itworldcanada.com

Understanding Cybersecurity Management in DeFi (UCM-DeFi) – DeFi Platforms (Article 3) - IT World Canada

Sepideh HajiHosseinKhani and Arash Habibi Lashkari

16-20 minutes

With the help of blockchain and smart contracts, DeFi platforms are shaking up the financial industry by offering a wide range of services without the need for intermediaries like banks or brokerages. From lending and borrowing to trading and even gaming, DeFi is changing the way we access financial services. But with great innovation comes great responsibility.

Understanding Cybersecurity Management in DeFi (UCM-DeFi), a five-article series, aims to discuss decentralized finance and explore a range of cybersecurity issues that impact DeFi and blockchain-based financial solutions. The articles in this series are based on the recent book titled *Understanding Cybersecurity Management for DeFi*, published by Springer this year. This third article will take a closer look at six of the most popular DeFi platforms and evaluate their security and safety features.

The previous two articles in this series are available here:

Understanding Cybersecurity Management in DeFi (UCM-DeFi) –

Contents

Top 6 Blockchains Powering DeFi Apps

DeFi platforms are built on top of various blockchains, which provide the foundation for decentralized applications like peer-to-peer lending, crypto loans, and decentralized exchanges. These blockchains support the innovative ecosystem that DeFi is shaping for the future of finance.

Let's take a look at some popular blockchains that host DeFi apps, covering the ways they are working to improve blockchain technology and systems,

1. Ethereum: The Leading DeFi Blockchain

Ethereum is a decentralized, open source blockchain platform with smart contract functionality. Its primary goal is to facilitate transactions between parties who don't have a basis for trust, such as geographical separation, incompatibility, or inconvenience. Ethereum enables developers to create consensus-based applications that offer scalability, interoperability, standardization, and ease of development.

Ethereum's smart contracts and decentralized applications can establish their own rules for ownership using a Turing-complete programming language. The platform has two types of account: externally owned accounts and contract accounts.

Externally owned accounts are controlled by private keys and are used to sign transactions, while contract accounts are controlled by their contract code and can read and write messages in response to inputs.

Ethereum's blockchain is made up of three key components that work together to execute transactions and maintain the integrity of the network:

- **Transactions** – Ethereum transactions are messages that are sent from one account to another and contain information such as the recipient's address, the amount of ether to transfer, and optional data.
- **States** – Ethereum's state consists of all accounts and their

balances, contract code, and storage. It is updated after each transaction is executed, changing the state of the accounts involved in the transaction.

- **Blocks** – Blocks in Ethereum contain a header, which includes metadata such as the block number and timestamp, as well as the previous block's hash. They also contain a body that includes a set of valid transactions which are executed to update the state of the blockchain.

2. Binance Smart Chain: High Performance Meets Smart Contracts

Binance launched Binance Chain in April 2019 to offer fast, decentralized trading. The Binance Smart Chain (BSC) is a parallel blockchain to the Binance Chain, providing a dual-chain architecture that combines high-performance trading with smart contract support. This solution enables interoperability and programmability, empowering users to build decentralized apps (dApps) and digital assets on one chain while conducting fast trading on the other.

The Binance Smart Chain boasts several advantages by integrating the best features of both technologies:

- reduces the time and cost of transferring assets
- supports cross-chain communication and Ethereum compatibility
- ensures safety and security for users and developers

BSC's native dual-chain interoperability enhances dApp performance and facilitates cross-chain communication. Built on 21 validators that validate transactions, BSC achieves

decentralization and fosters community involvement.

Binance Chain's primary focus is its decentralized application, "Binance DEX," which has demonstrated low-latency matching and large capacity headroom by handling numerous transactions in a short time. BSC's most extendable feature is its smart contract and virtual machine functionality. However, adding smart contracts to BSC would slow it down, so the solution is to create a parallel blockchain that retains high performance while supporting smart contracts.

3. Solana: High-Speed Blockchain with Proof of History

Solana is a groundbreaking blockchain that uses Proof of History (PoH) to verify the order and passage of time between events. PoH works alongside Proof of Work (PoW) and Proof of Stake (PoS) algorithms to improve the efficiency of Byzantine fault-tolerant replicated state machines. In simpler terms, these machines are designed to reach a consensus on shared data or state even when some nodes may behave maliciously or fail.

In Solana's system, a designated leader generates a PoH sequence, ensuring a verifiable passage of time. The leader sequences and processes messages to maximize throughput. Verifiers execute transactions on their copies of the state and publish their signatures as confirmations, which serve as votes for the consensus algorithm.

Solana relies on a cryptographic hash function to create a PoH sequence. The hash function is called iteratively, with the previous iteration's hash serving as the input for the next. The process

continues until a hash collides with a previous hash, and the series of repeated hash functions forms the PoH sequence.

4. Cardano: Blockchain Solving Problems

Cardano, a project initiated in 2015, aims to revolutionize cryptocurrency design and development. Its foundation is based on design principles and best practices instead of a detailed roadmap. Key principles include separating accounting and computation layers, implementing modular core components, interdisciplinary teamwork, decentralized funding mechanisms, enhancing cryptocurrency designs for security, engaging stakeholders, and incorporating optional metadata in transactions.

Cardano's research led to three main findings:

- Cardano emphasizes the importance of consensus among events recorded in a single ledger. It aims to ensure that all nodes in the network have the same version of the ledger, which is updated through a consensus algorithm. This helps to prevent double-spending and ensures the integrity of the blockchain.
- Cardano uses a Proof-of-Stake (PoS) consensus algorithm, which is an alternative to the energy-intensive Proof-of-Work (PoW) algorithm used by Bitcoin. PoS generates random numbers to select a validator to add the next block to the chain. This approach reduces energy consumption and makes the network more scalable.
- Cardano also addresses the lack of adaptability in most altcoins. It offers a flexible and modular architecture that can be upgraded over time. This allows Cardano to evolve and adapt to new use cases and changing market conditions.

These findings highlight the need for social consensus, as money is a social phenomenon, and the potential risks in manipulating metadata. Cardano focuses on addressing these issues to improve the current state of cryptocurrencies.

Avalanche: The Blockchain for Decentralized Apps

The Avalanche blockchain platform is a high-performance, scalable, customizable, and secure blockchain platform designed for highly scalable and distributed applications. It builds application-specific blockchains comprising both permissioned (private) and permissionless (public) deployments.

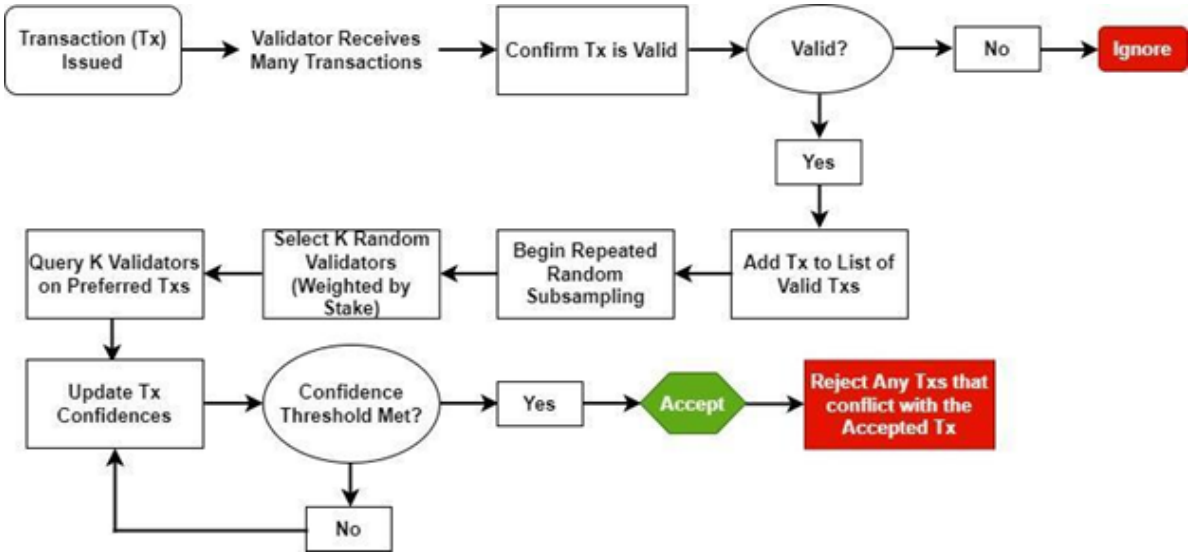
Avalanche is massively scalable, robust, efficient, and can provide strong security features to the blockchain system, withstanding more than 51 per cent of attacks. Avalanche is designed to be decentralized, interoperable, flexible, governable, and democratic.

Avalanche's architecture consists of the creation and operation of a number of subnets to decide who may enter it. Each blockchain is validated by one subnet, offering advantages such as reduced network traffic, trusted validations, and compliance.

The core component of Avalanche is its consensus engine, which combines the best properties of classical and Nakamoto consensus protocols to achieve low latency and high throughput. Avalanche protocols operate through repeated sub-sampled voting, in which K random validators are selected, and their confidence is measured in terms of their weighted stake. When the measured confidence meets a threshold value, the transaction is accepted. Otherwise, the confidence value is updated. Finally, all transactions that conflict with the accepted transaction are

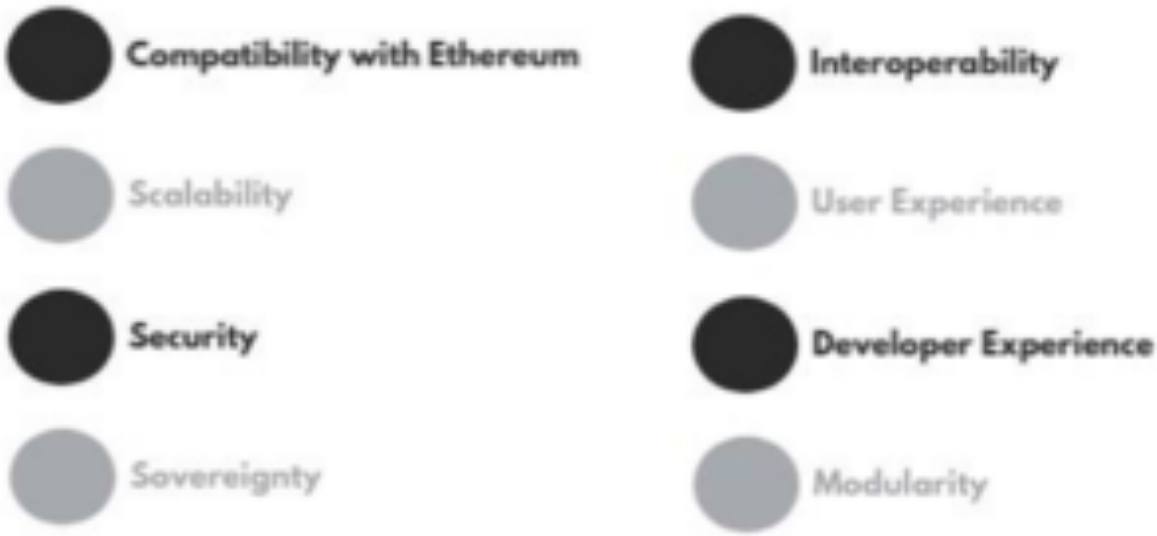
rejected.

Refer to the diagram below for a visualization of the Avalanch consensus protocol in action:



5. Polygon: Platform for Building Blockchains

Polygon is a protocol and framework for building and connecting Ethereum-compatible blockchain networks. It combines the scalability, flexibility, and sovereignty of standalone blockchains with the security, interoperability, and developer experience of Ethereum, characteristics which are summarized in the image below:



Polygon's architecture consists of four layers:

- **Ethereum layer** – refers to the use of Ethereum as a programmable blockchain. It allows Polygon chains to use Ethereum's ecosystem, including its smart contracts, decentralized applications (dApps), and other tools
- **Security layer** – the security layer provides a set of validators to periodically check the validity of Polygon blockchains
- **Polygon network layer** – provides consensus, transaction collation, and block production.
- **Execution layer** – is responsible for interpreting and executing transactions included in the Polygon network.

Polygon enables core components and tools to join the new, borderless economy and society. It provides a high level of independence and flexibility to enterprise networks as standalone networks and has its own validators to ensure security. Alternatively, secured chains provide "security as a service" either by Ethereum or by a pool of professional validators.

6. Fantom: Scalability-Focused Smart Contract Platform

Fantom is a Directed Acyclic Graph (DAG) based smart contract platform that attempts to solve the scalability issue of existing public distributed ledgers. It is being used across large industries such as telecommunication, finance, logistics, electric vehicle provision, and others to create a smart contract-based ecosystem that can be used by all industries. Fantom is open-source and aims to be easily transferable, irreversible, and economical in

terms of transaction fees.

To address the problems associated with existing blockchains, Fantom adopts a new protocol known as the “Lachesis Protocol” to maintain consensus. The protocol integrates into the Fantom Opera Chain, allowing applications built on top of the Fantom Opera Chain to leverage instant transactions and near-zero transaction costs. Fantom’s layered architecture includes a consensus layer, transaction layer, execution layer, and application layer.

Fantom aims to provide compatibility between all transaction bodies globally, create an ecosystem that allows real-time transactions and data sharing at a low cost, and provide high reliability for transactions using DAG technology. DAG technology breaks the sequential processing of transactions, improving the scalability and versatility of existing blockchain technologies.

Security and Safety of DeFi Platforms

DeFi is susceptible to several types of risks, including liquidity mismatches, high leverage, smart contract risks, Oracle risks, scams and cyber-attacks, and administrative and regulatory risks. Let’s take a closer look at what each of these risks entails:

- **Liquidity mismatches** – DeFi’s use of stablecoins and crypto assets can result in liquidity mismatches and exposure to market risks, which can increase the possibility of investor runs.
- **High leverage** – DeFi’s collateralization of funds allows for high leverage, which can induce procyclicality and ultimately lead to market instability.

- **Smart contract risks** – DeFi's use of smart contracts exposes it to several bugs that can be exploited by malicious actors, and the reliance on Oracles can provide exposure to manipulated or inaccurate data.
- **Oracle risks** – DeFi's reliance on Oracles to access external real-time data makes it susceptible to attacks and manipulation.
- **Scams and cyber-attacks** – DeFi platforms are susceptible to various scams and cyber-attacks, including rug pull scams, phishing attacks, fake Google ads, and others.
- **Administrative and regulatory risks** – DeFi's decentralized governance model introduces new risks, including governance attacks that can benefit token holders at the expense of other users. DeFi also faces regulatory risks similar to traditional financial systems, including registration, licensing, and examination of intermediaries.

  Decentralized finance (DeFi) is a rapidly evolving sector that offers financial services using automated protocols on blockchain and stablecoins. However, DeFi suffers from severe vulnerabilities that pose risks to its security and safety.

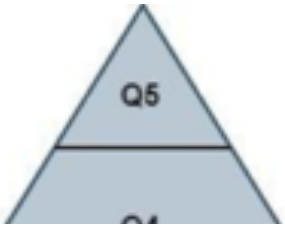
Evaluating the Security of DeFi Platforms

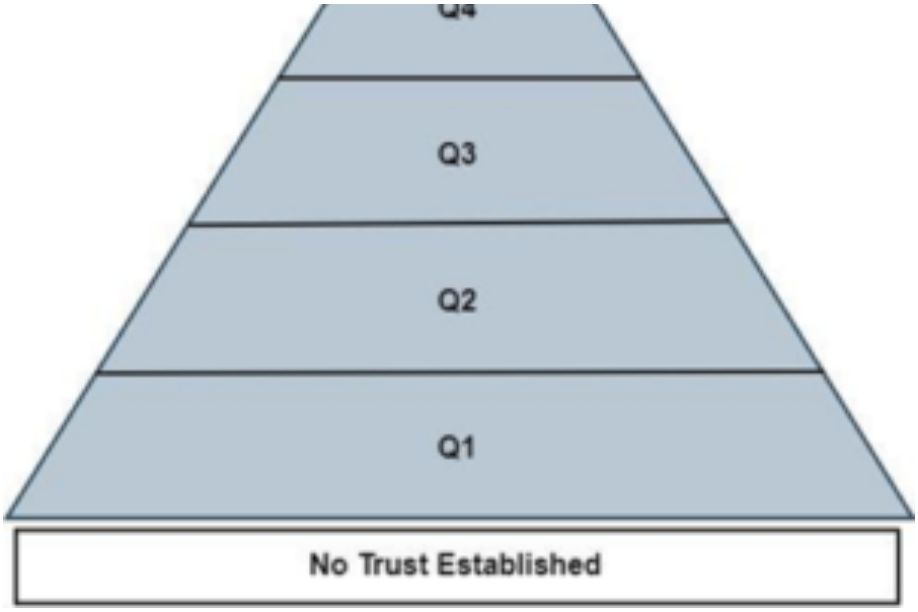
To evaluate the security of DeFi platforms and blockchains, investors should consider several layers of questions presented in the DeFi security evaluation pyramid. The questions start with no trust established and build to the position of trust depending on the answers:

1. **Is the network stack secure?** The network stack is the

underlying infrastructure of the blockchain platform. It includes the hardware, software, and protocols that make up the network. Investors should evaluate the security of the network stack to ensure that it is resistant to attacks and can handle the volume of transactions.

2. **Are the smart contracts audited according to industry standards?** Smart contracts are self-executing programs that run on the blockchain. They should be audited by professionals to ensure that they are free of bugs and vulnerabilities that could be exploited by attackers. Auditing also helps to improve the quality of the code and increase the overall security of the platform.
3. **Who are you transacting with?** DeFi platforms must be transparent about these service providers to restrict malicious actors. Fraudulent funds and trades should be flagged to prevent money laundering. Tainted assets should be prevented from converting back to fiat currency.
4. **Who are they transacting with?** DeFi platforms rely on service providers to carry out essential platform functions, such as providing liquidity and price data. Investors should be aware of these service providers and their reputations to avoid potential fraud or money laundering.
5. **Who are they accountable to?** Developers of DeFi platforms should be accountable to the jurisdictions where they operate to protect investors. Compliance with regulations can build stronger protection mechanisms for users.





The Smart Approach to Investing in DeFi

DeFi platforms are revolutionizing the financial industry by offering a range of services without intermediaries like banks or brokerages. However, these innovative systems are not without risks, and investors should be aware of the potential vulnerabilities. Understanding the security and safety features of popular DeFi platforms and the blockchains they run on is crucial in evaluating their potential as investment opportunities.

By asking key questions about network security, smart contract auditing, service providers, and accountability to regulations, investors can make informed decisions and help shape the future of DeFi.

What’s next

This article looks into six popular DeFi platforms and investigates the security and safety issues and risks of those platforms. Finally, it elaborates on the evaluation of the security of DeFi platforms. The next article of the series, “Understanding Cybersecurity

Management in DeFi: Blockchain Security," sheds light on various blockchain attacks and countermeasures to prevent or avoid those attacks.