BGIN Block #10 Meeting Report

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

Tokenization and Real-World Assets

bg
in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

Block#10 Day2_7

Keynote Session Report: Tokenization and Real-World Assets

Date: Monday, March 4, 2024

Location: Tokyo

Duration: Approx. 90 minutes

Summary

Introduction and Framework of Tokenization

- The session opens with an introduction to tokenization and real-world assets, emphasizing the confidentiality and recording of the discussion. The framework for tokenization is explained, distinguishing between narrowly defined security tokens and tokenized securities. The existing financial scheme is outlined, illustrating the roles of investors, transfer agents, and custodial banks, and the limitations of traditional security management.

Phases of Tokenization

- Discussion shifts to various phases of tokenization, starting from replacing shareholder registers with permissioned blockchain (Phase 1) to using permissionless blockchains (Phase 2). The benefits of high tamper resistance and potential compliance issues with using permissionless blockchains are debated, including privacy concerns and the need for AML/KYC compliance.

Technical and Compliance Considerations

- The conversation delves into technical aspects, such as the use of whitelists and smart contracts for compliance and privacy, and the potential for decentralized management of whitelists. The limitations of using permissionless blockchains for less liquid assets and the application of Zero-Knowledge Proofs (ZKPs) for maintaining privacy and settlement integrity are discussed.

Practical Application and Legal Framework

- The focus shifts to a practical application by Societe Generale Forge using MakerDAO, including the legal framework, the roles of various parties involved, and the mechanics of

the transaction. The importance of legal clarity in representing a decentralized community and the innovative use of french law to accommodate this are highlighted.

Efficiency and Transparency in Tokenization

- The discussion explores the efficiencies gained from tokenization, such as real-time transparency for investors and the valuation of traditionally less liquid assets. The potential for broader institutional investor participation and the impact on market value through reduced information asymmetry are considered.

Technical Details and Legal Considerations

- A discussant delves into the technical and legal considerations of their experiment with MakerDAO. He outlines the CAS framework for security token issuance, the use of a permissionless blockchain, and the legal structures that facilitated the transaction under French law. The roles of various agents in the transaction, such as the registrar, security agent, and collateral agent, are explained, along with the mechanisms for managing collateral and liquidation events.

Discussion on Efficiency and Blockchain Use in Banks

- The discussion addresses why banks announce successful blockchain projects but often don't integrate them into mainstream operations. Challenges include regulatory constraints, risk management, and the internal structure of banks. The conversation also touches on Project Guardian and its potential as a progressive blockchain initiative in banking.

Advancements in Blockchain Applications by Banks

- The group discusses how banks are using blockchain for settlement purposes, with examples like JPMorgan's Onyx platform. The distinction between public announcements of blockchain projects and the actual use of blockchain in more restricted, interbank contexts is highlighted. The conversation also explores how Societe Generale Forge's experiment with MakerDAO differed by directly using DeFi protocols rather than forking or cloning them for private use.

Societe Generale Forge's Experiment with MakerDAO

- A discussant continues to elaborate on Societe Generale Forge's experiment with MakerDAO, focusing on the benefits, such as improved transparency and real-time

tracking for investors. They discuss the potential for this approach to change how traditional financial instruments are valued and traded, emphasizing the importance of legal and technical frameworks that supported the experiment.

Potential for Broader Application and Final Thoughts

- The session concludes with discussions on the potential for broader application of blockchain in finance, the importance of transparency and efficiency gains, and the role of legal frameworks in facilitating blockchain experiments. Participants reflect on the unique aspects of Societe Generale Forge's experiment and the future possibilities for blockchain in traditional finance.

Transcript (anonymized):

03:50
The session is going to be divided into two parts. In the first 45 minutes, the discussion will focus on the security token scheme, particularly from the business aspect of tokenization, especially security tokens. Following that, the technical aspects of tokenization will be covered. The introduction includes a background as an academic visitor at a university and an employee at a major trust bank, having issued numerous security tokens, including digital bonds. Security tokens, which are tied to real assets as underlying assets, will be explored in more detail.

04:54
There's a mention of recovery from COVID-19 and an apology for any resultant voice issues. The conversation then shifts to the definition of security tokens, which are divided into two categories: narrowly defined security tokens, which are issued natively on distributed ledgers without underlying traditional securities, and tokenized securities, which represent traditional securities and are sometimes referred to as digital twins. The discussion clarifies that the term "security token" will specifically refer to tokenized securities in this context, despite the broader industry usage that might include both types. This is due to the narrow definition not being recognized as official security in many jurisdictions.

06:20
The presentation aims to clarify the use of the term "security token" within the document, focusing on tokenized securities. There is an acknowledgment of the potential confusion due to industry terminology. The discussion will also cover the existing financial schemes to illustrate the potential benefits of using blockchain for securities.

07:20
The importance of understanding the current financial system is emphasized, particularly in relation to blockchain's potential in securities. The speaker shares a background in the finance industry, specifically in managing private equity firms, and suggests that security tokens could democratize access to private equity investments for individual investors.

08:35
The explanation moves on to the phases of adopting blockchain in securities, starting with phase zero, which involves understanding the existing financial system. Phase one involves replacing shareholder registries with a permissioned blockchain. The speaker clarifies that the term "phase" is not indicative of progress or superiority but rather distinguishes different approaches. There is also a note on the ability of phase one participants to issue security tokens on a permissionless blockchain, though they choose to use a permissioned one for specific reasons.

10:11
To clarify, the term "phase" in this context refers to the degree of decentralization in the scheme. Phase two involves replacing the shareholder register with a permissionless blockchain. Subsequent phases introduce self-custodial wallets and on-chain markets, with further discussion on what phase five might entail. In the traditional finance model, investors looking to raise funds appoint a transfer agent to manage the shareholder register and custodian banks for shareholding. The transfer agent keeps track of all shareholder information, including the custodial bank managing each share. Despite securities being digitalized, the complex management involving multiple custodians means only the transfer agent has the complete shareholder register.

11:50
Illustrating with an example, a company issuing shares and appointing a transfer agent might have its shares managed by various custodian banks. If an individual purchases shares through a security company, they become the ultimate beneficial owner, but the security company is listed as the shareholder in the transfer agent's database, highlighting the separation between the shareholder's rights and the actual shareholder's identity. This dual-database management system underpins shareholder rights, emphasizing the complex nature of current securities management.

13:24
The discussion encourages participation and feedback, stressing the workshop's interactive nature. Moving on to phase one, where the traditional shareholder register is replaced with a permissioned blockchain, also known as private chains. This phase doesn't change the investor experience significantly, as transactions and securities management resemble traditional financial systems. However, the underlying technology shifts to a blockchain framework, aiming to streamline and secure the shareholder registration process.

15:02
In phase one, the permissioned blockchain maintains security token holder rights, but investors typically don't use self-custodial wallets due to the blockchain's permissioned nature. This phase aims to integrate blockchain technology while maintaining a familiar interface for investors, with transactions being managed through centralized exchanges and reflected on the permissioned blockchain.

17:03
A clarification is made regarding the non-necessity of self-custodial wallets in a permissioned blockchain setup, emphasizing that this phase's goal is to modernize the shareholder register management without altering the investor's experience or involvement in register management.

17:55
A distinction can be made between the types of permissions that blockchain technology enables. There's a potential architecture involving self-custodial wallets designed to ensure that transactions are initiated by their rightful owners. Meanwhile, the blockchain could be permissioned, allowing transactions only if specific criteria are met. The inclusion of self-custodial wallets for those desiring to verify their personal initiation of transactions could be beneficial.

18:39
The point made is quite significant. It highlights that the initial phase of discussion might be somewhat incomplete. The goal is to outline the current status across various projects under consideration. This leads to the suggestion of moving towards the next phases. Specifically, phase two involves transitioning shareholder registers to a permissionless blockchain. This phase appears similar to the initial one, with the key distinction being the adoption of a functional standard. There's an example of an application designed for smartphones, enabling users to purchase assets, with these transactions being recorded on a permissionless blockchain. This transition prompts a discussion on the potential advantages and disadvantages.

20:20
One clear advantage of this approach is the heightened resistance to tampering associated with permissionless blockchains. The question arises whether such a robust system is necessary in this context, especially considering the traditional finance sector where investors must trust the institutions managing databases on their behalf. This trust requirement is echoed in the first phase, which utilizes a permissioned blockchain, often criticized for its limited oversight.

21:41
There's a contemplation on the relevance of using a permissionless blockchain for this application, given the potential for equivalent trust issues as seen in the traditional and first-phase models. The discussion acknowledges the contentious nature of this topic.

22:49
Concerns are raised about the transparency inherent in using a permissionless blockchain, particularly regarding the visibility of shareholder details. Addressing this would require implementing privacy measures, especially in the earlier phases.

23:01
It's underscored that distinguishing between permissionless blockchains and permissioned smart contracts on such blockchains is crucial. Permissioned smart contracts on a permissionless blockchain are noted for their relative ease of maintenance and adaptability.

23:36
An additional aspect worth mentioning involves custodial wallets, specifically the challenge surrounding enterprise-grade wallets, such as those utilizing multisignature (multisig) technology. Incorporating this into the discussion or diagrams could significantly enhance understanding of workflow organization within the blockchain context.

24:00
Building on this, drawing parallels to traditional financial structures where shareholder rights are established could be beneficial. For example, the use of multisig wallets in traditional finance can be likened to certain security procedures, which could improve the clarity of the diagrams by highlighting these similarities. Furthermore, the focus on permissioned smart contracts is crucial, especially in the context of accountable wallet research, which involves making specific disclosures to access these contracts.

25:04
The process of accessing a whitelist for a smart contract necessitates certain disclosures, which on a permissionless blockchain, involves interacting with another smart contract to obtain a specific token. This "unlocking token" then enables trading with the new smart contract, thus continuing the dialogue in this direction. An oversight was mentioned regarding an important slide that was missed, which highlights the distinctions between the initial phase and the shareholder register phase.

25:56
In the traditional model (phase zero), multiple custodians and nominee shareholders are involved, contrasting with the security token model where such intermediaries might be unnecessary. The data change required upon the transfer of a security token is managed on-chain, potentially rendering the transfer agent's role redundant. However, it's acknowledged that transfer agents might still play a role in maintaining documentation and formalities related to securities.

27:32
The role of transfer agents could evolve to focus on reporting ownership rather than maintaining it. Moreover, the possibility of a company's shares being partially represented by securitized tokens necessitates that transfer agents maintain comprehensive shareholder data, albeit streamlined by blockchain technology. Privacy concerns in this context might be less about individual privacy and more about commercial confidentiality, especially concerning institutional investors.

28:57
The discussion then turns to the comparative disadvantages of employing a permissionless blockchain in certain phases, with a focus on compliance issues, particularly regarding Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) regulations. Despite potential concerns, the flexibility and programmability of smart contracts on permissionless blockchains have been highlighted as capable of maintaining compliance with AML/CFT regulations, thus mitigating perceived disadvantages.

30:25
To illustrate compliance with Counter-Terrorism Financing (CTF) standards, a large securities token platform based in Singapore is highlighted. This platform operates exclusively on a permissionless blockchain, integrating comprehensive AML, CTF, and Know Your Customer (KYC) protocols. The management of such compliance is facilitated through specific tokens, which are traded exclusively via smart contracts and are limited to whitelisted wallets. This

sophisticated system utilizes ERC-20 tokens, which are not Ethereum but are programmed and controlled by the issuing smart contract, ensuring they can only be transferred between approved participants.

31:26
Expanding on this, it's noted that the necessity for a permissioned blockchain is not absolute for conducting certain activities. It's possible to implement what are essentially permissioned smart contracts on a permissionless blockchain, allowing for control and modifications by designated owners without the need for the blockchain itself to be permissioned.

32:09
A suggestion is made to issue security tokens using standard ERC-20 programming, with potential solutions to be documented for addressing various challenges. This approach enables the issuer to maintain a whitelist, thereby knowing the ultimate beneficiary owner in every transaction, which is crucial for compliance and security.

33:40
The conversation then shifts to the importance of KYC processes for gaining access to whitelists, emphasizing that while not all tokens may require this, it should be a standard for all security tokens. Concerns are raised about the security of the whitelist system, highlighting it as a potential single point of failure and a privacy risk if not adequately protected.

34:43
The feasibility of assigning specific roles within smart contracts to manage updates and permissions is discussed, suggesting a practical approach to maintaining security and control within the system.

35:13
There's an inquiry about the technical possibility of using a multisignature mechanism, such as a Gnosis Safe, for contract control and updates, particularly for managing the whitelist.

35:33
It's confirmed that roles within a contract can be assigned to various types of addresses, including multisignature addresses, allowing for a flexible and secure system of control and administration. This method ensures that only authorized actions can be executed by the designated role, even within a permissionless blockchain environment, providing a layer of security and governance.

36:38
Clarification is sought on the role of the broker-dealer in the process of gathering customer information for inclusion on a whitelist. It is confirmed that the broker-dealer is indeed responsible for providing this information, irrespective of who administers the whitelist. Consequently, the issuer of the Digital Application Platform (DAP) must possess the requisite licensing to undertake such issuance.

37:13

It is discussed that managing the linkage between the blockchain address and the actual legal entity or individual permitted to perform specific actions necessitates off-chain management. This process remains essential, regardless of the blockchain framework employed.

37:37
A distinction is introduced between two blockchain utilization strategies. The first involves modeling contractual dynamics directly on the blockchain, which, unless privacy-enhancing blockchains are used, exposes these transactions to public scrutiny. This approach encompasses the use of ERC-20 tokens, among others. The alternative strategy employs blockchain primarily as a settlement layer, where contractual representations are managed off-chain, and only the settlement of these contracts is recorded on-chain, often utilizing zero-knowledge proofs. This method is favored for its potential to maintain private data off-chain while ensuring the integrity and compliance of the data through the blockchain.

38:50
The advantages of using zero-knowledge proofs within this context are further elaborated. This technique allows for the blockchain to serve as a secure log that only records transactions verified to comply with pre-established rules, without revealing the specifics of the transactions themselves. This approach simplifies blockchain usage by handling the complexities of contracts off-chain.

39:48
A query is raised regarding the advantages of this proposed method over traditional financial systems, particularly if transactions are managed off-chain in a manner similar to current practices.

40:08
The effectiveness of this approach is illustrated with the example of Tornado Cash, a platform that simplifies transaction execution while maintaining privacy. In this system, transactions are initiated off-chain, with only a hash committed to the blockchain, ensuring privacy and compliance.

40:49
The discussion extends to the application of this technology in tokenizing assets, such as rental agreements or bank guarantees. The contractual details are modeled off-chain and represented as a hash (referred to as a "zk hash" for its association with zero-knowledge proofs), which is then used to create an NFT. This NFT can then be used to verify certain contract features, such as the notional value, without revealing the contract's full details, thereby maintaining privacy and security.

41:48
The discussion shifts to the technical aspects of implementing contractual agreements on the blockchain. One approach involves creating a new smart contract, with bespoke Solidity code, to model the entire contractual workflow, including contract minting, agreement, and the associated cash flow, all represented on-chain. Alternatively, most of these processes could be managed off-chain, focusing on ensuring the consistency and validity of the contract, agreement by the

parties involved, and the linkage of payments, while maintaining confidentiality through obfuscation techniques.

42:45
The concept of using security tokens to enhance the liquidity of traditionally non-liquid assets, such as private funds, is acknowledged. However, concerns are raised regarding the application of privacy-preserving mechanisms like Tornado Cash in contexts with low transaction volumes, which might not provide sufficient transaction mixing for effective privacy.

43:43
Clarification is provided on the use of zero-knowledge proofs (ZKs) and their application beyond the Tornado Cash model, which was based on transferring specific amounts between buckets for privacy. The current focus is on obscuring the amount of tokens transferred in a transaction, rather than severing the link between wallets. This demonstrates the versatility of ZKs in preserving privacy while utilizing the blockchain primarily as a settlement layer.

44:43
As the discussion nears its close, it's suggested that the paper could summarize the various strategies for ensuring compliance and privacy in the use of blockchain for security tokens. This includes the potential of zero-knowledge proofs and other privacy-preserving technologies to maintain confidentiality within these systems. The conversation concludes with an acknowledgment of reaching the discussion's remit and a prompt to continue exploring these topics in future dialogues.

46:19
The discussion transitions from a broader framework level to a more specific implementation focus, highlighting a notable case of direct interaction between a DeFi protocol and a significant financial institution. This interaction is distinguished by its direct nature, avoiding intermediaries like forks or mere code utilization, marking a substantial institutional application within the DeFi space.

47:34
A specific use case involving a well-known French commercial and investment bank is introduced. This bank engaged directly with the MakerDAO protocol in a pioneering move towards the end of 2022, marking a significant step in the integration of traditional financial institutions with DeFi protocols. The speaker shares insights from personal involvement in the transaction, covering legal, technical, and credit aspects, aiming to explain the structure and implications of this collaboration in straightforward terms.

48:35
The discussion is set to cover various elements of the transaction, including the issuer, the collateral involved, the nature of the transaction, the parties involved, and DeFi-specific liquidation dynamics. Regulatory considerations under French law are also to be discussed, acknowledging that while some aspects may be specific to French jurisdiction, overarching frameworks might find parallels in other legal systems. The possibility of delving into more

technical details is left open, dependent on time constraints and audience interest, with a suggestion that more in-depth technical analysis might be reserved for a follow-up discussion or inclusion in a final paper.

49:40
The focus shifts to the issuer and the framework under which the transaction between the DeFi protocol and the bank was executed. This was facilitated by the bank's development arm, dedicated to exploring and implementing blockchain-based systems for financial services. This entity has transitioned from working on permissioned blockchains to engaging with permissionless, open networks, reflecting growing internal confidence and regulatory comfort. A specific framework for security token issuance, developed since 2018 and progressively implemented in various projects, is highlighted as a key component of this initiative.

50:50
Details are provided on the specific aim of the transaction, which involved refinancing through the issuance of security tokens on the Ethereum blockchain. These tokens were backed by a pool of COVID bonds, an asset class traditionally issued in substantial volumes by the bank in the conventional finance sector. This initiative represented an exploratory step towards diversifying the collateral base within the DeFi ecosystem, leveraging non-volatile, highly liquid assets.

51:53
The transaction was executed by a subsidiary of the bank, framed as an experimental venture into issuing security tokens backed by a cover pool of COVID bonds rated by Moody's. This initiative, set against the backdrop of a particularly challenging market environment in Europe during 2021, aimed to test the viability and potential benefits of integrating traditional financial assets with DeFi protocols on a permissionless blockchain platform.
53:12
The discussion moves towards the practical aspects of the bonds involved in the transaction, highlighting that these bonds offered minimal yield, making the transaction more of an experimental venture than a commercially driven one. This setup served as a testing ground rather than being based on the financial appeal of the structuring itself, providing a snapshot of the transaction's structure and flow.

54:25
The transaction's mechanics are outlined: Societe Generale Forge initiates the process by providing a USD loan to Societe Generale in exchange for transferring ownership of OFH tokens as collateral. Subsequently, Societe Generale Forge, holding the collateral, secures a loan in DAI from the Maker protocol, effectively lending to itself. This step involves using the OFH tokens as collateral for borrowing DAI, which does not alter the underlying structure of the protocol.

55:47
An inquiry is made regarding the responsibility for integrating pricing oracle data for the OFH tokens into the Maker protocol to ensure accurate DAI issuance.

56:02

The response details the use of a pricing model based on the underlying bonds' value, managed by a collateral calculation agent. This agent updates the pricing oracle to reflect any fluctuations in the bond values, employing a market-to-model approach distinct from traditional ERC-20 token pricing oracles. This setup was part of a broader discussion on enhancing and automating this calculation process in future iterations of the project, given its experimental nature for both parties involved.

57:30
The conversation then shifts to discussing the various roles and parties involved in the transaction. Societe Generale Forge acts as the registrar, maintaining the security tokens' register issued by the Societe Generale Group. The group holds the OFH tokens on the Ethereum blockchain, pledging these tokens to Societe Generale Forge and the MakerDAO community. This aspect of the transaction presented legal challenges, particularly in reconciling the concept of community pledging with French law, a unique consideration given the legal and regulatory context.

58:45
The conversation delves into overcoming legal challenges associated with integrating a decentralized DeFi protocol into a contractual framework recognized under French law. A significant hurdle was the lack of a centralized ownership of the DeFi protocol, which complicates traditional legal agreements. French law's concept of a community provided an intriguing solution, enabling a legal structure that accommodates the decentralized nature of the protocol.

59:31
To bridge the gap between the decentralized decision-making process of the Maker community and the legal requirements, a representative or trustee is appointed to execute legal agreements on behalf of the community. This representative must adhere to the decisions made by the community, including those regarding unwinding the structure or initiating a liquidation event, as voted on-chain. This arrangement translates the decentralized community's decisions into actionable legal terms.

01:00:38
The roles within the transaction are further clarified, including the security agent acting as an intermediary, the exchange agent responsible for converting DAI to USD or other currencies, and the collateral agent. The collateral agent, in particular, plays a crucial role in evaluating the market value of the OFH tokens and underlying bonds daily, ensuring the maintenance of agreed collateral thresholds to prevent or address potential liquidation scenarios.

01:01:43
Despite the transaction being more of an experimental venture than a high-yield financial strategy, its structure allowed for significant scalability. The experiment's success demonstrated the potential for substantial transactions within this framework, underscored by the ample collateral backing the underlying bonds. However, the focus was not on generating significant returns but on testing and validating the model's feasibility and operational integrity.

01:02:59
A critical distinction is made between liquidation events in traditional ERC-20 token-backed protocols and those involving security tokens with limited liquidity. The collateral tests are crucial in ensuring that the OFH tokens' market value aligns with the predetermined collateral percentage, a factor of paramount importance for maintaining the integrity and stability of the transaction within the DeFi protocol's ecosystem.

01:04:01
At this age, specific protocols must be met in tests; failing which, certain actions must be initiated, such as sending additional collateral or transferring funds to meet trigger points. Not doing so could result in liquidation and immediate repayment of loans. This contrasts with cryptocurrency loans where liquidations are automated by on-chain mechanisms.

01:04:53
Focusing on a particular protocol, the liquidation process resembles that of traditional markets, where certain parties offer repurchase solutions by buying back collateral. This involves regulatory considerations, conducted under the supervision of a prominent banking regulator in France, as part of an established program related to securities.

01:06:23
The agreement includes various clauses reflecting both regulatory and legal requirements, including insolvency provisions. This bond facility, which involves significant risk assessment of the underlying securities and the organization's creditworthiness, operates under stringent security protocols, making it relatively low-risk compared to other assets held by the protocol.

01:08:15
Questions are raised about the possibility of sharing the presentation, inquiring about any reports the bank might have published, the information shared with the market, and the likelihood of future similar products.

01:08:39
The experiment's structure led to its eventual closure, yet it served as a valuable pilot for learning about decentralized finance and autonomous organizations, highlighting both benefits and challenges for regulated institutions. Documentation on bond issuances on the blockchain has been public since 2021, with subsequent products developed for various client services.

01:09:58
The observation is made that banks often celebrate the success of innovative blockchain projects but then discontinue them, questioning the barriers to integrating such experiments into mainstream operations.

01:10:20
It's acknowledged that this pattern is common and that certain banks have pushed the boundaries more than others, particularly in directly interacting with decentralized finance protocols, which is seen as unique. The approach of creating subsidiaries to handle digital assets and riskier market aspects is highlighted as a key strategy enabling more adventurous endeavors.

01:11:23
The discussion points out that most banks operate these projects internally without the structural separation provided by subsidiaries, which limits their engagement with more innovative or risky projects, such as those involving decentralized finance protocols.

01:12:10
An addition is made, referencing a platform by a major bank that reportedly handles significant daily transactions through blockchain, suggesting that blockchain plays a central role in certain banking operations, especially in interbank settlements, although these advancements may not be as visible to the wider community or corporate clients.

01:13:08
Gratitude is expressed for the shared information, and a notable project is mentioned as a progressive example with potential for longevity, providing inspiration and context for the discussion on why some initiatives might be considered more pioneering or risky than others.

01:13:31
Mention is made of the dynamic nature of banking projects, particularly referencing past experiences with numerous projects in Australia that started but were eventually discontinued.

01:13:42
The conversation shifts to highlight that many banks are indeed settling transactions on permissionless blockchains, distinguishing this from utilizing the programmable aspects of third-party codes, which is far less common. The unique approach of not forking or cloning but directly using third-party contract programmability is emphasized as particularly innovative.

01:14:55
The discussion turns to the value capture within the supply chain, especially when banks are involved. It's noted that banks benefit from better pricing of securities through such innovative transactions, gaining access to alternative financing sources that wouldn't be available in traditional markets due to the efficiency gains from reduced intermediaries, despite the experimental nature of these initiatives.

01:16:18
A question is raised about the involvement of traditional institutional investors, such as pension funds, in such experimental projects and the potential improvements in efficiency and settlement they might bring compared to conventional approaches.

01:17:14
The conversation points out the benefits for underlying investors, such as enhanced diversification of funding sources, competitive pricing, and especially increased transparency, allowing investors to monitor the structure and its activities in real-time, a significant departure from the traditional monthly or quarterly reporting systems.

01:18:11

An efficiency gain is highlighted, stemming from the ability to value traditionally less liquid assets more effectively. This infrastructure boosts investor confidence and the perceptions of rating agencies towards these assets, thanks to more immediate valuations that don't require rapid reactions to underlying changes. This opens up avenues for further development and transparency.

01:19:05
The emphasis is on the broader impact of such experiments, leading towards increased transparency and on-chain visibility of asset valuations and transactions.

01:19:23
Inquiry about whether the experiment's framework has been adopted or forked by others post-event.

01:19:30
Post-experiment, the collateral vault was closed, and its debt ceiling was reduced to zero. However, the smart contract and legal frameworks developed for the experiment were made public, enabling potential future replication, especially the legal engineering aspect behind it, which is considered more critical than the smart contract code itself.

01:20:23
Discussion about the potential for decentralized autonomous organizations (DAOs) to adopt and legally represent the framework developed in the experiment, leveraging community ownership proxies under specific legal systems to manage liquidity positions effectively using similar protocols.

01:20:59
Explanation of the experiment's flow from a smart contract perspective, detailing the structure's components, including vault management, interaction conduits for transactions, and the requirement for token wrapping due to the use of a non-standard token type. This setup underscores the framework's simplicity and adaptability for similar applications.

01:22:16
Further details on the experiment's infrastructure, including the liquidation oracle for pricing securities, the roles of various agents in updating liquidation triggers, and the integration of an interest rate collection module that, while built, was not fully implemented during the experiment due to the need for a fully automated pricing model.

01:23:24
The speaker acknowledges the complexity of certain technical details but emphasizes the simplicity of the underlying structure of the experiment.

01:23:44
It's mentioned that the development was undertaken by the engineering team within a specific protocol, setting a standard for their subsequent projects.

01:24:07
The discussion shifts towards leveraging blockchain transparency for cost-effective fundraising, highlighting the importance of reducing information asymmetry. The speaker suggests that transparent and reliable disclosure of collateral information and its valuation could significantly enhance market value and trust in financial transactions.

01:25:31
The conversation concludes with the proposal to include in a paper the benefits of security tokenization and blockchain for improving transparency in the financial sector. The speaker calls for further research into traditional financial services to compare methods of enhancing transparency and wraps up the session, inviting any final comments or questions.