Research Intelligence

Blockchain Voting:

A Better Election System?

January 2024 Krungsri Research

krungsri Research

เครือ MUFG หนึ่งใน สถาบันการเงินที่ใหญ่ที่สุดของโลก

Contents

Subscribe Us

For research subscription, contact

krungsri.research@krungsri.com

Introduction

Blockchain technology has been widely discussed as a potentially world-changing innovation. Over the past decade, development of blockchain applications and their underlying technology have been relentless in both the public and private sectors, as well as in academia. Despite the significant interest in this technology, real-world use cases remain relatively limited both in Thailand and internationally. Most applications are often confined to the realms of digital assets and use in decentralized finance, or DeFi.

Domestic interest in blockchain technology was renewed following the conclusion of Thailand's most recent general election, held on May 14, 2023. This election generated considerable interest among the public, evidenced by a notable turnout of 75.71%. Many members of the public actively participated in observing the vote counting process, while media entities diligently provided real-time updates. Nevertheless, the official announcement of the election results occurred on May 25, 2023, indicating that it took 11 days for the election process to reach its conclusion. This then prompted **questions as to whether online voting would expedite and enhance the efficiency of ballot counting, and whether the integration of recent technologies like blockchain would further transparency.** Blockchain technology utilizes Distributed Ledger Technology (DLT), which does not necessitate a central authority to verify transaction accuracy. Consequently, incorporating blockchain into online voting could potentially foster transparency and mitigate tampering concerns.

Nathanon Ratanathamwat

Senior Analyst
nathanon.ratanathamwat@krungsri.com
+662 296 6389

Dr. Pimnara Hirankasi

Head of Research Division and Chief Economist
pimnara.hirankasi@krungsri.com
+662 296 6457

Blockchains and Online Voting

In principle, casting votes online should not only make the whole process easier and more convenient for both voters and those tasked with overseeing the election, it should also dramatically accelerate the process of counting votes. However, the success of online voting is built on four factors: (1) the internet, or the global interconnected computer network that allows for near-instantaneous communication and transfer of data; (2) hardware, or voting devices, which may include mobile phones, computers, or other internet-enabled devices that are accessible to and used by voters; (3) software, or the program or instruction set written to control the operations of a computer system, and; (4) cybersecurity, or the maintenance of security protocols that protect internet-enabled computer systems, software, networks, and data from the threat of unauthorized access and usage.

Whether local or national, when important elections involving a large number of voters are held online, it is imperative that these four factors are all at a high degree of preparedness. In many countries, voting has in fact already begun to move online for elections at a range of levels, though these have tended to be for local elections, or for those in smaller organizations or among more restricted groups of voters. Since 2018, blockchains have also been used in elections in a number of countries, and while these have been restricted to those that have been held within a single organization or that have extended over a limited geographical extent, this nevertheless marks an important step in the development of blockchain-enabled voting. Within Asia, blockchains have been used in smaller organizational or local elections in Thailand, Japan, and Russia, and these are thus the examples that are most often cited, while in the West, examples in the US have attracted the most interest from the media.

Table 1

Examples of Early Deployment of the Blockchain in Elections in 2018

Location	Purpose	Voting System	Developer
Bangkok, Thailand	Primary election to choose the leader of the Democrat Party	A live electronic voting system was used by over 120,000 party members as part of the process to select the new Democrat Party leader. Members were able to vote using either a device located at special voting stations or a mobile phone app (D-Elect).	Zcoin
Saratov, Russia	Local youth parliament election	The 'Polys' e-voting system was accessed by around 40,000 voters through special voting booths.	Kaspersky Lab
Tsukuba, Japan	Voting on social development programs for Tsukuba submitted by private companies, research units, and educational institutions	Voters accessed a computerized voting system located in the Tsukuba government offices, where special equipment was installed, including a card reader for voters' identity cards, also known as the 'My Number' card.	VOTE FOR
West Virginia, USA	West Virginia midterm elections	Soldiers and their families stationed overseas were able to vote in West Virginia midterm elections through the 'Voatz' mobile phone app. 144 individuals in 31 countries took advantage of the system to cast their votes.	Voatz

Source: Krungsri Research

Currently, although the use of blockchain in political elections has garnered increased attention, its actual usage has generated significant criticism. For example, in 2018, when West Virginia used blockchain-based voting for a limited subset of eligible voters, there were concerns regarding the security of the system and the accuracy of vote counting. These are matters that the public cannot definitively verify as neither the government nor the involved companies have disclosed essential information necessary to assess the success of using blockchain in elections. Experts have added their voices to the chorus of disapproval, suggesting a high probability of errors during system operation. They highlight risks to users' mobile phones, the election system network, and the servers handling data, all vulnerable to cyber exploits. Additionally, Voatz has been criticized over potential failures in the vote count. In practice, the voter's vote was sent digitally, as a PDF, to the county clerk staff for printing and inclusion in the tally alongside traditional paper ballots. While this process facilitated the post-vote tabulation audit, it did not contribute to the vote casting process. Online voters lacked the ability to verify the accurate recording of their vote or whether the automatically generated paper ballot truly reflected their intentions.[1/] Consequently, voters were compelled to rely solely on the integrity of state officials and the election management system, trusting that the recorded vote aligned with the cast vote. In fact, this instance exemplifies only one of the myriad concerns surrounding the adoption of blockchain-based voting systems.

Nevertheless, whether elections are conducted through traditional paper-based methods or online platforms, **transparency and data integrity remain at the heart of the election process that responsible authorities must always prioritize.** Officials tasked with organizing elections need to ensure that these concerns always remain front and center, and therefore, must be able to clearly demonstrate to voters, using credible evidence, that the election has indeed produced a "true winner.“

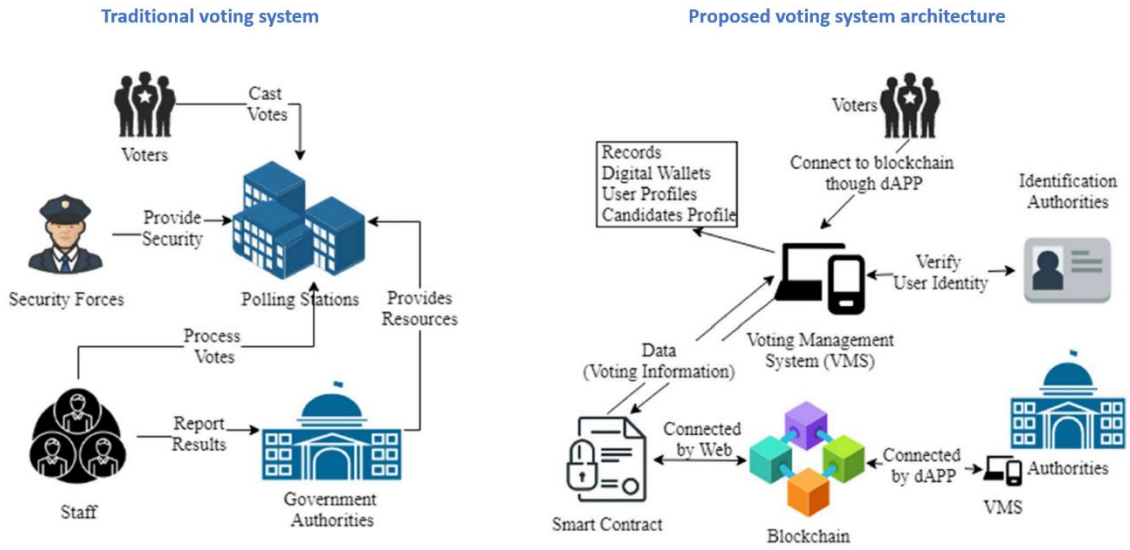
1/ https://slate.com/technology/2019/07/west-virginia-blockchain-voting-voatz.html

The BVMS – an example

A significant international effort has gone into researching blockchain-based voting and creating frameworks to ensure that this remains as transparent and secure as possible. Among these various proposals, the 'Blockchain-based Voting Management System' (BVMS) (Farooq, Ifthikhar & Khelifi, 2022) has achieved some prominence. BVMS proposes the use of a flexible consensus algorithm to govern system operations, enabling the adaptation of the consensus mechanism to accommodate a large number of users even while voting is underway. Moreover, it incorporates measures to prevent a 51% Attack,[2/] a potential threat during voting, and introduces a chain security algorithm to autonomously verify the correctness of the blockchain network. Additionally, BVMS integrates UTXO[3/] and smart contracts mechanisms to prevent incomplete or malicious transactions within the blockchain network, aligning with efforts to mitigate various vulnerabilities associated with blockchain-based voting systems. These endeavors distinguish BVMS from other systems.

Figure 1:

Traditional Voting System (Left) and the BVMS (Right)



Source: Farooq, Ifthikhar & Khelifi, 2022

2/ The 51% Attack refers to an assault aimed at altering transactions, distorting data, or gaining control over a blockchain network by miners with more than or equal to 51% of the network's hash power. This excessive mining control signifies that one miner has greater and/or faster mining capabilities than others in the network.

3/ UTXO is short for 'unspent transaction output', or the amount of cryptocurrency remaining in a wallet after a transaction has been processed and that can be used for future transactions. In this way, UTXO is similar to the change received when paying for an item with a bank note, which can then be spent on other goods in the future. Thus, the output (in the analogy, the change) from one transaction will be the input (or payment) for the next. UTXO therefore represents both the starting-point and the end-point of blockchain transactions.

In the BVMS election management system (Figure 1), eligible voters must have access to voting devices, such as mobile phones or computers, and they are required to register on the system to verify their identity beforehand. The BVMS advocates the utilization of smart contracts to verify whether (1) the voter is indeed eligible to vote and (2) if they have already exercised their voting rights. Upon successful completion of these verifications, the user's online wallet is credited with a single voting coin, which is then used for voting. Once used, the voting coin is deducted from the user's account, rendering them ineligible to cast another vote. Following the voting process, the system validates the transaction details, which are then recorded on the blockchain. Due to its structure, the BVMS system has the capacity to accommodate a large volume of voters concurrently, regardless of their geographical location. Additionally, every voter's transaction hash is stored on the blockchain alongside the result of the election, enabling registered users to check this on their screen displays or on the app's dashboard.

Table 2

Key Features of the BVMS

	The BVMS Framework
Flexible Consensus Algorithm	The system is designed to support multiple consensus mechanisms to accommodate a large number of voters. The default setting will be the Proof-of-Work consensus mechanism, but it can later be adjusted to other mechanisms, whether it be Proof-of-Stake, Proof-of-Vote, Proof-of-Trust, or Ripple, to maximize performance. (Descriptions of each consensus mechanism are shown in Box 1)
51% Attack	The system prevents 51% attacks by: (1) Recording the hash rate[4/] of each miner/verifier in advance within the system for monitoring purposes, thereby prohibiting miners with a hash rate exceeding 51% from mining during elections. (2) Implementing a pre-selection process for miners before elections, where miners are hired under the supervision of responsible authorities. During voting, continuous monitoring detects irregularities. If a miner attempts to add an unverified block, mining stops, and a 51% attack is declared. Nodes with larger chains win and monopolize the network. Permissioned blockchain requires Election Authority approval for node entry, preventing unauthorized access. Malicious nodes cannot join without credentials and permission verification at runtime.
Chain Security Algorithm	The Chain Security Algorithm ensures the integrity of the blockchain by automatically verifying the validity of the chain each time a new block is added or unauthorized changes occur in block data. The algorithm compares the hash values of the new and previous blocks. If the chain is valid, the Chain Security Algorithm allows replication on all nodes in the peer-to-peer network. If malicious activity is detected, the algorithm declares the chain invalid and informs all peers on the network.
Unspent Transaction Output (UTXO)	This system initiates a UTXO mechanism when a voter uses their voting coin to cast a vote, and ultimately, the coin will be transferred to the miner as their reward for processing the transaction in place of a transaction fee. When the voter uses their voting coin to vote and this is accompanied by their digital signature, the transaction will be registered, the mining operation will begin, and the UTXO value will be set to zero, thus preventing repeat voting.
Smart Contracts	A number of smart contracts may be created and deployed to serve different purposes. For example: (i) a contract that checks whether the user has the right to vote, and once this has been confirmed, the user will connect to a different smart contract that specifies which candidates the user may vote for; (ii) a smart contract linked to the user's national identification number and their wallet address that checks whether there is a voting coin in the user's wallet, and this will then be removed (or its quantity set to zero) after a vote has been cast (each user can vote once), and a notification sent to the user's registered mobile phone; and (iii) a smart contract that checks whether the user has not voted more than once by confirming their age and other personal details, as per their identification card.

Source: Krungsri Research

4/ The hash rate refers to the computational power of the network's miners in solving complex mathematical problems to validate and secure transactions on the blockchain. A higher hash rate indicates greater computational power and typically leads to increased security and efficiency in transaction processing.

Box 1 Summary of Consensus Algorithms

- **Proof of Work (PoW)**
  PoW systems typically involve individuals or organizations, known as 'miners,' who compete to solve complex mathematical problems. In an extremely simplified example, this might involve finding the two smallest numbers greater than 1 that are factors of a large number, e.g., 10,336,613. Once a miner proposes a solution to this (in this example, 2,903 and 3,571), the other network participants will confirm whether this is a valid solution to the problem, and if over 50% of these agree that it is, a reward will be provided to the miner that first proposed the solution. Because recording data to the blockchain operating under PoW requires that a majority of miners agree, it is difficult to make changes to data once it has been written into a block. However, PoW creates high competition among miners, thus requiring significant computing power and energy consumption. In this example, all miners are required to cycle through an algorithm to determine factors of large numbers and thus demand a lot of electricity. However, by comparison, confirming solutions, i.e., that 2,903 and 3,571 are indeed factors of 10,336,613, would be much simpler. [5/]

- **Proof of Stake (PoS)**
  PoS mechanisms randomly select validators to solve mathematical problems instead of miners competing against each other. The probability of a validator being chosen increases proportionally with the amount of money or coins staked by individual participants. Upon successful completion of the problem, validators receive a reward, while those providing incorrect solutions will have money or an equivalent deducted from their stake. PoS mechanisms are advantageous in terms of energy efficiency compared to PoW systems, primarily due to the absence of competitive mining. However, PoS consensus algorithms are not without their limitations. One significant concern is the potential for validators to collude and form cartels to share rewards, undermining the decentralization principles that underpin the transparency of blockchain processes.[6/]

- **Proof of Vote (PoV)**
  PoV mechanisms operate exclusively on consortium blockchains and utilize a voting mechanism to reach consensus, which is a conclusion accepted by all members of the group. This system has internal controls to balance power among members and ensures high security by separating voting rights from execution/bookkeeping rights, thus allowing members' consensus to determine operational control and the validation process of blocks without relying on external parties. Members in the group vote to select an execution team, with each applicant nominated by a member. This execution team consists of multiple individuals without a leader and works according to a predetermined term (followed by a new round of voting). The team is responsible for distributing transaction data to members for verification and voting, and transactions that receive a sufficiently large number of votes will be confirmed and recorded on the blockchain.[7/]

- **Proof of Trust (PoT)**
  PoT is a consensus algorithm that selects validators from within the decentralized network based on their 'trust score'. This score is calculated from an assessment of the validator's previous success in providing rapid and accurate verification of transactions, with the chance of being selected as a future validator weighted according to this score. Thus, network participants with a high trust score will have a higher chance of being chosen as validators for high-value transactions, resulting in their accumulating greater rewards over time compared to validators with low trust scores. PoT also incentivizes validators to act honestly, as failing to do so will result in a decrease in their trust score, reducing their ability to secure future rewards or payments.[8/]

- **Ripple and RPCA**
  The Ripple Protocol Consensus Algorithm (RPCA), developed by Ripple, is designed to be fast, scalable, and energy-efficient, making it ideal for processing high volumes of transactions in real-time. It utilizes an approach known as iterative consensus, where network nodes communicate to agree on transaction validity and order. This process involves continuously sharing and comparing transaction information until consensus is achieved, ensuring all nodes converge on a single valid ledger. The algorithm operates based on nodes in the blockchain, with each node creating a list of trusted peers known as the 'Unique Node List (UNL)'. When 80% of a node's UNLs agree on a transaction, the associated data is written into the blockchain. This process repeats every 2-3 seconds for each node.[9/]

Source: Krungsri Research

5/ https://www.krungsri.com/th/research/research-intelligence/the-merge-of-ethereum-2023

6/ https://www.krungsri.com/th/research/research-intelligence/the-merge-of-ethereum-2023

7/ https://www.researchgate.net/publication/323209703_Proof_of_Vote_A_High-Performance_Consensus_Protocol_Based_on_Vote_Mechanism_Consortium_Blockchain

8/ https://moralismoney.com/blog/what-is-a-proof-of-trust-consensus-protocol

9/ https://reasonabledeviations.com/notes/papers/ripple_consensus_protocol

In addition to the BVMS described above, many other protocols have been proposed as possible ways of meeting the challenges associated with integrating blockchains into online voting systems; but despite their differences, these all share the common goal of enhancing the transparency, safety, security, and independence of the electoral process, as well as to save costs associated with organizing large-scale elections. However, online voting can utilize various technologies beyond just blockchains, and this leads to another question: **Is online voting with blockchain better than without blockchain?**

Is blockchain voting really better?

For elections to be considered transparent and to maintain their integrity, they must demonstrate several qualities, but three of the most central include the following. (i) To ensure that voters' intentions are respected and that the overall process remains trustworthy, the individual votes cast and the count made must be verifiable and auditable. (ii) To prevent voter intimidation and block the possibility of vote-buying, ballots should be strictly secret, and votes should be anonymous. (iii) The management system, or the software, used in the election must be independent. Software independence means that any errors occurring in the election software must be detectable, traceable, and investigable to ensure fairness to candidates. Whether the errors are small or large, election managers must be able to explain them to the public to build confidence in the election results. Achieving these three fundamental principles is challenging for designers of online election management systems compared to using traditional paper ballots, due to the following constraints.

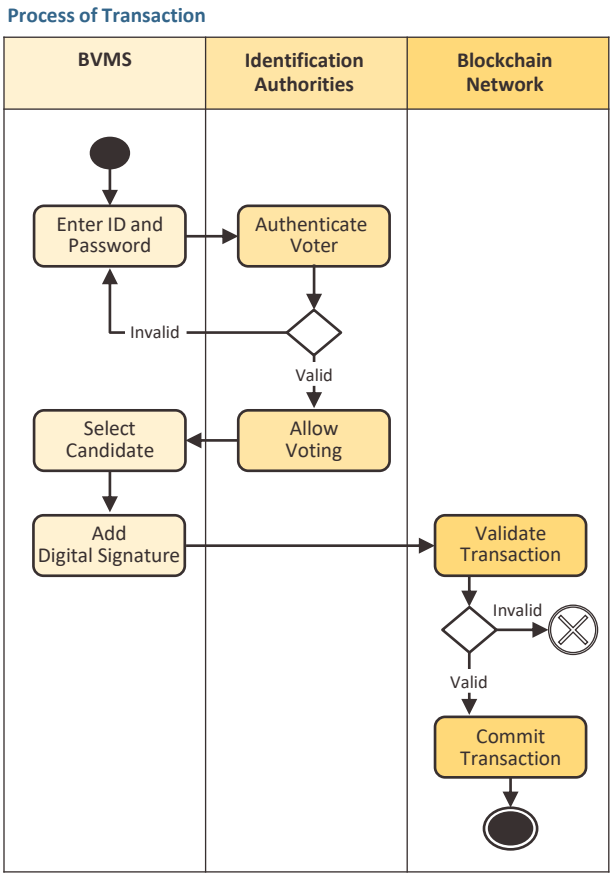
I. Verifiability and Auditability

The example of the 2018 West Virginia midterm elections described above illustrates how voters were unable to physically view the printed ballots included in the final count. Consequently, users had no means to verify if the actual ballot accurately reflected their voting intentions expressed in the app. Any errors in the electoral process would likely go unnoticed, but **blockchain technology can address issues like this with voter verifiability.** For instance, BVMS allows the hash of voters' blockchain records to be sent to their mobile phones, serving as a key for accessing the data on the blockchain. Access to this data is secured using the voter's public key and can be unlocked using the private key, enabling individuals to verify the transactions recorded in their wallet before confirming their vote. Data transmission is encrypted, and once the vote is confirmed, it cannot be altered. Additionally, adding a digital signature to the transaction will enhance the system's overall security. Utilizing blockchain technology in online voting, as proposed in BVMS, will thus restrict access to a voter's data to the voter alone, who can verify its accuracy and ensure that their recorded vote is the same as that which was originally cast.

Apart from voter verifiability, **auditability is also crucial in maintaining public trust in the electoral process.** Trust in election outcomes also depends on the ability to audit the system and verify the count, whether it is a centralized online voting system or a blockchain-based one. While blockchain systems may seem to offer advantages in security and transparency, online voting systems face various threats, including network security, user authentication, privacy maintenance, hardware vulnerabilities, and potential attacks on supporting infrastructure. Therefore, it may be concluded that, **for this issue, integrating blockchains into online voting systems does not automatically enhance the ease of auditing and verifying vote counts. In fact, the added complexity of blockchain systems may make this task even more challenging.**

Figure 2:

Proposed Ballot Verification Mechanism for Blockchain Voting



Source: Farooq, Ifthikhar & Khelifi, 2022; Krungsri Research

II. Ballot Secrecy and Voter Anonymity

Central to a healthy democracy is the protection of ballot secrecy and voter anonymity, guarding against intimidation, threats, and vote buying, thus enabling voters to express their genuine desires freely. Interestingly, research by Ostwald and Riambau on voting in Singapore shows that voting behavior changes when voters suspect that privacy and anonymity may have been compromised, even when in reality this was not the case and there were no-post election consequences for voters, however they had cast their ballots (Ostwald & Riambau, 2021). Ostwald and Riambau demonstrate that in these elections, when voters were worried that the secrecy of the ballot may not have been maintained, 3-5% of voters voted for the expected winner, even when this was not the party that they supported.[10/]

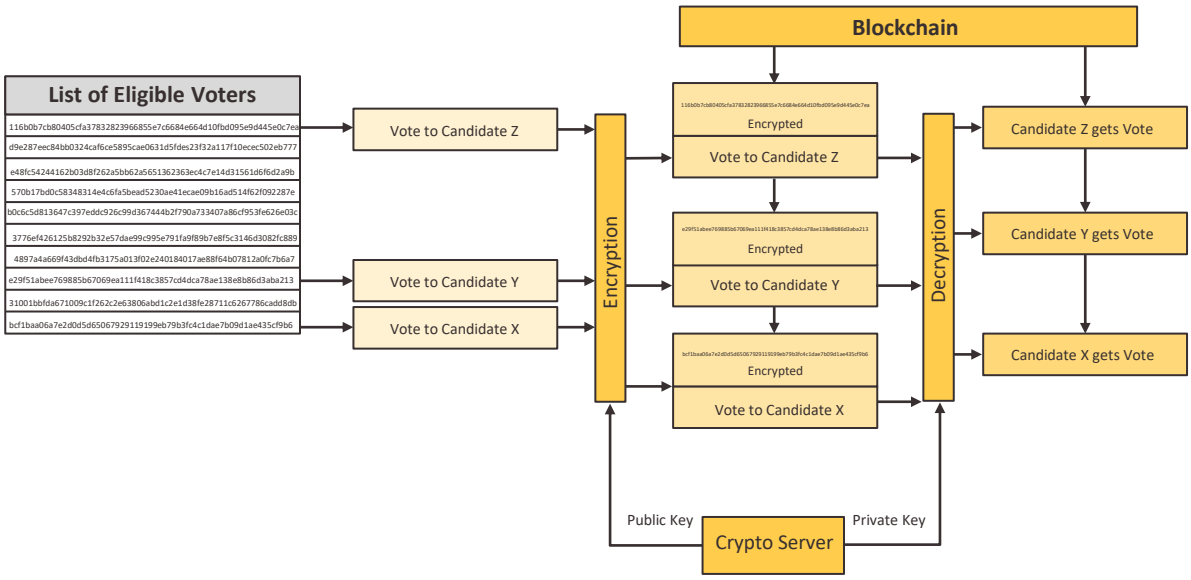
10/ For further details, please see Kai Ostwald and Guillem Riambau, 'Voting Behavior under Doubts of Ballot Secrecy: (Un)Intentionally Nudging Voters Towards a Dominant Party Regime', May 17, 2021.

Utilizing blockchains for election infrastructure offers several advantages over other technologies used in online voting. The decentralized and disintermediated nature of blockchain means there is no central authority, reducing the risk of data exposure and breaches of anonymity. Additionally, blockchain-recorded data is typically immutable, preventing tampering with voting records after ballots are cast. With encryption, both election officials and hackers have limited access to individual voting records, theoretically ensuring the confidentiality of election results until they are officially released.

Moreover, **using the blockchain as the data storage backbone will allow individual data from voters to be recorded as hashes, further helping to preserve anonymity.** One way this might be implemented is using Ethereum-based smart contracts (Alvi et al., 2022) designed to allow voters to identify themselves and establish their eligibility to vote without revealing personal information. On the blockchain, public keys function similarly to email addresses for identifying individuals, while hashes are used instead of the voter's personal data. These are combined, and the votes are encrypted to avoid exposing the link between ballots and voters. Once all the votes are collected and decrypted, the smart contracts transfer the voting coins to the relevant candidate without revealing any personal information. Throughout this process, anonymity is maintained, as shown in Figure 3.

Figure 3:

Proposed Mechanism for Maintaining Voter Anonymity



Source: Alvi et al., 2022; Krungsri Research

III. Software Independence

As mentioned earlier, trust in an electoral system hinges on its independence and the ability to audit all stages of the election process. **For online elections, this underscores the importance of 'software independence.' A voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome**(Rivest, 2008). In contrast, software that lacks independence may lead to significant errors or expose the election to cyber threats. For instance, if the software is not independent, a remote programmer could potentially access the system and modify its codebase. Even a minor alteration in the code could swiftly change millions of electronic ballots, unlike the scenario with traditional paper ballots, where altering them requires physical access and individual modification (Park et al., 2020). Consequently, the risks associated with online and analog election systems vary significantly in scale.

In principle, verifying whether an election management system is software independent should not solely rely on using software to check software, as this is currently challenging and may require advancements in technology to achieve error-free code. However, software is indispensable for online election management. Nevertheless, system designers should develop verification methods that minimize reliance on software or eliminate it entirely (non-software-based means). For instance, designing processes that enable the general public to verify without relying on technology or allowing individuals to use their own software for verification. Such system designs present significant practical challenges, irrespective of whether blockchain technology is employed in the management system or not.

Democracy — and the consent of the governed — cannot be contingent on whether some uncheckable software correctly recorded voters' choices.

Park, Specter, Narula & Rivest (2020)

Considerations of software independence are thus central to concerns regarding the operation of online elections, but contemplating these issues also raises further important questions. (i) If problems or security vulnerabilities are detected in the software, how confident can the public be that these concerns are genuine and not raised for ulterior motives? It is essential to recognize that while the auditing and verification process may be public at various stages, certain information remains private and accessible only to individual voters. Therefore, any reporting and discussion of potential issues should be grounded in publicly available evidence, regardless of when they occurred during the election process. (ii) When problems are identified and reported, is it feasible to promptly address and rectify them, and if not, what course of action will be taken? A well-designed system with software that exhibits a high degree of independence should enable the retrieval of data generated during the election using the digital footprint within the system. However, it remains uncertain whether currently available software meets these requirements adequately.

Box 2 The Nigerian election and the unique role of the Central Bank

Nigeria, the largest economy in Africa, had a total size of USD 477.38 billion in 2022,[11/] which is 94% of the size of the Thai economy in the same year. The country has seen significant growth in the development of financial technology in this region, particularly in blockchain. The Nigerian government is actively promoting digital technology as a central driver of economic development alongside the energy sector. As part of this initiative, the government's 2020-2030 National Digital Economy Policy and Strategy (NDEPS) places significant emphasis on its National Blockchain Adoption Strategy.

Picture credit: Naija247news

For several years, the Independent National Electoral Commission (INEC) of Nigeria has faced various challenges in organizing general elections in the country. This has spurred both governmental and academic interest in exploring the potential application of blockchain technology in elections, given Nigeria's perceived readiness in this domain. In early 2023, a study on Nigerian elections was published, highlighting the involvement of the banking sector in blockchain-based elections (Eghe-Ikhurhe et al., 2023). The study identifies voter registration as a crucial step, requiring individuals to register with the electoral management unit using a unique identifier, such as their national identity number or their biometrically-based Bank Verification Number (BVN) issued by the central bank of Nigeria. This process ensures that only those with a confirmed right to vote can do so and prevents anyone from voting repeatedly. **The high level of trust in Nigeria's central bank has led it to be entrusted with a significant role in verifying the identities of those registering for general elections using blockchain technology**, which is an "unconventional" role for a central bank.

Indeed, it is not just the central bank that has been accorded this recognition, as the banking and financial sector more generally has been widely acknowledged for its role in driving the development and adoption of technologically advanced innovations. These innovations have played a crucial role in enhancing transparency and efficiency across various sectors. This raises the question of whether there is a role for commercial banks in accelerating the adoption of blockchain technologies in broader contexts beyond finance, mirroring the trends observed in Nigeria.

Source: Krungsri Research

11/ https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/

Krungsri Research view: One size doesn't fit all

Transitioning to a new electoral system inevitably brings about challenges and introduces various new problems. Therefore, if we revisit the initial question of **whether blockchain-based electoral management is truly superior to the current system**, the answer that can be provided at this moment is **"Yes, but only partially."** While blockchain technology offers significant advancements, it cannot entirely address all the pain points of traditional paper-based elections. Although conducting online elections using blockchain technology may offer advantages in terms of convenience, data processing speed, and a high degree of public trust (because once data is securely recorded into the blockchain, it is extremely difficult for this to be altered, tampered with, or deleted), there are still limitations in addressing all dimensions of electoral challenges.

The flip side of this is that **the decentralized nature of blockchains** and the many participants active in the network **will likely introduce new problems when incorporated into online voting.** These issues will primarily pertain to governance and coordination, necessitating the development of more secure and complex systems and software compared to cases where data is managed on a single central server. This additional complexity will then bring with it a likely proliferation of bug fixes and the need to deploy new software, and when security vulnerabilities are found in blockchain applications, patching these is generally more difficult and more time-consuming than when providing updates for a centralized system.

Beyond this, despite the security inherent in the design of the blockchain and the additional assurances offered by measures like those implemented by the BVMS to prevent 51% attacks and automate checking for irregularities and threats, blockchain technology is not invulnerable. **It is impossible to completely eradicate underlying threats to the security of blockchain-based voting systems.** Because online elections, whether with or without blockchains, are conducted online, they will always be exposed to cyber threats. Unlike traditional paper-based ballots, vulnerabilities in the software may be exploited with significant effect, especially when compared to traditional paper-based election systems. For example, the 'INVDoS' vulnerability discovered by Braydon Fuller in 2018 (code CVE-2018-17145)[12/] allowed malicious peers to launch denial-of-service attacks by flooding fellow peers with randomly hashed messages relating to non-existent transactions, and this then had the potential to result in memory overflows and system failures. The Bitcoin software tracker reported that as of 2020, 27% of the Bitcoin network remained vulnerable to this threat (Park et al., 2020), and more generally, software developers accept that discovering vulnerabilities is a normal part of the blockchain development and tracking process.

12/ https://www.zdnet.com/article/researcher-kept-a-major-bitcoin-bug-secret-for-two-years-to-prevent-attacks/

In the event that a large-scale election involving many participants encounters problems, the authorities will need not only to urgently address the specific issues affecting the vote but also to provide the public with a clear explanation of what has happened, backed up by empirical evidence acquired from an investigation of the event. This is a point that needs careful consideration because explaining problems with software or networks to the public in an easily understandable form is not straightforward, particularly when contrasted with traditional paper ballots that can simply be recounted in front of observers to dispel public worries over the validity of the results.

For high-stakes national elections, **any new voting system or technology introduced should undergo rigorous testing beforehand. This could involve piloting the system in small-scale local elections and/or testing it in advance or remote voting scenarios multiple times until confidence is established that the online electoral management system is fully prepared for large-scale national elections.** It is possible that the development, testing, and patching of a new voting system could take a decade or longer, though the timetable for this would be at least partly determined by the pace and advancement of technological development.

Nevertheless, while blockchain-based online voting systems may not yet be suitable for national or general elections due to technological limitations, they present an intriguing possibility for smaller-scale elections with limited budgets or in remote areas with logistical challenges. This could extend to facilitating voting for overseas citizens or those who struggle to reach polling stations in person. Ultimately, maximizing the potential of blockchain will require finding tailored applications that suit the unique context of each election, as there is no one-size-fits-all solution.

References

Alvi et al. (2022) DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. Retrieved May 16, 2023 from https://www.sciencedirect.com/science/article/pii/S1319157822002221/pdf

Catalin Cimpanu (2020) Researcher kept a major Bitcoin bug secret for two years to prevent attacks [Blog post]. Retrieved August 10, 2023 from https://www.zdnet.com/article/researcher-kept-a-major-bitcoin-bug-secret-for-two-years-to-prevent-attacks/

Eghe-Ikhurhe et al. (2023) The Relevance of Blockchain Based Voting Adoption in Governance Structure. Evidence from Nigeria. International Journal of Economics, Commerce & Management, United Kingdom. Retrieved August 20, 2023 from https://ijecm.co.uk/wp-content/uploads/2023/01/1111.pdf

Farooq, Ifthikhar and Khelifi (2022) A framework to make voting system transparent using blockchain technology. IEEE Access. Retrieved May 16, 2023 from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9787540

Kai Ostwald and Guillem Riambau (2021) Voting Behavior under Doubts of Ballot Secrecy: (Un)Intentionally Nudging Voters Towards a Dominant Party Regime. Retrieved August 13, 2023 from http://guillemriambau.com/Ostwald%20Riambau%20Voting%20under%20doubts%20of%20ballot%20secrecy.pdf

Li et al. (2017) Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain [Conference paper]. Retrieved September 13, 2023 from https://www.researchgate.net/publication/323209703_Proof_of_Vote_A_High-Performance_Consensus_Protocol_Based_on_Vote_Mechanism_Consortium_Blockchain

Park et al. (2020) Going from Bad to Worse: From Internet Voting to Blockchain Voting. [Draft November 6, 2020] Retrieved May 17, 2023 from https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

Ronald L. Rivest (2008) On the notion of 'software independence' in voting systems. Philosophical Transactions of the Royal Society. Retrieved August 10, 2023 from https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2008.0149

Yael Grauer (2019) What Really Happened With West Virginia's Blockchain Voting Experiment? [Blog post] Retrieved July 22, 2023 from https://slate.com/technology/2019/07/west-virginia-blockchain-voting-voatz.html

KRUNGSRI RESEARCH

Pimnara Hirankasi, Ph.D.
Head of Research Division and Chief Economist

Macroeconomic Team

Sujit Chaivichayachat
Head of Macroeconomic Research

Wanicha Direkudomsak
Senior Economist

Churailuk Pholsri
Senior Economist (Forecasting)

Thansin Klinthanom
Economist

Krittabhorn Sirichaichingkun
Economist

Supasyn Itthiphatwong
Economist

Analytics & Intelligence Team

Pimnara Hirankasi, Ph.D.
Acting Head of Analytics and Intelligence Research Department

Nathanon Ratanathamwat
Senior Analyst

Narichaya Satafang
Analyst

Parinya Mingsakul
Analyst

Chanatta Thararos
Analyst

MIS and Reporting Team

Thamon Sernsuksakul
Administrator

Chirdsak Srichaiton
MIS Officer

Wongsagon Keawuttung
MIS Officer

Industry Team

Pimnara Hirankasi, Ph.D.
Acting Head of Industry Research

Taned Mahattanalai
Senior Analyst (Digital)

Poonsuk Ninkitsaranont
Senior Analyst (Healthcare, Mobile Operators)

Piyanuch Sathapongpakdee
Senior Analyst (Transport & Logistics)

Narin Tunpaiboon
Senior Analyst (Power Generation, Modern Trade, Chemicals, Medical Devices)

Thian Thiumsak
Senior Analyst (Energy, Petrochemicals)

Puttachard Lunkam
Senior Analyst (Construction Contractors, Construction Materials, Hotels, Industrial Estate)

Patchara Klinchuanchun
Senior Analyst (Real Estate)

Chaiwat Sowcharoensuk
Senior Analyst (Agriculture)

Prapan Leenoi
Analyst (ESG)

Supawat Choksawatpaisan
Analyst (Automobile, Electronics & Electrical Appliances)

Suppakorn Kornboontritos
Analyst (Agriculture, Food & Beverages)