**“Addressing Different Blockchain Implementations of Decentralized Finance.”**

**By**

**Eric Webb**

**Abstract:**

This narrative will explore and argue the validity of the security aspects Decentralized Finance(DeFi) provides through popular DeFi protocols and their proprietary blockchain implementations. This was done by conducting research on popular DeFi protocols with each of them having a different blockchain implementation as their underlying architecture. Each one of these DeFi protocols provides security to transactions in their own independent way. The information provided for each individual use case includes validity to why decentralized finance transactions are secure through these DeFi protocols’ blockchain implementations, while also bringing to light the potential flaws that needed to be addressed. A comparison review was conducted between the DeFi protocols to better understand and grasp when and where to implement their blockchain architecture and leads to an argument on to why one would take precedence in certain use cases.

**Keywords:**

Blockchain, Cryptocurrency, DeFi, DEX, Automated Market Maker, Non-Fungible Token

**Introduction:**

The conception of blockchain has led to a renaissance of wealth in the global economy. Since the birth of Bitcoin and other cryptocurrencies, new means of creating value have emerged on the world market. At a high level, some of these examples to create wealth in this new world economy of cryptocurrency include but are not limited to: Transactions, Mining, Staking, Creating Non-Fungible Tokens(NFT’s), Creating Smart Contracts, Lending, and Yield-Farming. A cornucopia of these topics has led to the foundation of what is known as Decentralized Finance (DeFi). In this statement “DeFi refers to a financial system which relies for its security and

integrity on distributed ledger technology.” (*Gudgeon, L., Knottenbelt, W., Perez, D., & Werner, S. 2020)* This is revolutionary because “Unlike regular finance where the identity of all participants is known, and correct behavior can be enforced via regulation, DeFi actors are pseudonymous and DeFi systems need other means to prevent users from misbehaving. In the absence of traditional credit-rating mechanisms, the system rules are typically enforced by incentivizing actors to behave according to the rules of the system.” (*Gudgeon, L., Knottenbelt, W., Perez, D., & Werner, S. 2020)* As you can see Defi is an umbrella term that can encompass many topics of conversation. The main one being how do these blockchain implementations establish trust between parties without relying on a centralized entity? And how can we be sure they are cryptographically secure?

**Introduction: Proof-of-Work VS Proof-of-Stake:**

Fundamentally all blockchain implementations have some type of consensus algorithm in place to come to an agreement when deciding rights to the network.

Not just a DAO (

“A Decentralized Autonomous Organization

(DAO) is an organization whose essential operations are

automated agreeing to rules and principles assigned in code without

human involvement. A DAO is a novel scalable, self-organizing

coordination on the blockchain, controlled by smart contracts”)

**Use Case: Uniswap  (UNI)**

**https://uniswap.org/blog/uniswap-v3/**

As a byproduct of per-LP custom price curves, liquidity positions are no longer fungible and are not represented as ERC20 tokens in the core protocol.

Instead, LP positions will be represented by non-fungible tokens (NFTs).

Uniswap v2 introduced time weighted average price (TWAP) oracles. These oracles serve as a critical piece of DeFi infrastructure, and have been integrated into dozens of projects, including Compound and Reflexer.

V2 oracles work by storing cumulative sums of Uniswap pair prices on a per-second basis. These price sums can be checked once at the beginning of a period and once at the end to calculate an accurate TWAP over that period.

Uniswap v3 offers significant improvements to the TWAP oracle, making it possible to calculate any recent TWAP within the past ~9 days in a single on-chain call. This is achieved by storing an array of cumulative sums instead of just one.

**Use Case: 0x (ZRX)**

**Use Case: Aave (AAVE)**

**Use Case: yEarn(YFI)**

NOTES:

1inch-is a DeFi aggregator and a decentralized exchange with smart routing that minimizes price slippage and finds the optimal trade for the users.

KAVA A decentralized financial services platform. Kava's principle product is a DeFi lending platform for cryptocurrencies.

The Graph is an indexing protocol and global API for organizing blockchain data and making it easily accessible with GraphQL.

KAVA

**References:**

*Annenkov, D., Milo, M., Nielsen, J., & Spitters, B.(2021). Extracting smart contracts tested and verified in Coq. In Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs CPP 2021.Association for Computing Machinery, New York, NY, USA, 105–121. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3437992.3439934*

*Arroyo, J., Hassen, S., & Faqir, Y.(2020). An overview of decentralized autonomous organizations on the blockchain. In Proceedings of the 16th International Symposium on Open Collaboration . Association for Computing Machinery, New York, NY, USA, Article 11, 1–8. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3412569.3412579*

*Gong, X ., Shen, L., Shi ,Z ., & Zhou, M. (2019). Architecture Design for Market-oriented Transaction of Distributed Generation Based on Blockchain. 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, 2019, pp. 2298-2302, doi: 10.1109/iSPEC48194.2019.8975338.*

*Gudgeon, L ., Harz, D., Klages-Mundt, A., Liu, J., & Minca. A. (2020). Stablecoins 2.0: Economic Foundations and Risk-based Models. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery, New York, NY, USA, 59–79. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3419614.3423261*

*Gudgeon, L., Knottenbelt, W., Perez, D., & Werner, S. (2020). DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies ( AFT '20 ). Association for Computing Machinery, New York, NY, USA, 92–112. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3419614.3423254*

*Jia, C., Lui, Q., & Yu, L. (2020). MovER: Stabilize Decentralized Finance System with Practical Risk Management.* 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, 2020, pp. 55-56, doi: 10.1109/BRAINS49436.2020.9223274.*

*Livshits. B. (2020). Technical perspective: Analyzing smart contracts with MadMax. Commun. ACM 63, 10 October 2020, 86. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3416259*