Modular Crypto Wallet Platform

Contents

Introduction

top

First I introduce the wallet proposal, outline the main ideas, functions and drivers in developing the Modular Crypto Wallet Platform.

Then I discus barriers to web3 applications and their adoption, and outline how the proposed wallet platform will solve some of these barriers.

The "3 Phase Development Plan" section outlines the 3 phase development plan, and tries to justify the approach we have decided to take. The main drivers in these decisions is to fist create a usable product in in the first development phase, this basic functional product will be able to be marketed and used as it will full fill the international remittance payment market. The second stage will develop the services and functionality used to deliver the wallet platform. The third phase will enhance the platform services with economic incentives to provide services and development of application available within the wallet platform.

"Development Timeline Gantt Chart" shows the individual development tasks and their initial time requirements as we understand them today. This chart gives an idea of the delivery times and how each developed functionality and services then flows into the next functional development task.

The "Technology and Development Approach" gives a high level overview of the technologies and approach we will be taking while developing the platform. These technologies may well be added to as we progress through the development phases and we understand better the issues that may arise in the development phases.

The Conclusion summaries the main points of the document, and tries to justify the decisions that have been made.

The Proposal

top

The Crypto Wallet Platform is an ecosystem that is made up of several functional parts and protocols that will allow users to manage and interact with their crypto assets, through a web interface or a dedicated smart phone application in a user friendly way. Both the web interface and the app will use a shared code base and api to the wallet platform functionality.

Users of the platform will be able to access multiple preconfigured blockchains in a user friendly way. The package module system within the wallet platform will allow the users to install and manage pre built packages that will allow users to access community contributed content based services, these being crypto services for payments, investment, and per to peer communications within the wallet platform.

All the services and package will be provided by developers and service providers, they will preconfigure these using standard methods, and this will allow them to offer their services and package application through the wallet platform. For providing these services and applications the contributors will earn rewards.

Justification for having service providers and application developers contributions;

https://www.zerohedge.com/crypto/whats-ailing-spotify - network commitment why??? a solution maybe

Need to build up useful functions (p2p coms, content access and distribution, smart contract interface, crypto chain data access, crypto investment access) to make sure users have attachment to the wallet as there are many options out there.

Need to attract service providers, so as to allow wallet access to decentralised services and to incentivise the service providers with rewards to provide these services and to help create a dedicated user base with an interest in the ecosystem growing and thriving.

Need to attract developers, to create and them to get rewards for their work through the wallet platform. Again helping to build a active user base that has an interest in the wallet platform growing and creating revenue for their work and services.

What should be focus of development?

- Secure Payments
- Package Management
- Web Services
- P2P communications
- Key Security
- Crypto Management
  Crypto Investments

The basic function of the wallet is to do the following

- Generate and Manage Private Keys
- Hold Crypto Assets
- Secure Crypto Payments
- Peer to Peer Networking
- Decentralised Web Services
- Module Functionality for the Creation, Deployment, and Management of wallet modules

Basic Wallet functionality ;

Key management, security and settings

Wallet application package management

- Key management, security and settings
- create
- import
- manage
- security (recover, backup, share, security tools)

Wallet application package management

- create a new package (admin function)
- manage a package (admin function)
- install
- remove
- manage

Crypto asset management

- stake
- mine
- funds
- manage

Smart Contract abi Interface

- import smart contracts
- manage smart contracts
- smart contracts usage logs

Web Service

- consume service
- publish service
- serverless application deployment
- serverless api
- serverless application scripting toolkit

Modular Crypto Wallet Service Stack

keys
networks
payments and transactions
services
contract abi interface
P2P networking

Lowering Barriers to Web3 Applications

top

Lowering barriers to adoption of web3 applications and their associated benefits for users and contributors is key to this proposed work. Web3 technologies have many benefits over the traditional web2 applications, these include enhancing privacy, usability, and the movement away from centralised proprietary software provision that benefits the third party company or owner of the software and towards a world or security, privacy, system transparency, and immutability. Where a central organisation can not change or censor some functionality that may give them finical benefit now or in the future, but possibly not the usability and open access to the services. In the web2 world the biggest example of this is where online ads have become the default means of a company to monetise their software, where as in the web3 world the users pays for the services used direct to the company providing, the rewards provided are pre defined and clear before any service is used or provided. These rewards are set as part of the protocol that the provider and user use to provide the service.

Currently web3 applications and wallets are focused on the more technical user just now, you need a level of technical knowledge to leverage these opportunities currently so that you understand the risk and potential benefit of the technology used. You do not need to be a computer scientist or engineer, but you do need to understand the key ideas and technologies so that you interact and benefit from them now.

An example of this is that many people use meta mask which is a good useful product to manage your private keys and interactions with a given blockchain, but the target audience has to understand the setup and configuration of this before they

even get into the opportunities that this tool gives them access to. Application developers have also leveraged wallet technology like meta mask, and provide interfaces that allow you interact withe their ecosystem functionality using a third party wallet. I think this has benefits and drawbacks. The benefits being that developers can create interfaces to their web3 functionality without having to worry about the key management side of the development equation. This as I see it is barrier to adoption by non technical users as users will have to invest the time and effort to understand and then leverage these technologies to use the web3 resources. There is not much in the way of support for the users to be helped along the way and believe this is slowing adoption.

The wallet platform aims to address these short comings by leveraging simple basic techniques to generate, secure, manage your keys, and make secure private payments. Adding to this a secure private peer to peer network with a cloud based services architecture, smart contract abi interface for importing already deployed smart contracts on any evm compatible blockchains, and a modular package system that can be used to script and bring together the feature and services to create user interfaces in a simple and intuitive way. This usage can then create contributions back into platform to fund the development and provision of the platform services and application in a structure and transparent way.

There has been some development focusing on enabling the casual user to access and gain the benefits of web3 technologies. However this should improved over the coming years as the technologies and tooling improves. Currently within the web2 application even if web based of smart phone app based, you are able to do most things is a user friendly easy manner. Wether that is payments, communication, and or access to shared compute resources. Not to mention many other use cases that are currently available in the web2 world, such as e-commerce, ticketing, events, delivery, sharing and earning though investments with you saved or spare assets. These assets could be crypto currency that could be deployed into a system that would earn a passive income, or from a spare computer and network resources that you may have available that could earn you rewards for the leasing of the usage of these resources.

The wallet platform aim will be to enable all users to access a rich ecosystem web3 services and functionality, through a platform that helps mitigate key management risks, provides tools to make mitigating risks and errors easier, and that can make the users experience within the web3 application space more simple in general.

---

3 Phase Development Plan

top

The Modular Crypto Wallet Platform will consist of an ecosystem of interfaces, services, nodes, and protocols. These together will allow the delivery of a decentralised modular crypto currency wallet platform. I have decided to approach the development in 3 phases, this will allow the initial development be focused on a know growing market, and then the following phases to build upon this at each stage. Extending the function to a potential new user base at each stage.

The initial target use case will be the international remittance payment market. This has been chosen as it is a proven and growing market that the wallet platform will be aimed at and marketed to from the start of the development process. The idea being that this will attract users of this target market. The first phase of development will focus on the implementation and development of the secure private transfers on the ethereum and polygon test and main networks. This work will form the foundation on to which all the other services offered through the wallet platform will sit upon. This first phase of development will aim to be delivered within a 3 months timescale and will make up the initial release.

The second and third development phases will aim to expand the use cases and user base that the wallet platform will target.

Firstly in phase 2 to the general use crypto user base will be targeted by providing further key management services, communication and collaboration tools and function through the peer to peer networking and content sharing services. We will also implement and introduce crypto assets management and investment services and functionality. All the services will be available and usable through the wallet platform application package system. The package system will allow developers to contribute scripted and configurable application functionality, that other users on the wallet platform will be able to activate, use, and interact with for a reward developer or not, this will depend on how the developer has configured the wallet platform packaged application to earn rewards. Some maybe free where the developer pays any fees for using the services, or it maybe a services that the developer actually gets a cut of the services fees and charges that the use of the application may incur.

For the final phase of development the focus will be on extending the use case to developers and service providers. In order to make the platform a truly decentralised platform and operating environment. Wallet users will be able to access and interact with the applications created, and the developers will be rewarded economically or by some other means depending on what the developers motivations where in creating the applications and publishing them to the wallet platform application store. The service providers will be able to earn rewards for providing remote compute and data services to the wallet platform, so as to enable the decentralised delivery of the wallet platform services and the applications that are published on the platform. The peer to peer network infrastructure underlying communications within the wallet platform will also be developed during this final phase of development. In the final phase of development there will also be a need to define the core development foundation and how this organisation is managed, and funded by the network activity and development improvement process.

Timescales

Timescales for the phase 1 are 3 months, phase 2 are 6 months and phase 3 are 6 months. However if after phase 1 development has been released and there is the motivation and funding to speed up the delivery times, the development team could be scaled up so as to speed up the delivery of phase 2 or 3 functions and services and to meet any demand that may have been created.

Features

The main features of the wallet platform will be, private key management, storage and recovery, secure private payments, a package based application repository, smart contract ABI interface, peer to peer network for communication within the wallet platform, and a decentralised web service functionality to allow the delivery and sharing of data in a truly decentralised manner. These features will combine to create a platform that will be easy to use for non technical users, private, secure, and have the ability to rewards developers and service providers with a rewards stream for the use of their services or work.

The wallet platform will allow crypto currency holders to make secure private transfers, manage their private keys, and access the wallet applications that will be contributed to it's app store by it's developer user base. These contributed applications will provide functionality that will allow the wallet users to interact with already published smart contracts on a variety of evm based blockchains, access crypto staking, mining, and investment applications, use the built in peer to peer network for communication, interaction, payments and commerce with others users or organisations that are using or have publish applications on the wallet platform.

The wallet platform will be targeted at everyday users providing a simple and usable experience within the web3 space. Where users need little to no understanding of the underlying function or the technology. The idea being that access to package functionality will be simple and accessible, provide access to secure private payments, and will help drive the adoption of crypto currency use in a private and commercial way, as it will provide these services in a similar manner to web3 commerce and content based system and platforms.

Peer to Peer Reward Structure and Wallet Foundation Features

The other main feature of the wallet platform is the decentralised nature of the system, and how it will allow users to contribute and earn rewards for their contribution to running and providing functionality on the platform. These rewards should have the affect of building a community that has a economic interest in the use and expansion of the platform, it's services, applications and function.

Much like the http protocol, databases, and scripting languages enabled the delivery on commercial and content services across the web2 world over 20 years ago. I envisage a platform where commercial enterprises could create functionality to sell, communicate, and interact with their client base in a simple and use friendly way. I believe this approach will allow the stream adoption of crypto currencies as a means of commerce, and communication.

Development Phases functionality and justification

The phased development approach will allow the development of the wallet platform functionality to optimise the development resources, and marketing potential as the development phases progress.

The phase 1 cycle will target secure private payments for the international remittance market sector of users. This was chosen as it is a growing and proven use case for international money transfers.

The phase 2 cycle will then target development of the core wallet platform services and how they interact to create the full core services and function of the platform.

Phase 3 will focus on the development of the decentralised elements and associated token, reward structures, protocols and interfaces to deliver these functions.

Development Plan

To deliver the platform we think a 3 phase approach is most appropriate. This allows the key function or the platform to be implemented in a way that focus first om the foundation of the platform, secure private payments. Then the wallet platform core services and their interactions and interfaces, and finally the decentralised reward elements and protocols to build commitment and a dedicated technical user base that will have a long term benefit in contributing the success of the platform moving forward.

Phase 1 Development Tasks

Key management - backup - recovery - import - export

Crypto Currency Payments and Transaction - send ethereum main network payments and transactions - send ethereum test network payments and transactions - send polygon main network payments and transactions - send polygon test network payments and transactions - send other layer2 solution network payments and transactions (optimisum, zkEVM)

Secure Private Payments - send private secure transaction ethereum main network - send private secure transaction ethereum test network - send private secure transaction polygon main network - send private secure transaction polygon test network - send private secure transaction layer2 rollup network (optimisum, zkEVM)

Wallet Interface - create a wallet interface to access all the features implemented in the phase 1 development cycle

Create the electron smart phone application from code base

Testing and Analysis of development phase 1

Phase 2 Development Tasks

Secure Payments service

Package Management service

Peer to peer wallet platform web service

Peer to peer communication service

Key Security and Management Service

Crypto Asset Management Service

Crypto Asset Investments Service

Smart Contract ABI User Interface Service

User Interfaces to access all the services developed in this phase 2 development cycle, these include; - Wallet Interface - App store Interface with basic set of application developed by core development team

Integrate Core Services

Testing and Analysis of development phase 2

Phase 3 Development Tasks

Define Reward Structure and Token Economics for the Platform - Define Developer Reward Protocol - Define Service Reward Protocol - Define Wallet Foundation for Managing Future Development and Structures - Define Wallet Foundation Funding Structure

Service Provider Reward protocol

Service Provider User Interface

Integrate the Core Services with the Service Protocol

Developer Reward Protocol

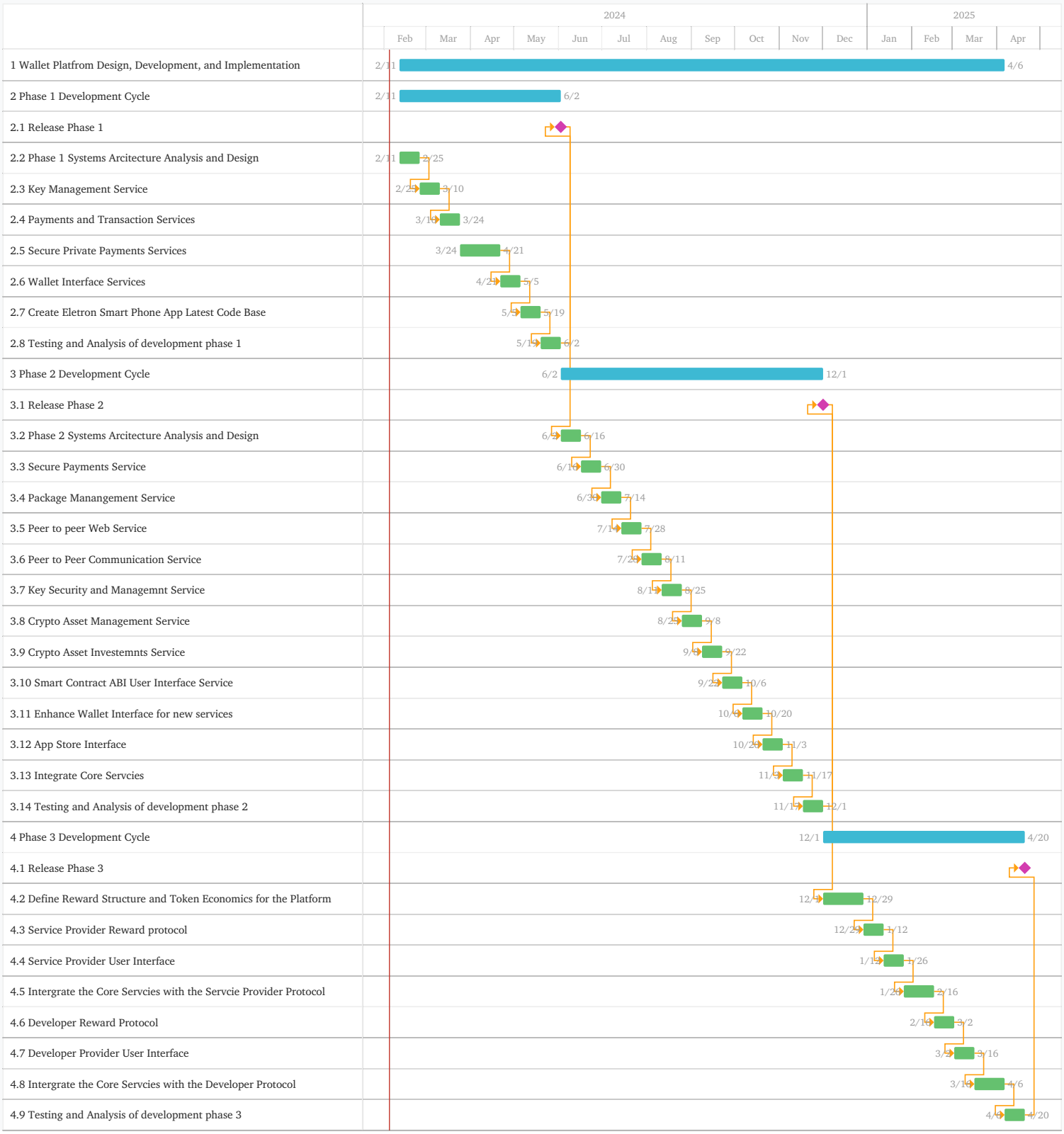
Developer Provider User Interface

Integrate the Core Services with the Developer Protocol

Development Timeline Gantt Chart

top

This shows the tasked above put onto the project timeline



Technology and Development Approach

top

This section give an overview of technologies to be used to build the functionality and platform and to justify how/why they will be used. The technologies and approach used are a work in progress, and will more than likely be updated as we progress through the development process, and as we learn from the implementation the services and functionality to date.

Technologies used to deliver the functional services and Wallet Platform

- nodejs as the primary development language
- electron to allow the creation of an electron app that can be targeted to mobile phone platform
- libp2p for the peer to peer networking and communications functionality
- ipfs as the initial means of sharing content between connected wallets
- ethers to interacted with the evm compliant blockchains
- solidity to create any smart contract functionality required to create the incentive and rewards structures and protocols, and network token.
- there will also be a requirement for other small nodejs modules to create the platform and these will be further defined by the overall development team and/or the individual developer work on that functionality at the time.

Development environment and approach

- github used for source code repository, version control, work flow actions, and continuous integration with built in testing and pull request integration into primary development and release code bases.
- hardhat for solidity development, testing, and deployment of solidity smart contract functionality.
- jest for unit testing and confirmation of correctness of code contributed.
- code reviews and amendment before pull requests to keep code base consistent, clean, readable.
- technical analysis of key functional flows by development team, so as to understand where risks may be, and how these best mitigated in the development process.
- Continuous Integration and Continuous Delivery/Deployment using github actions, which aims to streamline and accelerate the software development life cycle. Using devops and agile development techniques to help control and simplify the code base and interactions between the development team.

Conclusion

top

The implementation of The Modular Crypto Wallet Platform will not be a small undertaking. It will need to fully analysed and planned before the development of any services or decentralised features are implemented and integrated within the platform.

I believe the 3 phase development approach I have proposed is flexible and will allow the development process to adapt and scale as we progress through the development phases and allow any learning from this process to feedback into future decisions, focus, and implement features within the development tasks and technologies used.

The first development phase will target a proven market that is growing fast. I think by targeting this market at this stage it

allows us to create a strong foundation for the platform, while also giving a good focus for the initial development work and marketing to focus on. This I believe has the potential to create a initial user base on to which we can grow the more advanced user base, as the more advanced features and services become available during future development phases.

The second phase will then focus on creating the core services and defining how these services interact and function together. There is a level of complexity here, but this is minimised by splitting the decentralised features from this development phase so that we can focus the development of the wallet platform services and how the service interact make sure that usability is optimised and is the focus during this phase.

The third and final stage will then enhance the platform to create a truly decentralised ecosystem that rewords contributors to it. It will also define and create the Wallet Platform Foundation that will control and manage future development after the third phase of the development is completed.

I see this final development phase as the key stage of the platform development in creating a long term diverse user base. Thus making the wallet platform a more long term offering with the potential for creating a dedicated user base with a commitment to the platform, it's further development, and ecosystem management and adoption, as these users (service providers and developers) will have an vested interest in it's future and in it's further development and adoption.

---

top