BGIN Block #10 Meeting Report

- BGIN is a multi-stakeholder discussion body / distributed think tank.

Smart Contract Security

bg
in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

Block#10 Day2_10

Keynote Session Report: Smart Contract Security

Date: Monday, March 4, 2024

Location: Tokyo

Duration: Approx. 90 minutes

Summary

Security Concerns and MEV Discussion

- The conversation starts from security concerns in blockchain, particularly related to Maximal Extractable Value (MEV). A discussant elaborates on MEV, explaining its significance in blockchain transactions and its impact on security. The discussion highlights how MEV can lead to negative externalities like censorship and centralization risks, emphasizing the importance of considering MEV in security and governance perspectives.

Technical Explorations of MEV

- Discussants continue with a technical explanation of MEV, including its components such as execution reward, and how it's divided into issuance and execution levers. The talk delves into how MEV affects transaction ordering and the incentives for block proposers, touching on various strategies employed in the blockchain to maximize MEV gains.

Solutions and Challenges in Mitigating MEV

- The discussion explores potential solutions to mitigate MEV's impact on blockchain security and governance. A discussant presents various technical approaches, including encrypted mempools and sharding, highlighting their pros and cons. The complexity of completely eliminating MEV and its trade-offs with other factors such as decentralization and user experience are discussed.

Regulatory Perspectives and Market Implications

- The conversation shifts towards regulatory concerns and market implications of MEV and blockchain security. Questions arise about how regulators view practices akin to insider trading in the blockchain space and the challenges in regulating such activities. They discuss the need for a more profound regulatory focus on market manipulation within blockchain transactions.

Ecosystem Responsibility and Cybersecurity Concerns

- The session debates who holds responsibility for addressing cybersecurity issues in the blockchain ecosystem. The need for shared responsibility among developers, users, and possibly regulators is emphasized. The discussion also touches on how existing blockchain projects prioritize security and the potential for incentivizing the ecosystem to prioritize cybersecurity more effectively.

Closing Thoughts and Future Directions

- In closing, the discussants reflect on the need for theoretical and practical solutions to blockchain security challenges, particularly those related to MEV. The importance of community awareness and engagement in addressing these issues is highlighted. The session concludes with thoughts on the potential for developing mechanisms that incentivize security in a decentralized manner, recognizing the complex trade-offs involved.

Transcript (anonymized):

02:15:15
A discussion about the security requirements of smart contracts based on their application context is initiated, emphasizing the need for context-specific security measures in design.

02:16:08
The necessity of maintaining a high security standard for smart contracts, regardless of their intended importance, is highlighted to preserve trust in the technology, with a consideration for the cost of security measures.

02:16:58
A detailed explanation on the approach to cybersecurity, focusing on the varying levels of risk, impact, and threat based on the contract's significance and the potential adversaries, emphasizing the importance of context in designing security defenses.

02:18:00
The discussion shifts towards the responsibility for security in smart contracts, especially for parties who may not be technologically sophisticated, questioning the boundaries of accountability.

02:18:25
Agreement is expressed on the necessity for security measures to match the contract's importance and the cost of security, suggesting that smart contract code auditing could be a public good, beneficial for all, yet faces challenges in incentivization.

02:19:29
The issue of insufficient incentive for smart contract code auditing is discussed, underlining the need for an optimal incentive mechanism to ensure adequate security auditing efforts.

02:20:14
Concerns are raised about the limited availability of qualified blockchain cybersecurity auditors, the diversity of blockchain technologies complicating the auditing process, and the potential repercussions of security failures, including liability and dispute resolution.

02:21:22
Suggestions are made for improving code auditability, possibly through regulation, and the importance of auditor reputation and comparison mechanisms for inducing proper auditing efforts, acknowledging the challenges related to auditing costs.

02:23:28
The conversation transitions to technology specifics, with a focus on the role of trust, regulation, and incentives in mitigating security risks, leading to a shift towards a more technical presentation on the subject.

02:24:00
A presentation on MEV (Maximal Extractable Value) and security is introduced, focusing on the importance of understanding incentives for blockchain actors, including nodes and validators, and its relevance to both blockchain sustainability and traditional finance issues like front and back running.

02:25:42
MEV is broken down into two main components: issuance rewards and execution rewards, with a focus on the latter for the presentation. Execution rewards are further divided into priority fees, paid by users, and MEV itself, which is earned through the processing and addition of transaction blocks, mainly benefiting the block proposer or validator.

02:26:49
The complexity of MEV is elaborated upon, noting the involvement of various actors beyond the initial block proposer, such as transaction orderers and block builders, who contribute to maximizing MEV through sophisticated transaction searching and sorting algorithms.

02:28:09
The potential for MEV to exceed traditional gas fees awarded to validators is discussed, highlighting the significant incentives MEV offers compared to other blockchain rewards.

02:29:25
The relationship between MEV and security is examined, with a focus on how the pursuit of MEV rewards can compromise security, leading to negative externalities like censorship, centralization risks, and reduced quality of user transactions. The presentation includes an example of the high rewards associated with MEV, demonstrating its attractiveness to blockchain actors.

02:30:41
An explanation is provided on how validators choose transactions from the mempool, prioritizing those with higher gas prices or potential for maximal extractable value (MEV). The role of the block proposer, who is selected by the consensus algorithm, is highlighted, along with the process of block construction.

02:31:54
MEV is defined more precisely, with distinctions made between transaction ordering and signaling, emphasizing the diverse ways value can be extracted from blockchain transactions.

02:32:19
A clarification is requested regarding the potential for transactions to not be included in a block, leading to a discussion on how transactions with low gas fees might not be included, affecting transaction reliability and user experience.

02:33:22
The consequences of transactions not being included in a block are discussed, particularly the impact on users expecting goods or services in exchange for payments made via these transactions.

02:33:56
A scenario is described where one user's transaction could be preempted by another, taking advantage of transaction ordering to gain a low-risk reward, highlighting potential vulnerabilities in transaction processing.

02:34:30
A question is raised about possible solutions to prevent the issues discussed, such as front-running and transaction exclusion, indicating that solutions will be discussed later in the presentation.

02:34:37

MEV ordering and the concept of transaction bundles are explained, including strategies like flashbots for optimizing MEV extraction and the potential for profit through transaction ordering and selection, touching on advanced tactics like sandwich attacks and atomic arbitrage in decentralized finance (DeFi).

02:36:00
MEV is further explored with the concept of EB (Extractable Value) signals, which incorporate external information into transactions, often used in strategies like statistical arbitrage that combine on-chain and off-chain data. This includes DeFi arbitrage and copy trading strategies that rely on off-chain signals.

02:37:25
The relationship between MEV, security, and transaction ordering is discussed. Without MEV, transactions would be prioritized solely based on gas prices, which could simplify the process but also eliminate the diversity of rewards and potentially increase decentralization and stability in blockchain operations.

02:38:46
A solution to the challenges posed by MEV, known as PBS (Proposer Builder Separation), is introduced. PBS aims to reduce the diversity of rewards and outsource block construction to specialized builders, which could address some centralization concerns but also introduces new challenges in terms of performance and competition among validators.

02:40:26
The discussion shifts to the security benefits of a no-MEV situation and how PBS can mitigate MEV's impact by eliminating reward heterogeneity. The complexities of designing solutions in this vast research space are acknowledged, with a focus on potential approaches to mitigate MEV.

02:41:52
Several strategies for mitigating MEV are presented, including local construction of blocks sorted only by gas fees, the use of encrypted transactions to protect mempool information, and proposals for ensuring that certain transactions are guaranteed inclusion in blocks. The discussion also touches on improving protocol-level mechanisms to address censorship resistance and enhance usability in the context of MEV mitigation.

02:43:16
The presentation delves into the complexities of blockchain space allocation, like pre-confirmation actions, and highlights the potential consequences for users, such as decreased execution quality and increased vulnerability to attacks like front-running and sandwich attacks.

This increases the burden on users to utilize specific endpoints or participate in order flow auctions to avoid these issues.

02:44:39
The concept of "protection fees" as a new competitive arena is introduced, where a dominant block builder might emerge, exploiting its position to extract maximum value from users by offering protection against censorship, creating a market where users might have to pay for censorship protection.

02:45:59
The discussion shifts towards the trade-offs between maximizing MEV for usability and eliminating MEV for increased security. The governance direction chosen will significantly impact the future of blockchain security, with different blockchains potentially adopting various approaches.

02:47:17
The speaker concludes by emphasizing that while the presentation focused on Ethereum, the challenges and solutions related to MEV are applicable across all public blockchains. The aim is to encourage further exploration and understanding of MEV in various blockchain ecosystems.

02:47:45
A follow-up discussion raises concerns about the implications of MEV for security, questioning the rationale for its existence if its elimination would result in better security. This is particularly pertinent in the context of transactions involving significant financial stakes, where the risks associated with MEV might be unacceptable.

02:48:48
The discussion shifts to concerns about the suitability of blockchain technologies, like those using the Solidity programming language, for financial institutions. The skepticism is rooted in the security vulnerabilities inherent to these technologies and the stringent regulatory environment that financial institutions must navigate, which makes them cautious about adopting new, potentially risky technologies.

02:50:03
Questions are raised about the practical decision-making process within organizations considering the adoption of smart contract payments, highlighting the gap between technical possibilities and organizational trust and risk management.

02:50:23

The conversation touches on the legal and ethical implications of practices like front-running in financial markets, comparing traditional market practices to those emerging in the blockchain and cryptocurrency spaces.

02:50:54
A parallel is drawn between high-frequency trading in traditional financial markets, which can resemble front-running, and the challenges faced in blockchain markets, suggesting that while such practices may be minimized, they cannot be entirely eliminated, leading to discussions about acceptable levels of risk and countermeasures.

02:52:04
The encrypted mempool is proposed as a solution to issues like front-running and sandwich attacks, yet concerns about potential side effects and the lack of solutions for these side effects are acknowledged. The discussion also speculates on the possibility that encrypted mempools might increase the number of spam transactions, raising more questions about the feasibility and implications of this approach.

02:53:35
Concerns are raised about the trade-offs between added security layers and their impact on performance and costs, especially in the context of blockchain technology, which is already challenged by speed and efficiency issues.

02:53:58
A discussion about the necessity of an encrypted mempool for preventing sandwich attacks is initiated, proposing an alternative approach of randomizing transaction orders within a block to mitigate such attacks without the need for encryption, potentially simplifying the solution while maintaining security.

02:55:45
The concept of shuffling transactions as a potential solution is acknowledged, but concerns are raised about the possibility of increased spam transactions as a side effect, drawing parallels to previous issues encountered in different blockchain implementations like Polygon.

02:56:25
Clarification is sought on how shuffling transactions could incentivize spamming, leading to an explanation that attackers might exploit shuffling by flooding the network with transactions to increase the chances of their transactions being included in the desired order.

02:57:19

The effectiveness of shuffling in preventing sandwich attacks, despite potential increases in spam transactions, is debated, with the conclusion that while it might prevent specific types of attacks, the overall profitability and feasibility of spamming as a strategy in this context require further evaluation.

02:58:15
An opportunity for questions from the audience is provided, inviting participants to engage and share their thoughts or concerns.

02:58:34
The discussion shifts towards regulatory perspectives on activities such as front-running and sandwich attacks within blockchain transactions, questioning whether such activities could be classified as insider trading or unfair trading practices, and suggesting that stringent penalties might be necessary.

02:59:31
A historical reference is made to a significant financial scandal caused by insider trading, raising concerns about the potential for similar incidents within the blockchain space and questioning the current level of regulatory attention to these issues.

03:00:23
It's acknowledged that while regulators are aware of the challenges posed by blockchain technologies, including specific attacks like sandwich and front-running, the focus has primarily been on combating financial crimes such as money laundering, leaving market manipulation and other issues less addressed.

03:01:33
The conversation delves into potential solutions for mitigating unfair trading practices within blockchain transactions, including the use of encrypted mempools, while also contemplating the technical and regulatory complexities involved in addressing these issues effectively.

03:03:04
A distinction is made between traditional forms of insider trading, typically involving undisclosed information in the securities market, and the unique challenges presented by blockchain transactions, highlighting the need for a nuanced understanding of these issues within the context of blockchain and digital asset trading.

03:03:47

Interest in how regulatory bodies in different countries are addressing issues related to market abuses within blockchain transactions is expressed, with a specific inquiry about the Monetary Authority of Singapore (MAS).

03:04:09
It's suggested that these complex issues might not yet be a primary focus for some regulators, who may currently be more concerned with market abuses on centralized exchanges, indicating a gap in regulatory attention towards blockchain-specific issues like front-running and sandwich attacks.

03:04:47
The discussion shifts to governance and regulatory responsibility, questioning whether the responsibility for addressing these issues lies with traditional regulators or should be managed within the blockchain ecosystem itself. The importance of shared responsibility among various stakeholders in the ecosystem, including developers, service providers, and users, is highlighted.

03:07:12
The conversation explores who within the Ethereum ecosystem, including developers, the Ethereum Foundation, and various projects, is prioritizing cybersecurity, suggesting that the level of cybersecurity could influence cryptocurrency prices, thereby making it a concern for all stakeholders in the market.

03:08:17
A suggestion is made to rethink the reward structure within the blockchain ecosystem to better support cybersecurity efforts. The idea is to possibly redirect some rewards typically allocated to builders towards a dedicated security team to enhance the overall security posture of the ecosystem.

03:08:42
The discussion acknowledges that while investors have a vested interest in the value of cryptocurrencies, they often lack the capability or motivation to contribute to cybersecurity, effectively acting as free riders. The conversation touches on how systems like proof of work or proof of stake, along with specialized hardware like ASIC miners, inherently provide some level of incentive alignment towards maintaining security.

03:09:38
The concept of cybersecurity as a public good within the decentralized market is reiterated, highlighting the common issue of under-provision in such environments. The ideal solution is seen as developing a decentralized incentive mechanism to encourage investment in

cybersecurity, or alternatively, relying on a strong, centralized developer community whose interests are closely tied to the cryptocurrency's success.

03:10:43
The conversation contrasts the decentralized approach to cybersecurity with the corporate world, where security is recognized as everyone's responsibility, evidenced by practices like phishing training and comprehensive security measures. The challenge lies in instilling a similar sense of collective responsibility within the decentralized ecosystem.

03:11:43
The complexity of implementing decentralized cybersecurity measures is discussed, including the potential for creating financial assets or smart contracts that reward the absence of cybersecurity attacks. However, defining what constitutes a cybersecurity attack and the risk of incentivizing attackers present significant challenges to this approach, underscoring the difficulty of managing cybersecurity in a fully decentralized context.
03:12:51
The conversation acknowledges that some blockchain projects prioritize security by designing their programming languages and consensus mechanisms with built-in functional validations to ensure algorithmic security. This approach contrasts with chains like Ethereum, which may not have initially focused as much on security and are now working to enhance their security measures.

03:13:27
There's agreement that the success of these security-focused blockchain projects will ultimately be determined over time. However, waiting for a significant cybersecurity event to evaluate these systems is not ideal, underscoring the importance of proactive security measures.

03:13:51
The necessity of theoretically designing and analyzing blockchain structures to predict effective security mechanisms is discussed, highlighting the challenge of addressing cybersecurity proactively rather than reactively.

03:14:22
A suggestion is made to create documents or reports that raise awareness about the discussed topics, indicating a need for more extensive dissemination of information on blockchain security issues among stakeholders, including regulators.

03:14:52
The conversation concludes with the acknowledgment of a general lack of awareness about the complex challenges facing blockchain security, not just among regulators but also within the

developer community. The discussion raises the question of how to incentivize the broader community to prioritize long-term security considerations over immediate profit-making incentives. The session ends with an invitation for a coffee break, thanking participants for their contributions.