Absurd finance

Banking, reimagined

We present here a fully-compliant DLT-based banking software able to manage core banking functions using a blended on-chain and off-chain architecture.

V1.0.0 - March 3, 2023

Abstract

Absurd finance is an impossible project that aims at breaking the barriers between web2 and web3. So far the two worlds have mostly lived in parallel, with some attempts at creating bridges via asset tokenisation (RWA), digital copyright (NFT) or pegged tokens (stablecoins). We want more!

As there have been several attempts at introducing the blockchain into banks, examples are Ripple or Stellar, with mild to no real success, it is clear that replacing the current infrastructure with DLT isn't happening anytime soon. What we can do instead is to blend together the two worlds into a chimeric software that tries to be as decentralised as possible, whilst being fully compliant for PSD2 (in EU), GDPR and PCI requirements.

Contents

1 Introduction

Absurd finance is a fintech project that seeks to merge decentralised ledger technology (DLT) with finance in a practical and flexible way. This concept aims to address the observation that despite the significant development activities in web3, no project has directly impacted people's daily lives. Rather, most web3 users are traders or speculators who have little interest in the technology itself.

The mission of Absurd finance is to create a working example of how DLT and fintech can work together effectively, while maintaining a high level of flexibility. To achieve this goal, Absurd finance emphasises the importance of practicality over idealistic, yet unrealistic, ideas such as complete decentralisation or no-KYC. Instead, Absurd finance acknowledges the limitations and regulations surrounding finance and seeks to find ways to leverage blockchain and fintech to make a meaningful impact on people's daily lives.

By leveraging DLTs in a practical way, Absurd finance aims to create a new financial ecosystem that is accessible and beneficial to everyone. This ecosystem will prioritise the needs and interests of both web3 and "traditional" users, while also complying with regulatory requirements. Ultimately, the goal is to show that DLT and the exiting financial world can work together to create real-world solutions that positively impact people's daily lives beyond basic speculation.

1.1 Benefits of using a blockchain

A blockchain is an excellent backend for a bank because it offers several benefits that traditional databases and systems cannot match. Some reasons for that include:

- **Security**: A blockchain is an immutable, decentralised database that is virtually tamper-proof. This makes it ideal for storing sensitive financial data and transactions, as it eliminates the possibility of fraud, manipulation, or hacking.

- **Transparency**: A blockchain provides transparency and accountability by allowing every participant to see and verify transactions in real-time. This feature is particularly important in banking, where trust is essential.

- **Efficiency**: A blockchain can automate several banking processes, such as clearing and settlement, reducing operational costs, and improving efficiency.

- **Speed**: Blockchain transactions can be completed in seconds, compared to traditional banking methods that can take days to process. This is critical for international transactions and cross-border payments, where speed is crucial. L2 and zk-chains are able to outperform existing solutions with high throughput and negligible gas costs.

- **Compliance**: Banks are subject to numerous regulations and compliance requirements, and a blockchain can help ensure compliance by providing an auditable and transparent trail of all transactions. Moreover, as the EU has announced a pilot program to use zero knowledge tech for digital identities, it seems more and more valuable to use privacy-preserving ways of user identity validation (KYC) with partial disclosure via zk-proofs.

Overall, a blockchain provides a secure, transparent, efficient, and compliant backend for a bank, making it an ideal technology for the financial industry.

1.2   The competitor landscape

Absurd was born to tackle the inefficiencies of existing "crypto" banks and stablecoins creating a blended architecture able to overcome the intrinsic issues of a fully on-chain system like stablecoins, or loosely DLT-based models like crypto cards.

Stablecoins are indeed one of the best crypto-fintech examples, yet they are far from perfect. First of all their value is highly volatile, as their legal status is not clear and market heavily prices this constant regulation risk. On the other side, converting stables to fiat is a pricey process, especially for small sums, totally destroying the ethos of crypto to be the *bank for the unbanked* and being more like the *playground for whales.*

Furthermore, both USDC and USDT (the two main dollar-pegged stables) may have a transfer tax in the future.

Moving to **crypto cards**, existing examples are simply traditional banks or BaaS-powered cards with a CEX that swaps crypto to fiat. Basically combining Binance and Revolut, resulting in double fees for the end user.

2 Core Concepts

This section summarises the core features, design choices, technical challenges and possible ways around.

2.1 Smart Contracts

The on-chain part is made of the following elements.

2.1.1 Accounts

Every user will have a smart contract wallet acting as an *Account*, linked to their identity via a zk-KYC system. Through this Account, users will be able to interact with Absurd core features either in a permissionless or permissioned way. The former requires them to have a web3 wallet and pay gas fees directly, in the latter account abstraction will totally hide any web3 jargon and subsidise seed phrase management and gas costs on behalf of the user. Doing so, Absurd can target both web3 native users and newcomers, without having the typical blockers of DeFi (i.e. wallets, seed phrase, gas costs, transaction monitoring, error management, etc.).

A user can have one and only one Account per identity. Via zero knowledge proofs we can implement mandatory SCA (Secure Customer Authentication) requiring them to submit an OTP (One Time Password) for critical actions like sending transfers or swapping money above a certain value.

2.1.2 Fiat tokens

As the upcoming EU MiCa regulation states, on-chain tokens can legally represent fiat deposits as long as the custodian allows for prompt slippage-free redemption of these tokens 1:1 with fiat reserves and those are not invested in risky assets.

Absurd uses ERC777 tokens linked to held deposits for each supported currency. Tokens are transferred, minted and burnt according to user actions, for instance in case of a P2P payment there is just a single transfer, a fiat deposit corresponds to a token minting event, instead if a SEPA/SWIFT transfer is issued then tokens are burnt as the exit the off-chain world.

ERC777 hooks allow for arbitrary logic implementation; examples are:

- *customer transfer limit verification* as stated by the European AML requirements, transfers must be limited on a daily basis;

- *fund freezing* by locking a certain amount of tokens on the user Account we can implement *hold* transactions, typical of hotels and car rentals, where a lump sum is frozen and can be pulled if a certain event happens (car crash, damage to the room);

- *payment streaming* allowing recursive captures, users will be able to subscribe for recurrent payments or open a payment stream: imagine paying or being paid second by second rather than one-off per month, how many more things could you afford to do?!;

- *any custom logic* actually any type of custom logic can be applied, fostering the development of novel financial products linked to the payments sector;

These tokens are transferrable to whitelisted customers only, but can be swapped for DeFi stablecoins internally and then bridged to any major chain. See 2.1.5 for more.

2.1.3 Governance

Governance will consist of two parts, a **DAO** made of all customers who can express their preferences or proposals via quadratic voting and the **Core Committee** made of shareholders who have veto rights over the DAO, if proposals are not legally acceptable. DAO voting will be done via soulbound tokens while the Core Committee uses legally-tokenised shares under the Swiss DLT law, that can be sold to other accredited investors on the open market.

2.1.4 Currency swaps via AMM

By leveraging automated market makers (AMM) technology, Absurd will support on-chain foreign currency swaps with minimal slippage and best rates. Any user can actually earn by being a liquidity provider, deepening liquidity reserves on the AMM.

2.1.5 DeFi bridge

Using the aforementioned AMMs, customers can swap their ERC777 tokens for any of the majour stablecoins like USDC, EUROC, DAI and transfer them to their wallets (*EOA - Externally Owned Accounts*) via LayerZero bridging technology.

2.1.6 Crypto deposits and withdrawal

The DeFi bridge also accounts for crypto interoperability. Users can send inbound transfers, who are subject to an automated AML and KYC check to verify the source of funds, and charge their accounts. Or vice versa, swap their fiat tokens for any supported cryptocurrency and send it out to their EOA.

2.2 Backend

The off-chain part consists of several microservices running on AWS and designated to the following tasks.

2.2.1 Transfer processor

This piece is responsible for idempotent processing of SEPA or SWIFT transactions, thus creating the XML object msg to be sent to the clearing bank in the case of an outgoing transfer, or to parse the incoming XML in the case of an incoming transfer.

2.2.2   Auditing

A watcher process listens to events generated by the Absurd smart contracts and logs any event on a database that is sent to the regulators in case of (suspected) fraud, money laundering or any other criminal activity. The granularity of events accounts for a non-public ledger, thus preserving GDPR as smart contracts internal storage slots are not publicly accessible.