**Literature Review on Fairness of Smart Contracts**

**All Papers Introductions:**

**Introduction to Fairness in Smart Contracts:**

Fairness in smart contracts is a critical aspect of ensuring equitable and unbiased execution of contract terms in decentralized environments. Smart contracts, self-executing agreements encoded on blockchain platforms, offer a decentralized mechanism to enforce rules without relying on a central authority. However, achieving fairness in these contracts is complex due to various factors including transaction ordering, cryptographic security, and the integrity of oracles and other data sources. This literature review examines several papers that address fairness in smart contracts, covering applications such as voting systems, digital goods transactions, cloud services, and lottery schemes.

* FASTEN: Fair and Secure Distributed Voting Using Smart Contracts:

The FASTEN protocol focuses on fairness in decentralized voting systems, addressing voter anonymity, vote concealment, vote immutability, and double voting inhibition. It ensures that votes are anonymous and concealed until the voting window closes, preventing undue influence and ensuring the integrity of the vote count. The use of blockchain enhances the transparency and immutability of the voting process. Despite its strengths, FASTEN relies on the honesty of the Election Commission and faces financial constraints due to Ethereum's gas fees.

* Proxy Re-encryption based Fair Trade Protocol for Digital Goods Transactions:

This protocol leverages blockchain and proxy re-encryption to ensure fair digital goods transactions. It guarantees that either both parties receive what they want, or neither does, by using smart contracts to autonomously manage and verify transactions. The protocol enhances security and privacy through encryption, ensuring that digital goods remain encrypted until payment is confirmed. However, it assumes the integrity of the initial encryption by the seller and faces potential issues with smart contract vulnerabilities and blockchain transaction fees.

* Towards Automated Verification of Smart Contract Fairness:

The FairCon framework offers a systematic method to verify fairness in smart contracts through truthfulness, efficiency, optimality, and collusion-freeness. Using symbolic execution and formal verification, FairCon translates smart contract code into mathematical models to detect fairness violations. While it presents a significant advancement in fairness verification, it relies on the correctness of contract annotations and faces computational challenges as the number of participants increases.

* Toward Fairness of Cryptocurrency Payments:

This paper explores methods to achieve fairness in cryptocurrency transactions, focusing on timelocking, optimistic fair exchange (OFE), and blockchain-based signatures. Each method has its strengths and limitations: timelocking provides basic fairness but is vulnerable to network delays; OFE balances fairness and timeliness but depends on a trusted third party; blockchain-based signatures ensure strong fairness but are less flexible due to the need to store signatures on the blockchain.

* Fair Payments for Verifiable Cloud Services Using Smart Contracts:

This paper examines fairness in cloud service transactions, proposing proof-based and replication-based verifiable computation methods. Smart contracts ensure that cloud providers are paid only for correct computations, verified through cryptographic proofs or replication. While the approach enhances fairness without a central authority, it faces challenges related to high blockchain transaction costs and computational overhead.

* Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts:

The proposed system uses multiple smart contracts to manage transactions and ensure fairness in payment and asset delivery. Key contributions include a pre-verification mechanism, consumer-generated pickup codes, and a comprehensive return process. While the approach enhances transparency and accountability, it is complex and may face scalability issues, particularly on the Ethereum blockchain.

* Blockchain-based Fair Payment Smart Contract for Public Cloud Storage Auditing:

This paper introduces a non-interactive public provable data possession (NI-PPDP) scheme to ensure fair payments in cloud storage services. The scheme reduces communication overhead and ensures CSP accountability through automated penalties and payments. However, scalability and complexity remain concerns, and the approach relies heavily on blockchain's capabilities.

* Making Smart Contracts Smarter:

The paper identifies fairness issues in Ethereum smart contracts, such as transaction-ordering dependence and incentive misalignment. It proposes enhancements to Ethereum's operational semantics and tools like OYENTE for pre-deployment bug detection. While significant progress has been made in addressing these issues, gaps remain in fully ensuring equitable outcomes.

* An Overview on Smart Contracts: Challenges, Advances, and Platforms:

This review synthesizes challenges related to fairness in smart contracts, such as overcharging, transaction-ordering dependence, and the need for trustworthy oracles. While advances have been made in optimizing performance and ensuring equitable execution, ongoing research is needed to address privacy and security concerns comprehensively.

* BanFEL: A Blockchain-based Smart Contract for Fair and Efficient Lottery Scheme:

The BanFEL scheme ensures fairness in lottery systems through secure multi-party computation (SMC) and blockchain verification. It addresses limitations in traditional lottery systems by ensuring random number generation and public verification. While it enhances transparency and tamper-resistance, computational complexity and reliance on blockchain infrastructure remain challenges.

**Paper [1]:**

FASTEN: FAIR AND SECURE DISTRIBUTED VOTING USING SMART CONTRACTS

**Introduction:**

Fairness in smart contracts, particularly within the context of voting systems, revolves around ensuring transparency, privacy, and trust lessness in decentralized environments. The concept is pivotal in applications like decentralized voting, where fairness must be maintained to uphold democratic principles. Smart contracts, leveraging blockchain technology, offer a mechanism to distribute trust and enforce rules without relying on a central authority, thus enhancing fairness. The attached paper, "FASTEN: Fair and Secure Distributed Voting Using Smart Contracts," explores these themes in depth, proposing a protocol that addresses multiple fairness concerns inherent in voting systems.

**Critical Analysis:**

The FASTEN protocol is designed to ensure a fair and secure election (FSE) by implementing four key properties: Voter Anonymity (VA), Vote Concealment (VC), Vote Immutability (VI), and Double Voting Inhibition (DVI). These properties collectively contribute to the overall fairness of the voting process.

* **Voter Anonymity (VA):** FASTEN ensures that votes cannot be traced back to the voters, either during or after the election. This is achieved by separating the voter's identity from their vote using unique tokens distributed off-chain by a trusted entity, the Election Commission (EC)​​.
* **Vote Concealment (VC):** The value of each vote remains hidden from the system until the voting window has expired, preventing any premature influence on the election's outcome. This is facilitated using encrypted votes which are only decrypted post-voting period by the smart contract​​.
* **Vote Immutability (VI):** Once cast, a vote cannot be altered by anyone. This immutability is ensured by the blockchain’s inherent properties, where data stored in the ledger is permanent and tamper-proof unless a significant majority of the network’s nodes are compromised.
* **Double Voting Inhibition (DVI):** The protocol ensures that a voter can only vote once by maintaining a hash database of issued tokens, preventing any duplicate entries. This mechanism significantly reduces the risk of fraudulent voting practices.

**Comparison with Existing Literature:**

The FASTEN protocol offers a simplified yet robust approach to achieving fairness in voting systems compared to other protocols that rely heavily on complex cryptographic techniques. For instance, Micali et al.[21] 's protocol, while secure, places significant trust in a centralized entity and lacks scalability. Adida’s [22] Helios protocol, another widely discussed system, depends on the security of a single server, making it unsuitable for large-scale elections. In contrast, FASTEN's reliance on blockchain distributes trust across the network, enhancing both security and scalability.

**Gaps and Limitations:**

Despite its strengths, FASTEN assumes the honesty of the Election Commission in distributing tokens and does not address potential collusion among wardens managing the decryption keys. Furthermore, the protocol's reliance on Ethereum's gas fees for transaction costs could pose financial barriers in large-scale deployments.

**Conclusion:**

The FASTEN protocol marks a significant advancement in designing fair and secure voting systems using smart contracts. By addressing key fairness properties and offering a scalable solution, it sets a new standard for decentralized applications in democratic processes. However, future research must explore mechanisms to mitigate the risks associated with trusted entities and transaction costs to fully realize the potential of blockchain-based voting systems.

**Paper [2]:**

Proxy Re-encryption based Fair Trade Protocol for Digital Goods Transactions on Smart Contracts

**Introduction:**

Fairness in smart contracts, especially within the context of digital goods transactions, is essential to ensure that both parties, typically a buyer and a seller, receive their respective due benefits. This concept is critical to preventing either party from being unfairly disadvantaged during transactions. The paper "Proxy Re-encryption based Fair Trade Protocol for Digital Goods Transactions on Smart Contracts" addresses these concerns by proposing a protocol that leverages blockchain technology and smart contracts to replace the traditional Trusted Third Party (TTP), thus enhancing fairness through decentralization and transparency.

**Critical Analysis:**

The proposed protocol in the paper introduces a passive Proxy Re-Encryption (PRE) scheme to ensure fairness in digital goods transactions. Key fairness aspects include:

* **Fair Exchange:** The protocol guarantees that either both the buyer and seller get what they want, or neither does. This is achieved by using smart contracts to manage and verify transactions autonomously.
* **Security and Privacy:** By utilizing PRE, the protocol ensures that the digital goods remain encrypted until the transaction is confirmed, protecting data privacy. Additionally, the encryption keys are only transferred upon successful payment verification, which prevents unauthorized access.
* **Anonymity and Non-repudiation:** The identities of the parties involved are protected, and neither party can deny their participation in the transaction due to the immutable nature of blockchain records.

**Comparison with Existing Literature:**

Compared to traditional TTP-based methods, which are reliant on the trustworthiness of the third party, the proposed blockchain-based solution offers enhanced fairness by decentralizing trust. Existing solutions such as the one by Guan et al., [23] which also use blockchain, partially automate the process but still require off-chain interactions for key exchanges. The proposed protocol, however, fully automates the transaction process, eliminating the need for off-chain trust dependencies and minimizing interaction times.

**Gaps and Limitations:**

Despite its innovative approach, the protocol assumes the integrity of the initial digital goods encryption

by the seller and the correctness of the smart contract code. Potential issues include the need for buyers to trust the seller's initial setup and the inherent risks of smart contract vulnerabilities. Moreover, the reliance on blockchain transaction fees might pose financial constraints for large-scale or frequent transactions.

**Conclusion:**

The paper's protocol significantly advances the fairness of digital goods transactions using smart contracts by addressing key fairness properties and offering a decentralized, transparent alternative to TTP-based systems. Future research should focus on enhancing the protocol's resilience against smart contract vulnerabilities and exploring cost-effective solutions for blockchain transaction fees to fully capitalize on the potential of decentralized fair-trade systems.

**Paper [3]:**

Towards Automated Verification of Smart Contract Fairness

**Introduction:**

Fairness in smart contracts is pivotal for maintaining trust and equitable outcomes in decentralized systems. Smart contracts are self-executing contracts with the terms directly written into code, running on blockchain platforms. The paper "Towards Automated Verification of Smart Contract Fairness" explores a framework, FairCon, designed to verify fairness in smart contracts by examining properties such as truthfulness, efficiency, optimality, and collusion-freeness. This framework is essential for ensuring that participants in smart contracts do not suffer from unfair practices or logical flaws within the contract code.

**Critical Analysis:**

The FairCon framework introduced in the paper addresses the need for automated verification of fairness properties in smart contracts. Key aspects of fairness discussed include:

* **Truthfulness:** Ensuring participants reveal their true preferences without strategic manipulation.
* **Efficiency:** The allocation of resources should maximize total value, reflecting a fair and optimal distribution.
* **Optimality:** The protocol should achieve maximum net profit, ensuring that outcomes are financially optimal for all parties.
* **Collusion-Freeness:** Preventing participants from collaborating to gain unfair advantages over others. FairCon uses a combination of symbolic execution and formal verification to translate smart contract code into mathematical models, allowing for the verification of these fairness properties. This approach is particularly effective in detecting violations and proving fairness for common contract types like auctions and voting systems.

**Comparison with Existing Literature:**

Existing studies on smart contract fairness often rely on manual analysis or partial automation, limiting their scalability and effectiveness. For instance, traditional methods using Trusted Third Parties (TTPs) introduce centralization risks. FairCon, by contrast, offers a decentralized solution that enhances transparency and trust through blockchain technology. Compared to other automated tools, FairCon's integration of game-theoretic concepts and symbolic execution provides a more robust framework for comprehensive fairness verification.

**Gaps and Limitations:**

While FairCon presents a significant advancement, it assumes the correctness of smart contract annotations and depends on predefined fairness properties. Additionally, the reliance on symbolic execution for model extraction can become computationally expensive as the number of participants increases. Moreover, the framework’s effectiveness in detecting more complex forms of collusion or strategic manipulation remains to be fully explored.

**Conclusion:**

The FairCon framework represents a critical step forward in ensuring fairness in smart contracts. By providing a systematic method to verify key fairness properties, it enhances the reliability and trustworthiness of decentralized applications. Future research should focus on optimizing the computational efficiency of FairCon and expanding its capabilities to handle a broader range of smart contract types and fairness concerns.

**Paper [4]:**

Toward Fairness of Cryptocurrency Payments

**Introduction:**

Fairness in smart contracts is a critical yet underexplored area, particularly in cryptocurrency transactions where participants often do not trust each other. This concept ensures that all parties involved in a transaction fulfill their obligations, mitigating risks of fraud or non-compliance. The attached paper, "Toward Fairness of Cryptocurrency Payments," explores various strategies to achieve fairness in cryptocurrency exchanges, focusing on fair payment-for-receipt scenarios.

**Critical Analysis:**

The paper identifies the inherent challenges of fairness in blockchain-based transactions. Traditional cryptocurrency schemes like Bitcoin ensure security but fall short in guaranteeing fairness. The paper introduces three primary methodologies for enhancing fairness: timelocking, optimistic fair exchange (OFE), and blockchain-based signatures.

**Key Points and Findings:**

* **Timelocking Mechanism:** This method allows a payer to reclaim their payment within a set period if the recipient does not fulfill the contract. While it provides a basic level of fairness, it fails to ensure strong timeliness and is vulnerable to network delays and attacks.
* **Optimistic Fair Exchange (OFE):** OFE leverages a trusted third party (TTP) only in cases of dispute, ensuring that honest parties can complete transactions without the TTP’s involvement. This approach balances fairness and timeliness effectively but depends on the reliability of the TTP.
* **Blockchain-Based Signatures:** This method eliminates the need for a TTP by using the blockchain to verify and confirm signatures. Although it ensures strong fairness and timeliness, it introduces invasiveness since the signature must be stored on the blockchain, making it less flexible.

**Comparative Analysis:**

The paper contrasts these methods, highlighting that while timelocking and OFE provide efficient solutions under certain conditions, they do not universally ensure strong fairness and timeliness. The blockchain-based signature approach, though robust, imposes structural limitations on the exchanged items.

**Gaps and Limitations:**

The study reveals gaps in existing solutions, particularly in achieving noninvasiveness and avoiding dependency on third parties without compromising fairness. Furthermore, while the paper provides theoretical and prototype-based evaluations, real-world applicability and scalability remain less addressed.

**Conclusion:**

The paper’s findings underscore the need for further research into hybrid approaches that can amalgamate the strengths of existing solutions while mitigating their weaknesses. Future work should also focus on formal verification techniques and privacy-preserving methods to enhance the overall fairness and usability of smart contracts in diverse transaction environments.

**Paper [5]:**

Fair payments for verifiable cloud services using smart contracts

**Introduction:**

Fairness in smart contracts is crucial to ensuring that all parties in a transaction or computation receive what they are entitled to without the need for a central authority. Smart contracts, which are self-executing agreements coded on blockchain, offer a decentralized approach to enforcing fairness. The paper "Fair Payments for Verifiable Cloud Services Using Smart Contracts" examines fairness in the context of outsourcing computations to cloud services, aiming to ensure that cloud service providers are paid if and only if they return correct computations.

**Critical Analysis:**

The paper proposes solutions for fair verifiable cloud computations using smart contracts. Key aspects of fairness discussed include:

* **Proof-based Verifiable Computation:** This method uses cryptographic proofs to ensure that the computation was done correctly. The smart contract ensures that the cloud service gets paid only when the client verifies the correctness of the result.
* **Replication-based Verifiable Computation:** This involves outsourcing the same computation to multiple cloud providers and comparing the results. If all results match, the computation is deemed correct, and payments are made accordingly.
* **Smart Contract Mechanisms:** The paper proposes smart contracts that handle deposits from both clients and providers to incentivize honest behavior. Deposits are refunded or forfeited based on the correctness and timeliness of the computations.

**Comparison with Existing Literature:**

The approach contrasts with traditional models that rely on trusted third parties for fairness, which can be costly and potentially unreliable. The proposed smart contract-based models offer a decentralized solution, leveraging blockchain's transparency and immutability. Compared to earlier work, such as Kumaresan and Bentov's [24] Bitcoin-based fair computing model, the use of Ethereum smart contracts allows for more complex and verifiable computation processes due to Ethereum's Turing-complete language.

**Gaps and Limitations:**

The study identifies that while smart contracts provide a robust framework for ensuring fairness, they are not without limitations. The high costs associated with blockchain transactions and the computational overhead for verifying complex proofs are significant concerns. Additionally, the system's reliance on the assumption that at least one honest participant is present may not always hold true in adversarial environments.

**Conclusion:**

The paper's protocols for fair verifiable computations using smart contracts mark a significant advancement in ensuring fairness without the need for a centralized authority. However, addressing the high costs and computational overhead remains a challenge. Future research should focus on optimizing these protocols for practical scalability and efficiency.

**Paper [6]:**

Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts

**Introduction:**

Fairness in smart contracts is paramount for ensuring trust and equity in digital transactions, particularly in the context of cryptocurrencies and asset delivery. The concept of fairness addresses the equitable treatment of all parties involved in a contract, preventing scenarios where one party may cheat or gain undue advantage over another. The paper "Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts" provides an in-depth analysis of protocols designed to enhance fairness and auditability in smart contracts, focusing on mitigating issues such as trust deficits and fraud in online transactions.

**Critical Analysis:**

This paper proposes a comprehensive system using blockchain and smart contracts to ensure fairness in payment and asset delivery. Their approach involves three types of smart contracts (identity, merchant-consumer, and merchant-logistics) to manage transactions and ensure transparency and accountability. The key contributions of the paper include:

* **Pre-verification Mechanism:** The logistics company verifies the authenticity of goods before dispatch, preventing fraudulent activities such as goods being switched during transit.
* **Consumer-Generated Pickup Codes:** By allowing consumers to generate pickup codes, the system mitigates risks of fraudulent activities induced by fake pickup codes sent by logistics companies.
* **Complete Return Process:** For the first time, a smart contract system is designed to handle returns and refunds comprehensively, ensuring consumer satisfaction and reducing disputes.

**Main Points on Fairness:**

The paper highlights several essential elements to achieve fairness:

* **Transparency:** Utilizing blockchain's immutable ledger to record transactions ensures that all actions are traceable and verifiable by all parties.
* **Accountability:** Smart contracts enforce predefined rules, ensuring that all parties adhere to the terms agreed upon without relying on a central authority.
* **Security:** The system uses cryptographic methods to secure transactions and prevent unauthorized actions, thereby ensuring that funds and assets are only transferred when all conditions are met.

**Gaps and Limitations:**

While the proposed system enhances fairness significantly, it also presents some limitations:

* **Complexity:** Implementing and managing multiple smart contracts can be complex and resource intensive.
* **Scalability:** The approach may face scalability issues as the number of transactions increases, particularly in a high-traffic e-commerce environment.
* **Dependence on Ethereum:** The reliance on the Ethereum blockchain may introduce limitations related to transaction costs and network congestion.

**Comparison with Other Literature:**

Compared to existing literature, it approaches provides a more holistic solution by integrating payment and physical asset delivery into a single, auditable framework. Other studies, such as those by Zhao et al. (2018) [25] and Hasan and Salah (2018) [26], focus primarily on either payment or delivery, lacking the comprehensive scope presented in this paper. Furthermore, the introduction of consumer-generated pickup codes and a thorough return process addresses gaps that previous studies did not cover.

**Conclusion:**

This paper significantly advances the discourse on fairness in smart contracts by proposing a robust, auditable system that ensures equitable treatment in online transactions. While challenges remain in terms of complexity and scalability, the proposed framework provides a valuable foundation for future research and practical applications in ensuring fairness in digital commerce.

**Paper [7]:**

Blockchain-based fair payment smart contract for public cloud storage auditing

**Introduction:**

Fairness in smart contracts is a crucial aspect ensuring equitable and transparent transactions, particularly within blockchain and cloud storage ecosystems. The concept involves mechanisms that guarantee all parties adhere to contractual obligations, thereby preventing fraud and ensuring trustworthiness. The paper "Blockchain-based Fair Payment Smart Contract for Public Cloud Storage Auditing" by Wang et al. focuses on enhancing fairness in cloud storage through blockchain and smart contracts, aiming to replace traditional third-party auditors with decentralized, automated systems.

**Critical Analysis:**

Wang et al. [7] introduce a blockchain-based system to ensure fair payments in cloud storage services. The core innovation is the use of Non-Interactive Public Provable Data Possession (NI-PPDP), which allows a Cloud Service Provider (CSP) to prove data integrity without direct interaction, thereby reducing communication overhead.

**Key Points on Fairness:**

* **Non-Interactive Verification:** The NI-PPDP scheme ensures that CSPs can verify data possession without interacting with the verifier, thereby maintaining fairness through reduced dependency on manual checks.
* **Automated Penalties and Payments:** The system ensures CSPs are only paid if they pass data integrity checks. Failure to do so results in penalties, thus enforcing accountability.
* **Public Auditing:** By utilizing blockchain, the verification process becomes transparent and immutable, ensuring that all parties can independently verify data integrity and fairness.

**Gaps and Limitations:**

* **Scalability Issues:** The reliance on blockchain could lead to scalability problems, especially as data and transaction volumes grow.
* **Complex Implementation:** Setting up and managing the NI-PPDP and smart contracts involves significant computational resources and expertise, posing a barrier to widespread adoption.

Comparison with Existing Literature Compared to traditional TPA-based systems and other blockchain approaches, Wang et al.'s model stands out for its non-interactive nature and comprehensive integration of payment and data integrity verification. Studies like those by Zhang et al. (2018) [27, 28] still rely on interactive protocols, which can be less efficient and more costly. Wang et al.’s approach offers a more streamlined and autonomous solution.

**Conclusion:**

This paper significantly advances the fairness paradigm in smart contracts by introducing a novel, non-interactive auditing mechanism that ensures equitable treatment in cloud storage services. While challenges in scalability and complexity remain, the proposed framework provides a robust foundation for future research and practical implementations in enhancing fairness in digital transactions.

**Paper [8]:**

Making Smart Contracts Smarter

**Introduction:**

Fairness in smart contracts refers to the equitable and unbiased execution of contract terms for all participants. Smart contracts, self-executing contracts with the terms directly written into code, are implemented on blockchain platforms like Ethereum. Despite their potential for automating trust and reducing the need for intermediaries, fairness issues arise due to various factors including transaction ordering, incentive misalignment, and the transparency of user inputs. Addressing these concerns is essential to enhance the reliability and adoption of smart contracts in decentralized applications.

**Critical Analysis:**

The paper "Making Smart Contracts Smarter" by Luu et al. [8] highlights several fairness-related issues in Ethereum smart contracts. One key problem is transaction-ordering dependence (TOD), where the order of transactions can be manipulated by miners to achieve favorable outcomes, thus compromising fairness. The paper also discusses incentive misalignment, particularly in gambling applications using commit-reveal schemes, where players may not follow through with the protocol if they foresee a loss, undermining the fairness of the game.

Additionally, the authors identify the lack of cryptographic techniques in some contracts, which can lead to biased outcomes. For instance, contracts that perform computations based on user inputs stored in plaintext are vulnerable to manipulation by malicious users who can influence the outcome to their advantage. The study emphasizes the need for better cryptographic solutions to ensure fair computation and data integrity.

The paper further explores the limitations in existing security measures, proposing enhancements to Ethereum's operational semantics and introducing tools like OYENTE for pre-deployment bug detection. Oyente's evaluation on real-world contracts revealed that a significant number of them are susceptible to fairness-related vulnerabilities, underscoring the prevalence of these issues.

**Comparative Analysis:**

Comparatively, other literature such as Hawk [**29**] and Town Crier [30] focus on enhancing privacy and providing trustworthy data feeds to smart contracts, addressing fairness from a data integrity perspective. However, these approaches are often platform-specific and may not be universally applicable across different blockchain environments.

The integration of findings from various studies indicates that while significant progress has been made in identifying and mitigating fairness issues in smart contracts, there remain gaps in fully ensuring equitable outcomes. Future research should focus on developing more robust cryptographic protocols and incentive-compatible mechanisms to bolster fairness in decentralized systems.

**Paper [9]:**

An overview on smart contracts: Challenges, advances and platforms

**Introduction:**

Fairness in smart contracts is a critical aspect ensuring equitable and unbiased execution of contractual terms. Smart contracts, enabled by blockchain technology, automate the execution of contract clauses once predefined conditions are met, thereby eliminating the need for intermediaries and enhancing efficiency. However, ensuring fairness within this automated framework presents significant challenges. This review synthesizes insights on fairness from the attached research paper "An overview on smart contracts: Challenges, advances and platforms" and other relevant literature.

**Critical Analysis:**

The concept of fairness in smart contracts encompasses several dimensions: equitable access, unbiased execution, and protection against malicious behaviors. The paper identifies key challenges such as the potential for overcharging, transaction-ordering dependence, and the need for trustworthy oracles.

Overcharging occurs when smart contracts consume excessive computational resources, leading to unfair costs for users. Chen et al. [31] highlighted that over 90% of real smart contracts on Ethereum exhibit gas-costly patterns, necessitating tools like Gas Reducer to optimize bytecode and reduce costs​​.

Transaction-ordering dependence can lead to inconsistent outcomes, as the order of transaction execution is not guaranteed. This issue is critical in maintaining fairness, as different execution orders can benefit or disadvantage specific parties. Recent advances propose mechanisms like transaction counters and predefined contracts to address these anomalies​​.

Trustworthy oracles are essential for integrating real-world data into smart contracts. The reliability of oracles directly impacts the fairness of contract execution. Solutions such as Town Crier [32] and Adler. J [33] have been proposed to ensure the integrity and decentralization of data sources, thus enhancing fairness​​.

The paper also discusses the privacy and security concerns inherent in smart contracts, which can affect fairness. Ensuring transactional privacy and protecting against scams and malicious attacks are crucial for maintaining a fair and trusted system​​.

**Conclusion:**

This paper provides a comprehensive overview of the challenges and advances related to fairness in smart contracts. While significant strides have been made in addressing issues like overcharging, transaction-ordering dependence, and trustworthy oracles, ongoing research is needed to enhance the fairness and reliability of smart contracts further. Comparing these findings with other literature in the field highlights a consistent focus on optimizing performance and ensuring equitable access and execution. However, gaps remain, particularly in integrating advanced privacy-preserving mechanisms and robust security protocols. Overall, achieving fairness in smart contracts requires continuous innovation and rigorous evaluation of emerging solutions.

**Paper [10]:**

BanFEL: A Blockchain based Smart Contract for Fair and Efficient Lottery Scheme

**Introduction:**

Fairness in smart contracts is a critical aspect, particularly in applications like lotteries, where trust and transparency are paramount. The concept revolves around ensuring that all participants have equal opportunities and that the outcomes are not influenced by any single entity. This review synthesizes insights from the BanFEL scheme proposed by Li et al.,[10] which aims to address fairness issues in lottery systems using blockchain technology and compares it with other existing literature.

**Critical Analysis:**

The BanFEL scheme introduces a blockchain-based smart contract for lotteries, emphasizing fairness through random number generation and public verification. The scheme leverages secure multi-party computation (SMC) and blockchain's decentralized nature to ensure that the lottery results are genuinely random and verifiable by all participants. This contrasts with traditional centralized lottery systems, where the potential for corruption and unfair manipulation is higher.

Key points from the BanFEL scheme include:

* Random Number Generation: The use of SMC ensures that the winning numbers are generated in a manner that cannot be predicted or manipulated by any single party.
* Public Verification: All transactions and lottery results are recorded on the blockchain, allowing participants to verify the fairness of the lottery process.
* Tamper-Resistance: The smart contract's design prevents tampering with lottery ticket submissions, enhancing the integrity of the process.

Compared to other studies, such as the Ethereum-based lottery proposed by Bartoletti et al., [34] which suffers from low efficiency due to pairwise comparisons, BanFEL offers a more scalable solution. Others also explains blockchain-based system also focuses on security but fails to ensure the verifiability of randomness, a gap that BanFEL effectively addresses.

However, the BanFEL scheme is not without limitations. The computational complexity of SMC can be a bottleneck, though the authors argue that the use of high-performance servers and outsourcing can mitigate this issue. Additionally, while the scheme ensures fairness through transparency, it relies heavily on the integrity of the blockchain and the security of cryptographic protocols.

**Conclusion:**

In conclusion, the BanFEL scheme provides a robust framework for ensuring fairness in lottery systems through blockchain technology. By addressing the limitations of existing schemes and emphasizing transparency and verifiability, it represents a significant step forward. However, practical challenges such as computational overhead and the reliance on blockchain infrastructure must be considered in future implementations. This review highlights the ongoing evolution in the field and the need for continuous improvement to achieve truly fair and efficient smart contract systems for lotteries.

References:

1. Damle, S., Gujar, S., & Moti, M. H. (2021, May). Fasten: Fair and secure distributed voting using smart contracts. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-3). IEEE.
2. Zhang, P., Wei, J., Liu, Y., & Liu, H. (2023). Proxy Re-encryption based Fair Trade Protocol for Digital Goods Transactions via Smart Contracts. *arXiv preprint arXiv:2306.01299*.
3. Liu, Y., Li, Y., Lin, S. W., & Zhao, R. (2020, November). Towards automated verification of smart contract fairness. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 666-677).
4. Liu, J., Li, W., Karame, G. O., & Asokan, N. (2018). Toward fairness of cryptocurrency payments. *IEEE Security & Privacy*, *16*(3), 81-89.
5. Dorsala, M. R., Sastry, V. N., & Chapram, S. (2020). Fair payments for verifiable cloud services using smart contracts. *Computers & Security*, *90*, 101712.
6. Wang, S., Tang, X., Zhang, Y., & Chen, J. (2019). Auditable protocols for fair payment and physical asset delivery based on smart contracts. *Ieee Access*, *7*, 109439-109453.
7. Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., & Susilo, W. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, *519*, 348-362.
8. Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254-269).
9. Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.
10. Li, J., Zhang, Z., & Li, M. (2019, November). BanFEL: A blockchain based smart contract for fair and efficient lottery scheme. In *2019 IEEE conference on dependable and secure computing (DSC)* (pp. 1-8). IEEE.
11. Dziembowski, S., Eckey, L., & Faust, S. (2018, October). Fairswap: How to fairly exchange digital goods. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 967-984).
12. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*, 2901-2925.
13. Danzi, P., Angjelichinoski, M., Stefanović, Č., & Popovski, P. (2017, October). Distributed proportional-fairness control in microgrids via blockchain smart contracts. In *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 45-51). IEEE
14. Kalra, S., Goel, S., Dhawan, M., & Sharma, S. (2018, February). Zeus: analyzing safety of smart contracts. In *Ndss* (pp. 1-12)
15. Levy, K. E. (2017). Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, *3*, 1-15
16. Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., ... & Song, D. (2019, June). Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 185-200). IEEE
17. Zhang, E., Li, M., Yiu, S. M., Du, J., Zhu, J. Z., & Jin, G. G. (2021). Fair hierarchical secret sharing scheme based on smart contract. *Information Sciences*, *546*, 166-176
18. Payeras-Capellà, M., Mut-Puigserver, M., & Cabot-Nadal, M. À. (2018, November). Smart contract for multiparty fair certified notifications. In *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)* (pp. 459-465). IEEE
19. Yang, X., & Zhang, K. (2024). A Fair and Trusted Trading Scheme for Medical Data Based on Smart Contracts. *Computers, Materials & Continua*, *78*(2).
20. Metin, S., & Özturan, C. (2024). Quantised and Simulated Max–min Fairness in Blockchain Ecosystems. *Future Generation Computer Systems*, *151*, 260-271.
21. Silvio Micali and Michael O Rabin. Cryptography miracles, secure auctions, matching problem verification. *Communications of the ACM*, 57(2):85–93, 2014.
22. Ben Adida. Helios: Web-based open-audit voting. In *USENIX security symposium*, volume 17, pages 335-348, 2008.
23. Zhangshuang Guan, Xiaobei Shao, and Zhiguo Wan. Secure fair and efficient data trading without third party using blockchain. In *iThings/GreenCom/CPSCom/SmartData*, pages 1395–1401. IEEE, 2018.
24. Kumaresan, R., & Bentov, I. (2014). How to Use Bitcoin to Incentivize Correct Computations. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.
25. Y.Zhao,Y.Li,Q.Mu,B.Yang,andY.Yu,‘‘Secure pub-sub:Blockchain- based fair payment with reputation for reliable cyber physical systems,’’ *IEEE Access*, vol. 6, pp. 12295–12303, 2018.
26. H.Hasan and K.Salah,‘‘Blockchain-based proof of delivery of physical assets with single and multiple transporters,’’ *IEEE Access*, vol. 6, no. 1, pp. 46781–46793, Dec. 2018.
27. Y. Zhang, R.H. Deng, X. Liu, D. Zheng, Blockchain based eﬃcient and robust fair payment for outsourcing services in cloud computing, Inf. Sci. 462 (2018) 262–277, doi:10.1016/j.ins.2018.06.018.
28. Y. Zhang, R.H. Deng, X. Liu, D. Zheng, Outsourcing service fair payment based on blockchain and its applications in cloud computing, IEEE Trans. Serv. Comput. (2018) 1, doi:10.1109/TSC.2018.2864191.
29. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy, SP ’16. IEEE Computer Society, 2016.
30. Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. Town crier: An authenticated data feed for smart contracts. Cryptology ePrint Archive, Report 2016/168, 2016. http://eprint.iacr.org/
31. T. Chen, Z. Li, H. Zhou, J. Chen, X. Luo, X. Li, X. Zhang, Towards saving money in using smart contracts, in: 2018 IEEE/ACM 40th Inter- national Conference on Software Engineering: New Ideas and Emerging Technologies Results, ICSE-NIER, IEEE, 2018, pp. 81–84.
32. F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: An authenticated data feed for smart contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270–282.
33. J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, A. Kastania, Astraea: A decentralized blockchainoracle, 2018, arXiv preprint arXiv:1808.00528.
34. Bartoletti, Massimo, Tiziana Cimoli, and Roberto Zunino. ”Fun with Bitcoin smart contracts.” International Symposium on Leveraging Ap- plications of Formal Methods. Springer, Cham, 2018.