Revolutionizing Blockchain Consensus: Towards Deliberative and Unanimous Agreement

Syed Badruddoja[1], Ram Dantu[2], Mark Dockendorf[2], Abiola Salau[2] and Kritagya Upadhyay[3]
[1] *Dept. of Computer Science, California State University, Sacramento, 6000 J Street, Sacramento, California, 95819, U.S.A.*
[2] *Dept. of Computer Science, University of North Texas, 3940 N. Elm Street, Denton, Texas, 76207, U.S.A.*
[3] *Dept. of Computer Science, Middle Tennessee State University, 1301 E Main St, Murfreesboro, TN 37132, U.S.A.*

Keywords: Blockchain, Consensus Protocol, Deliberative Consensus, Algorithm, Artificial Intelligence.

Abstract: Consensus algorithms require a majority of nodes in a distributed system to agree on a single value. Blockchain systems commission these consensus algorithms to ensure security and trust in decentralized applications. However, current consensus algorithms do not address the requirements of high-stake applications that demand unanimous consensus with deliberation. For instance, a trial case at a court requires unanimous consensus to decide the fate of a criminal. With limited agreement structure and no deliberation, the current consensus protocol cannot handle the consensus problem. Our research determines the requirements of a deliberative unanimous consensus model for high-stake applications. Moreover, we propose a family of consensus models that agree on the answer's correctness and the methods used to reach it.

1 INTRODUCTION

Shrinking Trust in Real-world Consensus: The trustworthiness of judicial systems is challenged by bias and manipulation, which have adverse effects on society (K.Lin, 2023). According to a recent survey by the Pew Research Center, less than half of Americans (44%) currently hold a favorable view of the court. At the same time, a slim majority (54%) harbor an unfavorable opinion. Over the last two years, the court's favorable rating has plummeted by 26 percentage points. Moreover, according to the monthly survey conducted by the NJC (National Judicial College), most judges hold the belief that systemic racism exists within the criminal justice system of the United States(Firth, 2020). In the scientific fields, erroneous scientific consensus can arise unexpectedly without any obvious vested interests (Socol et al., 2019) due to various reasons. The varied interests can introduce biases, ultimately shaping the consensus. Such cases suffer from decisions made with low to no trust. (Abraham et al., 2023; McKenzie et al., 2022).

Blockchain - Not a Deliberative Consensus: Blockchain consensus mechanisms offer to establish agreement and trust within decentralized networks, eliminating reliance on a central authority (Lin and Liao, 2017). This decentralization guarantees that transactions are validated and recorded by a distributed network of nodes, enhancing security, resilience, and resistance to amendments. However, the consensus mechanism of blockchain is fairly simple and does not reflect a true deliberative consensus. The agreement in computer systems is limited to matching the same outcome irrespective of any argument or arbitration (Xiao et al., 2019). Figure 1 shows the problems with current consensus protocols.

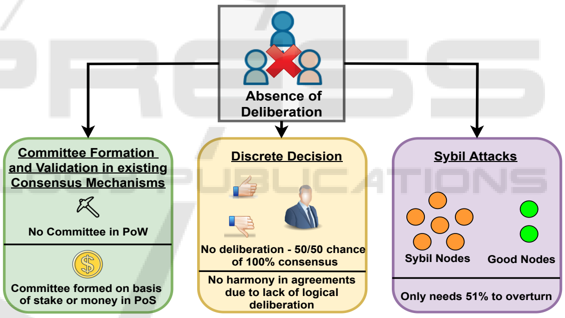
Absence of Deliberation
Committee Formation and Validation in existing Consensus Mechanisms
No Committee in PoW
Committee formed on basis of stake or money in PoS
Discrete Decision
No deliberation - 50/50 chance of 100% consensus
No harmony in agreements due to lack of logical deliberation
Sybil Attacks
Sybil Nodes
Good Nodes
Only needs 51% to overturn

Figure 1: Current consensus protocol limitations and problems that cannot solve high-stake consensus problem and fails to deliberate among participants.

Unreliable Consensus Protocols: Consensus problems in distributed systems have to agree on a specific issue even in the presence of faulty/malicious agents(Kshemkalyani and Singhal, 2011). (Lamport and Fischer, 1982) in 1982 described the Byzantine general's problem. This scenario depicts a communication problem among a certain number of gener-

Badruddoja, S., Dantu, R., Dockendorf, M., Salau, A. and Upadhyay, K.
Revolutionizing Blockchain Consensus: Towards Deliberative and Unanimous Agreement.
DOI: 10.5220/0012813400003767
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 21st International Conference on Security and Cryptography (SECRYPT 2024)*, pages 786-791
ISBN: 978-989-758-709-2; ISSN: 2184-7711
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

Table 1: Existing Consensus Protocols and the limited Consensus Agreement Percentage.

Protocol Name	**Consensus Type**	**Committee/Leader Selection**	**Adversary Tolerance**	**Network Synchrony**
Snow White (Daian et al., 2019; Buterin et al., 2020)	PoS (Sleepy Model)(Kiayias et al., 2017)	MPC	< 51% stakes	Asynchronous
Ouroboros (David et al., 2018)	PoS	MPC (PVSS)	< 51% stakes	Partial Synchrony
Ouroboros Praos(Gilad et al., 2017)	PoS	VRF	< 51% stakes	Partial Synchrony
Algorand (Bentov et al., 2016)	PoS-BFT, PoS-based for block proposing and Byzantine agreement for block finalization	VRF (Cryptographic sortition)	< 33% weighted users	Asynchronous periods between synchronous periods
Casper FFG (Nakamoto, 2008)	Light-weight PoS layer over Ethereum PoW	PoW-based leader selection BFT for block checkpoint justification	< 51% validators	Partial Synchrony
Bitcoin (Kwon, 2014)	PoW	Based on hash	< 51% computing power	Asynchronous
Tendermint (Buchman, 2016)	PoS-BFT	Round-robin	< 33% voting power	Partial Synchrony

als located in different locations, which is a challenge of validating messages sent from one to the other. However, they lack the basis for a consensus in certain real-life situations or systems that require or even mandate true deliberation, such as a jury consensus problem. To add more to it, the traditional consensus mechanisms fail to address the high-stake consensus demands of real-world situations. In the PoW system (Lin and Liao, 2017), the block creation is confirmed by verifying the nonce of the block that produces an equivalent or lesser hash value than the target value proposed by the prover. In PoS systems (Chen and Micali, 2019), the block proposers propose a block with a random hash value in their block proposal. However, there is hardly any relation between the consensus protocol and real-world high-stakes consent problems where a group of people must decide on the fate of a crime committed by a criminal.

Limited Agreement Quorum: Various blockchain consensus protocols follow different agreement percentages concerning proving the majority agreement of the agreement problem. PoW, PoS, consider a 51% majority agreement, whereas Pure PoS with practical byzantine fault tolerance failure method follows a two-third majority validation rule(Gilad et al., 2017). While these types of agreements are favorable from a computer failure perspective, they do not guarantee that the decision can be trusted for any real-life consensus problem. Table 1 summarizes some of the major consensus protocols that fail to address unanimity in consensus.

We investigate the requirements for creating a deliberative consensus for high-stake applications such as ”Jury Trial Decisions” and propose a high-level solution for the same.

- We outline the requirements of unanimous consensus for blockchain applications that will support critical high-stake applications.
- We propose an architecture for consensus in three formats: Unanimous Consensus with Weak Deliberation (UCWD), Unanimous Consensus with Strong Deliberation (UCSD), and Unanimous Consensus with Algorithmic Election (UCAE).
- For each consensus proposal, we proposed an agreement method to achieve unanimous consensus under specific circumstances using algorithmic proofs.

2 LITERATURE REVIEW

Biased Consensus in Real-World: The bias in courtroom decisions has plagued the judicial systems and affected the social welfare of the people over the last few years. According to the National Judicial College (University of Nevada, Reno) 's monthly survey of its alumni published in 2020, the majority of judges believe that racism is systemic in the United States criminal justice system (Firth, 2020). In the survey, 65 percent of the 634 judges believe that systemic racism exists in the criminal justice system. More than 200 judges left comments with their votes, and the consensus among the majority was that racism is mostly of the implicit or unconscious kind. Another example of biased consensus is seen in Scientific research. Socol et al. mentioned that, human scientists are susceptible to bias, influenced by political and economic interests (Socol et al., 2019).

Agent-based Consensus: Multi-agent consensus system addresses the consensus problem through deliberations. Hadfi et al. (Hadfi and Ito, 2022) propose the development of autonomous and intelligent conversational agents that can augment the deliberative capacities of citizens in social media. The authors proposed an approach that quantifies deliberation in online argumentative discussions. Moreover, Zhang et al. developed a web tool that enables *people to create and evaluate Machine Learning models in order to examine the strengths and shortcomings of past decision-making and deliberate on how to improve future decisions*. The authors applied the tool to improve graduate school admission decisions (Zhang et al., 2023). However, these developments assume that data input for unbiased decisions is pristine and does not guarantee immutability.

To the best of our knowledge, no work has been found to address high-stake, deliberative digital consensus that is tamper-proof and handles real-world applications. This paper proposes a novel approach to true consensus by recommending requirements and introducing an algorithmic deliberation approach to solve the consensus problems discussed so far.

3 REQUIREMENTS FOR UNANIMITY

Valid Belief and Selection of Participants: Currently, in blockchain's consensus protocol mechanism, the belief in the designated validators and block proposals is solely based on money and computational power or both without any deliberations. Some participants in the consensus mechanism might have less stake or power but more knowledge, facts, and experience, which could be more valuable in coming to a proper agreement and decision-making process. Although the current systems only allow that participant to be the validator or decision-maker who has the highest stake or the highest computational power, there should be a provision where the participants for the consensus would not be ruled out just based on their comparatively fewer stakes and computational power than others.

Rake and Quantify Trust: The systems that involve multiple peers, entities, and nodes are anonymous and lack accountability in blockchain. Therefore, this leaves the door open for the entities and nodes with malicious intent that can corrupt the decision-making process and put unanimity on hold. Nevertheless, once the trust is gathered from the set of prospective entities in the form of their knowledge, experience, stakes, and computational power through different series of exhaustive deliberations, each entity or peer in the system can be assigned a unique trust value based on the gathered data.

Logic on Deliberations to Arrive at a Result: There should be a formal model and logic in which the involved entities and nodes in the consensus handle and perform their deliberation. For instance, the Quaker-based model can be used for the deliberation process.

Broadcast and Synchronize the Deliberation: All the arguments, proofs, and theorems used for the deliberation should be shared and synchronized across multiple sites, institutions, or geographies and made accessible to all involved entities for the decision-making process.

Detect and Prevent Gang-Up Coalition: In spite of the fact that unanimity or 100% consensus is the major goal of the paper to establish trust, it does not mean that unanimity by force or unanimity by coalition is left undetected and overlooked as it defeats the whole purpose of 100% consensus via deliberation. Hence, the detection and prevention of the gang-up alliance is a significant requirement.

Forward-Looking Consensus Model: With quantum and AI architectures rising to join classical computers, there is a need to allow multiple fundamentally different architectures to form consensus together. Some of these will be predefined/scripted programs; others will be "smart" entities that are capable of machine learning. Figure 2 shows a paradigm shift of traditional real-world consensus to true deliberative

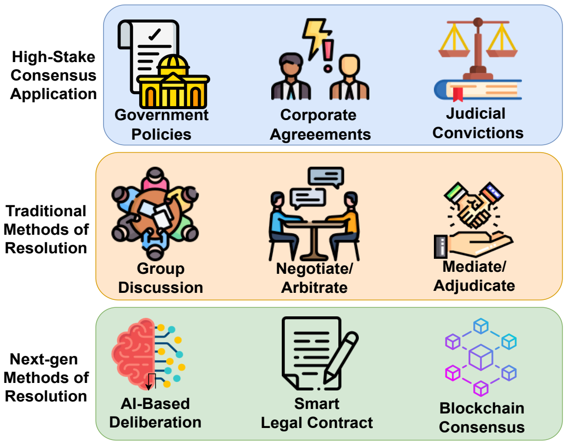

Figure 2: Paradigm shift from traditional biased real-world consensus to distributed deliberative consensus applications for high-stake applications.

digital consensus for high-stake applications that will reduce bias and increase trust in the system.

4 ARCHITECTURE

We describe three variations of unanimous consensus (UC): Unanimous Consensus with Strong deliberation (UCSD), Unanimous Consensus with Weak Deliberation (UCWD), and Unanimous Consensus with Algorithm Election (UCAE). While all of these examples require all committee members (deliberators) to be honest, it only requires that at least one is provably correct to form a consensus. Furthermore, UCWD and UCSD do not require deliberators to have the same architecture or execute the same instructions to reach a consensus. This allows these two forms of UC to be used in systems with a mix of classical and quantum machines.Figure 3 is our proposed architecture. We develop our consensus protocol with 4 phases. In phase 1, decentralized application users request transactions on the blockchain. In phase 2, the transactions are dequeued and sent to phase 3 for deliberation in different consensus engines. Phase 3 completes consensus and sends the results for block creation in phase 4. One example of a formal method of deliberation is mathematical proving, as mathematics serves as a ground truth for all modern science. With automated theorem proving, it is possible to prove/disprove mathematical statements within stated bounds.

Validation: The correctness of an algorithm is solidified by a proof. Before an algorithm is accepted, its proof is checked to ensure it is correct by ensuring

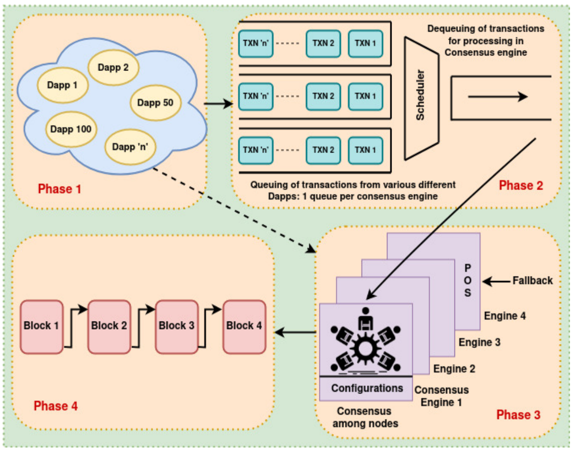

Figure 3: Ideal architecture of unanimous consensus where various transactions from various DApps in the network are queued and then dequeued for extensive deliberation in the consensus engine.

every logical step follows from the previous step(s) within the stated constraints. Secondly, the evidence input to the algorithm must fit the constraints. Finally, the algorithm must result in the desired output. For instance, if the network graph were to have negative edges, Dijkstra's algorithm to compute the shortest path would be invalid due to data incompatibility with the constraints of the proof for Dijkstra's algorithm. Similarly, in a jury consensus, a deliberator can declare that they cannot solve the problem. If a deliberator declares they cannot solve the problem, this counts as an abstention. A verdict cannot be reached if any deliberators abstain at the end of the round (this means that another round of deliberations is needed). Suppose a deliberator cannot solve a problem initially (i.e., lacks a necessary algorithm). In that case, they can adopt an algorithm that was offered by one of the other deliberators and proven correct.

Analysis: This phase varies by deliberation type. Weak and strong deliberation consists only of running the selected algorithm to find the answer. In unanimous consensus with algorithm election, a validated algorithm is elected first, and then each deliberator runs the selected algorithm. UCAE should use only deterministic algorithms.

Outcome: There will be several rounds of deliberation for consensus in a deliberative blockchain consensus system. After all rounds have been completed, there are two possible states: verdict or hung for a jury consensus case. If all deliberators cannot agree that the output is correct or all deliberators agree that they cannot solve the problem, then the deliberators are hung. This is equivalent to other consensus algo-

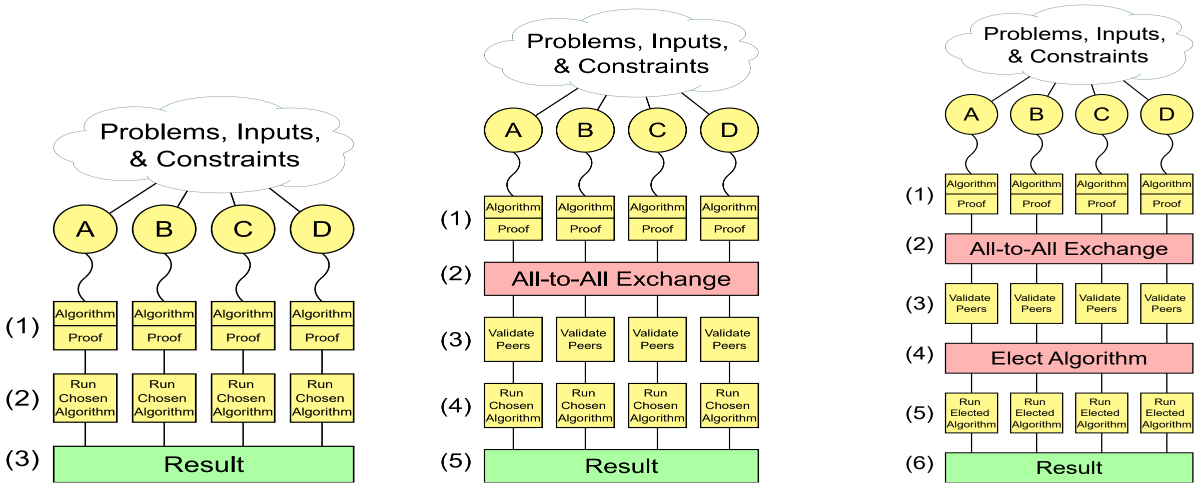

Figure 4: From the left, the first one is the UCWD type consensus algorithm, in the middle is the UCSD consensus algorithm, and on the right is the UCAE consensus algorithm.

rithms failing to form a consensus (e.g., for a block in a blockchain network) and should be expected to have similar consequences. When a verdict is reached in weak deliberation, it means that all deliberators agree that the provided output is correct. When a verdict is reached with strong deliberation, all deliberators agree that each deliberator's method to obtain the output is correct (proven and peer-reviewed) and the output itself is correct. A verdict in algorithm election means an algorithm was selected from the proposed algorithms, which had correct proofs, all deliberators ran the selected algorithm, and the outcome was correct according to the deliberators. Figure 4 shows three types of blockchain-based unanimous consensus discussed in this section.

4.1 Unanimous Consensus with Strong Deliberation (UCSD)

To reach a strongly deliberated unanimous consensus, all deliberators must agree on the answer and agree that the algorithms used by their peers to reach their conclusions are correct. This is done by exchanging algorithms and their corresponding proofs early in the consensus round and validating their peers' proofs. Even if all deliberators agree, another round of consensus may be needed as it is possible to reach the correct output with incorrect logic. If multiple outputs are produced by deliberators and multiple outputs are not desired, which may be possible with some problems (e.g., shortest path, minimum spanning tree, etc.), answers can be (but are not required to be, as the algorithm was proven correct earlier) checked to ensure they are correct (e.g., all minimum spanning trees for a graph should have the same total edge weight), then a vote is held to elect an answer among the correct outputs. The user can set heuristics for selecting the desired correct answer (e.g., majority, lowest hash, etc.).

4.2 Unanimous Consensus with Weak Deliberation (UCWD)

Weak deliberation is an optimization that skips the need to check algorithm proofs if all deliberators reach the same initial conclusion. This optimization relies upon at least one deliberator being correct. In realistic systems where strong deliberation has been resolved reliably on the first round with similar problems, UCWD can provide large speedups. These speedups will be more readily noticeable when the time complexity of proving the algorithm dominates the time complexity of running the algorithm: O(algorithms) ¡ O(validation). If UCWD fails to reach a consensus in the first round, it can fall back to strong deliberation (UCSD). This can be considered ”only deliberate if we need to”. Weak deliberation should not be used when the problem likely has multiple correct answers.

4.3 Unanimous Consensus with Algorithm Election (UCAE)

Beyond strong deliberation, the algorithm must be the same for all machines. Unlike the previous two mechanisms, this one will require either a virtual environment or similar hardware. Unlike strong and weak deliberation, which allow the mixing of quantum and classical computers, algorithm election requires that all hardware perform the selected algorithm. This form of unanimous consensus is the closest to existing consensus algorithms: it is provable that performing the same operations in the same environment with the same input values results in the same output (e.g., executing a smart contract should yield the same result for all machines – this allows blockchains with embedded programs to form consensus). Despite its shortcomings, algorithm election excels in one area: forming a unanimous consensus around a single output when a problem may have multiple correct answers.

5 CONCLUSION

Blockchain consensus protocols evolved to guarantee the security of applications with a consensus-based agreement between multiple parties in the network. However, real-world high-stakes applications such as trials at a jury cannot depend on blockchain for the output of consensus agreements as it suffers from incomplete agreement percentages and non-deliberative decisions. Hence, the consensus mechanisms of blockchain suffer from low trust. To overcome this difficulty, we proposed a deliberative consensus protocol with unanimous agreement. First, we described the requirements of unanimous consensus. Secondly, we proposed solutions under UCSD, UCWD, and UCAE to achieve a consensus on blockchain. It takes more time and effort to reach a conclusion when the decision is made by deliberation and unanimity. In our future work, we will explore and solidify the theoretical work for unanimous consensus.

REFERENCES

Abraham, J. et al. (2023). *Science, politics and the pharmaceutical industry: Controversy and bias in drug regulation*. Routledge.

Bentov, I., Pass, R., and Shi, E. (2016). Snow white: Provably secure proofs of stake. iacr cryptol. eprint arch.

Buchman, E. (2016). *Tendermint: Byzantine fault tolerance in the age of blockchains*. PhD thesis, University of Guelph.

Buterin, V., Reijsbergen, D., Leonardos, S., and Piliouras, G. (2020). Incentives in ethereum's hybrid casper protocol. *International Journal of Network Management*, 30(5):e2098.

Chen, J. and Micali, S. (2019). Algorand: A secure and efficient distributed ledger. *Theoretical Computer Science*, 777:155–183.

Daian, P., Pass, R., and Shi, E. (2019). Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake. In *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*, pages 23–41. Springer.

David, B., Gaži, P., Kiayias, A., and Russell, A. (2018). Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part II 37*, pages 66–98. Springer.

Firth, A. (2020). Most judges believe the criminal justice system suffers from racism. National Judicial COllege, University of Nevada, Reno.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., and Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles*, pages 51–68.

Hadfi, R. and Ito, T. (2022). Augmented democratic deliberation: Can conversational agents boost deliberation in social media? In *Proceedings of the 21st International Conference on Autonomous Agents and Multiagent Systems*, pages 1794–1798.

Kiayias, A., Russell, A., David, B., and Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference*, pages 357–388. Springer.

K.Lin, C, D. (2023). Favorable views of supreme court fall to historic low. Pew Research Center.

Kshemkalyani, A. D. and Singhal, M. (2011). *Distributed computing: principles, algorithms, and systems*. Cambridge University Press.

Kwon, J. (2014). Tendermint: Consensus without mining. *Draft v. 0.6, fall*, 1(11):1–11.

Lamport, L. and Fischer, M. (1982). Byzantine generals and transaction commit protocols.

Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, 19(5):653–659.

McKenzie, N. D., Liu, R., Chiu, A. V., Chavez-MacGregor, M., Frohlich, D., Ahmad, S., and Hendricks, C. B. (2022). Exploring bias in scientific peer review: an asco initiative. *JCO oncology practice*, 18(12):791–799.

Nakamoto, S. (2008). Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 9:15.

Socol, Y., Shaki, Y. Y., and Yanovskiy, M. (2019). Interests, bias, and consensus in science and regulation. *Dose-Response*, 17(2):1559325819853669.

Xiao, Y., Zhang, N., Li, J., Lou, W., and Hou, Y. T. (2019). Distributed consensus protocols and algorithms. *Blockchain for Distributed Systems Security*, 25:40.

Zhang, A., Walker, O., Nguyen, K., Dai, J., Chen, A., and Lee, M. K. (2023). Deliberating with ai: Improving decision-making for the future through participatory ai design and stakeholder deliberation. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW1):1–32.