Smart Financial Contracts on Distributed Ledgers

Nick Van den Broeck, Casper Association

February 12, 2024

Contents

1 Introduction

In recent years, the blockchain industry has witnessed significant progress in the realm of smart contracts, particularly within the domain of Decentralized Finance (DeFi), enabling programmable currencies governed by the principle of "code is law". However, this paradigm falls short when applied to real-world financial contracts, which often necessitate legal jurisdiction and enforcement mechanisms. For instance, consider a loan agreement where the borrower defaults on payments; in such scenarios, traditional legal recourse becomes essential. While smart contracts excel in many cases, enforcing obligations tied to legal concepts like bankruptcy or contractual disputes remains challenging without overcollateralization.

To address these limitations and unlock a broader array of use cases, the industry must transition from smart contracts to smart financial contracts. These are on-chain representations of financial agreements embedded within specific legal jurisdictions. Essentially, a smart financial contract encapsulates an agreement from which future cashflows derive, incorporating jurisdiction-specific mediation.

The development of smart financial contracts hinges on two pivotal innovations: a standardized representation of financial contracts in code and enhancements in blockchain transaction throughput and privacy controls. This essay delineates these innovations and elucidates their synergistic implementation for smart financial contract realization.

2 The Importance of Smart Financial Contracts

Why integrate the ACTUS standard with the Casper blockchain? This question embodies three distinct facets: the relevance of ACTUS to the financial industry, the advantages of leveraging blockchain technology, and the implications for the Casper ecosystem.

Firstly, the financial sector grapples with pervasive issues, characterized by cycles of regulatory intensity and opacity in risk assessment. Addressing these challenges necessitates increased transparency and standardization in financial reporting. The ACTUS protocol offers a solution by standardizing

financial contract representation, enabling comprehensive risk analysis and regulatory oversight.

Secondly, integrating ACTUS with blockchain technology introduces unparalleled benefits in privacy, security, and scalability. By leveraging the immutable and transparent nature of distributed ledgers, financial institutions can enhance data integrity and streamline compliance processes.

Finally, the integration of ACTUS with Casper presents a strategic opportunity for the blockchain platform to distinguish itself in the competitive landscape. By catering to the specific needs of the financial industry and fostering innovation in smart contract technology, Casper can carve out a unique value proposition, attracting both developers and enterprises seeking a robust and compliant blockchain solution.

3 Use Cases for ACTUS on Casper

Effective risk analysis hinges on accurate and relevant data. However, contemporary financial reporting suffers from inherent limitations, including data opacity and heterogeneity. By adopting the ACTUS standard and integrating it with Casper, financial institutions can unlock a myriad of use cases, ranging from decentralized trading platforms to streamlined contract management in traditional finance.

Central to this endeavor is the concept of homogenized data representation. The ACTUS standard offers a comprehensive taxonomy of financial contracts, enabling uniform data reporting and facilitating collaborative risk analysis across diverse institutions. This standardization fosters transparency and accountability, mitigating systemic risks and enhancing market resilience.

Moreover, integrating ACTUS with Casper empowers financial institutions to embrace decentralized finance while preserving privacy and security. By leveraging blockchain technology, institutions can transact with confidence, knowing that their financial data remains tamper-proof and auditable.

4 The ACTUS Standard

At the core of the integration between ACTUS and Casper lies the ACTUS standard—a comprehensive framework for representing financial contracts in a standardized manner. Each financial contract is encoded with a set of terms and dependencies, culminating in predictable cash flows over time. The ACTUS taxonomy comprises 32 distinct contract types, each characterized by algorithmic cash flow generation and comprehensive risk assessment.

Key to the ACTUS standard's efficacy is its ability to fulfill stringent requirements, including compact expression, compression potential, analytical robustness, and compatibility with accounting principles. By encapsulating financial contracts within a standardized framework, ACTUS facilitates comprehensive risk analysis and regulatory compliance while streamlining financial reporting processes.

5 The Need for an L2

While the Casper blockchain offers a robust foundation for smart contract execution, the integration of ACTUS necessitates enhancements in transaction throughput and privacy controls. This imperative underscores the need for Layer 2 (L2) solutions, which augment the capabilities of the underlying blockchain.

Critical to the realization of ACTUS on Casper is the adoption of Zero-Knowledge Proofs (ZKPs), which offer unparalleled privacy and scalability benefits. ZKPs enable verifiable computation without disclosing sensitive information, paving the way for efficient and confidential smart contract execution. By implementing ZK-based L2 solutions, Casper can accommodate the diverse needs of the financial industry while maintaining the integrity and security of its blockchain.

6 Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) constitute a cornerstone of privacy-preserving computation, allowing parties to prove knowledge of a statement without

revealing the underlying information. This cryptographic technique holds immense promise for blockchain scalability and confidentiality, enabling efficient transaction processing and secure data transmission.

Central to the efficacy of ZKPs is their ability to compress information and preserve privacy. By generating succinct proofs of computational integrity, ZKPs facilitate efficient transaction validation and enable granular control over data disclosure. Moreover, Zero-Knowledge Rollups (ZKRs) offer a novel approach to blockchain scalability, aggregating multiple proofs into a single verifiable statement.

7 Building an L2 ZKR on Casper

The implementation of ACTUS on Casper necessitates the development of a robust Layer 2 Zero-Knowledge Rollup (ZKR) solution. This endeavor encompasses several key components, including contract representation, ZK proof generation, consensus integration, data availability, rollup compression, and L2 node infrastructure.

Central to this initiative is the Rust implementation of the ACTUS standard, which provides a standardized framework for financial contract representation. Concurrently, ZK prover systems must be deployed to generate and verify ZK proofs for ACTUS contracts, ensuring computational integrity and confidentiality.

Moreover, the consensus layer of Casper must be augmented to accommodate L2 transactions, incorporating ZK proof verification and validation mechanisms. Similarly, a robust data availability layer is essential for ensuring transparency and auditability in L2 transaction execution.

Furthermore, the rollup software must be developed to aggregate ZK proofs and facilitate efficient transaction processing on Casper. Finally, the deployment of L2 nodes is paramount, providing a scalable and decentralized infrastructure for ACTUS contract execution and validation.

8 Minimum Viable Product (MVP)

The MVP phase of the ACTUS-Casper integration project aims to deliver a fully functional L2 ZKR solution on the Casper blockchain while prioritizing privacy and usability. This entails the implementation of ACTUS contracts, ZK proof generation, consensus integration, and data availability in a centralized framework.

Key components of the MVP include Rust-based ACTUS implementation, ZK prover integration, consensus layer augmentation, centralized data availability, rollup compression, and deployment of a single L2 node. This streamlined approach ensures rapid deployment and validation of the ACTUS-Casper integration concept, laying the groundwork for future scalability and decentralization.

9 Long-Term Vision

Looking ahead, the long-term vision for ACTUS on Casper revolves around enhancing usability, scalability, and decentralization. This entails the development of user-friendly SDKs, decentralized data availability solutions, and distributed L2 node infrastructure.

Central to this vision is the democratization of financial contract management, enabling seamless integration with existing systems and fostering innovation in decentralized finance. By prioritizing user experience and scalability, Casper aims to position itself as a leading blockchain platform for the financial industry, offering unparalleled transparency, security, and efficiency.

10 Conclusion

In conclusion, the integration of ACTUS with the Casper blockchain represents a pivotal step towards revolutionizing financial contract management and compliance. By leveraging standardized contract representation and Zero-Knowledge Proofs, Casper can address the diverse needs of the financial industry while maintaining privacy and security.

Moving forward, the Casper ecosystem is poised to drive innovation in

smart financial contracts, offering a robust and scalable platform for decentralized finance. Through strategic partnerships and continued development, Casper aims to solidify its position as a leading blockchain solution for the financial industry, delivering unparalleled transparency, security, and usability.