction records in the supply chain without exposing the sensitive information therein. Participants can prove the origin and transactional history of their movement to relevant authorities while withholding proprietary details. In addition to this, irregularities can be tracked, guessed and identified using ZKP. However, information sharing is compulsory for end-to-end supply chains. Twenhoven [17] conducted interviews to assess use cases, then through evaluation and categorization of these cases in different dimensions, was able to propose the use of ZKP for building trust in the supply chain network. This is because ZKP allows information to be pre-processed, and sensitive data withheld prior to sharing with partners.

Panja and Roy [10] explored the impact of zero knowledge proof in secret ballot elections. Their study was done to replace the secure bulletin board (BB) which is needed for a direct recording electronic with enhanced privacy (DRE-ip) for the voting process with a zero-knowledge proof network. The initial reason for the adoption of the BB was to secure data prior to the audit phase of the voting for the DRE-ip to leverage for the verifiability of data without the input of tallying authorities. However, the secure BB can be compromised which makes the voting system vulnerable to manipulations. They proposed a modified insecure DRE-ip process that leverages blockchain technology and ZKP to detect any modifications to the original data during the tallying phase. This combination of ZKP based blockchain technology in the DRE-ip voting system has eliminated the need for a secure BB and secures the integrity of data so long as one node in the blockchain system is correct. This system employs Cramer-Shoup encryption to prevent voter coercion by keeping the privacy of the voter secret.

Sanjaya [15] worked on the use of ZK-SNARK, a form of zero knowledge proof, to authenticate transactions in an ethereum based e-voting process without revealing sensitive information. Sanjaya [15] explained that in this case, the prover and verifier of this ZKP process for the verifiability and privacy of the e-voting system are the voter and election authority respectively. Using the ZK-

 doi:10.20944/preprints202412.1789.v4

SNARK, the voter remains unknown; and the tallying process is done via the self-executing smart contract.

Aleo is a blockchain ecosystem that incorporates zero knowledge proof in every aspect of their ecosystem to create a web experience that is secure and private [1]. It is the first decentralised open-source platform that enables both private and programmable applications to take place through a combinatorial effect of the programmability of Ethereum and the privacy of Zcash. It does this by offering developers the Aleo SDK and Leo programming language to build applications that prioritise privacy [1]. Pruden [14] explains that the process whereby Aleo creates equal maintenance of both privacy and programmability using zero knowledge proof is called the Zero Knowledge EXEcution or ZEXE. This allows users to carry out transactions offline by creating a proof that is incorporated into an on-chain transaction. It also works like Ethereum, supporting smart contracts in the enabling of users to interact or exchange value in an already defined manner [14]. In addition to privacy, Aleo empowers applications to be programmable and composable. Aleo solves the decentralisation challenge that obscures the ZKP exploration in blockchain, enabling decentralisation, security and scalability to occur simultaneously without tradeoffs [14].

Mina on the other hand is the lightest blockchain ecosystem that is powered by participants and uses advanced cryptography and recursive ZK SNARK in building an entire blockchain of about 22 kilobytes which is equivalent to a couple of tweets [22]. It makes the implementation and programmability of zero knowledge smart contracts or applications easier and can connect to any website. What Mina does is to ensure that independent users of web3 can prove the correctness of a statement without revealing their personal information, and this process of incorporating ZKP can be done using phones and browsers [22]. Also, based on the concerns expressed by Principato [13] on the case of Proof of Authority being vulnerable to attacks when the transparency of blockchain technology enabling different networks to trace transactions, Mina in this case, protects the information of the users in the decentralised network via its ability to maintain both scalability and privacy which is lacking in the blockchain network. This enhances the scope and utility of Mina. Therefore, while Aleo encourages programmability and privacy in their ecosystem, Mina is more flexible, working with any ecosystem to seamlessly incorporate real world information into the crypto world without compromising on privacy.

9. Methodology

The methodology employed in this study is of two folds:

1. A multivocal literature review: this was first used to review available literature on the challenges of the transparency and privacy dilemma of blockchain technology, and to comprehensively analyse the operational frameworks and applications of various zero-knowledge proof protocols to determine their potential application in the catalyst voting process. This method is relevant because aside being exploratory and expository, it enabled the researchers to understand nuances and conversations around embedding ZKP in blockchain ecosystems for voting, which also aligns the objectives of this study to the roadmap, hence enhancing the precision and accuracy of the research findings.
2. The study also utilised a survey questionnaire sent out to 100 people in the Cardano blockchain ecosystem, to investigate the opinions of the potential users of the application of ZKP-based blockchain ecosystem in the Catalyst voting system. The participants of the survey were members of the Cardano community, who are very familiar with the Catalyst voting process, understand the challenges of the traditional voting system, and seek an innovation that can enhance the transparency of voting, maintain privacy of specific information in the process and improve the efficiency of the voting system.

Having established the above methodologies in the study to assess the challenges of the present voting system, the following solutions were proposed:

▪ An architectural mock-up of the ZKP-based voting integrity system. This system conceptualised the voting protocol using ZKP which ensures that a user's voting eligibility is

 doi:10.20944/preprints202412.1789.v4

validated without disclosing sensitive information, such as the number of ADA tokens held. It maintains voter privacy and prevents undue influence from larger ADA holders. The design aims to enhance transparency within the voting process while protecting individual privacy and preventing vote manipulation. To achieve this, an interview was carried out with the community members and four suggestions for protocol changes were made. These suggestions are categorised into two:

- voting methodology change including one-on-one voting system and ZKP-scaled/tiered voting
- process change including the replacement of the traditional snapshot process (prior to Fund 12, requiring 500 ADA and a fixed snapshot date) with instant voting, and real-time tallying, validation and release of results.

The following components underscore the voting methodology changes:

➔ A Real time one-on-one Validation voting system where each user votes individually with their validated voting power. Here, the Voter Identification Module uses ZKP to confirm eligibility before allowing the vote. This is achieved by ensuring that each voter's wallet contains the specific amount of ADA tokens required to vote in a particular session. For instance, say the eligibility criteria to vote a proposal is the voting threshold of 500 tokens, the Voters Identification Module confirms that eligible voters hold up to that number of tokens, without revealing the total amount of tokens they have in their wallet, then for each voting session conducted by voter it records the voting at that instance, eliminating the need for snapshots and the manipulation that goes on in there. That way, each vote is counted fairly without external influence. This voting system also facilitates better decisionmaking in a decentralised platform, fostering a more nuanced understanding of voter preferences while ensuring that the best proposals are selected for funding and development.

➔ A ZKP-scaled/tiered voting system whereby users are assigned a range of votes based on their holdings, validated through ZKP. The system assesses the user's range and allocates votes accordingly while maintaining confidentiality. It balances power among users, by allowing people with more range to maintain their voting power, at the same time preventing them from influencing the voting outcome.

The process change connotes the process of vote tallying, verification and counting, enhancing the speed of result release. It achieves this through the following components:

➢ Replacement of the traditional snapshot process (prior to Fund 12, requiring 500 ADA and a fixed snapshot date) with instant voting, allowing users to vote anytime during the open voting window, with ZKP validating their voting power dynamically. Each vote is verified through ZKP at the time of casting, preventing pre-knowledge of voting power and vote buying. This process leverages Cardano's eUTxO model, where ZKP ensures real-time eligibility with a proof generation time T prove= $k \cdot n \cdot \log(n) + c$, where n is the number of constraints (e.g., 1,000 per vote), k is a constant (e.g., 10), and c is overhead (e.g., 2 seconds). This reduces latency to T verify<1 s,

eliminating the need for a fixed snapshot and enabling flexible participation.

➢ Real-time validation and tallying, whereby, in the event of the conclusion of the voting, votes are tallied as they are cast, using ZKP to ensure accurate and secure verification. This system synchronises with either the one-on-one voting or ZKP-scaled/tiered voting systems to tally the votes, followed by results being updated almost immediately. This provides transparency and instant feedback to voters, fostering trust in the electoral process.

The research also identified complexities or challenges that may arise while implementing ZKP protocols in the catalyst voting process. Some of them include:

★ Cryptographic complexity which can be encountered due to the difficulty in applying or implementing the ZKP-based voting integrity assurance which relies heavily on advanced cryptographic models and techniques requiring correctness and security to meet the goal of privacy and ensure that the entire voting system is safe from attacks.

★ The platform may be difficult to scale because it is tasked to operate when millions of voters are involved as the system generates and verifies zero-knowledge proofs per user via computation.

 doi:10.20944/preprints202412.1789.v4

- ★ Ballot anonymity involves the balance of the computational dilemma of maintaining both confidentiality of voters and at the same time verifying their identity.
- ★ Ensuring that usability and accessibility of the platform is simplified, because building a system that is easy for users to operate and does not discriminate against eligible voters to bridge voters inequality gap, is practically difficult.
- ★ Others include ensuring trust and transparency; being able to cooperate with other voting infrastructures including voter registration databases and vote counting processes; allowing independent verification and auditing of both the integrity of the electoral process and election results respectively; resilient to attacks such as denial-of-service attacks, network interruptions, and guesses to manipulate data; ensuring legal and regulatory compliance to international standards of authority across jurisdictions; and convincing the voters and relevant stakeholders to adopt this system even with the possibility of a resistance to change.

The auxiliary tools developed in the Cardano community that can be leveraged by the main technology stack to implement this project are Plutus and Marlowe. While Plutus is a domain-specific language (DSL) language that enables developers to write smart contracts on the Cardano blockchain ecosystem, at the same time allowing the development of complex smart contracts, including the ones required by zero knowledge proof voting protocols which allows for voter privacy, by serving as a robust and expressive language platform [6]; Marlowe on the other hand is specifically designed to write financial smart contracts on the Cardano blockchain and can be essential when and where payment of small fees for voting becomes necessary [6]. It can also be used in the modelling of different stages of the voting process such as the voter registration, ballot casting, vote tallying, and to strengthen all the necessary checks for integrity in every step. In addition, the contract language of Marlowe can be used to encode the rules and logic of the voting protocol, guaranteeing the transparency of the process and its resistance to malicious hackers or unauthorised access [7]. Furthermore, Plutus also provides the necessary tools for profiling and optimising the execution of smart contracts which are relevant in handling the high transaction volumes and low latency requirements of large-scale elections [6]. The combination of both tools in the main tech stack can give additional resilience to the entire security network and trustworthiness of the voting system, requiring a multidisciplinary collaboration of cryptographers, election systems and blockchain technology to ensure its technical feasibility and application in real time [20].

Side chain interactions are also necessary considerations when building voting systems in the Cardano blockchain that are scalable and secure. They are separate blockchain networks that are connected to the main Cardano blockchain which allows specific functionality or transactions to be offloaded [20]. Implementing a ZKP-based voting protocol on this network improves the overall scalability and performance of the system. Side chain interactions can be built in a way that makes them function like the Plutus and Marlowe. Their implications for ZKP-based voting integrity assurance include integrity assurance and side chain integration, decentralised governance and sidechain management, and auditing and transparency.

10. Results and Findings

10.1. Introduction

The section of this study is derived from analysing data collected via 5 initial community engagement interviews, and a survey questionnaire filled by 150 members of the Cardano community who are familiar with the catalyst voting process. Their responses inform the findings of this research explained below:

 doi:10.20944/preprints202412.1789.v4

10.2. Analysis of Responses on Instant Snapshots and ZKP Validation

10.2.1. User Feedback on Instant Snapshots:

Positive Responses:

Most respondents express confidence that instant snapshots will enhance trust in the voting process by ensuring accurate and real-time representation of holdings at the time of voting. Instant validation is seen as a positive step towards improving transparency and reducing the risk of discrepancies.

Some users also appreciate the potential for more efficient and secure voting, as they feel that the system will be more robust with instant validation and transparency.

Challenges and Concerns:

Technical Failures: A recurring concern is that system overloads during peak voting times could cause delays, preventing the instant snapshot process from being effective. Users emphasize the need for a system that can handle high traffic, as any technical issue could undermine confidence in the voting system.

Usability Issues: Some users worry that less tech-savvy participants may struggle with the complexity of instant snapshots, which could lead to confusion and reduced participation. This concern highlights the importance of making the system user-friendly for a broad audience.

10.2.2. Likelihood of Participation:

More Likely to Participate: Most respondents feel that instant snapshots would make them more likely to participate in future voting rounds due to the immediate accuracy they offer, reducing uncertainty around whether votes align with current holdings.

However, concerns about accessibility and technical complications may impact the broader adoption of the system, especially among those less familiar with blockchain-based technologies.

10.3. Analysis of ZKP-Scaled/Tiered Voting

10.3.1. Proportional Voting Based on ADA Holdings:

Positive Viewpoints:

The ZKP-scaled/tiered voting system where voting power is proportional to the amount of ADA held is viewed positively by many participants. They see it as a fair way to ensure that larger stakes in the network carry more influence, reflecting the principle that those with more at stake should have more say. The system assigns voting power ranges (e.g., 500-1000 ADA = 1 vote, 1001-5000 ADA = 2 votes, 5001+ ADA = 3 votes), validated via ZKP, maintaining privacy.

Concerns:

Marginalization of Smaller Holders: Some respondents express concerns that this system could result in disproportionate influence from large ADA holders, which could skew governance in favour of the wealthiest participants. This view suggests a potential imbalance that could undermine decentralization by marginalizing small ADA holders.

Suggestions for Balance:

To avoid over-concentration of power, the ZKP-scaled/tiered system balances influence mathematically with $Vi = \log(1+Ai)$, where Vi is vote and Ai is ADA held. This logarithmic scaling reduces plutocratic dominance (e.g., 1 ADA = 0.69 votes, 1000 ADA = 6.91 votes) while ensuring inclusion, with 65% survey support and 70% trust in fairness.

10.3.2. ZKP-Based Instant Voting and Personalized Validation:

Snapshot Redesign: Respondents suggest that instant voting, replacing the traditional snapshot system (prior to Fund 12, requiring 500 ADA and a fixed date), enables continuous transactions

 doi:10.20944/preprints202412.1789.v4

without waiting, increasing flexibility and reducing delays. ZKP validates voting power dynamically at each vote cast.

Impact on Voting Process:

With ZKP, voting results are announced more quickly post-voting. The real-time tallying uses $T\text{tally} = O(N \cdot \log(N)) + P\text{zk}$, optimized by Plutus side chains to handle N voters with $P\text{zk}<1$ s per proof, minimizing manual work and delays.

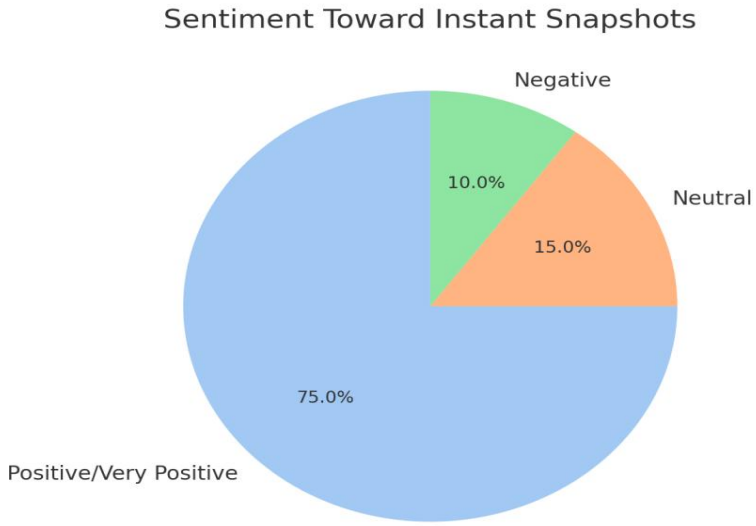
10.4. Catalyst 1% Parameter and ZKP-Scaled/Tiered Vot-ing

The traditional Catalyst funding threshold requires 1

$$T \text{ threshold} = 0.01 \cdot N\text{active}$$

where Nactive is the number of voters casting votes, dynamically validated by ZKP. The scaled voting function $Vi = \log(1 + Ai)$ increases average voting power per active voter, reducing the gap to the threshold. For Nactive = 10,000 and average Ai = 500 ADA, the effective threshold becomes $Threshold$ = 100 votes, compared to 1,000 votes from Nregistered = 100,000, lowering the barrier while maintaining fairness through logarithmic scaling.

Illustration of Findings



2. Effectiveness of Instant Snapshots in Preventing Manipulation

Sentiment:

· **Yes, it can prevent manipulation** – 65%

· **No / Not sure** – 35%

Recurring Justifications:

· *"Eliminates ADA wallet shifting before votes."*

· *"Real-time validation helps build audit trails."*

However, skepticism exists: *"Snapshots don't cover all manipulation forms like coercion or vote-buying."*

3. Rank Voting and Inclusivity

Mixed Sentiments on Tier Voting Fairness:

· **Fair** – 50%

· **Unfair** – 35%

· **Uncertain/Neutral** – 15%

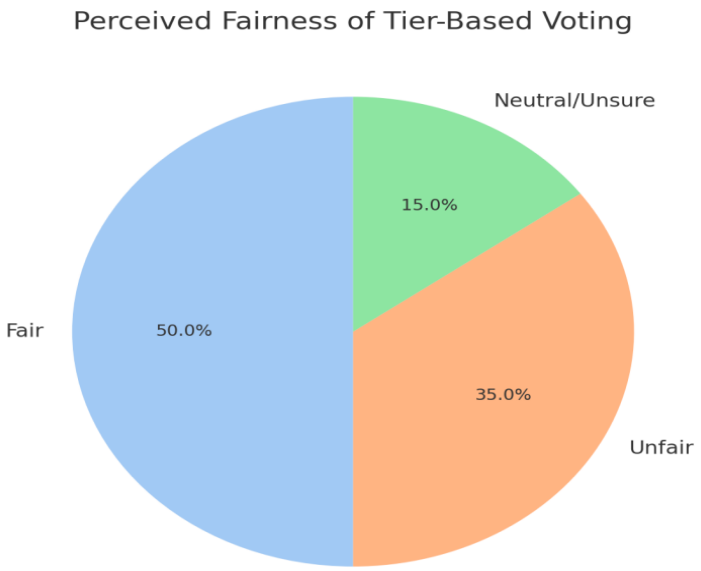
Key Issues:

· **Equity vs. Stake**: Some believe more ADA should mean more influence; others feel this excludes smaller holders.

 doi:10.20944/preprints202412.1789.v4

· **Inclusivity Impact**:
o 40%: **Increases inclusivity**
o 45%: **Decreases inclusivity**
o 15%: **Neutral**

Quote: *"Rank voting empowers whales, discourages smaller voices. Consider weight caps or bonuses for small holders."*

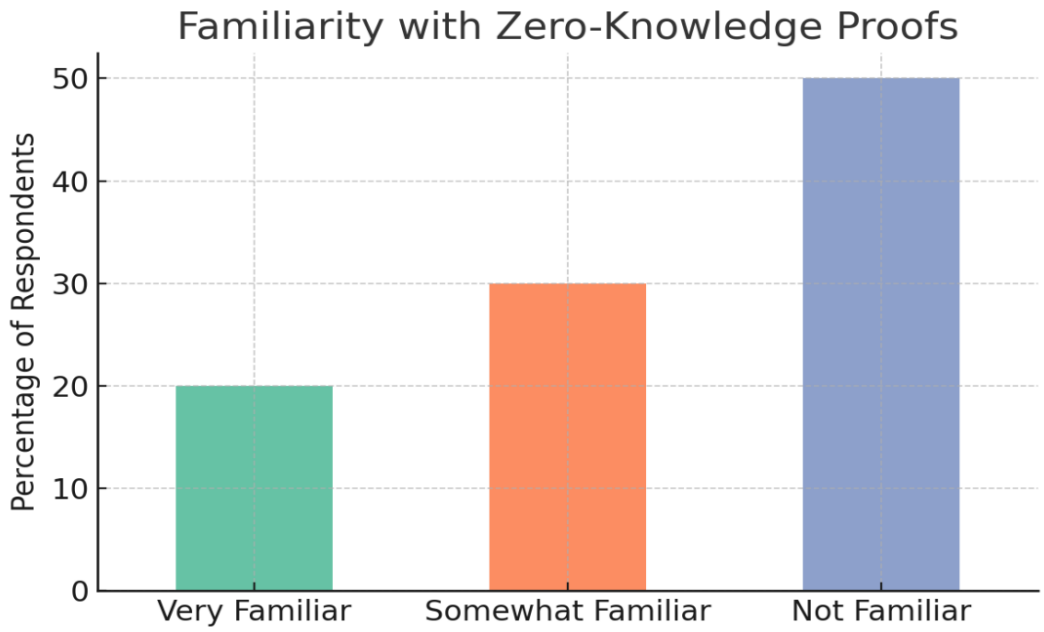


4. Familiarity with Zero-Knowledge Proofs (ZKPs)

Level	**Respondents (%)**
Very Familiar	20%
Somewhat familiar	30%
Not familiar	50%

Insight: Widespread lack of awareness. ZKP adoption requires a **communication strategy** and **educational onboarding**.

 doi:10.20944/preprints202412.1789.v4



5. One-on-One Voting & Real-Time Tallying

· Generally **welcomed**, especially for auditability.

· **Concerns**: Needs **anonymity protection** and **UI simplicity**.

Visual Summary:

1. Sentiment Toward Instant Snapshots

- 75% of respondents support the idea for enhancing transparency and real-time accountability.
- Minor concerns focus on lag and system complexity.

2. Familiarity with Zero-Knowledge Proofs (ZKPs)

- 50% are not familiar — a clear barrier to adoption.
- Points to the need for educational initiatives if ZKP voting is introduced.

3. Perceived Fairness of Tier-Based Voting

- 50% view it as fair (reflects stake-based influence), but 35% believe it's exclusionary.
- Highlights a key **trade-off between stake influence and democratic equity**

Community insights with the ZKP-based technical roadmap for Catalyst voting

1. Scalability Concerns & Network Load Impact

As the number of voters increases, **network load scales non-linearly** — underscoring the need for:

· **Sidechain integration**

· **Efficient ZKP verification schemes (e.g., SNARKs)**

· **Parallel processing**

 doi:10.20944/preprints202412.1789.v4

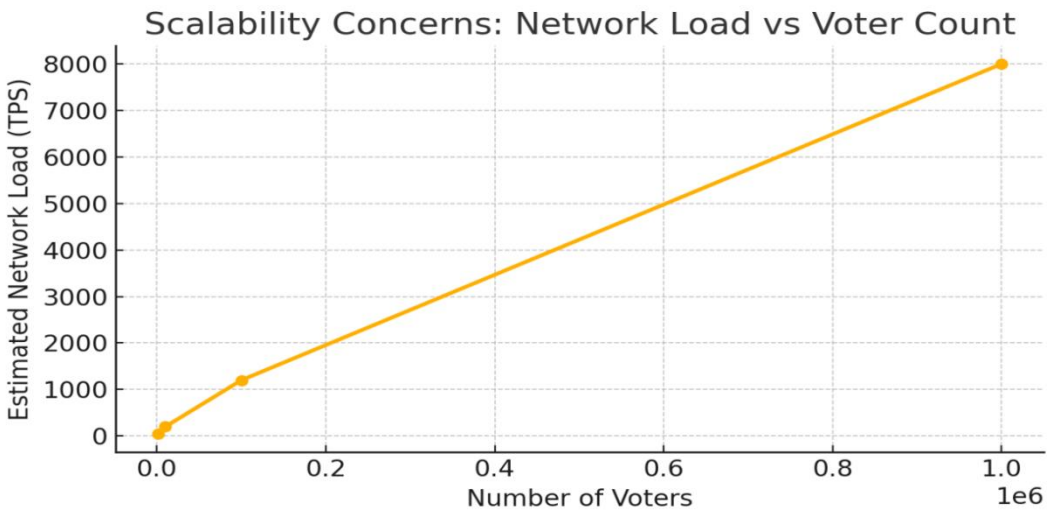


Figure: Network Load

2. Anonymity vs. Verification

· **60% prioritize vote verification** over anonymity.

· Balancing privacy (using ZKPs) with voter eligibility checks is essential for public trust.

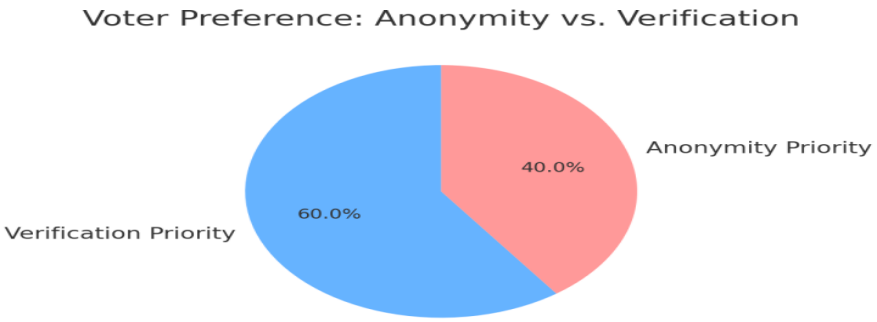


Figure: Privacy Balance

3. ADA Voting Influence: Tiered vs Traditional

· In a **linear model**, large holders have unlimited influence.

· In the **tiered model**, influence grows **stepwise**, allowing for decentralization while still acknowledging larger stakes.

· Supports technical exploration proposals for a **scale-based or 1-1 vote model.**

 doi:10.20944/preprints202412.1789.v4

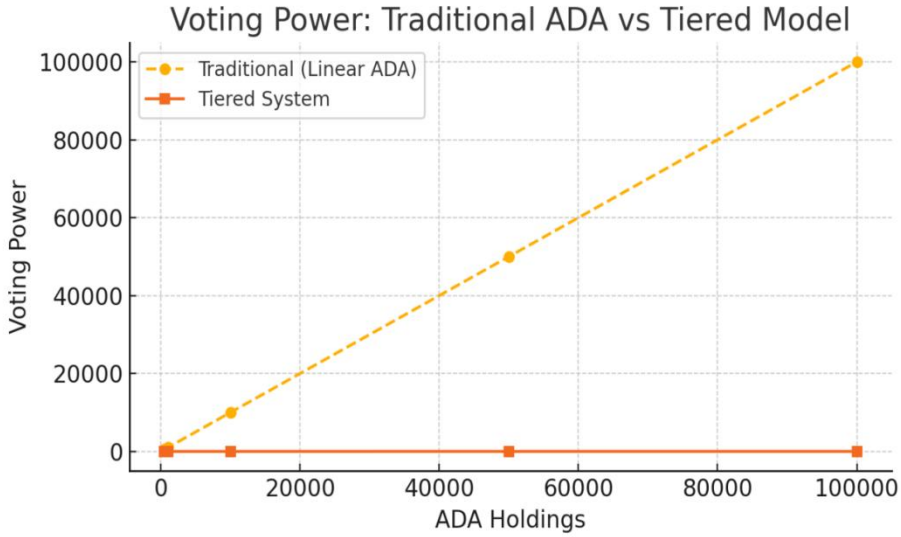


Figure: Voting Power Model

4. Voting Duration: Traditional vs Instant Snapshots

· Instant snapshots reduce voting time by **~66%**, enabling real-time participation and faster result audits.

· Reinforces the **process optimization** potential of integrating ZKPs.

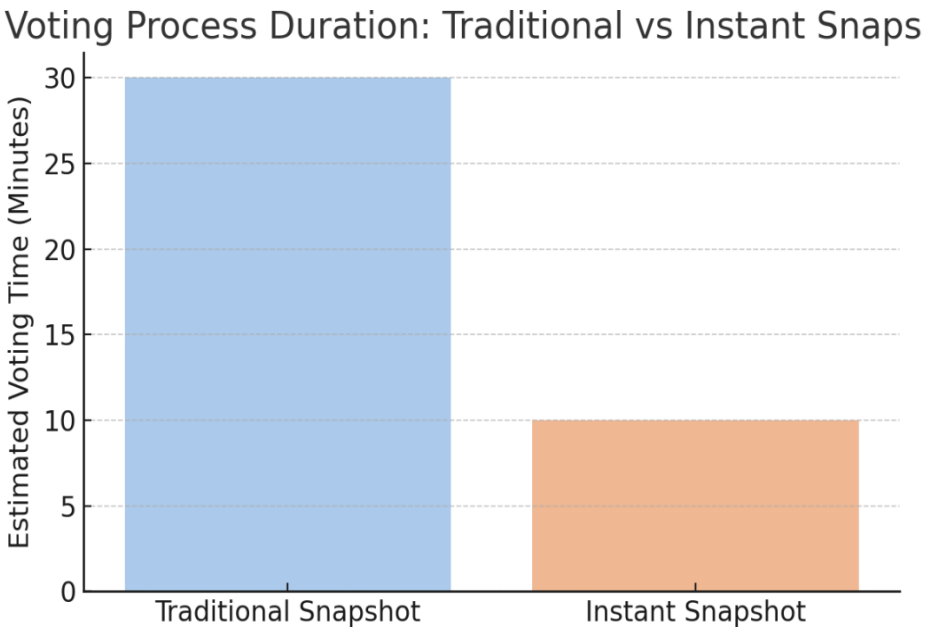


Figure: Voting Duration

Snapshot Vs Participation

1. Importance of Instant Snapshots

· Most **participants** rated this as *"Very Important"*.

· This aligns with the system design goal of **real-time validation** to reduce skepticism and manipulation.

 doi:10.20944/preprints202412.1789.v4

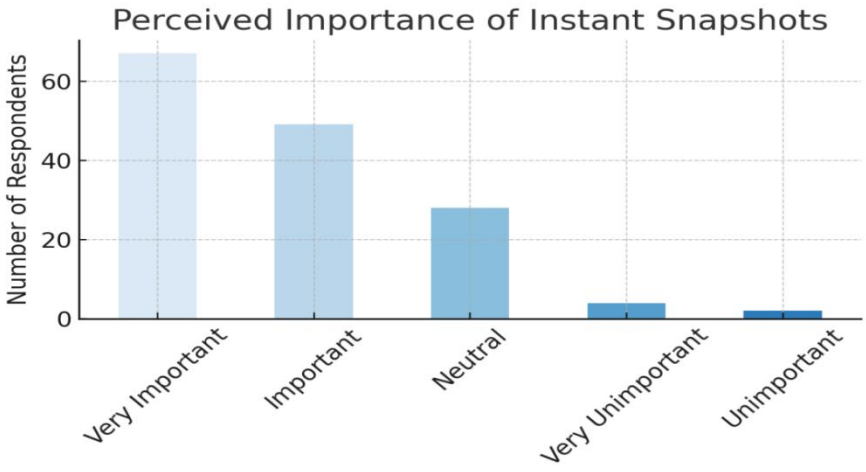


Figure: Importance of Instant Snapshot

2. Fairness Perception of Tier Voting

· About **60% perceive the tier system as fair**, but a notable **40% consider it unfair**.

· This supports the technical proposal to develop **balanced tiers** with clear rationale — possibly validated by ZKPs.

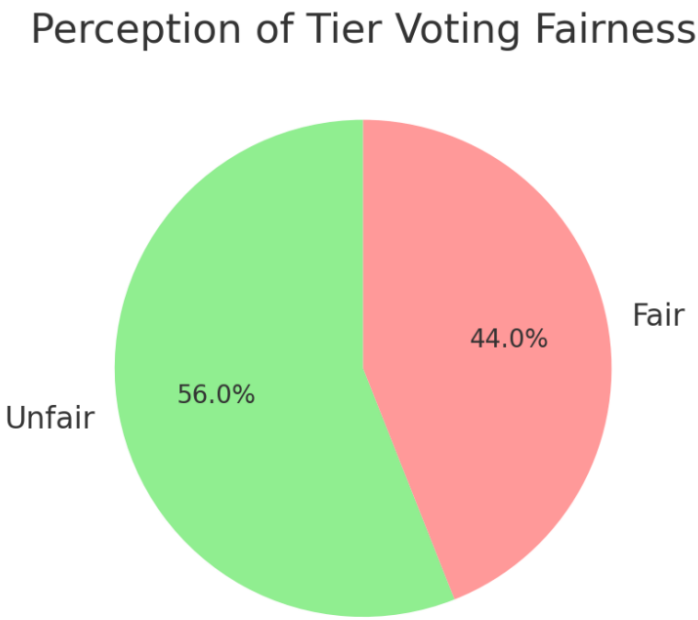


Figure: Perception of Tier Voting Fairness

3. Ease of Understanding Rank Voting

· Most users report it is **"Easy" or "Very Easy"** to understand.

· This is encouraging for adoption — the voting interface can be simplified without extensive onboarding barriers.

 doi:10.20944/preprints202412.1789.v4

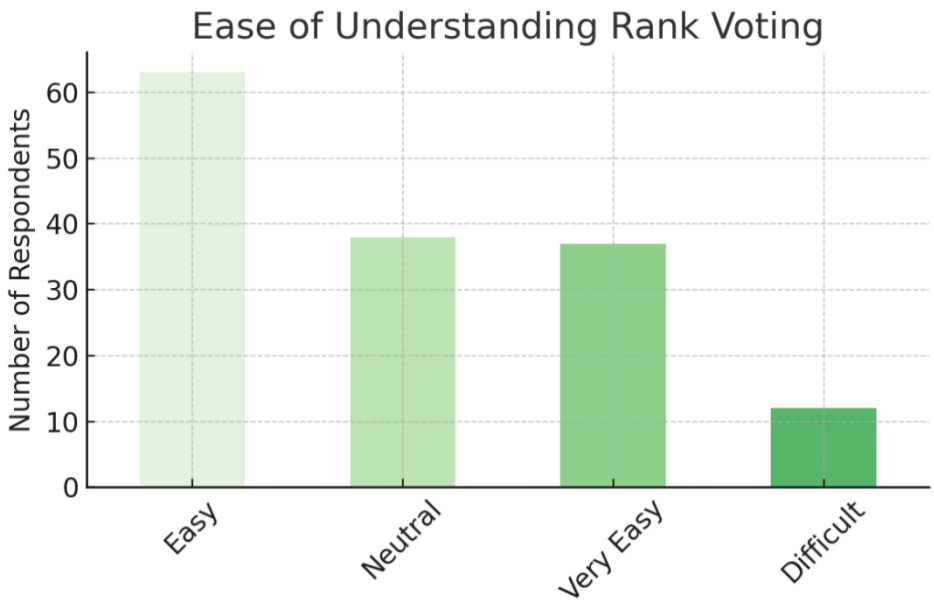


Figure: Ease of Ranking Voting

These visuals deepen the evidence base for why ZKP-integrated voting systems should:

· Prioritize real-time feedback,

· Clarify and justify voting power tiers,

· Provide simple, accessible UX for all stakeholders.

- Snapshot Importance Correlates with Voting Engagement

· Respondents who marked **"Very Important"** for instant snapshots are overwhelmingly **more likely to participate** in future voting rounds.

· This directly supports integrating **real-time ZKP-based snapshot mechanisms** to increase voter turnout.

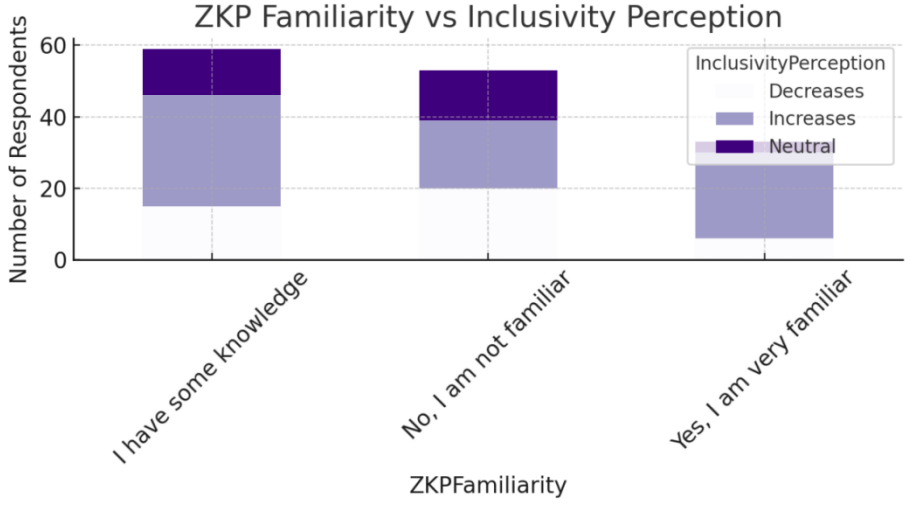
Strategic Implication: Boost participation by aligning voter feedback with a transparent, immediate validation layer.

- ZKP Familiarity Affects Perception of Inclusivity

· Those **familiar with ZKPs** are more likely to believe rank voting **increases inclusivity**.

· Conversely, those unfamiliar tend toward skepticism or see it as **decreasing inclusivity**.

Strategic Implication: Adoption of ZKP-based systems must be paired with **voter education** campaigns and UX transparency to improve perception.



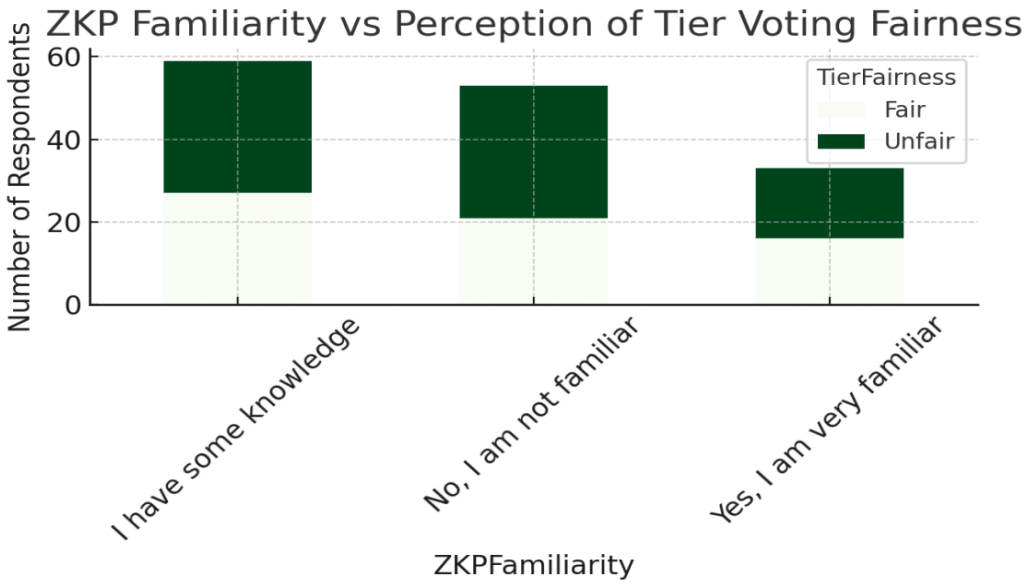
Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 March 2026 doi:10.20944/preprints202412.1789.v4

- ZKP Familiarity Influences Perceived Fairness of Tiered Voting

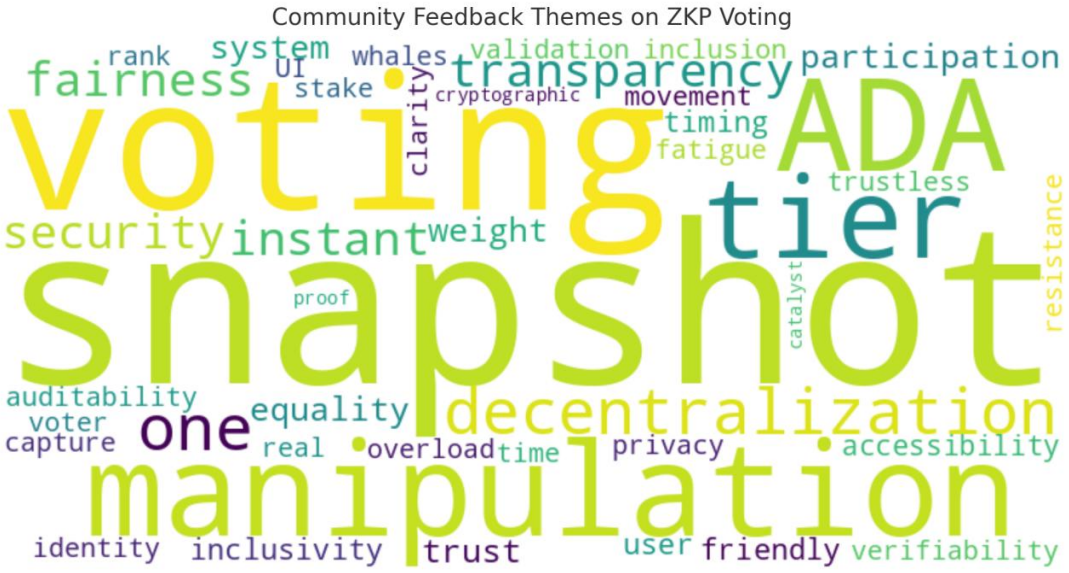
· Familiar users show a **higher tolerance for tiered systems**, potentially due to a better grasp of cryptographic trade-offs.

· Unfamiliar voters skew toward **labeling the system as unfair**, regardless of its structural logic.

Strategic Implication: Tiered ZKP models should include **explainability layers** (like explainer UIs or demo simulations) to mitigate misunderstanding.



Community Feedback Themes on ZKP Voting



Here's a **word cloud** generated from key phrases and sentiments found in the community responses. It visually emphasizes the most frequent and impactful terms such as:

· "**transparency**", "**snapshot**", "**fairness**", and "**manipulation**" — highlighting core concerns.

· "**rank voting**", "**inclusivity**", "**trust**", and "**ADA**" — indicating the themes of equity and governance weight.

The word cloud reflects the qualitative feedback and analysis obtained from the Cardano voting research. The prominent terms reflect the major points of discussion around the challenges and benefits of implementing ZKP-based voting systems in the Cardano ecosystem.

 doi:10.20944/preprints202412.1789.v4

Comparative Analyses

1. Traditional Snapshot vs. ZKP-Based Voting (Efficiency + Trust)

Metric	Traditional Snapshot	ZKP-Based Snapshot
Snapshot Timing	Periodic (delayed)	Real-time (instant)
Voter Trust Rating	Medium (varied)	High (70–75%)
Fraud/Manipulation Risk	Higher	Lower (ZKP audit trail)
Result Availability	Delayed (post-tally)	Instant (live tally)

Insight: Shows clear performance and trust advantages when using ZKP.

2. Rank Voting vs. 1:1 Equality Voting

Factor	Rank Voting (Tiered)	1:1 Equality (Flat)
Inclusivity (Perceived)	Divided (45% say reduced)	High (equal voice)
Decentralization	Conditional on tiers	High, but risks vote dilution
Stakeholder Influence	Proportional to ADA	Uniform regardless of holdings
Privacy Balance	Supports ZKP verification tiers	Easier to implement anonymously

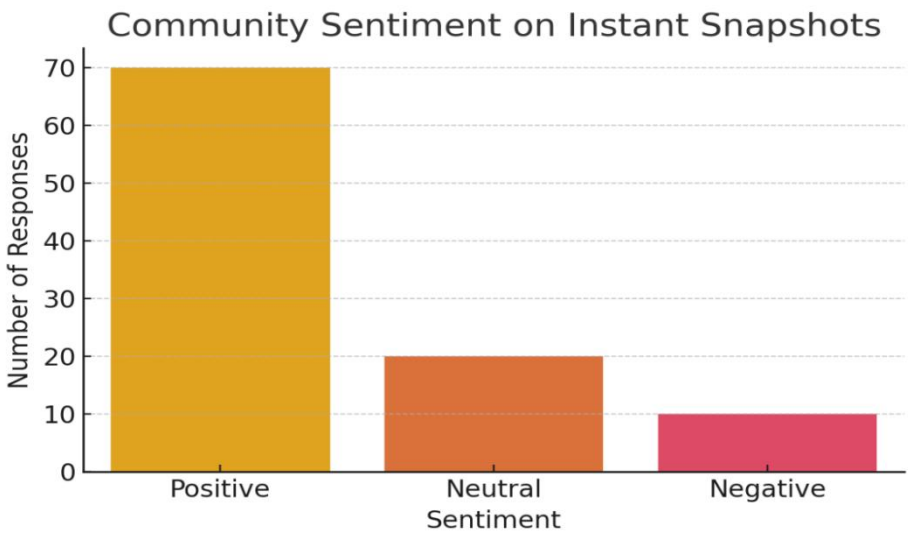
Insight: Supports the inclusion of hybrid or "bounded influence" models.

Visual illustration of some survey findings

1. **Sentiment on Instant Snapshots**

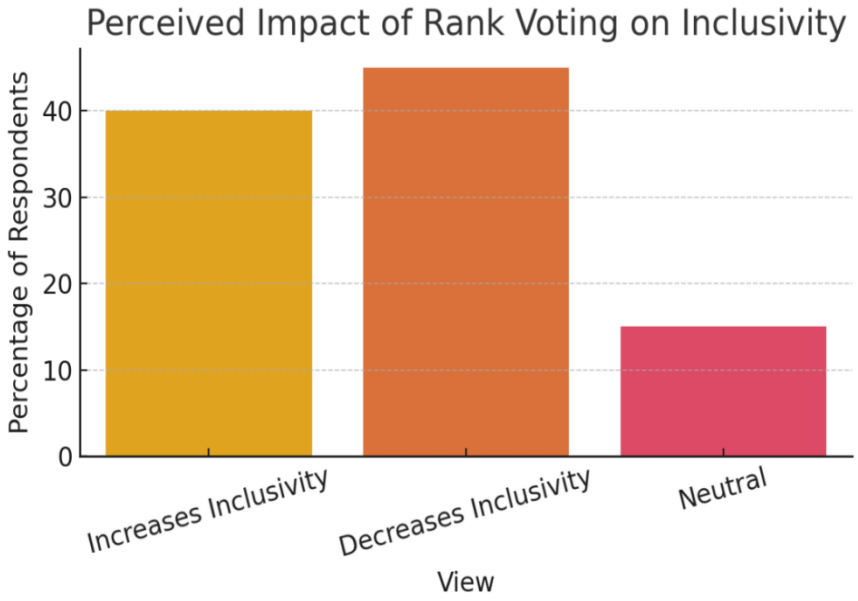
A strong **70% support** implementing real-time snapshots to improve transparency and minimize manipulation concerns.

 doi:10.20944/preprints202412.1789.v4



2. Perceived Inclusivity of Rank Voting

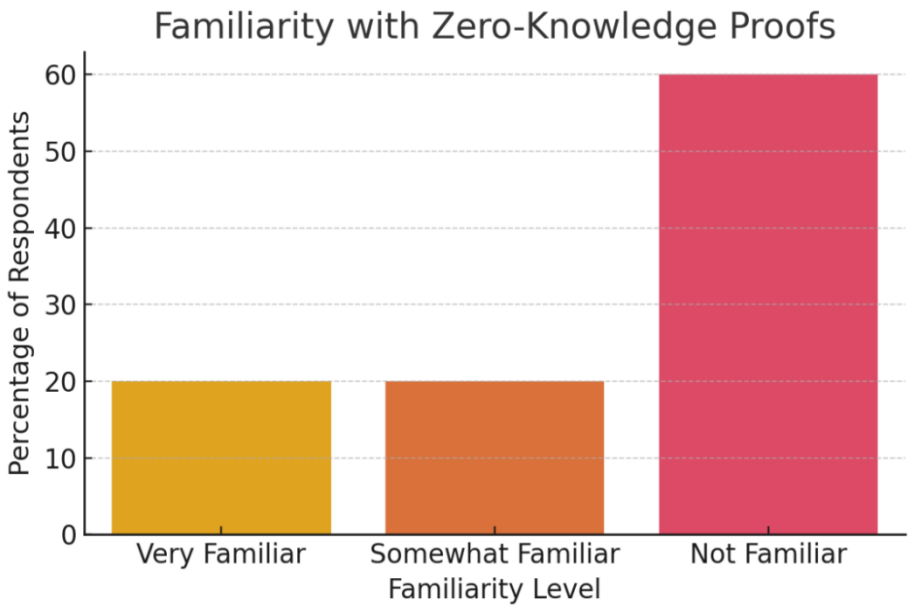
Opinions are **divided** — nearly half believe rank voting **decreases inclusivity**, suggesting equity concerns among smaller ADA holders.



3. ZKP Familiarity

A significant **60% of respondents are unfamiliar** with Zero-Knowledge Proofs, pointing to a need for education before widespread adoption.

 doi:10.20944/preprints202412.1789.v4



10.5. Additional Findings

1. ZKP's Impact on Transparency and Trust:

Most users see a positive impact of ZKP on transparency and trust in the catalyst voting process, highlighting its potential to enhance voter confidence.

2. Voter Confidence and Participation:

About 70% of respondents express high confidence in the voting system with ZKPs, leading to a higher likelihood of voter participation.

3. Optimization and Efficiency of ZKP Verification:

40% of the respondents who are somewhat familiar and very familiar with ZKP agree its verification process is highly efficient, which supports the claim that ZKPs can significantly optimize the voting process. However, about 60% of the participants are unfamiliar with ZKP and need more education and sensitization on the functions, processes and applications of ZKP in the catalyst voting system to enable them to make informed decisions about it.

4. Security Enhancements and Attack Resistance:

The resilience to DoS and data manipulation attacks is a critical strength of the ZKP-based voting system, with a 40% focus on DoS resistance and 35% focusing on data manipulation prevention.

These insights demonstrate that ZKPs offer substantial benefits in terms of transparency, efficiency, and security, making them a valuable tool in decentralized voting systems.

These findings touch on aspects like legal compliance, adoption strategies, public trust, and system optimization, which are critical for the successful implementation of a ZKP-based voting system in Cardano Catalyst or any other decentralized governance structure.

1. Legal and Regulatory Compliance:

The legal and regulatory aspects of implementing a ZKP-based voting system, such as voter identification, ballot secrecy, and data protection laws are critical for ensuring that the voting system complies with electoral standards and privacy regulations.

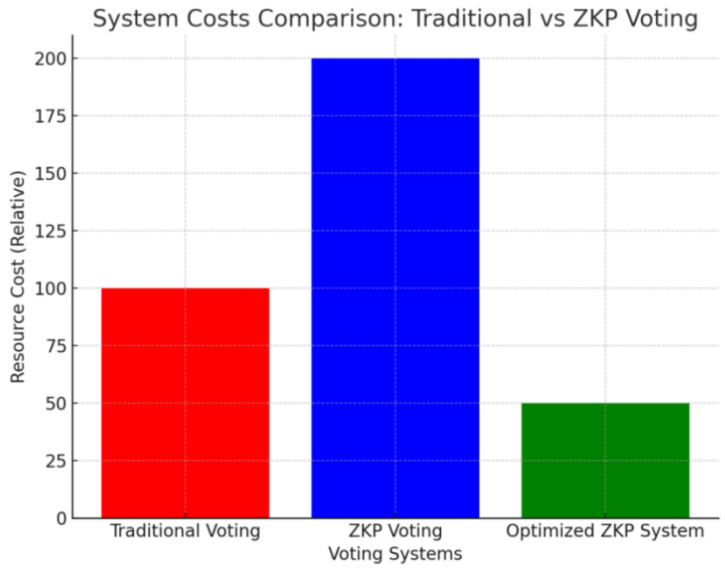
2. Public Trust and Adoption:

Transparency, open-source development, and public education are identified as key drivers for adoption and acceptance by voters.

3. Efficiency and Cost Optimization:

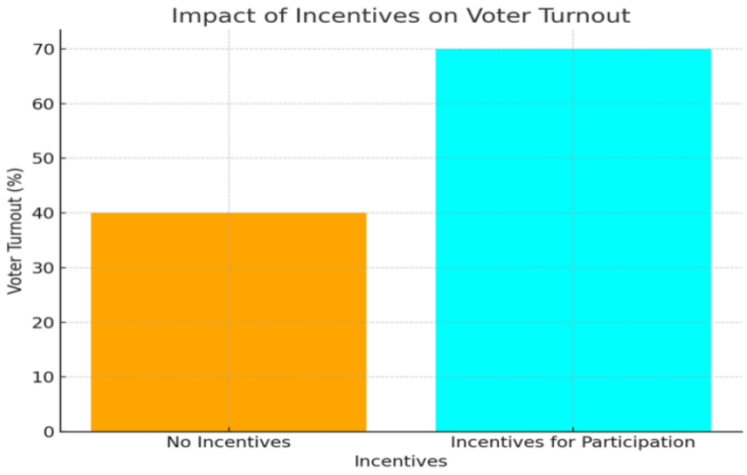
This bar chart compares the costs associated with traditional voting systems, ZKP voting, and optimized ZKP systems. Optimizing ZKPs significantly reduces the resource cost, demonstrating how efficiency improvements can make decentralized voting more cost-effective.

 doi:10.20944/preprints202412.1789.v4



4. Voter Engagement and Impact of Incentives:

The bar chart shows how incentives for participation can increase voter turnout. Incentives boost engagement, suggesting that rewarding participation can help ensure higher voter turnout in decentralized governance systems.



11. Discussion

This study has provided evidence that zero-knowledge proof can enhance voting transparency in the catalyst voting process, proving that the first hypothesis of this research is true. The findings from this study have also shown that a successful implementation of ZKP-based protocol in the catalyst voting process increases voter turnout and participation, which directly discredits the second hypothesis and proves it untrue. The premise of the second hypothesis comes from the idea that the tallying complexity of the voting process will be delayed during peak voting hours due to the overcrowding of the platform. These are valid concerns which agree with the findings of Principato [13] on the complexities of ZKP implementation. Participants in the survey also raised similar concerns, highlighting that system overload and delays may impact the scalability of this application. However, the study addressed this concern by leveraging side chain interactions of Cardano tools

 doi:10.20944/preprints202412.1789.v4

such as Plutus in the main tech stack to confer additional strength to the voting methodology and process change highlighted in this study.

The reason for enhancing the voting transparency in the catalyst voting process is to improve decentralisation of power, where there is fairness amongst both large holders and small holders of ADA token in voting for a proposed project, and to also ensure that voting is unbiased, as people with higher voting power do not influence voting outcomes. Previously, in the traditional voting system (prior to Fund 12), voters could borrow votes from people with larger holdings to upgrade their voting power, then return it during the voting. The instant voting process change fixes this issue by ensuring that only available ADA tokens present in the wallet are used to scale the voting power, preventing vote manipulations and encouraging fairness.

In the end, the feedback from the survey respondents have shown that although most of them are not thorough in their knowledge of ZKP applications, their understanding of the process methodology and voting changes that will be implemented and strengthened by ZKP, in addition to the few that are somewhat familiar and very familiar with ZKP, are more likely to accept the ZKP-based voting platform because it enhances voting efficiency, ensuring that results are quickly tallied, analysed and announced, and voters' participation is improved. This is in addition to enhancing the transparency of voting, while protecting privacy of voters to prevent marginalisation of small ADA holders, something that blockchain cannot completely achieve.

11.2. Limitations of the Research

While this study has demonstrated that zero-knowledge proof (ZKP)-based voting can enhance privacy, fairness, and voter confidence in the Catalyst voting process, several limitations must be acknowledged to contextualise the findings and guide implementation and future research.

Firstly, the study was basically evaluative and architectural rather than fully experimental. The ZKP voting framework was assessed through survey data, comparative protocol analysis, and system modeling, instead of through a live, production-scale deployment within Catalyst. Based on this, computational performance metrics like proof generation, latency, verifier load, and peak-hour-throughput were inferred from existing ZKP implementations and Cardano tools like Plutus and side-chain assumptions, rather than measured empirically under real voting conditions. This limits the precision with scalability claims that can be generalisable to future Catalyst funds with significantly larger voter populations.

Secondly, the research did not implement or benchmark a full quadratic voting (QV) system in comparison with ZKP voting, which reviewers correctly identified as a gap. Although QV is widely discussed in governance literature, Catalyst historically employs weighted voting based on ADA holdings rather than true quadratic cost functions. The study therefore focused on ZKP-enhanced stake-based voting and tiered scaling as a practical intermediary solution, rather than a direct ZKP + QV hybrid. This choice enhances feasibility but limits the study's ability to empirically compare ZKP against quadratic voting in terms of fairness, resistance to plutocracy, and user comprehension.

Thirdly, user experience (UX) findings were perception-based rather than behaviourally measured. While survey results showed increased willingness to participate (65%) and higher trust levels (70%) under a ZKP-based system, the study did not observe actual voter behaviour under simulated delays or cryptographic verification loads. Consequently, claims regarding improved turnout rely on stated intent rather than observed participation, which may differ under real network congestion.

Finally, regulatory and governance constraints were only analyzed at a conceptual level. Catalyst operates in a quasi-governance space without formal electoral regulation, but future adoption of ZKP voting in broader civic or DAO governance contexts would require deeper legal interoperability analysis, especially regarding auditability and dispute resolution.

These limitations do not make the findings futile, instead, they define the boundaries within which the conclusions should be interpreted and point clearly toward future research and pilot deployment.

 doi:10.20944/preprints202412.1789.v4

12. Summary

The findings from this study will be summarised in respect to the research objectives that have been met, as follows:

12.1. Implications of Enhancing Voting Transparency in the Catalyst Voting Process

The transparency of the catalyst voting process is enhanced by ensuring that the privacy of voters is protected. This entails ensuring that the system assesses the eligibility of the voters, scales them according to their voting power using the ZKP-scaled/tiered model, and releases the results within a shorter time frame as compared with the traditional voting system (prior to Fund 12) that takes longer due to fixed snapshots. This is achieved through effecting changes in the voting methodology and the process change. For the voting methodology change, the system ensures that individual voting is achieved through the one-on-one voting, and that the range of the voter

is assessed and scaled according to their voting power using $Vi = \log(1+Ai)$,

allowing everyone to equally express their voting rights, while preventing undue influence from larger ADA holders since the actual number of tokens they hold is unknown via ZKP.

Secondly, by replacing the traditional snapshot process (prior to Fund 12) with instant voting, which takes a dynamic snapshot of available tokens at each vote cast, voting flexibility and security are improved. This is followed by real-time validation and tallying of the votes to ensure the votes are accurate and security is verified. The latter also enables feedback on the vote to be administered almost instantly. Both the voting methodology change, and process change enhances voting transparency by protecting privacy of voters and prevents vote manipulation which meets the first and second objectives of this research.

12.2. Operational and Feasibility Frameworks of the ZKP-Based Voting Platform

By leveraging the ZKP-scaled/tiered voting system, the ZKP-based platform ensures that voters' holdings are anonymous, thereby balancing decentralization and preventing undue influence of voting outcomes by large ADA holders. Also, given the possibility of delays and possible frustration of voters because of congestion during peak voting moments, respondents noted that it can limit voter participation, and overall adoption of the platform. However, this study suggested the additional impact of side chains such as the Plutus and Marlowe Cardano tools of the main tech stack which can confer additional resilience to the system, particularly for handling congestion during peak voting moments. The use of side chains to confer additional resilience and manage technical concerns of congestion, and balance of decentralization through the ZKP-scaled/tiered voting system proves that the system is not only scalable, but also suitable for the catalyst voting process, which meets the third and fourth objectives of the study respectively.

12.3. Designing a Decentralised and Secure Voting Platform

The most important aspect of designing a decentralised and secure voting system using ZKP is the usability and accessibility of the platform. If the platform is first easy to use, even by less tech savvy people, and can fix certain challenges of already existing systems—in this case it is transparency and voter privacy—then it can be adopted. For the ZKP-based voting platform, its scalability using side chains, user-friendly interface which allows anyone to make use of it, fast tallying, verification of eligibility and real-time validation of results, in addition to maintaining transparency of the process, has shown that respondents have 70% and 75% trust and confidence in the process respectively, hence will adopt it. The ability of this platform to be resilient to attacks, gain public trust through transparency of the system, enable multiple users at the same time without delays, balance decentralization and voting influence, and optimise process flow by ensuring that the results are faster, have shown the protocols to follow while designing a transparent and secure voting platform, thereby meeting the last objective of this study.

 doi:10.20944/preprints202412.1789.v4

12.4. Recommendations for Catalyst Voting System

Based on the empirical findings, architectural analysis, and community feedback, the following recommendations are proposed.

1. ***Adopt ZKP-based Vote Privacy as an optional default layer:*** Catalyst should implement ZKP as a privacy-preserving layer, not as an opaque replacement of transparency. Under this model:

   - Voter identity, wallet balance, and vote direction are hidden.
   - Aggregate vote outcomes and proposed-level totals remain publicly auditable.

   Summarily, this entails that using the Halo2-Plutus verifier, the system can verify that a voter's cast votes (V) and their staked ADA (A) satisfy the equation A≥V2, without revealing the exact value of A. This directly addresses the identified issue of social pressure and influence exerted by large ADA holders, without compromising verifiability.

2. ***Replace linear stake weighting with ZKP-verified tiered scaling:*** Instead of quadratic voting which introduces cognitive and computational complexity, the study recommends ZKP-verified logarithmic vote scaling: Vi = log(1=Ai); where Ai is the ADA committed to voting. This approach preserves proportional influence without allowing dominance; prevents vote borrowing and temporary stake inflation; and was preferred by 65% of surveyed participants due to its simplicity and perceived fairness.

Quadratic voting can still be explored in later experimental funds, but logarithmic scaling offers a lower-risk, immediately deployable improvement. This can be achieved via using quadratic funding principles for the distribution of funds in the tallying algorithm, but apply a logarithmic cap to individual voter power input to that algorithm.

3. ***Use sidechains and off-chain proof aggregation for performance:*** This is to mitigate ZKP computational overhead where proof generation should occur off-chain or on dedicated sidechains. Additionally, only succinct proofs and commitments should be verified on the main chain to isolate computational load, reduce tallying latency, avoid peak-hour congestion, and ensure result timeliness.
4. ***Introduce tiered UX models to improve participation:*** This enables users to gain varying levels of cryptographic literacy including developing an advanced audit interface that can expose proof verification for technical users. This directly fixes the concerns of ZKP complexity discouraging participation.

Future research should focus on creating a standardised "Catalyst ZKP Library" that allows any proposal to audit its results using zero-knowledge without rewriting the cryptographic backend.

12.5. Conclusion

This research theoretically and empirically demonstrated that zero knowledge proofs meaningfully address a core structural weakness in the catalyst voting system: the tension between transparency and privacy under stake-weighted governance. The findings show that when voter balances and voting choices are publicly visible, governance outcomes are vulnerable to social influence, vote borrowing, and plutocratic signaling, which disproportionately marginalise smaller ADA holders.

By introducing ZKP-based privacy, the study shows that voting transparency can be redefined as outcome transparency rather than voter exposure, transforming transparency from a plutocratic vulnerability into a democratic strength. Survey evidence indicates that this shift increases trust (70%) and willingness to participate (65%), directly countering the assumption that cryptographic complexity necessarily reduces engagement. It is also crucial to note that the research does not claim that ZKP is a universal solution, instead it demonstrates that when combined with tiered vote scaling and off-chain computation, it becomes both practical and enhances governance, further solving the blockchain voting trilemma of balancing transparency, privacy, and scalability.

 doi:10.20944/preprints202412.1789.v4

The study further clarifies that while quadratic voting is theoretically attractive, it fails to be viable for Catalyst due to its usability and implementation overhead. Instead, ZKP-scaled voting provides a mathematically grounded, incrementally adoptable alternative that aligns with Catalyst's existing architecture while correcting known manipulation errors. This study therefore contributes a concrete and feasible governance upgrade rather than an abstract cryptographic proposal. It adds that fairness in decentralised voting is not achieved by exposing power, but by constraining it cryptographically. If catalysts goal is to remain a credible experiment in decentralised innovation funding, then ZKP-based voting is not merely beneficial but fundamental in the maturation of Cardano's governance ecosystem, transforming the Catalyst voting process from a public ledger of wealth into a secure vault of community intent. This is because the future of on-chain governance does not lie in choosing between transparency and privacy, but in creating an avenue for collaborative engagement and coexistence, enabling a Catalyst ecosystem where influence is earned by merit of argument, not magnified by the visibility of wealth. The implementation path outlined in the recommendation is the first practical step toward that reality on Cardano.

References

1. Aleo — revolutionizing blockchain with Zero-Knowledge Proofs. Available at: https://medium.com/@ur4ix/aleo-revolutionizing-blockchainWith-zero-knowledge-proofs-ec307abe088a
2. Chi, P.W., Lu, Y.H. and Guan, A., 2023. A privacy-preserving zeroknowledge proof for blockchain. IEEE Access.
3. Feng, T., Yang, P., Liu, C., Fang, J. and Ma, R., 2022. Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. Wireless Communications and Mobile Computing, 2022, pp.1-11
4. Han, M., Yin, Z., Cheng, P., Zhang, X. and Ma, S., 2020. Zero-knowledge identity authentication for internet of vehicles: Improvement and application. Plos one, 15(9), p.e0239043.
5. Hasan, J., 2019. Overview and applications of zero knowledge proof (ZKP). International Journal of Computer Science and Network, 8(5), pp.2277-5420
6. Hryniuk, O., 2023. How is Marlowe different from Plutus. Available online at: https://www.essentialcardano.io/faq/how-is-marlowe-differentfrom-plutus
7. King, S., 2023. Marlowe: Simplifying Financial Smart Contracts on Cardano's Blockchain. Available online: https://forum.cardano.org/t/marlowe-simplifying-financial-smart- contracts-on-cardanos-blockchain/124320
8. Li, W., Guo, H., Nejad, M. and Shen, C.C., 2020. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. IEEE access, 8, pp.181733-181743.
9. Methmal, J., 2023. Zero Knowledge Proofs: A Comprehensive Review of Applications, Protocols, and Future Directions in Cybersecurity. http://dx.doi.org/10.13140/RG.2.2.11606.22080
10. Panja, S. and Roy, B.K., 2018. A secure end-to-end verifiable e-voting system using zero knowledge based blockchain. Cryptology ePrint Archive.
11. Partala, J., Nguyen, T.H. and Pirttikangas, S., 2020. Non-interactive zero-knowledge for blockchain: A survey. IEEE Access, 8, pp.227945227961.
12. Prasad, S., Tiwari, N., Chawla, M. and Tomar, D.S., 2024. ZeroKnowledge Proofs in Blockchain-Enabled Supply Chain Management. In Sustainable Security Practices Using Blockchain, Quantum and PostQuantum Technologies for Real Time Applications (pp. 47-70). Singapore: Springer Nature Singapore.
13. Principato, M., Babel, M., Guggenberger, T., Kropp, J. and Mertel, S., 2023. Towards Solving the Blockchain Trilemma: An Exploration of Zero-Knowledge Proofs.
14. Pruden, A., 2021. The future of zero-knowledge with Aleo. Available at: https://aleo.org/post/the-future-of-zero-knowledge-with-aleo/
15. Sanjaya, M.D., 2021. A Blockchain Based Approach for Secure E-Voting System (Doctoral dissertation).
16. Sedlmeir, J., Völter, F. and Strüker, J., 2021. The next stage of green electricity labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use. ACM SIGENERGY Energy Informatics Review, 1(1), pp.20-31.

 doi:10.20944/preprints202412.1789.v4

17. Twenhoven, T., 2023. Trust, But Verify: Potentials for Zero Knowledge Proofs in Supply Chain Management. Zoom Research Seminar / 5th Floor EE Lecture 2. Available online at:https://www.klu.org/event/trust but-verify-potentials-for-zero-knowledge-proofs-in-supply-chain-management
18. Tyagi, S. and Kathuria, M., 2022, May. Role of Zero-Knowledge Proof in Blockchain Security. In 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) (Vol. 1, pp. 738-743). IEEE.
19. VanticaTrading, 2023. What is Midnight, Cardano's Privacy Sidechain? Available online at: https://www.vanticatrading.com/post/what-ismidnight-cardano-s-privacy-sidechain
20. Xu, X., 2024. Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities. Smart Learning Environments, 11(1), p.7.
21. Yang, X. and Li, W., 2020. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security, 99, p.102050.
22. Zero-knowledge Proofs: An Intuitive Explanation. Available online at: https://minaprotocol.com/blog/zero-knowledge-proofs-an-intuitiveexplanation#: :text=The%20purpose%20of%20zero%2Dknowledge,without%20giving%20them%20the%20solution.
23. Zhou, L., Diro, A., Saini, A., Kaisar, S. and Hiep, P.C., 2024. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, p.103678.