SUREHIVE CORE VERSION ONE

August 2021

Prof. E Pindza
with input from the Surehive team

surehive

CONTENTS

Abstract

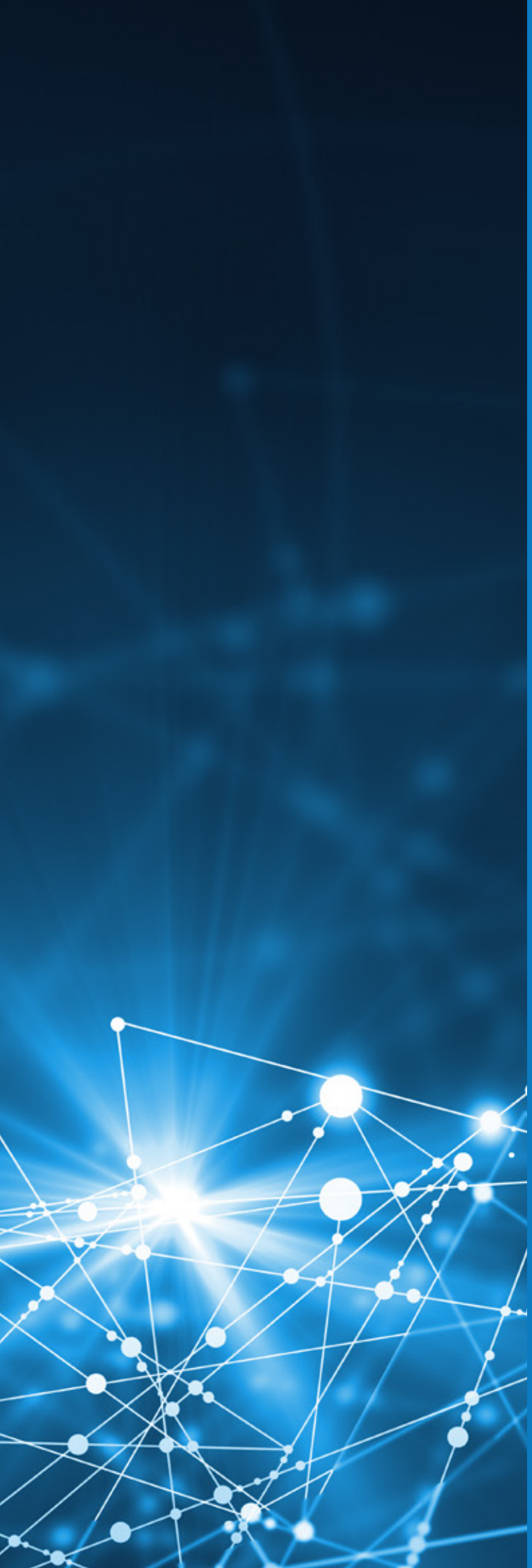
This paper introduces Surehive, a non-custodial Decentralised Finance (DeFi) protocol and crypto-token marketplace implemented on the Cardano blockchain network. It allows users to swap, borrow, lend, save and perform yield farming in a seamless manner. Surehive is built on the premise of flexibility to liquidity providers through Customisable Liquidity Allocation (CLA) and Constant Ellipse Automated Market Markers (CEAMMs) to improve capital efficiency and reduce slippage on the Cardano network.

Keywords:
Automated Market Makers, Cardano, Customisable Liquidity Allocation (CLA)

Disclaimer:
This paper is intended for education and information purposes only and not as financial advice or service. Use or application, of whatever nature, of the contents hereof, is at the reader's own risk. The opinions reflected herein are subject to change without this document being updated.

01

Introduction



The unprecedented growth in trading activity and development of Decentralised Finance (DeFi) platforms and ecosystems has given rise to new, previously thought inconceivable economic models powered by blockchain through smart contracts. Decentralised Exchanges (DEXs) are at the forefront of this new era of censorship-resistant financial innovation. From May 2020 to May 2021, the Total Value Locked (TVL), which is the sum of all liquidity provided to a given protocol, locked in DeFi protocols ballooned by 100x from 800 million USD to 80 billion USD [6].

DeFi is a suite of products that facilitate permissionless deployment and replication of traditional financial instruments through well-orchestrated smart contracts running on public blockchain networks. DEXs are a subset of DeFi that allow network participants to trade any arbitrary crypto tokens without needing a trusted intermediary. This is facilitated by Automated Market Makers (AMMs).

AMMs, in a DEX context, was first introduced by the Bancor protocol in 2017 and later earned popularity through the success of the decentralised exchange protocol, Uniswap. In Uniswap (v1 and v2)'s instance, the AMM stands ready to quote prices on any crypto pair that it supports. The protocol achieves this by applying a Constant Function Market Maker (CFMM) on the supplied liquidity pools and is thus able to price any marginal liquidity-taker based on the size required. It achieves this based on the pricing function and the on-chain liquidity pools without any pricing context on the pair from any other sources external to the protocol [8].

Several successful DEXs operate on blockchains such as Ethereum, Binance Smart Chain and other Ethereum Virtual Machine (EVM) blockchains. Surehive is built on Cardano, a third-generation, Delegated Proof of Stake (DPoS) blockchain whose accounting model is based on an extended Unspent Transaction Output (eUTXO). Cardano's technology stack is discussed in the coming sections.

The remainder of this document is organised as follows. Section 2 restates the problems encountered in the DeFi ecosystem and proposes solutions thereto. Section 3 outlines the advantages of building Surehive on Cardano. Section 4 explains the Surehive protocol on the Cardano eUTXO model. Section 5 deals with the Surehive tokenomics (IVEnomics). Section 6 presents the Surehive roadmap. Section 7 concludes the paper.

Current Challenges Affecting DeFi Solutions

2.1 Protocol Design Challenges

2.1.1 High Impermanent Loss

Impermanent loss describes the temporary loss of funds occasionally experienced by liquidity providers because of volatility in a trading pair. Impermanent loss cannot be entirely avoided in AMMs, but can be made more transparent to the liquidity provider. In most current AMMs, liquidity providers are not aware that their liquidity is at an impermanent loss until withdrawing their liquidity from the pool.

Surehive aims to reduce impermanent loss and make it more transparent to the liquidity provider by providing real-time profit and loss analytics and portfolio updates through targeted email and social media notifications.

2.1.2 High Slippage and Front-running

Slippage refers to the difference between the price expected when the trader submits a swap transaction and the price at which the transaction is confirmed on the blockchain. Two scenarios create slippage when trading on a DEX: high trading volume or low liquidity. High slippage is prevalent in second-generation blockchains such as Ethereum with low transaction throughput due to their consensus mechanism, Proof of Work (PoW).

Surehive implements a Constant Ellipse Automated Market Maker (CEAMM) on Cardano to minimise front-running and reduce slippage. The Cardano environment is unique in how it handles fees, as fees do not go directly to the block producer. Instead, they are pooled and then distributed to all pools that created blocks during an epoch. This way of implementing the fee rewards notably discourages the front-runners from abusing the system. CEAMM is computationally efficient, more robust against front-runner (slippage) attacks. Its tangent line slope function changes very smoothly and stays in a relatively small interval making the token price fluctuation fairly smooth.

2.1.3 High Trading Fees

Most DeFi transactions take place on the Ethereum blockchain. To settle on the blockchain, each transaction costs a certain amount of gas fees. Due to the rising popularity of DeFi in 2020, transaction costs have exponentially increased in the last few months meaning simple transactions can cost up to $20 and complicated interactions with smart contracts up to $200 depending on the current usage of the blockchain.

To solve this problem, Surehive is built to be a first-class citizen of the Cardano blockchain. The Cardano blockchain has several advantages compared to other Ethereum Virtual Machine (EVM) blockchains. Cardano has high transaction throughput with low transaction fees, thanks to its Delegated Proof of Stake (DPoS) consensus mechanism. This minimises the barrier to entry for new users.

2.1.4 Low Capital Efficiency

AMMs have been criticised for requiring large amounts of liquidity to achieve the same level of capital efficiency as an order book based exchange. This is due to the fact that a substantial portion of AMM liquidity is available only when the pricing curve begins to turn exponential. As such, most liquidity will never be used by rational traders due to the extreme slippage experienced.

AMM liquidity providers have no control over which price points are being offered to traders, leading some people to refer to AMMs as “lazy liquidity” that’s underutilised and poorly provisioned. Meanwhile, market makers on order book exchanges can control exactly at which price points they want to buy and sell tokens. This leads to very high capital efficiency, albeit with the trade-off of requiring active participation and oversight of liquidity provisioning.

Surehive implemented a high capital efficiency and low slippage AMM. It used the idea of a Constant Ellipse Automated Market Makers (CEAMMs) together with the concept of Customisable Liquidity Allocation (CLA) through price ranges in liquidity pools. Liquidity providers have the choice of providing liquidity within a price range allowing them to receive transaction fees within an active area of trading.

2.2 User Experience Challenges

Current DeFi platforms are cumbersome and error-prone to navigate for newbies. For example, in order to swap any two arbitrary tokens, a user will have to ensure that they first install a web browser extension wallet like Metamask (for Ethereum and BSC). After that, they need to ensure that they have selected the correct network with enough funds on the base token they intend to swap for another. To get funds of the base token, they will have to buy them through a centralised exchange or another Over-The-Counter (OTC) crypto platform and send those tokens to their Metamask wallet before swapping the said token to their desired token. Furthermore, they need to ensure that there is enough liquidity on the platform before swapping.

The user experience is notoriously complex and understanding how to interact with different DeFi protocols is not a skill everyone can master with ease. This leads many industry insiders to believe we haven't seen the eventual global-adoption ready DeFi protocol.

Surehive is an end-to-end solution that enables users to perform all DeFi activities without leaving the platform. It is set to lead the DeFi ecosystem by providing a friendly user experience, bringing simplicity and reliability in a total package as well as an efficient product that will focus on creating seamless and smooth DeFi experiences without compromising high-security measures and standards.

To help users navigate with confidence, Surehive has implemented on-chain analytics and opt-in notifications. Making the right decisions at the right times not only improves the user's DeFi outcomes, but also gives them more control over their digital asset portfolios.

Having the right information at hand, round the clock, is critical for this to be achieved, the reason why a number of analytics and update mechanisms have been implemented to enable users to analyse the effects of their moves and keep tabs on all developments that may impact their outcomes.

Data analytics features include the user's ability to calculate impermanent loss, calculate profit and loss, calculate liquidation, as well as general analytics.

Updates solutions include an optional subscription-based service that notifies users of events that may influence their portfolios on the Surehive platform.

2.3 Accessibility Challenges

Decentralised finance is so complex to the extent that it prevents meaningful participation of non-finance and non-tech users. Surehive provides humanised support through ongoing education and community-driven support. These ensure that everyone can participate and enhance their knowledge and confidence at their own pace.

The Surehive University will ensure DeFi inclusivity by creating bridges into and out of the DeFi ecosystem to facilitate participation of users side-lined by the Centralised Financial (CeFi) system.

2.1 Protocol Design Challenges

2.1.1 High Impermanent Loss

Impermanent loss describes the temporary loss of funds occasionally experienced by liquidity providers because of volatility in a trading pair. Impermanent loss cannot be entirely avoided in AMMs, but can be made more transparent to the liquidity provider. In most current AMMs, liquidity providers are not aware that their liquidity is at an impermanent loss until withdrawing their liquidity from the pool.

Surehive aims to reduce impermanent loss and make it more transparent to the liquidity provider by providing real-time profit and loss analytics and portfolio updates through targeted email and social media notifications.

2.1.2 High Slippage and Front-running

Slippage refers to the difference between the price expected when the trader submits a swap transaction and the price at which the transaction is confirmed on the blockchain. Two scenarios create slippage when trading on a DEX: high trading volume or low liquidity. High slippage is prevalent in second-generation blockchains such as Ethereum with low transaction throughput due to their consensus mechanism, Proof of Work (PoW).

Surehive implements a Constant Ellipse Automated Market Maker (CEAMM) on Cardano to minimise front-running and reduce slippage. The Cardano environment is unique in how it handles fees, as fees do not go directly to the block producer. Instead, they are pooled and then distributed to all pools that created blocks during an epoch. This way of implementing the fee rewards notably discourages the front-runners from abusing the system. CEAMM is computationally efficient, more robust against front-runner (slippage) attacks. Its tangent line slope function changes very smoothly and stays in a relatively small interval making the token price fluctuation fairly smooth.

2.1.3 High Trading Fees

Most DeFi transactions take place on the Ethereum blockchain. To settle on the blockchain, each transaction costs a certain amount of gas fees. Due to the rising popularity of DeFi in 2020, transaction costs have exponentially increased in the last few months meaning simple transactions can cost up to $20 and complicated interactions with smart contracts up to $200 depending on the current usage of the blockchain.

To solve this problem, Surehive is built to be a first-class citizen of the Cardano blockchain. The Cardano blockchain has several advantages compared to other Ethereum Virtual Machine (EVM) blockchains. Cardano has high transaction throughput with low transaction fees, thanks to its Delegated Proof of Stake (DPoS) consensus mechanism. This minimises the barrier to entry for new users.

2.1.4 Low Capital Efficiency

AMMs have been criticised for requiring large amounts of liquidity to achieve the same level of capital efficiency as an order book based exchange. This is due to the fact that a substantial portion of AMM liquidity is available only when the pricing curve begins to turn exponential. As such, most liquidity will never be used by rational traders due to the extreme slippage experienced.

AMM liquidity providers have no control over which price points are being offered to traders, leading some people to refer to AMMs as “lazy liquidity” that’s underutilised and poorly provisioned. Meanwhile, market makers on order book exchanges can control exactly at which price points they want to buy and sell tokens. This leads to very high capital efficiency, albeit with the trade-off of requiring active participation and oversight of liquidity provisioning.

Surehive implemented a high capital efficiency and low slippage AMM. It used the idea of a Constant Ellipse Automated Market Makers (CEAMMs) together with the concept of Customisable Liquidity Allocation (CLA) through price ranges in liquidity pools. Liquidity providers have the choice of providing liquidity within a price range allowing them to receive transaction fees within an active area of trading.

03

Why Cardano

Cardona has become by far the most trusted blockchain technology. This is because Cardano took a unique approach of research-first, peer-reviewed scientific papers as well as the deployment of formal verification to its codebase.

Cardano uses a Delegated Proof-of-Stake (DPoS) consensus mechanism and other innovative built-in governance and Ouroboros protocol to improve the scalability and transaction throughput while at the same time using less storage space on the network's nodes. The speed is mainly due to the fact that each user who connects to the network generates 10 heads, which can be seen as 10 lanes for data and transactions. Each 'head' on the network would process around 1,000 transactions per second. This would mean that with a number of 1000 heads, the network could scale up to a million transactions per second allowing it to achieve microtransactions.

Plutus, the native smart contract language, is based on Haskell, which, as a purely functional language, offers a multitude of advantages for development, not the least of which are flexibility, natural formal verification and elimination of whole classes of bugs.

The Cardano's Alonzo hard fork brought native Turing complete smart contracting to the Cardano blockchain. Alonzo added various new opportunities for businesses and developers by enabling the development of decentralised applications and smart contracts for decentralised finance. Alonzo achieves this by extending the simple multi-signature scripting language (multi-sig) used in Cardano Shelley by applying a systematic approach focused on formal methods and verification.

With an update to the Plutus Core language, multisig provides more efficient and stable scripting options. The Alonzo ledger provides advanced scripting by implementing the extended Unspent Transaction Output (eUTXO) accounting model. This implementation is enabled through the use of IOHK's hard fork combiner technology. This leads to smart contracts that allow efficient automated trading applications and large cash movements. We also have Cardano transactions validation experimentation tools to customise them. The APIs library has been expanded, allowing Plutus Core code to be deployed and operated while communicating with wallets and the ledger.

04

Surehive Protocol on the Cardano eUTXO Model

The Cardano blockchain has been designed and verified by an industry-leading cohort of engineers and academic experts in the fields of blockchain and cryptography. It has a primary focus on sustainability, scalability and transparency. It is a fully open-source project that aims to deliver an inclusive, fair and resilient infrastructure for financial and social applications on a global scale. The diagram below shows the Cardano architecture that Surehive aligns to.

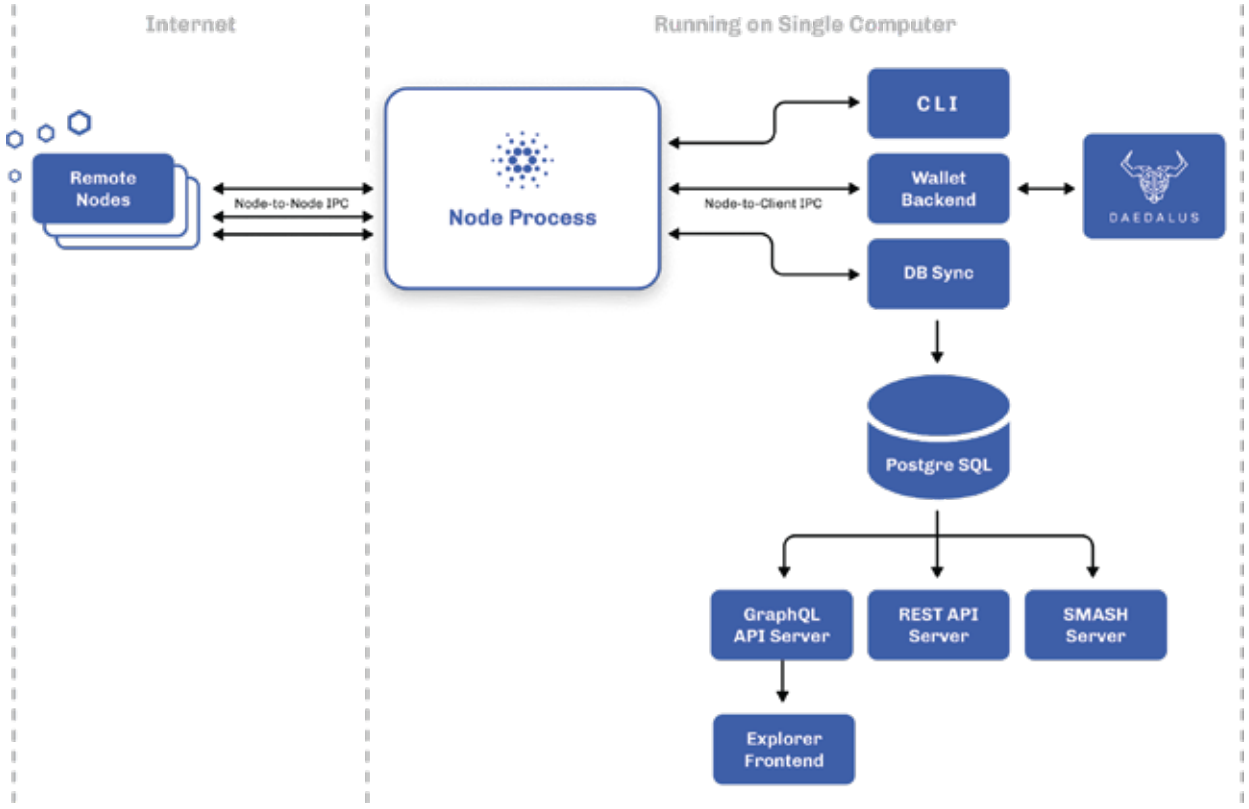


Figure 1: Cardano Technical Architecture

The Surehive protocol is built on a modular micro-service architecture (see Figure 2 below) where components work independently of one another, but through well defined interfaces, are able to communicate with one another seamlessly. Surehive also contains a bridge module that allows traders to convert tokens from other chains into Surehive's Cardano ecosystem.

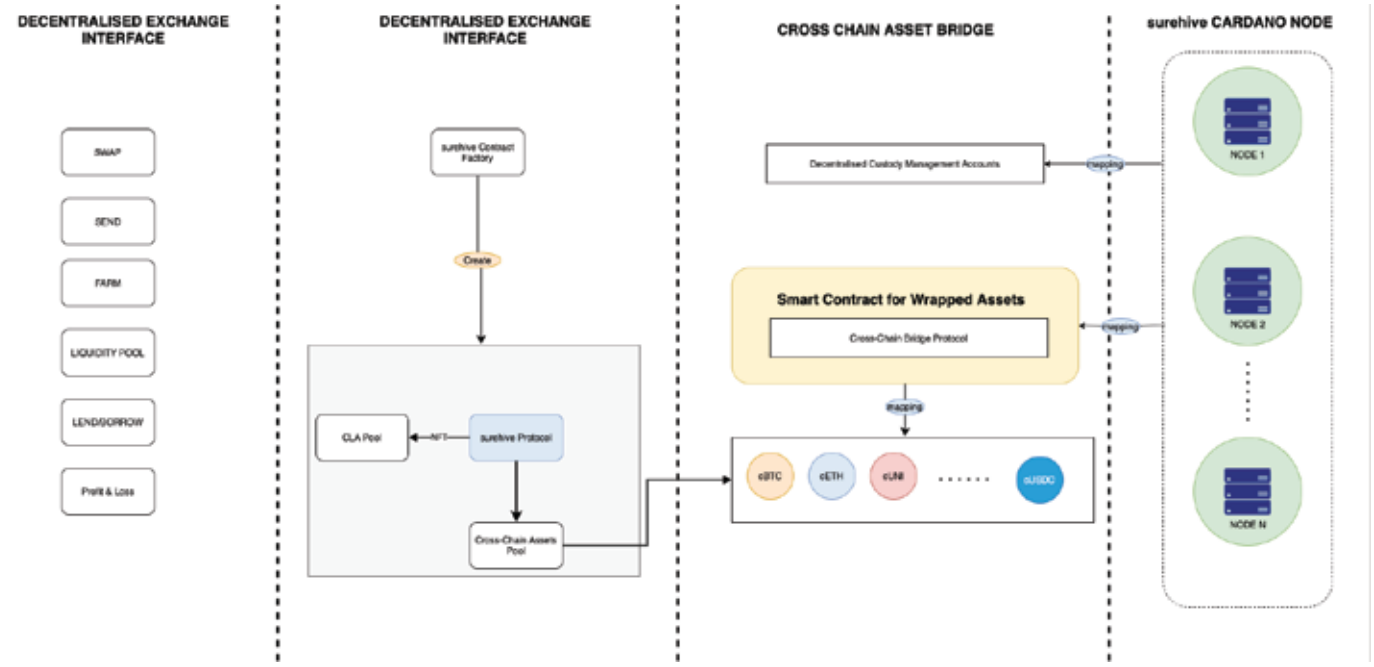


Figure 2: Surehive Technical Architecture

05

Surehive Tokenomics

In the Surehive ecosystem, there exist three categories of platform users: traders, liquidity pool creators and liquidity providers (LPs). The design of Surehive's token economy will engage these user categories and ensure that the platform functions effectively for all of them.

IVE tokens will be launched and have practical utility such as governance rights, group pooling and trading fee discounts on the Surehive platform. A new, non-transferable gIVE token will be launched to serve as Proof of Ubuntu (PoU) in Surehive's loyalty program.

gIVE tokens can be minted at a fixed rate of 1 gIVE = 50 IVE. In addition to the same benefits provided by IVE tokens, gIVE tokens will grant holders trading fees, dividends, referral and membership rewards. In order to encourage long-term membership, redeeming gIVE tokens to IVE tokens will incur an exit fee determined by various factors of the withdrawal. Trading mining will be rolled out to incentivise more interactions with the Surehive platform.

IVE and gIVE: Token Utilities and Benefits

IVE: The Surehive token has been granted several vital features in addition to its governance function. IVE token will provide the following benefits to its holders:

- Governance rights: holders can create and vote on proposals; 1 IVE = 1 vote.
- Trading fee discounts.

gIVE: gIVE token serves as a user's Proof of Ubuntu (PoU) in Surehive's loyalty program. Benefits for gIVE token holders include the following:

- Governance rights: holders can submit and vote on proposals. 1 gIVE = 50votes.
- Trading fee discounts: holding gIVE will give the Surehive users a discount on their transactions.
- Dividends paid out from trading fees: a proportion of the trading fees accrued on the platform will be distributed to gIVE holders.
- gIVE loyalty rewards: IVE reward tokens will be distributed to gIVE holders every block.

gIVE: Minting and Loyalty Rewards

Holders can stake 50 IVE tokens to mint one gIVE token. gIVE tokens are NOT transferable. gIVE token holders receive IVE reward tokens. Specifically:

1. Seven (7) IVE reward tokens are released and distributed to gIVE holders in every block.

2. gIVE holders receive IVE reward tokens directly proportional to their shares of gIVE. That is, the number of IVE tokens they get is 7 times their gIVE balance divided by the number of gIVE in circulation.

3. gIVE holders can invite others to mint gIVE tokens using their referral links. Such holders will get extra loyalty rewards to the value of 12% of the number of gIVE tokens minted by the invitee.

4. To encourage early birds to experiment with gIVE loyalty rewards system, there will be 14 IVE reward tokens per block during the first 5 days.

gIVE: Redemption and Exit Fee

In order to redeem gIVE back to IVE tokens, holders will need to pay a fee-to-exit in gIVE tokens, which will be immediately distributed to all remaining gIVE loyal holders who have not exited. A statistical measure called the IVE Loyalty Index (ILI) will be introduced, which can be defined as:

ILI = (number of gIVE in circulation * 50)/(IVE in circulation).

All things equal, when gIVE gets minted, the number of gIVE in circulation increases, the number of IVE tokens in circulation decreases, and the ILI increases. The exit fee structure is that the higher the ILI, the lower the exit fee rate: When the ILI is above 0.5, the exit fee is at its minimum of 5%. As ILI decreases, the exit fee rate increases. When the ILI is less than 0.1, the exit fee is at its maximum of 15%.

More specifically, the exit fee rate formula is:

If ILI > 0.5, exit fee rate = 0.05
If ILI < 0.1, exit fee rate = 0.15
If 0.1 < ILI < 0.5, exit fee rate = 0.175 - 0.25 * ILI
Note that ILI cannot exceed 1, since no IVE token would be available to be staked to mint gIVE tokens.

IVE: Hard Cap

The tokenomics (IVEnomics) can be broken down as follows: 1 Billion IVE hard cap. The expected date to reach the hard cap is November 2026.

Surehive: Token Distribution

The initial assignment is as follows:

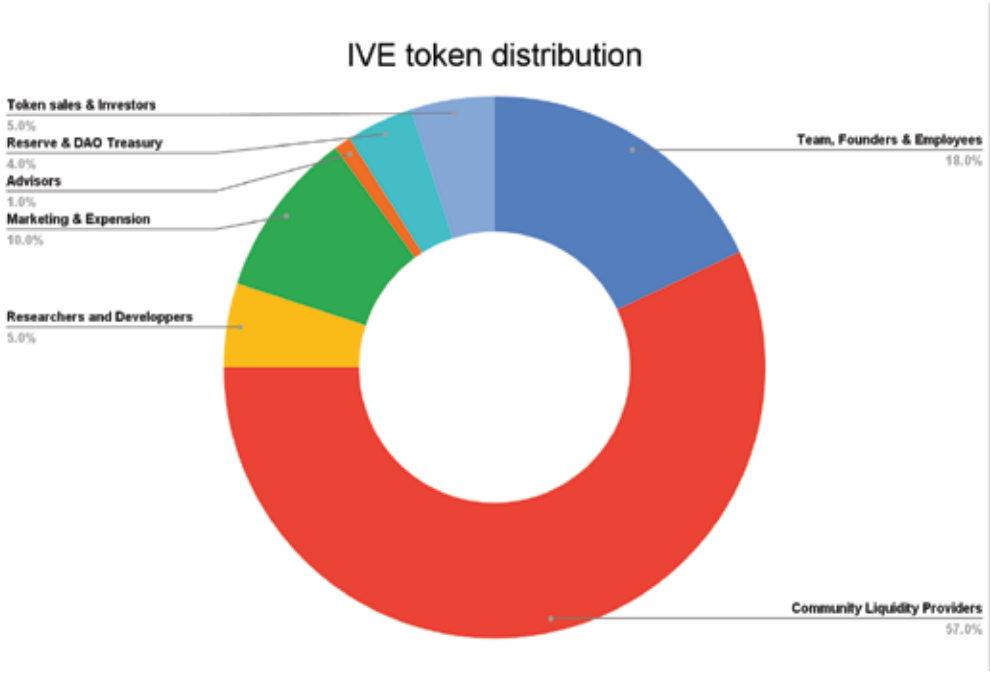


Figure 3: IVE Token Distribution

06

Surehive Roadmap

2021 - Q2 (Done)

- Tech Infrastructure Setup
- Protocol Research and Design
- Integrations & Partnerships Research
- SureHive UX/UI Design
- Whitepaper Draft

2021 - Q3 (Done)

- Litepaper Draft
- Refactoring SureHive Protocol for Cardano
- Technical Architecture Documentation
- Marketing and Brand Awareness
- Whitepaper v0.1
- Litepaper v0.1
- Sign-up Website Launch

2021 - Q4

- Litepaper & Whitepaper v1.0 Release
- Testnet v1.0 launch
- Website Launch
- Cardano Staking Pool Launch
- Initial Stake Pool Offering (ISO) Preparation
- TokenBridge Testnet v1.0 Launch

2022 - Q1-Q2

- Private IVE Sale
- Farming
- Borrowing & Lending
- Testnet v2.0 Launch
- Security Audit
- Mainnet Launch

2022 - Q2 - Q4

- Public IVE Sale
- NFT Marketplace Testnet v0.1 Launch
- DAO Testnet Launch
- Governance UI/UX launch
- DAO Testnet Launch
- Launchpad Testnet Launch
- DAO Mainnet Launch
- Launchpad Launch
- Multi-chain Protocol Launch

2023 - Q1-Q2

- DAO Mainnet Launch
- Launchpad Launch
- Multi-chain Protocol Launch

07

Conclusion

We have presented the Surehive protocol and ecosystem, and how it is used to solve existing challenges in decentralised finance. However, there will be subsequent improvements to our protocol as we evolve on the Cardano blockchain.

References

1. Othman, A. [2012], Automated market making: Theory and practice, PhD thesis, Carnegie Mellon University.

2. Angeris, G. and Chitra, T. [2020], Improved price oracles: Constant function market makers, in 'Proceedings of the 2nd ACM Conference on Advances in Financial Technologies', pp. 80–91.

3. Peterson, J. and Krug, J. [2015], 'Augur: a decentralised, open-source platform for prediction markets', arXiv preprint arXiv:1501.01042.

4. https://cybernews.com/crypto/flash-boys-2-0-front-runners-draining-280-million-per-month-from-crypto-transactions/

5. https://debank.com/ranking/lending?date=1Y&select=liquidate

6. DeFi Pulse. 2021. Defi Pulse. https://defipulse.com/

7. Yongge Wang, Implementing Automated Market Makers with Constant Ellipse, March 2021.

8. Uniswap. Uniswap v2 core, March 2020. https://uniswap.org/whitepaper.pdf.