B58 Finance: A DeFi Wallet on Cardano

Francis Luz, Flavio Rasseli, Gabriel Guarnieri
contact@b58.finance

June 2021

Abstract

B58 Finance is a decentralized finance wallet built on top of Cardano Blockchain. Which provide the basic access to the blockchain where you can interact with by checking balances, sending transactions, making payments, registering metadata, providing liquidity, lending, borrowing and voting. In the tradicional Financial world it can be seen as an *Internet Bank* or *Mobile Bank*. Whereas decentralized finance provides the power to be your own bank, using a *Peer-to-Peer* communication with no 3rd party involved in the process supported by the Cardano blockchain. Finally, we aim to bring the *Next-Generation* of wallets to mainstream users. As parallel we want to provide the same experience that users have today by using mobile banks like Revolut[20] and N26[21] in the context of blockchain features, removing the complexity of the decentralized world, with out-of-box integration in commonly used language.

1 Introduction

The Wallet is the core component of *Decentralized Finance (DeFi)[1]*, which provides basic access to interact with the Cardano Blockchain[2] as your *Monetary System*. We chose to start with the wallet as a way of bringing consistency and better user experience to our users. With that in mind users will have access to a host of DeFi services from their wallet, making the integration seamless and natural. Moreover we'll also provide connectivity to *Decentralized Application (DApp)[3]* outside of our Platform.

Regarding basic access to interact with the Cardano Blockchain that will be available to the user is summarized as follow:

- **Multi-Account Management:** Provides the ability of creating multiple wallets aka *"Accounts"* where users can name it eg. Personal, Business, Alice, Bob, etc. Every account has its own unique context and they're not shared between them.
- **Send/Receive Transactions:** In the context of Cardano you can transact ADA the current *"Currency Token"* of the blockchain as well as NATIVE TOKENS that could be a *Collectible Items* or a Tokenized version of other Currencies and Cryptocurrencies.
- **Savings:** This is known as *Stake* in the blockchain world, which provides rewards by *Delegating* your ADA to a designated *Stake Pool*. The user's balance will remain in their control. No one, other than the owner of the wallet, can transact it.
- **Voting:** The Cardano Blockchain has a voting feature that is available today via Project Catalyst where you can vote for funds to projects developing in the ecosystem, and it can be extended in the future.
- **Buy/Sell ADA:** The buy and sell feature gives the user the ability to Buy ADA from their local currency aka *Fiat.* This service will be provided through a Liquidity Provider with this Solution in the market *To Be Defined TBD*.

As part of our basic access, we'll introduce our *Stake Pool* which will support our ***Savings*** feature and provide funds to this entire platform. Our *Stake Pool* will be integrated with our wallet to bring a smooth interaction to our users. We also thought about our community and the mission driven Pools, where we'll enable users to select missions to support.

Next, we're going to introduce our own *Token* which will be as part of some of our offerings. Details about the Tokenomics, distribution and use will be discussed in another whitepaper.

Finally, in the following sections we're going to discuss more details about features and protocols that we're working on at B58 Finance that will support the mass adoption strategy of Cardano Blockchain.

2 Preliminaries

2.1 Proof-Of-Transparency Protocol

Our work on what we're calling Proof-Of-Transparency, will be enabled by the Cardano infrastructure already implemented, with the use of Cardano's *UTXO (Unspent Transaction Outputs)[4]* introduced to the blockchain in the Shelley era[5][19] with Allegra hard fork.

For the purpose of our work in this feature we're going to focus on the ability to attach a Metadata into a transaction and register this information on-chain. Which means from now on we've the possibility to store key value pairs and enrich the transaction giving a meaning to it.

The Proof-Of-Transparency is the underlying logic behind our *Mission Transparency* that is explained in section 3. Where a transaction between two parties is built, and metadata are also attached to it, this metadata contains the Sender and Receiver where the receiver information has to be registered in an off-chain database to be used as a way to identify it. Which will contain Public Name, Image Logo, Address and Contact in our Identity registry and also integrate with *Atala Prism[22]* the Cardano Identity system that could provide unique government issued or otherwise certified identity. Is also important to mention that the Sender can decide whether or not its information remains anonymous as you're going to see the real use case of it i.e, Section 3.

A visual representation of the workflow can be seen as follow:

$$metadata = (PublicName + Logo + Address + Contact)$$

$$\downarrow$$

$$transction = \left(body \begin{bmatrix} sender \\ receiver \\ fee \end{bmatrix}, witnesses, metadata\right)$$

$$\downarrow$$

$$utxo = transaction$$

With this transaction store on-chain we'll be able to validate this information on the *Cardano Explorer* and also through our own *Transparency Explorer* where the user will be able to see a human-translated and visual representation of the transaction.

Finally the Proof-Of-Transparency is a utility implementation on top of the underlying Cardano Transaction Model. In the same way that a cryptocurrency is an application of the UTXO Model, we're extending Cardano to new ways of using it, and bringing another level of Transparency to transactions that need this protocol.

2.2 Social Proof for Micro Lending

The Social Proof algorithm will be the backend of our Social Lending feature detailed in Section 4.

This algorithm aims to determine the number of Social Proof that a Borrower needs from the inputs used to calculate it. The inputs are: *Minimum Threshold (MiT), Maximum Threshold (MaT), Amount(A), Maximum Amount and Amount Percentage Cut (APC)* that can contain numbers from 0 to 99. Which will return a *Social Proof Number (SPN)* in the form of a natural positive integer.

The formal definition of the formula developed by our team expresses our opinion, in initiative to be fair with the distribution of the Social Proof required. Inspired by Kiva's Micro Lending model we've derived the idea into this formula that can be seen as follow:

$$SPN = \begin{cases} MiT & \text{if } MaT \div (\frac{MA}{A - (A \cdot (APC \div 100))}) < MiT \\ \lceil MaT \div (\frac{MA}{A - (A \cdot (APC \div 100))}) \rceil & \text{if } MaT \div (\frac{MA}{A - (A \cdot (APC \div 100))}) > MiT \end{cases}$$

Whereas the property of SPN which is the number of Social Proofs required, is higher if the amount requested is closer to the maximum amount, and is lower if the amount requested is closer to minimum, because the higher the requested amount is, the more Social Proof will be needed to bootstrap the micro lending in its initial Private stage.

Considerations: This is the first formal definition, so that it can be improved in the implementation phase, with the validation and broad test case scenarios.

3 Mission Transparency

The Mission Transparency is a feature based on the core nature of the Cardano Blockchain with its Immutability and Auditability. On top of that we're adding our Proof-Of-Transparency protocol which is described in detail in Section 2.1.

Our work consists in bringing visibility to transactions related to Donations, where one party Donator and the other party a Non-profit Organization (NGO), will have a Metadata Transaction registered in the blockchain.

The inspiration comes from the Stake Pool Operators[6], which dedicate part of its revenue to support institutions around the world, but today lacking in tools for transparency leading them to develop alternative solutions. Not only that, the traditional way of doing this is through annual reports[7] issued by the NGOs.

To address this in a Decentralized manner we're introducing the *Transparency Explorer* where anyone will be able to track live information about projects that users support.

4 Social Lending

The Social Lending feature is our Microlending platform that will be backed by our Social Proof algorithm described in Section 2.2.

Inspired by Cardano's Mission to *Banking the Unbanked* and specially focused on countries in Africa[8], where users don't have a financial identity.

With the mission to be Next-Generation of wallets, we'll provide access to B58 Accounts to those countries using the right technology for the user be it a smartphone or a simple text message based phone. We're going to be developing features to support and help users' financial life.

Then we'll be developing a fair and decentralized credit score, and also providing micro-loans for small businesses through a crowdfunding platform where Projects will have two stages of publication being Private, when the borrower will be required a bootstrap fund from Friends and Family[9] according to their SPN result which will be impacted by the amount requested over the maximum available in the contact pool. Then will have the Public stage where other users of B58 Finance will be able to contribute to the project with a small fraction of the total loan required.

After a period of time to be determined, the contract will be locked and no contributions will be accepted, the borrower will be able to claim the value raised in a Stablecoin[10] available or developed on the Cardano blockchain.

Risks and Mitigation: There's a Risk of Default due to the fact that no collateral is requested on the Social Lending, which we aim to void or reduce using our decentralized credit score system based on the repayment done by the Borrower where a fail or a delay of it will decrease his score and ability to borrow in the future.

To Mitigate this Risk, we aim to partner with local Operators to provide and collect repayments as well as share a portion of the interest generated by the contract.

5 Borrowing and Lending

The Borrowing and Lending feature will be based on smart contracts with crypto-pairs, where users putting a collateral will be able to get a Loan in the crypto asset required.

Well known projects like Compound[11], Maker Protocol[12] and others have introduced this protocol to the blockchain, which will be translated to Cardano's world enabling another Decentralized Finance tool to users of B58 Finance wallet.

Lenders will be able to provide liquidity to contract pools, and receive yields according to the borrowing rate to be defined at the launch of each pool.

Borrowers will be paying interest by using the pool, and the repayment will be due every 5 days which is an Epoch on the Cardano Blockchain.

Contract pools will be secured by using decentralized wallets managed by the contract only, with no risk of the balance being used by an unauthorized party.

6 Pay with ADA Debit Card

The Debit Card is a feature that will bring the next level of adoption where users will be able pay their daily expenses using ADA.

It will be implemented using a regulated financial company in the market to be defined between options available in the market[13][14].

The conversion process between Fiat-Crypto will be transparent. The Merchant will receive the amount in the current local fiat, with automatic integration on the users Debit Card account, which will be separated from the main account. This separation gives the user control of the amount available to be spent, and improves the security over it.

Finally, this card will be issued by country basis where the provider offers coverage. Any user that requests this feature will be required to pass through a Know your Customer (KYC[15]) and Anti-Money Laundering (AML[16]) process defined by current legislation.

7 Buy/Sell ADA

The Buy and Sell ADA is a feature that will enable users to convert their fiat currency to ADA through Credit Card, Debit Card or Apple Pay.

It will be an integration via API using a partnership in the market to be defined. We aim to bring a better user experience when you're buying your ADA direct from the wallet. This is an important entry point for users that are not in the crypto world yet, increasing the adoption and also providing local currency conversion.

The security of the transaction will be guaranteed via encryption and the partner API will only have access to the user public address, the process related to the fiat and card payment will be done in their platform with security compliance checks done by our team.

8 Token Swap

The Token Swap is a feature based on the well known *Uniswap Protocol*[17], that enables B58 Finance to be a decentralized exchange for arbitrary token pairs.

Our work consists in the implementation of it using the translated version of the protocol for Cardano, with the Plutus Contracts Uniswap[18]. The technical modules definition can be seen as follow:

- **On-Chain:** Smart contract with validation logic that will evaluate the trading pairs, as well as communication with the liquidity pool to make sure that the pairs are from the right pool.
- **Off-Chain:** Here it's the Plutus Application Backend that provides the API endpoint and also the client interaction features. Which will also communicate with the liquidity pool.
- **Pools:** Liquidity Pools that define the rules of the swap and pairs available to be traded on each, as well as functions that are needed by both on-chain and off-chain code.

Finally, this is a high level definition of the work to be done where we're going to do a deep dive in on topics like incentives, yield rate, and other aspects that are relevant to this feature.

9 Conclusion

Our aim with this whitepaper is to provide an initial thought about features and our opinion about how a Next-Generation wallet might be, by providing a seamless user experience with Decentralized Finance features, that will enable users to use their accounts from where they need without the complexity of today's wallets.

On the technical side we've discussed algorithms and protocols that will be implemented in our product, bringing new capabilities to our users.

One of the most important outcomes of this is to increase the adoption of Cardano Blockchain, supporting the same vision of the future and giving back to the community that has been a firm believer of the project.

Furthermore, our decision is to bring a whole set of features to our platform, beginning from the core wallet, bringing the same experience that users have with Traditional Finance, which has its merits in the technological development when it comes to user experience, all while pushing the boundaries of what is possible by taking advantage of one of the most evolved blockchain platforms available today.

Next, we will be implementing features to support African users with their needs and applying the right technological tool to it. We know the challenge that we're embracing and ultimately, we aim to help everyone through their journey towards the financial identity which most don't have today.

Finally, our platform will provide the ability of users of B58 Finance to be their own bank without a need for a 3rd party involved in most of our services, which will enhance the peer-to-peer interaction and financial freedom in Cardano Blockchain.

References

1. Decentralized Finance. In: Wikipedia: 2021. https://en.wikipedia.org/wiki/Decentralized_finance
2. Discover Cardano. In: Cardano. https://cardano.org/discover-cardano
3. Decentralized Application. In: Wikipedia: 2021. https://en.wikipedia.org/wiki/Decentralized_application
4. Understanding Unspent Transaction Outputs in Cardano. In: Emurgo: 2019. https://emurgo.io/ja/blog/understanding-unspent-transaction-outputs-in-cardano
5. PolinaVinogradova, Andre Knispel. In: IOHK Research: 2020. https://hydra.iohk.io/build/5949624/download/1/shelley-ma.pdf

6. Driving Adoption and Purpose. In: Mission Driven Pools. https://missiondrivenpools.org
7. Funding and Financial Overview. In: World WildLife - WWF: Updated 2020. https://www.worldwildlife.org/about/financials
8. West Africa Decentralized Alliance: DeFi and Microlending for Africa. In: Project Catalyst Fund 6: 2021. https://cardano.ideascale.com/a/dtd/340138-48088
9. The journey of a Kiva loan. In: Kiva. https://www.kiva.org/about/how
10. Ergo Foundation, EMURGO, and IOG: The AgeUSD Stablecoin Protocol. In: GitHub: Updated 2021. https://github.com/Emurgo/age-usd
11. Robert Leshner, Geoffrey Hayes: The Money Market Protocol. In: Compound: 2019. https://compound.finance/documents/Compound.Whitepaper.pdf
12. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. In: Maker Protocol: Published 2020. https://makerdao.com/en/whitepaper
13. Global Cryptocurrency Debit Card Issuer. In: Swipe: 2021. https://swipe.io/
14. The fiat/crypto infrastructure for the entire world. In: Simplex: 2021. https://www.simplex.com
15. Know your customer. In: Wikipedia: 2021. https://en.wikipedia.org/wiki/Know_your_customer
16. Money laundering. In: Wikipedia: 2021. https://en.wikipedia.org/wiki/Money_laundering
17. Hayden Adams, Noah Zinsmeister, Dan Robinson: Uniswap v2 Core. In: Uniswap: 2020. https://uniswap.org/whitepaper.pdf
18. Plutus Contracts Uniswap. In: Plutus IOHK Dev: 2021. https://alpha.plutus.iohkdev.io/doc/haddock/plutus-use-cases/html/Plutus-Contracts-Uniswap.html
19. Philipp Kant, Lars Brunjes, Duncan Coutts. In: IOHK Research: 2019. https://hydra.iohk.io/build/790053/download/1/delegation_design_spec.pdf
20. A better way to handle your money. In: Revolut: 2021. https://www.revolut.com/en-IE
21. N26 The Mobile Bank. In: N26: 2021. https://n26.com/en-eu
22. Atala PRISM a decentralized identity solution. In: Atala PRISM: 2021. https://atalaprism.io/app