GDAŃSK UNIVERSITY
OF TECHNOLOGY

A Trust-Centric Approach To Quantifying Maturity and Security in Internet Voting Protocols

Stanisław Barański

2024-10-28

Voting

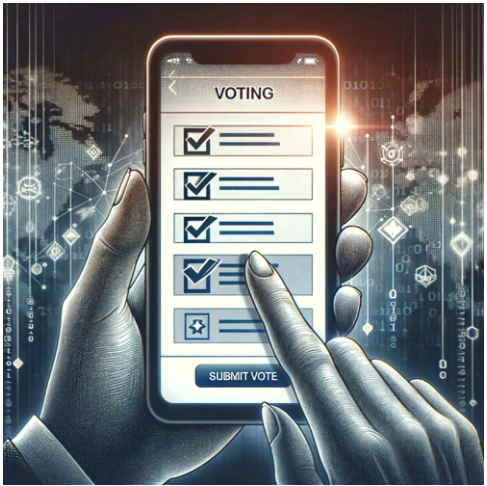
Voting is one of the most popular mechanisms for collective decision-making.

Voting

Used in:

- Political Elections, Referendums, Corporate boards, Homeowners Associations, Unions, Non-Profit Organizations, Reality TV Shows, Awards, Surveys and Polls, Student Government Elections, Faculty Decisions, ...
- Social Media, Menu Selection, Crowdsourced Data Labeling,
- Decentralized Autonomous Organizations (DAOs), Cryptocurrency Governance,
- Consensus, BFT, Proof of Authority (PoA), Delegated Proof of Stake (DPoS)

Yet, it's still something we can not do securely online.

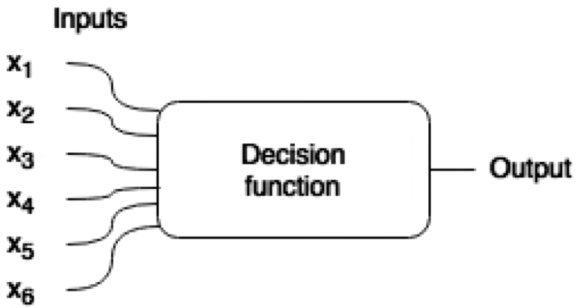


Internet Voting, Motivation

Internet voting is the most conventional, cheapest, fastest, and safest (e.g., during the outbreak of COVID-19), and hence, a desired method for conducting voting.

- **Convenience, and safety.** No need to leave your home to participate in voting.
- **Cheap.** No need to print ballot papers or hire people to coordinate the voting process.
- **Transparent.** Users don't need to trust the authorities that their votes have been included and that the counting process has been correct.
- **Increased turnouts and the frequency of votings.**
- Catalyse the **further development of modern democracy**. Enabling practical applications of direct democracy, liquid democracy, and all other sorts of voting methods like Quadratic Voting, Approval voting, Alternative voting, Score voting, and many others.

Internet voting should be easy



Buterin, V. (2017, December 17). Notes on Blockchain Governance. https://vitalik.eth.limo/general/2017/12/17/voting.html

Internet voting is hard

Secure voting requires four main properties:

- **Correctness**, all and only eligible votes are counted.
- **Censorship resistance,** any eligible user that wants to cast a vote can do it.
- **Privacy,** no one can tell which candidate the voters voted for, or even if they voted at all—preventing preliminary results and guaranteeing freedom of choice.
- **Coercion resistance**. voters can not prove to anyone how they voted even if they want to—preventing selling votes as there is no way of verifying if they indeed voted on the paid candidate.

They are hard to satisfy together. And even if they are satisfied, there are more fundamental problems.

Internet voting is hard

Secure voting requires four main properties:

- **Correctness**, all and only eligible votes are counted.
- **Censorship resistance,** any eligible user that wants to cast a vote can do it.
- **Privacy,** no one can tell which candidate the voters voted for, or even if they voted at all—preventing preliminary results and guaranteeing freedom of choice.
- **Coercion resistance**. voters can not prove to anyone how they voted even if they want to—preventing selling votes as there is no way of verifying if they indeed voted on the paid candidate.

They are hard to satisfy together. And even if they are satisfied, there are more fundamental problems.

Internet voting is hard

Secure voting requires four main properties:

- **Correctness**, all and only eligible votes are counted.
- **Censorship resistance,** any eligible user that wants to cast a vote can do it.
- **Privacy,** no one can tell which candidate the voters voted for, or even if they voted at all—preventing preliminary results and guaranteeing freedom of choice.
- **Coercion resistance**. voters can not prove to anyone how they voted even if they want to—preventing selling votes as there is no way of verifying if they indeed voted on the paid candidate.

They are hard to satisfy together. And even if they are satisfied, there are more fundamental problems.

Scepticism

- Wiki: "Security experts have found security problems in every attempt at online voting, including systems in Australia, Estonia, Switzerland, Russia, and the United States."
- The resistance lies—among others—in insufficient confidence in the technology and a need for trust in the authorities controlling the voting process.
- The criticism against internet voting comes down to two arguments:
  1. **Device related.** No software is flawless, therefore it can not be trusted.
  2. T**rust related.** There is too strong a trust assumption in authorities controlling the voting process.

1. Device related. No software is flawless, there

GDAŃSK UNIVERSITY OF TECHNOLOGY

trusted

Table 1: **Four categories of voting systems.** The top row (green) is *software-independent* and far less vulnerable to serious failure than the bottom row (red). The bottom row is highly vulnerable and thus unsuitable for use in political elections, as explained further in §2.

	In person	Remote
Voter-verifiable paper ballots[3]	*Precinct voting*	*Mail-in ballots*
Unverifiable or electronic ballots	*DRE*[4] *voting machines*	*Internet/mobile/blockchain voting*

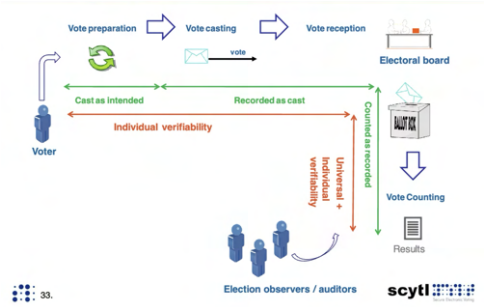
- Recent advances in cryptography can **guarantee correct program execution** using zero-knowledge proofs [13].
- Generally, it is believed that **cybersecurity is getting better, not worst** [23].
- Moreover, the authors of [24] claim that "**there is no perfect, infallible way to count votes.** All methods including optical scan, touchscreen, and hand counting—are subject to errors, procedural lapses, and deliberate manipulation." Therefore, the argument is not about security or lack of it, but how much secure it is, and what are the trust assumptions.

2. Trust related. There is too strong a trust ass
authorities controlling the voting process

- **Evidence-based election: Ideally**, the whole voting process should be completely trustless, meaning that, there should be no trust assumptions other than in our perception.
- **In practice**, we rarely monitor the whole process of elections. Rather, we delegate that duty to staff responsible for conducting voting. We believe that at least one person is an honest observer who will alarm if something goes wrong.

Voting

- They differ in what the server can or cannot do. honesty of the trusted third party determines some of the properties: censorship-resistance, anonymity, privacy or coercion-resistance.
- According to the report by the Switzerland's Federal Council,
  1. Systems to be used for up to the 50% of electors are required to provide methods for **individual verifiability**
  2. Systems for up to 100% of the electorate are required to provide complete verifiability, while also enforcing the **separation of duties** on operations impacting the privacy, integrity and verifiability of the system.



A Trust-Centric Approach To Quantifying Maturity and Security in Internet Voting Protocols

STANISŁAW BARAŃSKI, Gdansk University of Technology, Poland
BEN BIEDERMANN, Islands and Small States Institute, University of Malta, Malta
JOSHUA ELLUL, Centre for DLT, University of Malta, Malta

Research questions:

- What security properties the internet voting protocols achieve?
- What level of separation of duties do they achieve?
- What are the trust models underpinning these protocols, and how do they impact their practical application?
- What is the difference between blockchain-based and traditional internet voting systems?
- How to measure it?
- How to compare them?

Contribution

- Systematizing the knowledge on internet voting protocols, targeted at decision-makers.
- Conducting a trust model analysis of the most popular internet voting protocols.
- Quantifying the level of trust in security properties.
- Establishing a maturity score for quantifying the security of internet voting protocols.

Internet voting protocols, stages

1. **Pre-Election (Setup)**: Includes sub-steps such as Key Generation, Election Preparation, and Printing of Voting Cards.
2. **Election (Voting)**: Involves Candidate Selection, Vote Casting, Vote Confirmation, the Benaloh Challenge, and the Generation of Zero-knowledge Proofs.
3. **Post-Election (Counting/Processing/Tally)**: Comprises Mixing (Shuffling), Decryption, Tallying, and Inspection.

Internet voting protocols, parties

1. **Administrator**: Also known as the Election Authority or Organizer. They are responsible for election preparation, including the preparation of eligible voters' lists, candidate lists, and key generation.
2. **Identity Provider**: Also referred to as the Credential Authority, Registration Service, Census Service, or Print Office. This role is responsible for voter authentication and/or authorization, as well as the generation and distribution of authentication codes.
3. **Collector**: Often called the Ballot-box or Bulletin Board, stores ballots securely during the voting process.
4. **Key-Holders**: Also referred to as Trustees or Board Members. They hold shares of decryption keys and perform partial decryption.
5. **Processor**: Performs tasks such as ballot authorization, double-vote prevention, shuffling, mixing, decryption, and tallying.
6. **Auditors**: These entities are granted additional permissions to inspect and validate the correctness of each component's operations and the integrity of the data flow between them throughout all stages of the voting process.

Internet voting protocols, security properties

1. **Voter Anonymity**: This property addresses the question, "Who must collude to establish a link between the recorded ballot and the real identity of the voter?" It concerns the protection of voter identities from exposure.
2. **Voting Secrecy**: This property addresses the question, "Who must collude to decrypt a single vote or all votes before the voting process is complete?" It ensures that the content of votes remains confidential until the end of voting.
3. **Individual Verifiability**: This property addresses the question, "Who must collude to falsely convince a voter that their ballot has been recorded correctly and included in the final tally?" It ensures that voters can verify the integrity of their individual votes.
4. **Universal Verifiability**: This property addresses the question, "Who must collude to falsely convince observers that the voting procedure was correct, that no one voted twice, and that the final tally accurately represents the collected votes?" It ensures that the entire voting process is transparent and trustworthy.
5. **Eligibility Verifiability**: This property addresses the question, "Who must collude to falsely convince observers that only eligible voters cast ballots?" It ensures that only authorized voters participate in the election.

National and Local Government Elections

- **Estonian i-Voting system (IVXV)** is one of the most well-known and widely deployed internet voting protocols, used in national elections since 2005. Its primary purpose is to allow citizens to cast votes remotely, offering a convenient alternative to traditional in-person voting. Unique functionalities include the use of national digital ID cards for secure voter authentication and end-to-end verifiability features, ensuring that each vote is correctly tallied while maintaining voter anonymity.
- **Scytl's online voting platform** is used in various local and national elections across several countries, including France and Switzerland. It utilizes a microservice architecture for enhanced scalability and security, with Control Components that isolate critical operations like vote mixing and decryption. The system's use of Choice Return Codes offers end-to-end verifiability without compromising voter privacy.
- **CHVote** is an internet voting system developed by the canton of Geneva and used in Swiss cantonal and federal elections. Its key features include strong cryptographic guarantees for both individual and universal verifiability, ensuring transparency without compromising voter privacy. The system was primarily designed for both resident and

Dataset

Organizational, Academic, and Low-Stakes Elections

- **Helios** is an open-source, web-based voting protocol designed for low-coercion environments, such as academic institutions and organizations. Helios focuses on providing open-audit, end-to-end verifiability while maintaining voter privacy, making it ideal for low-stakes elections. Notably deployed in the University of Louvain's presidential election in 2009, it has proven its effectiveness in academic settings.
- **Belenios** is an open-source internet voting system widely used for academic, non-profit, and organizational elections. Built upon Helios, Belenios adds features such as eligibility verifiability and protection against ballot stuffing. It supports various voting methods and has been used in over 1,400 elections yearly.
- **Open Vote Network** is a decentralized, self-tallying voting protocol suited for small-scale elections, such as boardroom voting. It maximizes voter privacy by requiring full collusion among all voters to breach confidentiality. It is primarily suited for environments with lower coercion risks due to the lack of robust coercion resistance mechanisms.

Dataset

DAO Governance and Blockchain-Based Voting

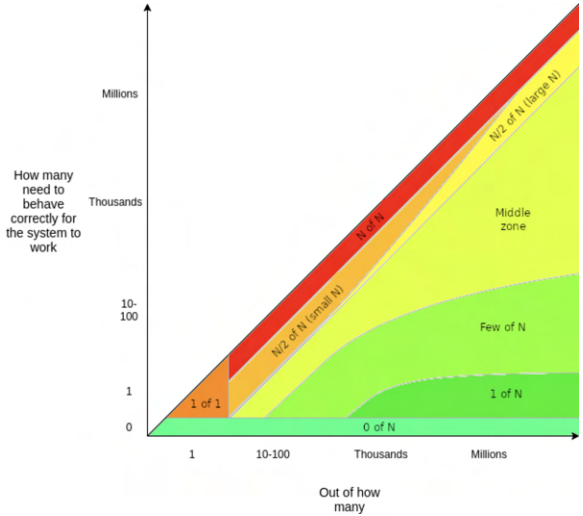
- **Snapshot** is a decentralized, off-chain voting platform widely used by DAOs, DeFi protocols, and NFT communities for governance purposes. Snapshot enables gasless voting and supports flexible voting mechanisms, such as Quadratic Voting and Approval Voting. It has seen widespread adoption, with 96% of DAOs using it and over 500,000 monthly active users.
- **Snapshot X** is the fully on-chain version of Snapshot, built on Starknet. It integrates trustless execution and on-chain verifiability, improving censorship resistance and security while retaining flexibility for DAOs. Snapshot X is designed for decentralized governance models that require robust decentralization and security.
- **Vocdoni** is a decentralized voting protocol designed for large-scale governance in DAOs and blockchain-based communities. The system integrates with Ethereum for added transparency and has been deployed in various contexts, including the Votecaster platform on Farcaster's blockchain-based social media.
- **Cicada** is an on-chain voting protocol built on Ethereum. Using time-lock puzzles and homomorphic encryption, Cicada enables private, non-interactive voting, but struggles

Dataset

Participatory Democracy and Public Goods Funding

- **Decidim** is an open-source platform for participatory democracy, originally developed by the Barcelona City Council. It supports a wide range of democratic processes, including participatory budgeting and consultations, and is used by over 400 entities globally, including cities like Helsinki and the European Commission.
- **MACI (Minimal Anti-Collusion Infrastructure)** is an on-chain voting protocol focused on mitigating collusion and bribery, making it ideal for Quadratic Funding (QF) and decentralized governance. MACI has been successfully deployed in QF rounds, distributing over $1M to public goods projects via platforms like `clr.fund` and Gitcoin Allo stack.
- **Votem's Proof of Vote** is an end-to-end verifiable voting protocol leveraging blockchain technology, primarily designed for remote and mobile voting in public elections. Votem has been deployed in high-profile elections such as those in the State of Montana and the Rock and Roll Hall of Fame.

Trust Models



Trust model quantification

- **0 – None:** The protocol does not achieve the property.
- **1 – One:** The property holds as long as one party is honest.
- **2 – All of a few:** The property holds as long as all of a few parties are honest.
- **3 – Majority of closed network:** The property holds as long as a majority of a closed network is honest.
- **4 – Majority of open network:** The property holds as long as a majority of an open network is honest.
- **5 – Theory:** The property is achieved without any assumption of honest parties.

Trust model quantification

- **0 – None:** The protocol does not achieve the property of trust minimization.
- **1 – One:** The property holds as long as one party behaves honestly.
- **2 – Two independent parties:** The property holds as long as two independent parties behave honestly.
- **3 – One of a few or a majority of a closed network:** The property holds as long as at least one of a few or a majority of a closed network acts honestly.
- **4 – One and one of a few or a majority of closed network:** The property holds as long as a single party and at least one of a few or a majority of a closed network are honest.
- **5 – One and Majority of open network:** The property holds as long as a single party and a majority of an open network are honest.

Trust model quantification

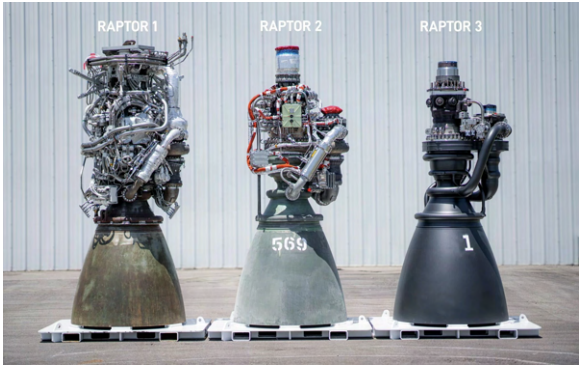
- **6 – A Few and Majority of closed network:** The property holds as long as a few parties and a closed network are honest.
- **7 – A Few and Majority of open network:** The property holds as long as a few parties and an open network are honest.
- **8 – Majority of closed network and majority of open network:** The property holds as long as a closed and an open network are honest.
- **9 – Majority of open network:** The property holds as long as a majority of an open network acts honestly.
- **10 – Cryptography:** The property is achieved without any assumption of honest parties.

Trust model quantification

Name	CMPX	PU	SEC	ANON	IVF	UVF	EVF	CRES
Estonian e-voting system	9	3	4	2	4	4	1	0
Scytl	11	2	4	2	6	6	1	0
CHVote	7	3	4	4	6	6	1	0
Belenios	8	1	3	2	4	4	1	0
Helios	7	1	3	1	4	4	1	0
Decidim	7	2	3	1	4	4	1	0
Votem, Proof of Vote	29	2	3	4	6	6	3	0
Agora	19	2	3	4	6	6	1	0
Vecdoni	28	1	3	10	3	3	10	0
zkSnap	6	0	1	10	1	1	10	0
Stellot	4	0	1	10	9	9	1	0
MACI	4	1	1	1	9	9	1	1
Cicida	4	0	0	10	9	9	1	0
OpenVoteNetwork	3	0	9	1	9	9	1	0
Snapshot	6	2	3	0	1	1	10	0
Snapshot X	6	1	3	0	9	9	10	0

Table 1. The table represents the final quantification of Complexity, Trust model, and Practical Usability. CMPX is Complexity (lower is better), PU is Practical Usability, SEC is Voting secrecy, ANON is Voter anonymity, IVF is Individual Verifiability, UVF is Universal Verifiability, EVF is Eligibility verifiability, and CRES is Coercion Resistance. Green indicates the best value, yellow is moderate, and red indicates the worst.

Complexity



Complexity

- **1: Single dedicated component**, the simplest form of independent unit of functionality, which operates autonomously without reliance on other components.
- **2: Public network**, which is not maintained by the system (e.g. Bitcoin, Ethereum, IPFS, or DRAND), and operates independently with decentralized control, providing services such as consensus or data storage without direct oversight from the system in question.
- **3: A few independent parties**, typically auditors or observers, who operate autonomously and do not need to coordinate or collaborate with one another to complete their tasks, ensuring decentralized verification or validation within the system.
- **4: Multi-party computation (MPC)**, a process that requires multiple independent parties to collaborate and jointly compute a result, ensuring that sensitive data is processed without any individual party having access to the complete input (e.g. decryption key).
- **5: Dedicated network**, a closed distributed system (e.g., Private Blockchain) that must be maintained and managed by the system itself, requiring full control over its infrastructure, security, and consensus mechanisms.

Complexity

Name	Parties and their trust models	CMPX
Estonian e-voting system [45]	Organiser (1), Collector (1), Processor (1), Registration Service (1), A Few Talliers (MPC, 4), A Few Auditors (3)	9
Scytl [62]	Election Administrators (1), Voting Server (1), Print Office (1), A Few Control Components (CCR and CCM) (MPC, 4), A Few Board Members (Key-Holders) (MPC, 4), A Few Auditors (Auditors, 3)	11
CHVote [49]	Administrator (1), Printing Authority (1), A Few of Election Authorities (MPC, 4), A Few of Auditors (3)	7
Belenios [24]	Server administrator (1), Credential authority (1), Voting Server (1), A Few Trustees (MPC, 4), A Few of Auditors (3)	8
Helios [2]	Administrator (1), Helios Server (1), A Few of Key-holders (MPC, 4), A Few of Auditors (3)	7
Decidim [6]	Administrator (1), Decidim Server (1), A Few of Key-Holders (MPC, 4), A Few of Monitoring Committee (3)	7
Votem, Proof of Vote [67]	Election Authority (1), DKG/Decryption Trustees (MPC, 4), Authentication Authorities (MPC, 4), Authorization Authorities (MPC, 4), Ballot Distribution Servers (MPC, 4), Mix-Network Nodes (MPC, 4), Private Blockchain Nodes (PBFT, 5), Public Verifiers (Auditors, 3)	29
Agora [4]	Election Authority (1), Private Bulletin Board Blockchain (5), Cothority (MPC, 4), Cotena (MPC, 4), Bitcoin Blockchain (2), Valeda Auditors (3)	19
Vecdoni [95]	Voting Organiser (1), Census Service (1), Scrutinizers (MPC, 4), Keykeepers (MPC, 4), Oracles (Private network, 5), Decentralised Storage (Public external network, 2), Gateways (MPC, 4), Vochain Private BC (5), Public blockchain (2)	28
zkSnap [46]	Organiser (1), Trusted Coordinator (1), DRAND (Public external network, 2), Public Blockchain (Public external network, 2)	6
Stellot [7]	Organiser (1), TDS (1), Public Blockchain (2)	4
MACI [37]	Organiser (1), Trusted Coordinator (1), Public Blockchain (2)	4
Cicida [47]	Administrator (1), Off-chain solver (1), Public BC (2)	4
Open Vote Network [68]	Organiser (1), Public Blockchain (2)	3
Snapshot [93]	Admin (1), Snapshot-hub (1), Shutter network (Public external network, 2), IPFS (Public external network, 2)	6
Snapshot X [82]	Admin (1), Mana (1), Shutter network (Public external network, 2), Starknet Blockchain (Public external network, 2)	6

Complexity

- **1: Not used in production** – Protocols in this category are in the prototype phase, without any documented instances of deployment in actual election environments.
- **4: Used in low-stakes elections** – These protocols have been deployed in environments with minimal risk, such as elections in academic institutions, student government bodies, or internal organizational decisions.
- **7: Used in medium-stakes elections** – A score of 2 is assigned when the protocol has been used in elections with moderate significance, such as local government elections, corporate governance voting, or elections in non-governmental organizations (NGOs).
- **10: Used in high-stakes elections** – Protocols that have been implemented in high-stakes environments, such as national or regional government elections, are given a score of 3. These elections carry substantial political or social consequences.

Practical usage

Name	References	PU
Estonian e-voting system [45]	[34, 33]	3
Scytl [62]	[79, 36, 78, 80]	2
CHVote [49]	[80, 40, 48]	3
Belenios [24]	[25]	1
Helios [2]	[3]	1
Decidim [6]	[29]	2
Votem, Proof of Vote [67]	[92]	1
Agora [4]	[88]	1
Vecdoni [95]	[91]	1
zkSnap [46]	–	0
Stellot [7]	–	0
MACI [37]	[19]	2
Cicida [47]	–	0
Open Vote Network [68]	–	0
Snapshot [93]	[54]	2
Snapshot X [82]	[82]	1

Table 3. Practical Usages of e-voting systems based on their references.

The maturity score for a protocol, denoted as EVMI(p), is calculated as a weighted sum of eight factors:

$$\begin{aligned} EVMI(p) = w_c \log \mathsf{CMPX}(p) + w_p \log \mathsf{PU}(p) + w_s \log \mathsf{SEC}(p) + w_a \log \mathsf{ANON}(p) \\ + w_i \log \mathsf{IVF}(p) + w_u \log \mathsf{UVF}(p) + w_e \log \mathsf{EVF}(p) + w_r \log \mathsf{CRES}(p) \end{aligned} \quad (1)$$

Here, $w_c, w_p, w_s, w_a, w_i, w_u, w_e$, and w_r represent the weights assigned to each factor, reflecting their relative importance. The values for each component are determined as follows:

- $\mathsf{CMPX}(p)$, the complexity score.
- $\mathsf{PU}(p)$, the Practical Usability score.
- $\mathsf{TM}(p)$, the trust model score, is composed of the security properties: SEC(p), ANON(p), IVF(p), UVF(p), EVF(p), and CRES(p).

Results

Internet Voting Systems				Weight	n.a.	-2	n.a	1	n.a.	3
ID	Name, p	Rank	Normalised EVMI(p)	EVMI(p)	Complexity	CMPX(p)	Trust Model	TM(p)	Used in Practice	PU(p)
1	Estonian e-voting system	3	0.7846	3.875	9	1	2.875061263	2.875061263	10	1
2	Scytl	5	0.6840	3.544	11	1.079181246	3.167317335	3.167317335	7	0.84509804
3	CHVote	1	1.0000	4.583	7	0.903089987	3.389166084	3.389166084	10	1
4	Belenios	9	0.4198	2.676	8	0.9542425094	2.77815125	2.77815125	4	0.602059991
5	Helios	10	0.3974	2.602	7	0.903089987	2.602059991	2.602059991	4	0.602059991
6	Decidim	6	0.6192	3.331	7	0.903089987	2.602059991	2.602059991	7	0.84509804
7	Votem, Proof of Vote	12	0.3497	2.445	29	1.477121255	3.593286067	3.593286067	4	0.602059991
8	Agora	11	0.3653	2.496	19	1.301029996	3.292256071	3.292256071	4	0.602059991
9	Vecdoni	8	0.4486	2.770	28	1.462397998	3.888965344	3.888965344	4	0.602059991
10	zkSnap	16	0.0000	1.296	6	0.84509804	2.985875357	2.985875357	1	0
11	Stellot	14	0.2889	2.246	4	0.6989700043	3.643452676	3.643452676	1	0
12	MACI	2	0.9265	4.341	4	0.6989700043	3.204119983	3.204119983	7	0.84509804
13	Cicida	15	0.1974	1.944	4	0.6989700043	3.342422681	3.342422681	1	0
14	Open Vote Network	13	0.3353	2.398	3	0.6020599913	3.602059991	3.602059991	1	0
15	Snapshot	7	0.5460	3.091	6	0.84509804	2.245512668	2.245512668	7	0.84509804
16	Snapshot X	4	0.7495	3.759	6	0.84509804	3.643452676	3.643452676	4	0.602059991

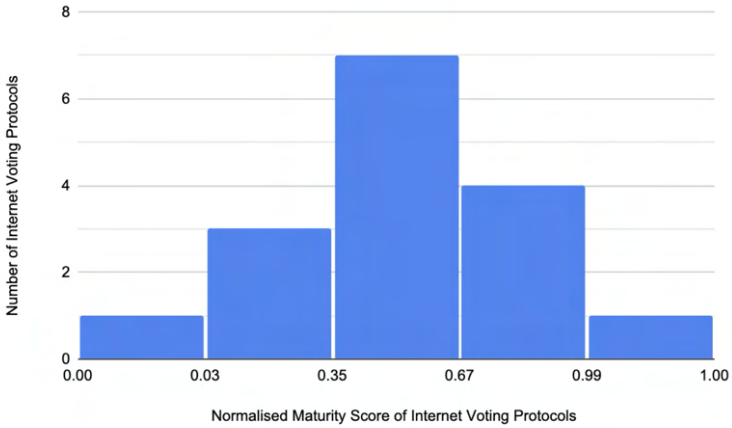


Fig. 1. Histogram of normalised Maturity Score of Internet Voting Protocols

Observations

- Blockchain-based internet voting protocols offer a significant advantage in terms of common knowledge and verifiability
- The biggest vulnerability often lies in the process of preparing, and distributing voter credentials
- The challenge of Eligibility Verifiability becomes more pronounced as the size of the voter base grows.
- Coercion resistance remains one of the most difficult properties to implement effectively.
- Blockchain-based internet voting systems have a distinct advantage in achieving common knowledge natively, thereby eliminating the need for external auditors.
- Authentication mechanisms vary depending on the use case.
- Introducing additional parties and performing secure multi-party computation is a straightforward way to improve a system's trust model, however at the expense of the system complexity.
- Private blockchain systems offer no significant advantage over traditional distributed systems in terms of trust.

GDAŃSK UNIVERSITY
OF TECHNOLOGY