AUC Block-A-Thon 29-6-2022
Final Report

Assessment

This grant was set to bring awareness to blockchain in general and Casper in particular.
The future of any technology depends on the community supporting it between the developers and the users. Universities are one of the best areas to start community engagement. If we are able of sparking the students' interest in blockchain technology early on and help guide them through it, we would be able of opening the doors to generations of talent that could accelerate blockchain adoption.

This pilot grant aims at conducting a university-level conference associated with a mini codathon for hands-on development. Targeting an audience of 50-100 government, faculty, industry, and students.
The first event was to be held at the American University in Cairo (AUC).
Two events were held, the first at the AUC as shown in previous reports, and another in Alexandria as shown in the pictures.

Wallet Generation
Roughly 80-100 wallets have been generated as a result of the blockathon. It is hard to track all of them, however, the registration for both events supports the numbers.

Projects

As presented in the previous reports 5-7 projects started on Casper, with varying degrees of completion.

Certificates

The following certificates were generated in collaboration with the AUC for VIP speakers and students.

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Judge Mohamed Marei

Thank you for

VIP Speaker

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

Blockathon Certificate

Ahmed Gamal

Thank you for

VIP Speaker

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Dr. Karim Seddik

Thank you for

VIP Speaker

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Medha Parlikar

Thank you for

VIP Speaker

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Caroline Mikhail

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Haneen Kotb

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO
Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Azza Shehata

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Karma Yosry

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO
Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Kenzy ElMessiry

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO
Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Khaled Bassiouny

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO
Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Mariam Taha

Thank you for

Organization & Support

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Kareem Kassab

Thank you for

RECYCLE Token Team

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Omar Osman

Thank you for

RECYCLE Token Team

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

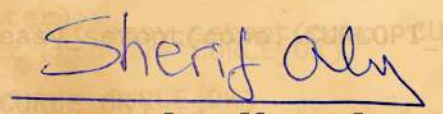
THE AMERICAN UNIVERSITY IN CAIRO

Blockathon Certificate

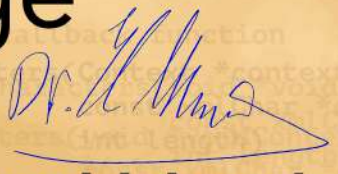
Zeina Basiouny

Thank you for

Language Exchange



Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo



Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Malak Elmessiry

Thank you for

Language Exchange

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO
Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

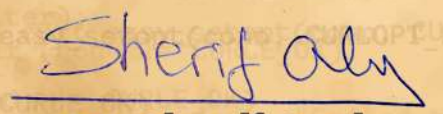
THE AMERICAN UNIVERSITY IN CAIRO

Blockathon Certificate

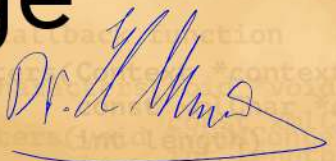
Ziad Basiouny

Thank you for

Language Exchange



Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo



Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Mohamed Sharaf

Thank you for

Ardy Team

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Mohamed Yasser

Thank you for

Ardy Team

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

THE AMERICAN UNIVERSITY IN CAIRO

BLOCKATHON CERTIFICATE

Mohamed Fekry

Thank you for

Ardy Team

Dr. Sherif G. Aly
Professor and Chair
Department of Computer Science and Engineering
The American University in Cairo

Dr. Adel ElMessiry
President & Co-Founder
AlphaFin, Inc

DRAPER GOREN HOLM

DEV x DAO Decentralized Autonomous

Casper

ALPHA FIN

VerifiedImpactNFTs

NFT PUNK

Academic Progress

Due to the blockathon, about a dozen students have selected to study blockchain as their final project. Two groups have been assembled under the supervision of Dr. Mohamed Sedky and Dr. Adel ELMessiry. The groups selected to use Casper as the main chain of the projects to implement.

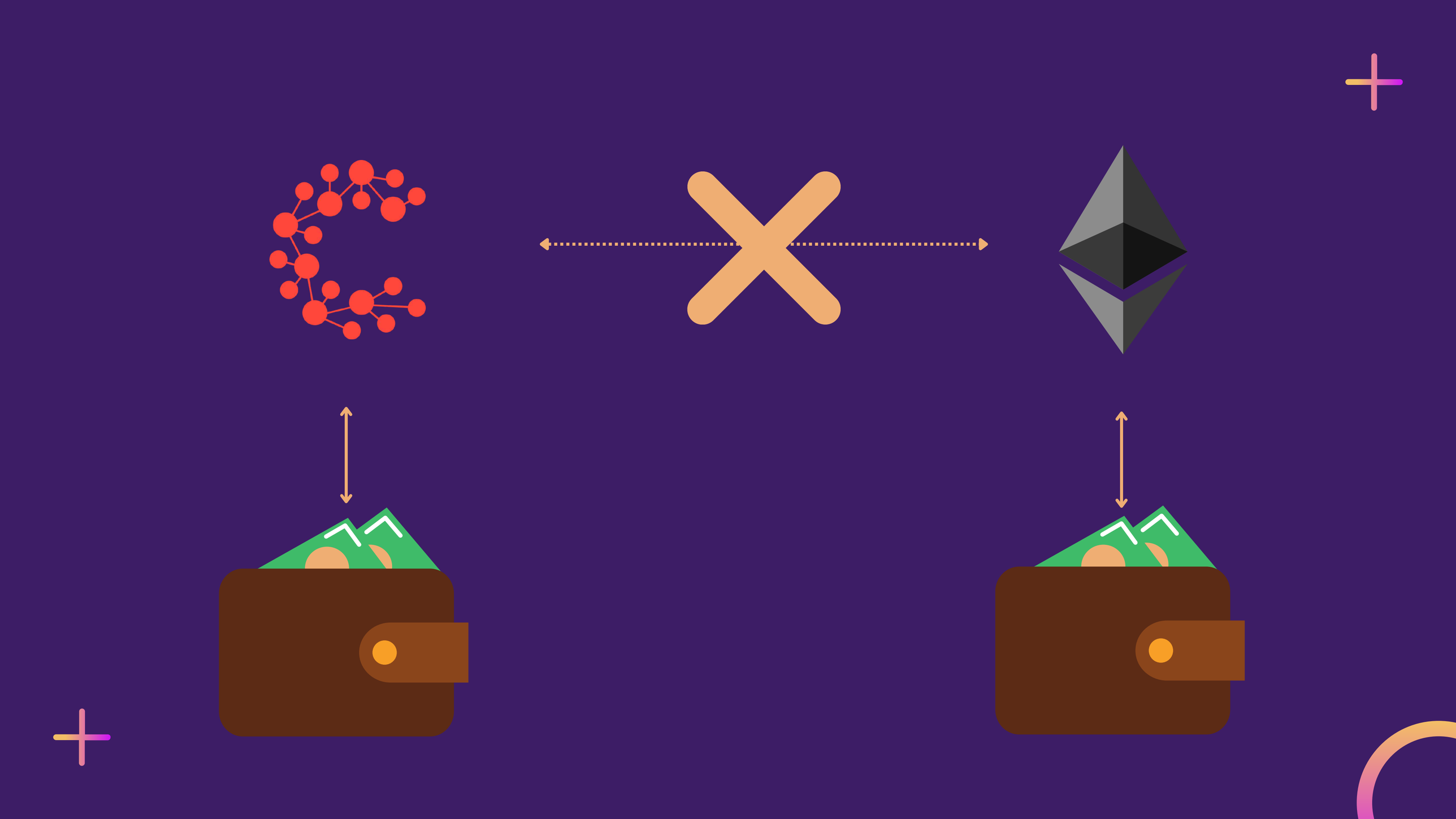
The projects are:
Dahab Wallet:
https://www.youtube.com/watch?v=vogU1MYm9eM&list=PLj_abWUvJ2F0qDp2TbGw6WmqrIiLETqNn&index=4

And
Land registry
https://www.youtube.com/watch?v=xs--kpYFzMo&list=PLj_abWUvJ2F0qDp2TbGw6WmqrIiLETqNn&index=8

PROGRESS
PRESENTATION I

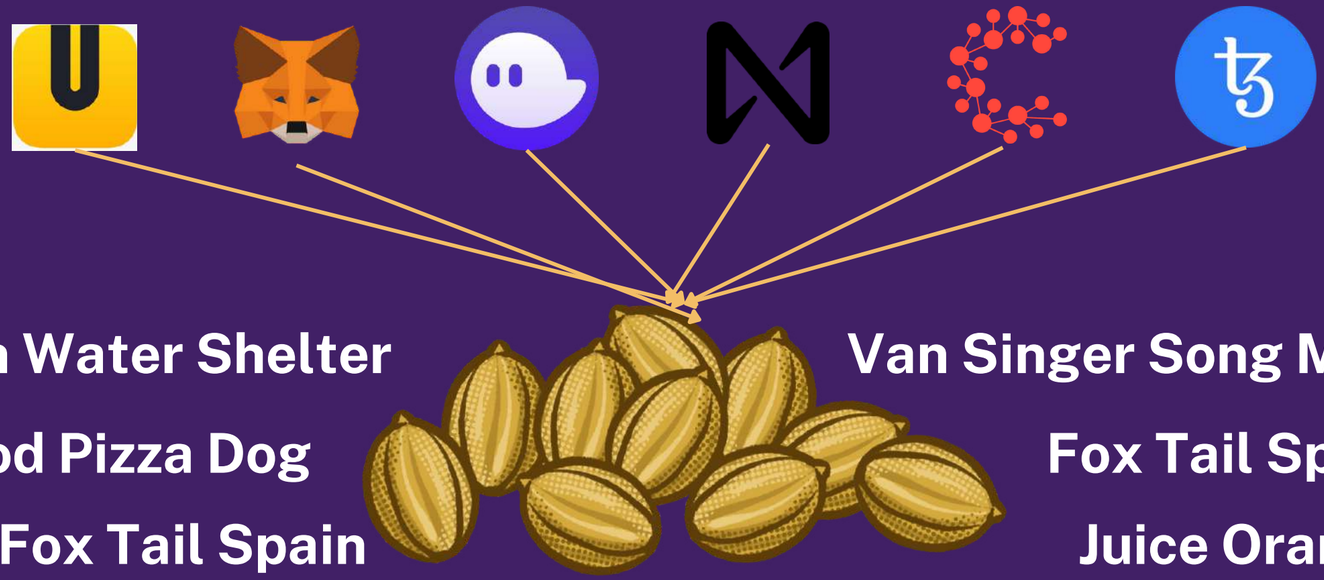
CROSS CHAIN WALLET

Major Problem



Problems

Convenience Gap



Dog Cat Train Water Shelter

Eat Sleep Food Pizza Dog

Shelter Date Fox Tail Spain

Van Singer Song Music Guitar

Fox Tail Spain Cairo ox

Juice Orange fruit word

Decentralization Gap

Exchanges

Custodial
Bridges

Legal Gap

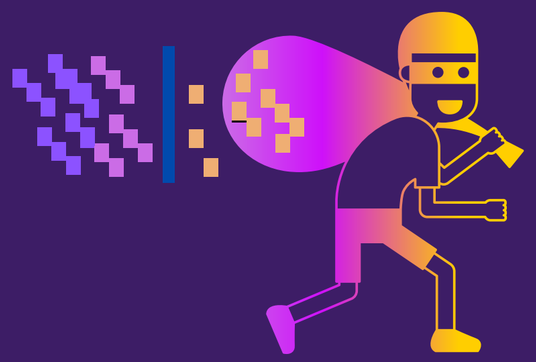
Implicit Ban

Absolute Ban

Language Gap

Some wallets Support Arabic
But no Multi-Chain wallets do

Security Gap



Date	Victimization Agreement	Type of attack	Cross-chain operation position
2021 July	Chainswap	Check for defects	After signing/cross-chain
2021 August	Poly Network	Hash collision/check defect	signature
2022 Jan	Qubit Bridge	Incorrect setup/check defect	Before cross-chain
2022 Jan	Multichain	Interface compatibility issues	Before cross-chain
2022 Feb	Meter Bridge	Inspection defects	Before cross-chain
2022 Feb	Wormhole	Interface verification problem	signature
2022 March	Li Finance	Inspection defects	Before cross-chain
2022 March	Ronin Network	Validator Control	signature

Literature Review

Lit Review :

Mnemonics

The Privacy/Convenience tradeoff

Ultimate Convenience

A wallet can be achieved by having a single private key and address that can be reused for everything.

This will create privacy issues as anyone can track and correlate all the transactions performed by that key.

Ultimate Privacy

The best scenario for ensuring privacy is using a new key for every transaction

This approach is very difficult to manage and affects the convenience of the wallet.

Best Scenario

Issues

The best wallet design is the one that can balance convenience and privacy in the best way

Deterministic vs Non-Deterministic Wallets

Non-Determenestic

The keys are not related to each other, and each key is independently generated from a random number.

key generation

Determenestic

All the keys are related to each other and all the keys are derived from a single master key ("seed")

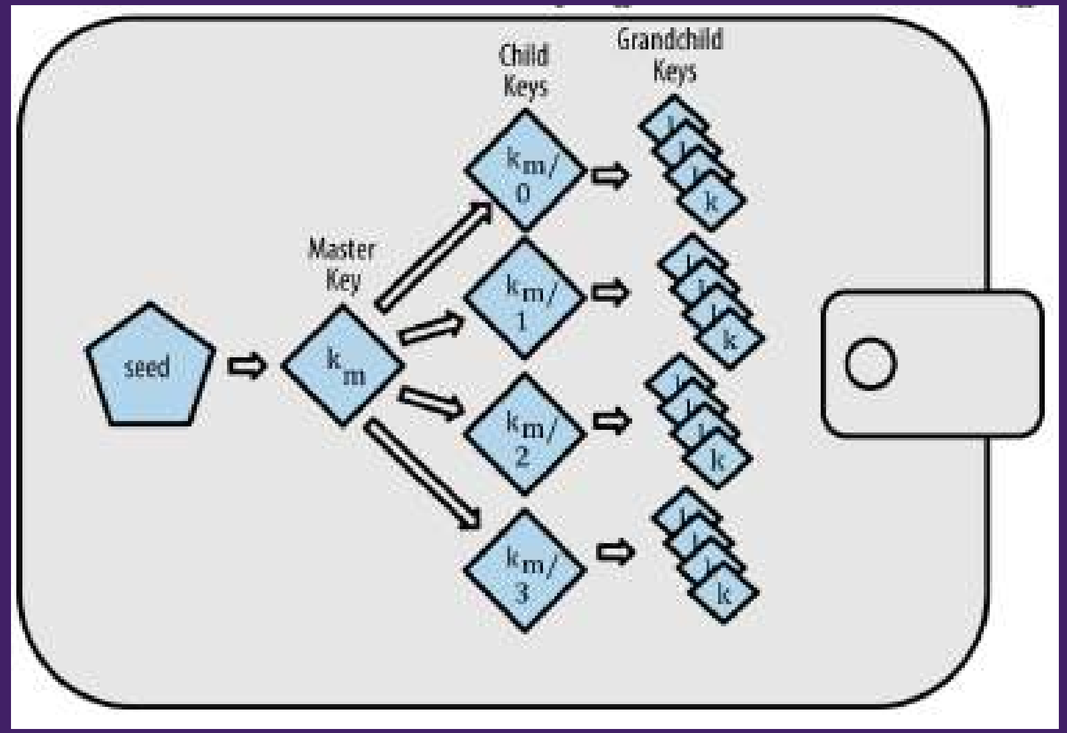
The most common derivation method is “Hierarchical Deterministic Wallets (BIP-32/BIP-44)”

Hierarchical Deterministic Wallets

In Deterministic (Seeded) Wallets, ***the seed is a randomly generated number combined with additional data, like an index number or “chain code” to derive any number of private keys.*** The seed is sufficient to recover all the derived keys, and to export or import the keys allowing for easy migration of all the keys between different wallet implementations

Hierarchical Deterministic Wallets

The hierarchical deterministic wallets contain ***keys derived in a tree structure***. The ***parent key*** in HD wallets ***can derive a sequence of child keys***, and each child key can derive a sequence of grand-child keys.



Advantages of HD wallets over simpler deterministic wallets

The tree structure

The first advantage is that the tree structure can be used to express additional organizational meaning.

Hidden private keys

The users can create a sequence of public keys without having access to the corresponding private keys

Advantages

Applications

One branch of subkeys can be used to receive incoming payments and another one can be used to receive change from outgoing payments.

Allows using the HD wallets on insecure servers or in a watch-only or receive-only capacity

Seeds and Mnemonic Codes (BIP-39)

The currently preferred method for ***encoding a private key*** for secure backup and retrieval is using ***a sequence of words in a specific order (“mnemonic”)*** that can uniquely recreate the private key. Shown below is an example for this methodology.

Hexadecimal seed for an HD wallet: FCCF1AB3329FD5DA3DA9577511F8F137

Mnemonics: wolf juice proud gown wool unfair wall cliff insect more detail hub

Wallet Best Practices

Common industry standards have emerged to make the wallets easy to use, flexible, secure, and broadly interoperable. ***These standards also allow wallets to derive keys for multiple different cryptocurrencies from a single mnemonic.***

These common standards include:

- Mnemonic code words, based on BIP-39
- HD wallets, based on BIP-32
- Multipurpose HD wallet structure, based on BIP-43
- Multi-currency and multi-account wallets, based on BIP-44

There are many examples that adopt these standards like:

Software wallets: Jaxx, MetaMask, MyCrypto, and MyEtherWallet.
Hardware wallets: Keepkey, Ledger, and Trezo.

Mnemonic Code Words (BIP-39)

Deterministic wallet applications that implement wallets with mnemonic words show the user a sequence of ***12 to 24 words when first creating a wallet.*** That mnemonic words can be used to recover and recreate all the keys in the same or any compatible wallet application. Most current mnemonic codes are defined in BIP-39.

BIP-39 can produce multi-currency wallets supporting Ethereum, whereas Electrum seeds cannot. **BIP-39 defined the process of creating mnemonic codes and seeds in nine steps.** The process is split into two parts: steps 1 through 6 are **“Generating mnemonic words”** and steps 7 through 9 are **“From mnemonic to seed”.**

Generating mnemonic words

The wallet starts with ***a source of entropy, then adds a checksum, and finally maps the entropy to a word list:***

1. Create a cryptographically random sequence S of 128 to 256 bits.
2. Create a checksum of S by taking the first length of S ÷ 32 bits of the SHA-256 hash of S.
3. Add the checksum to the end of the random sequence S.
4. Divide the sequence and checksum concatenation into sections of 11 bits.
5. Map each 11-bit value to a word from the predefined dictionary of 2,048 words.
6. Create the mnemonic code from the sequence of words, maintaining the order.

Generating mnemonic words

Figure 2: Generating entropy and encoding as mnemonic words

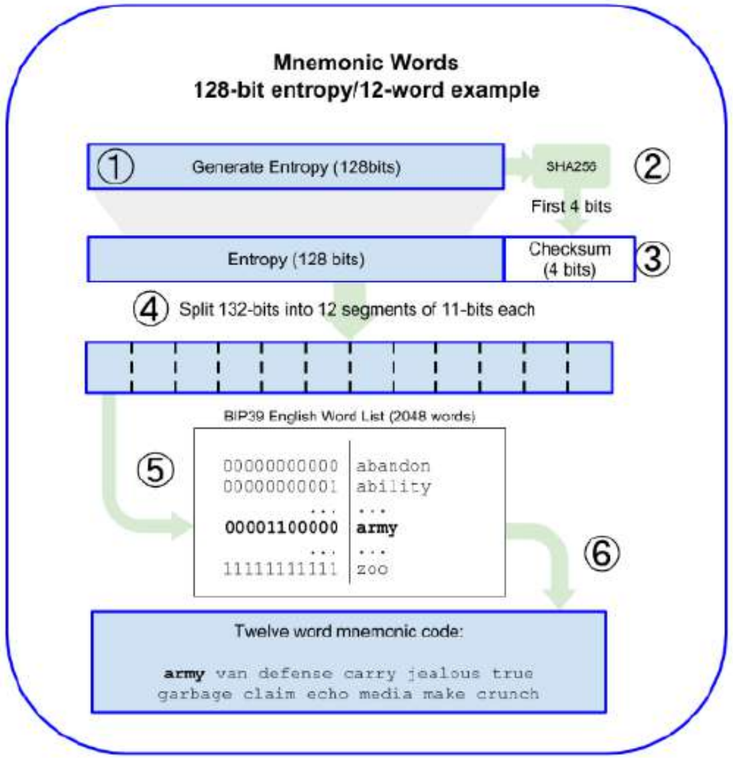
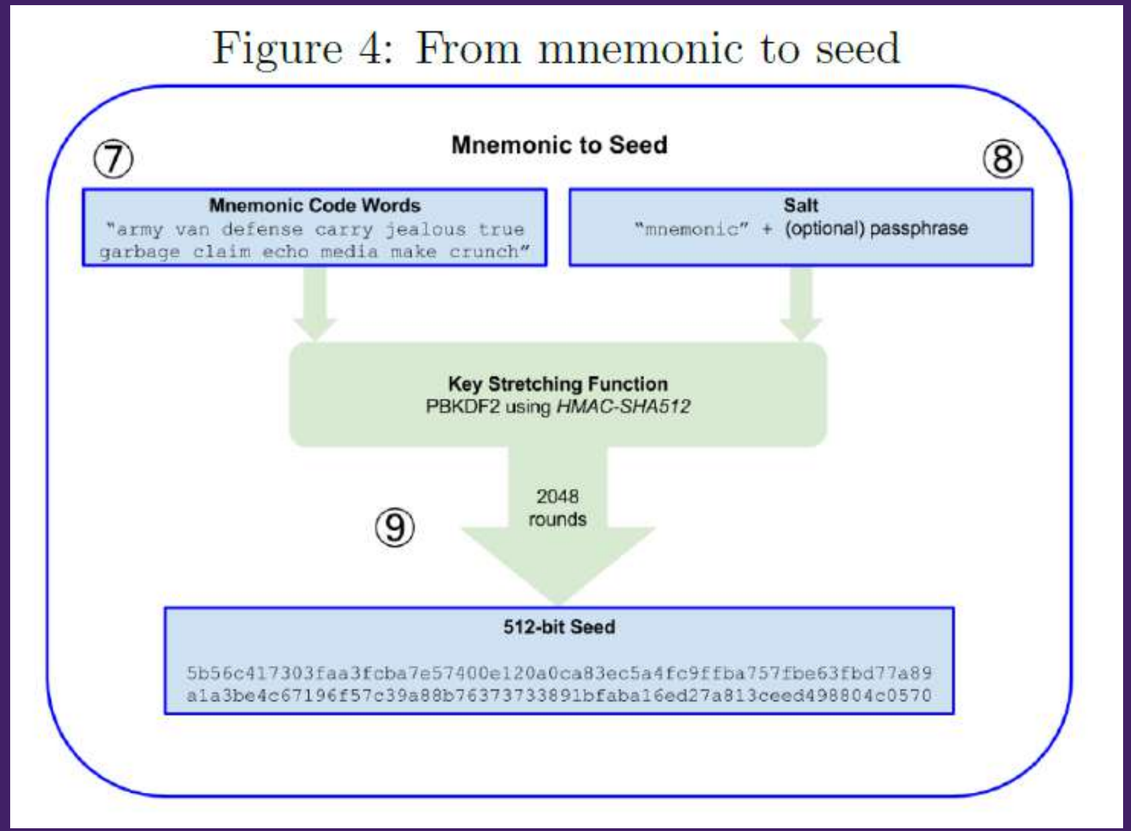


Figure 3: Mnemonic codes: entropy and word length

Entropy (bits)	Checksum (bits)	Entropy + checksum (bits)	Mnemonic length (words)
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

Process of converting mnemonic to seed

- The mnemonic words are ***128 to 256 bits length entropy that is used to derive a longer (512-bit) seed*** using a key-stretching function ***“PBKDF2”.***
- The seed is then used to build a deterministic wallet and derive the keys.
- PBKDF2 ***takes two parameters: the mnemonic and a salt,*** which makes it difficult to build a lookup table enabling a brute-force attack.
- Additional purpose of ***salt*** in the BIP-39 is ***introducing a passphrase that serves as an additional security factor*** protecting the seed.



Optional passphrase in (BIP-39)

Every passphrase in BIP-39 leads to some wallet, which unless previously used will be empty. The passphrase introduces important features.

Memorized password

This feature makes the mnemonic useless on its own which increases security.

Advantages

Plausible deniability

A chosen passphrase leads to a wallet with a small amount of funds, used to distract from the wallet that contains the majority of funds

Optional passphrase in (BIP-39)

No passphrase

With passphrase

Entropy input (128 bits)

0c1e24e5917779d297e14d45f14e1a1a

Mnemonic (12 words)

army van defense carry jealous true garbage claim echo media make crunch

Passphrase

(none)

Seed (512 bits)

5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

128-bit entropy mnemonic code, no passphrase, resulting seed

Entropy input (128 bits)

0c1e24e5917779d297e14d45f14e1a1a

Mnemonic (12 words)

army van defense carry jealous true garbage claim echo media make crunch

Passphrase

SuperDuperSecret

Seed (512 bits)

3b5df16df2157104cfdd22830162a5e170c0161653e3afe6c88defeefb0818c793dbb28ab3ab091897d0715861dc8a18358f80b79d49acf64142ae57037d1d54

128-bit entropy mnemonic code, with passphrase, resulting seed

Lit Review :

Wallet Types

Software vs Hardware Wallet

1. Software -> programs running on PC or smartphone
2. Hardware -> USB-like devices containing your funds
3. Our wallet will have a software model

Hot Storage Wallets

Pros	Cons
Very convenient	Always connected to the internet
	Security Issues
e	

Cold Storage Wallets

Pros	Cons
Secure	Not so convenient
e	

Desktop and Mobile Wallet

1. Example: Desktop -> Atomic; Mobile -> Coinomi
2. Cold Wallets - > runs on a PC or smartphone
3. Disadvantage: if the device is destroyed, your funds are gone

The Ideal Scenario

1. Combination of hot and cold wallets
2. Divide your money into two parts;
3. Major part -> Cold
4. Minor part -> Hot

Wallet Comparison

wallet/feature	Type	Custody	NFTs
liquality	**hot**	**non-custodial**	**yes**
wirex	**hot**	hybrid	**yes**
onto	**hot**	non-custodial	**yes**
zengo	**hot**	Key-less face scan stored on server	**no**

Lit Review :

Custody

Custodial vs Non-custodial

1. The private key is used to prove the possession of the tokens

NOT YOUR KEYS NOT YOUR COINS

2. The private key can have differnt storage locations

3. Wallets can be divided into cusotidal and non-custodial wallets

Custodial | **Non-Custodial**

e

Custodial Wallets

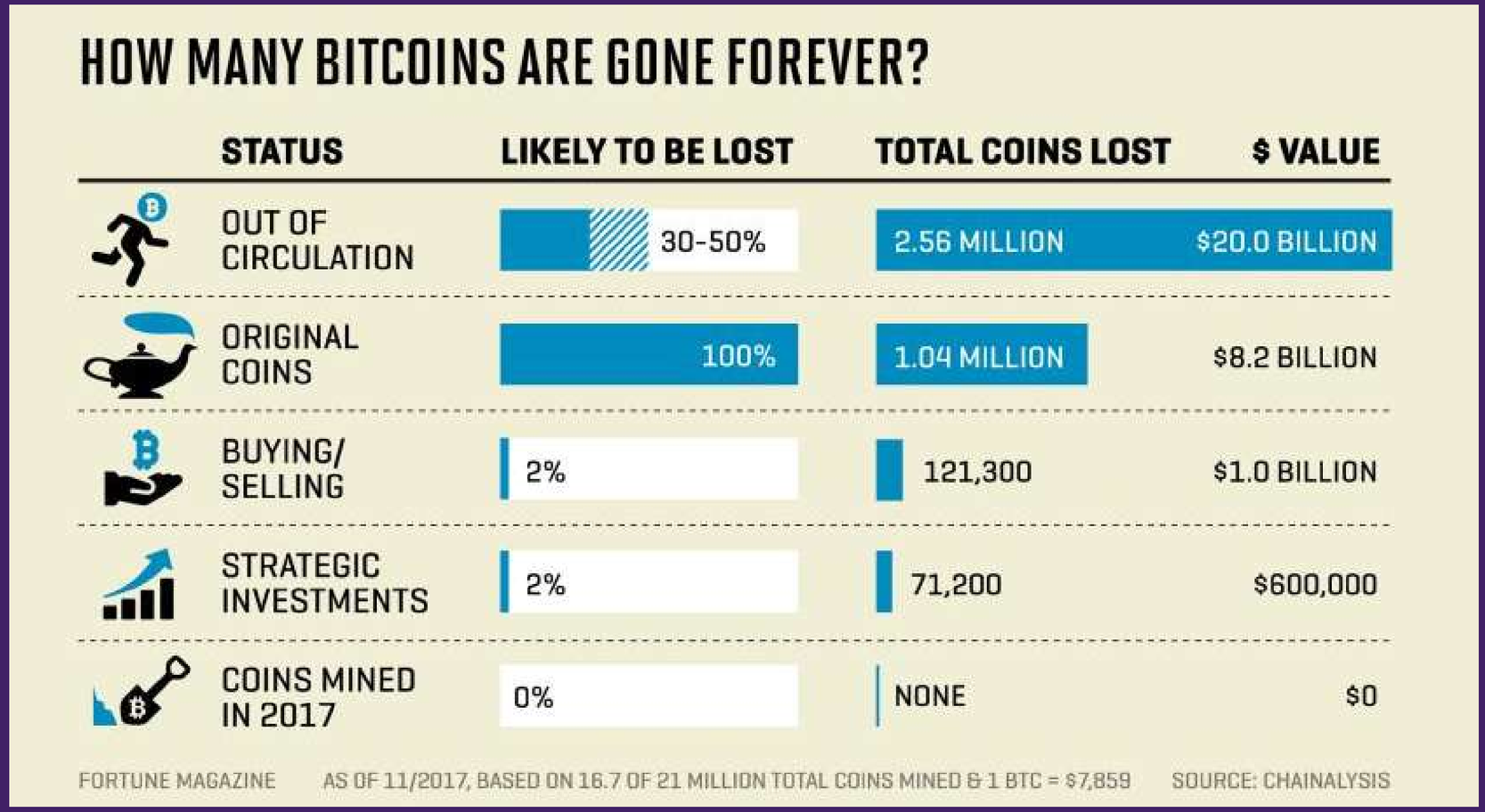
Pros	Cons
They do not require much responsibility	Less Secure
More convenient	
The password can be reset if forgotten	

Non-Custodial Wallets

Pros	Cons
More Secure	Losing the private key is losing the money
Eliminate the third party between the user and the assets	

Non-Custodial Challenges

According to a number of blockchain analytics firms, people have lost access to approximately 20% or **3.7-4 million** of all bitcoins That's roughly **$223 billion** as of **December 2021**



Non-Custodial Challenges

To get a solution for this problem without compromising the security, a number of wallets generate a seed phrase that is used to back up the private keys and re-generate them if lost

MNEMONIC

indoor dish desk flag debris potato excuse depart ticket judge file exit

Model Choice Jusitification

1.Our chosen model is to create a hybrid design that strikes a middle ground between the custodial and non-custodial models.

2. This design can fit the newbies as well as professionals at the same time.

3. As for the novice people, they tend to use custodial wallets to take off the headache of storing the private keys on their own.

4. On the other hand, experts in the field are willing to keep their private keys offline to guarantee more security.

Wallet Platform

1 The wallets can be run on different platforms as mobile, desktop,
web, and hardware devices.

2. It is intended for our product to be a web-based product that can be accessed through a browser extension for the ease of user experience.

3. That is why our storage model is chosen to be a hot storage.

4. This design choice will introduce other challenges related to security because being connected to the internet will make the product vulnerable to hacks and thefts

Additional Factors

1.Our wallet is intended to be a regulated custodian that is legalized by following a government’s blockchains policy and legislations.

2.Although introducing an additional asset to our wallet will bring extra security challenges, our wallet custody should support various assets (200+) and not be limited to a few of them.

3. Our custody should have insurance to compensate for any money loss in case any problem happens.

4. Our custody will be audited by well-known auditors to be a more credible product.

5. It is advised to use our own on-site infrastructure to have full control of it.

6. our custody can add additional features such as transfer assets on death to facilitate digital assets inheritance after the owner’s death

Progress :

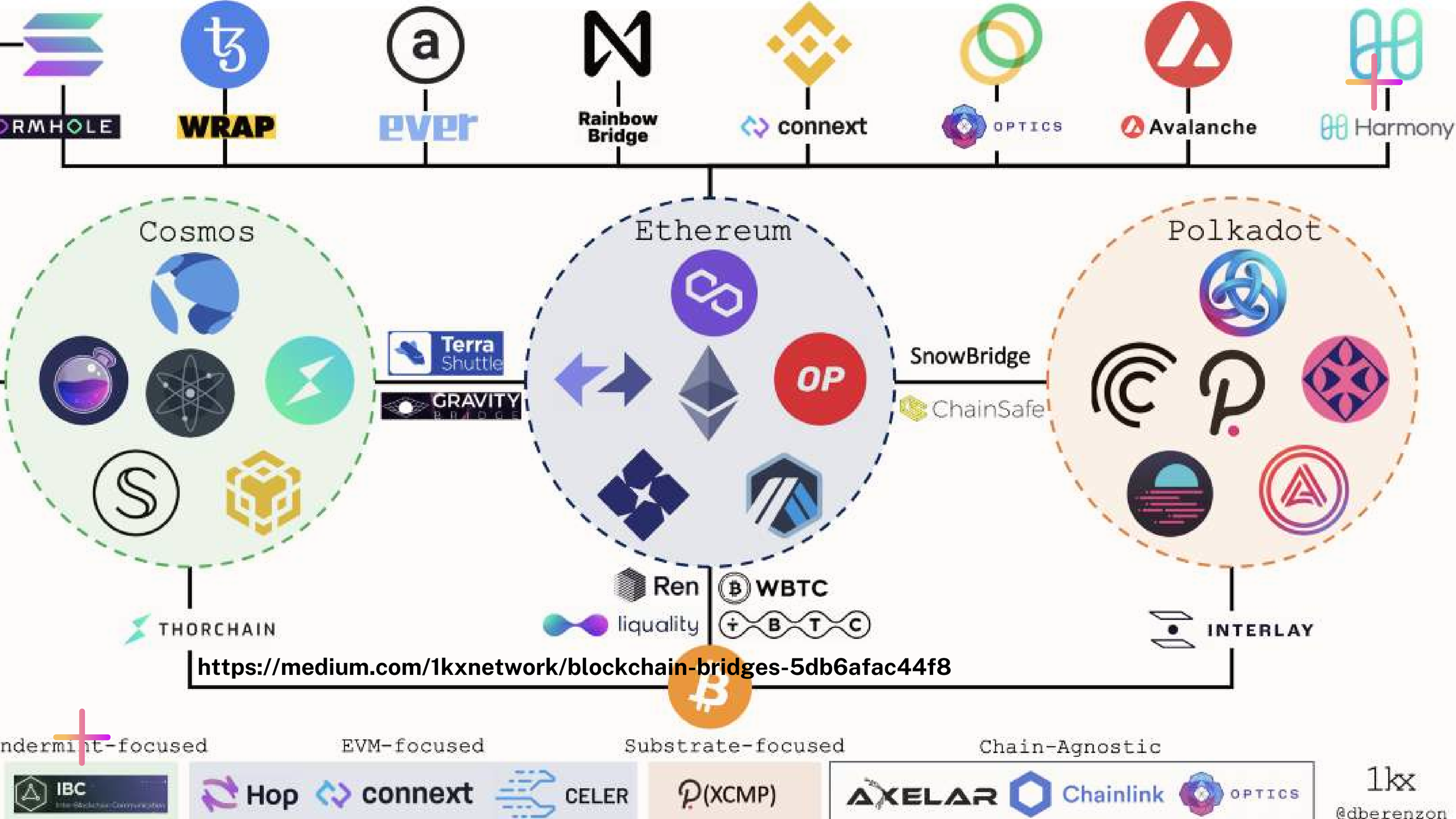
Bridges

What we reached from the literature review

A map of blockchains and bridges

Classification of bridges

Bridges Criteria


RMHOLE
WRAP
ever
Rainbow Bridge
connext
OPTICS
Avalanche
Harmony
Cosmos
Ethereum
Polkadot
Terra Shuttle
GRAVITY BRIDGE
SnowBridge
ChainSafe
OP
THORCHAIN
Ren
liquality
WBTC
BTC
INTERLAY
https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8
ndermint-focused
EVM-focused
Substrate-focused
Chain-Agnostic
IBC
Hop
connext
CELER
(XCMP)
AXELAR
Chainlink
OPTICS
1kx
@dberenzon

Bridging Trillema

Trustlessnes

Extensibility

Generalizability

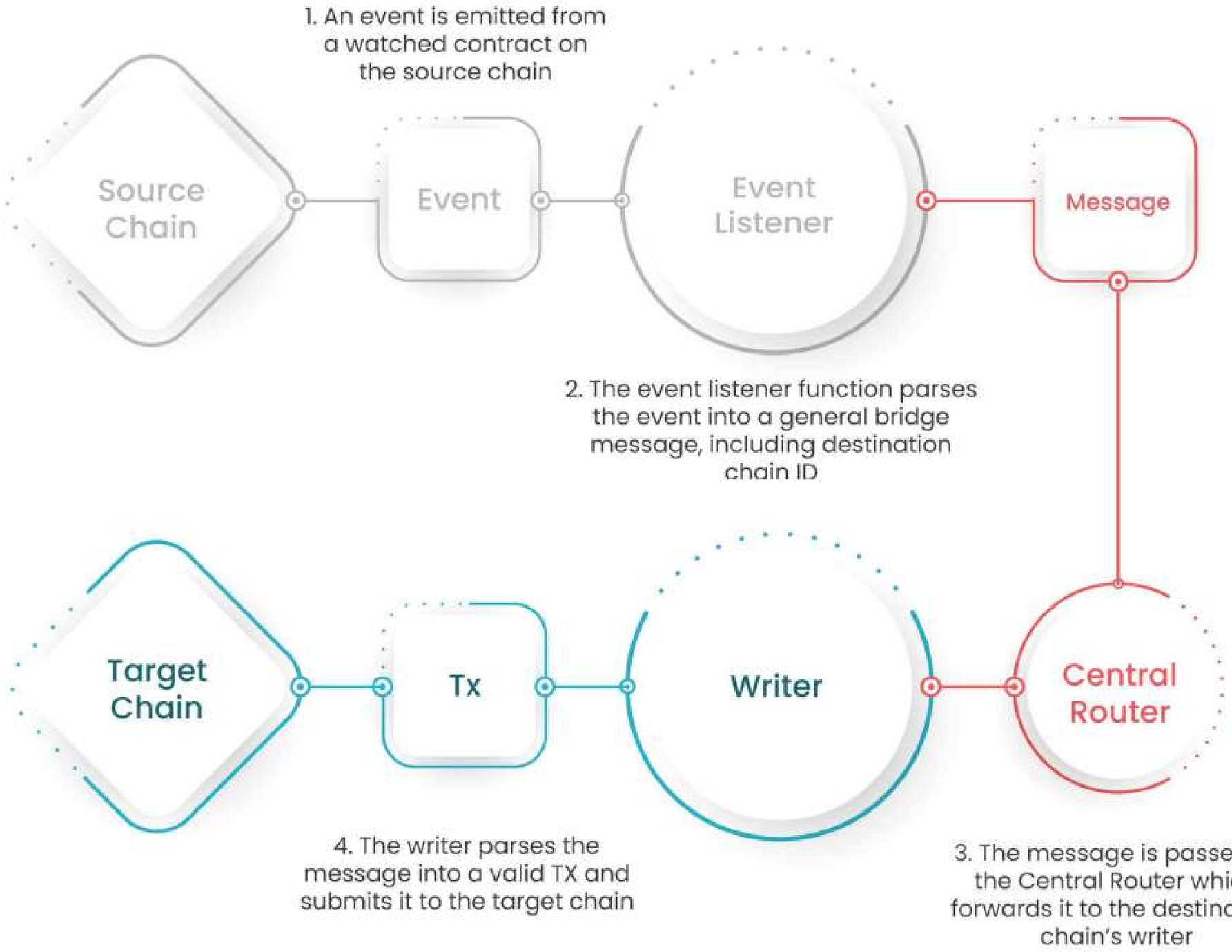
Classification

Liquidity Networks

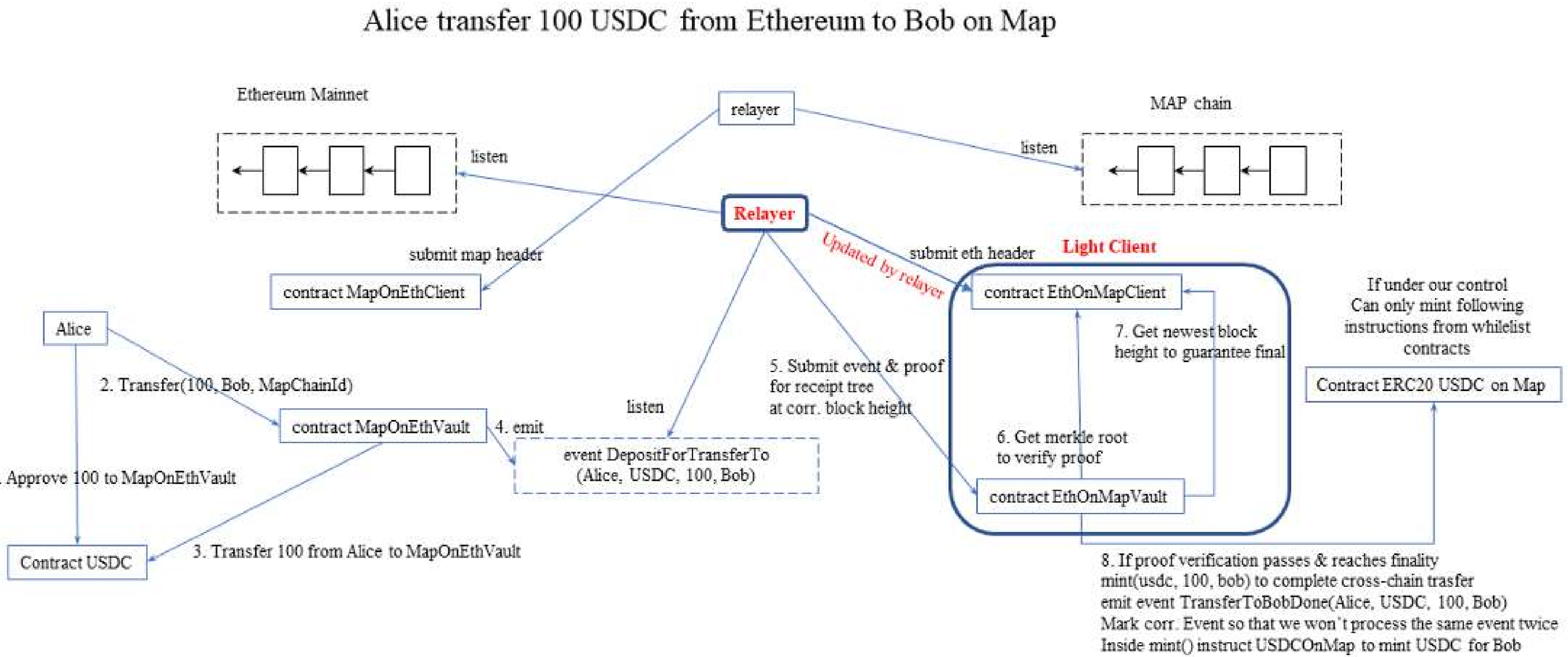
light client +
Relayer Network

External Validators

Liquidity Network: Router protocol example



Relayers Network: Map protocol example



https://www.maplabs.io/blog/understanding-cross-chain-communication-relay-light-client/

Practical choice rationale

Open Source?

connext

liquality

Developer Experience (Documentation, community, etc...)

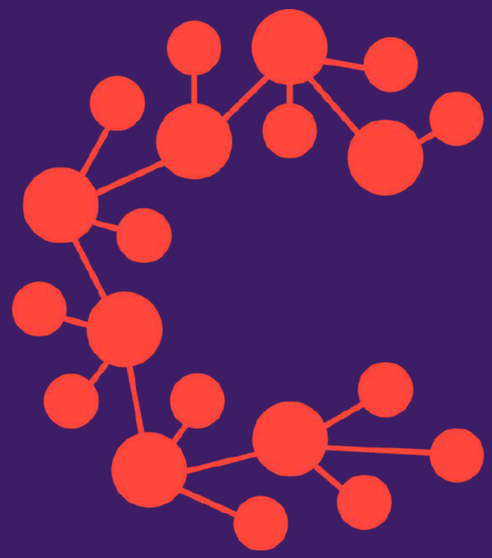
Ease of integration of a new chain

connext

Choices for the MVP

connext

liquality



?

What's next?

Make Casper the home chain:

1- Authenticity

2- availability of guidance

3- Gained some experience by now..

Casper Bridging

1- Casper to EVM, BSC, Solana

2- Ferrum Network

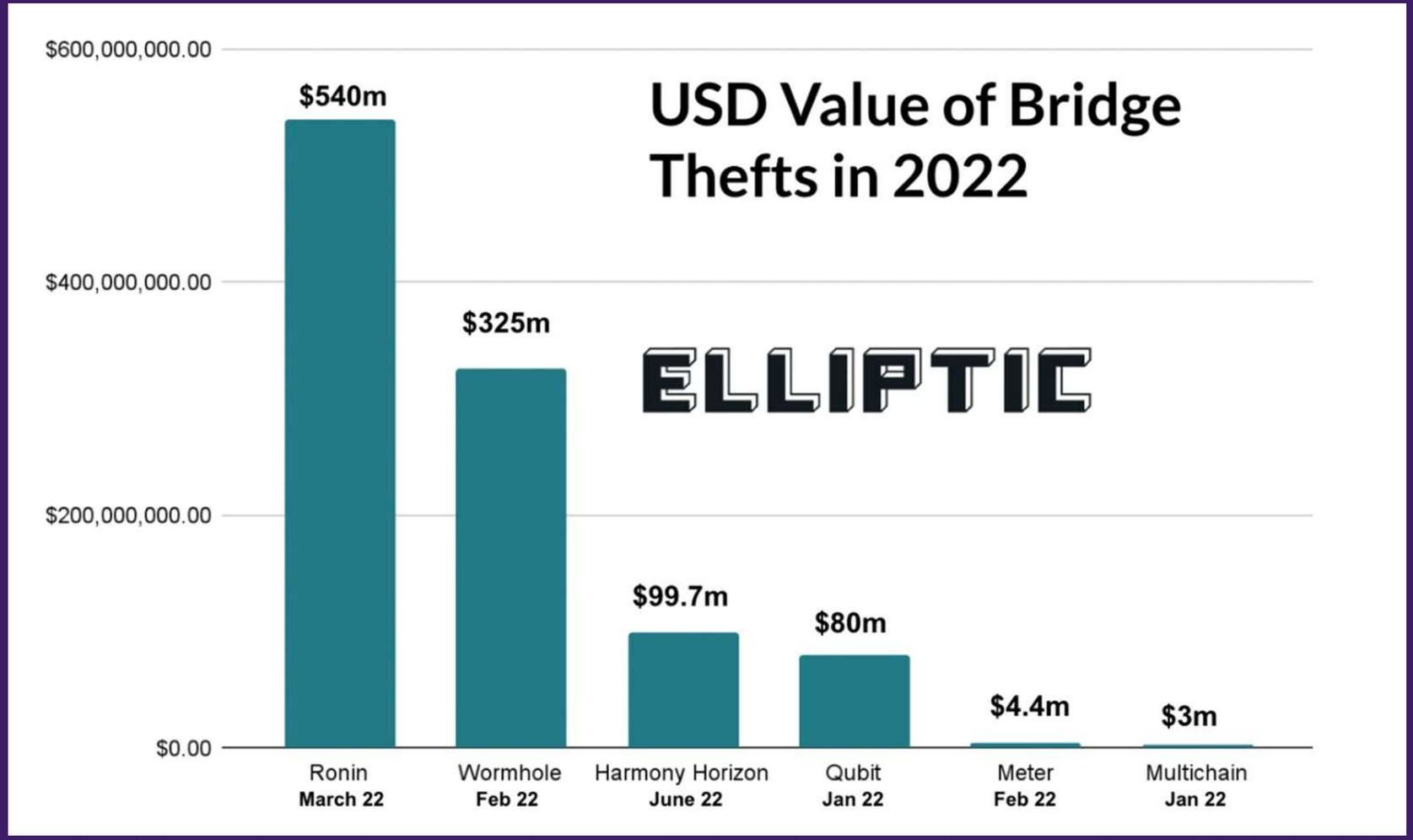
3- Dot.Oracle: mint+lock/burn+unlock

Lit Review :

Security

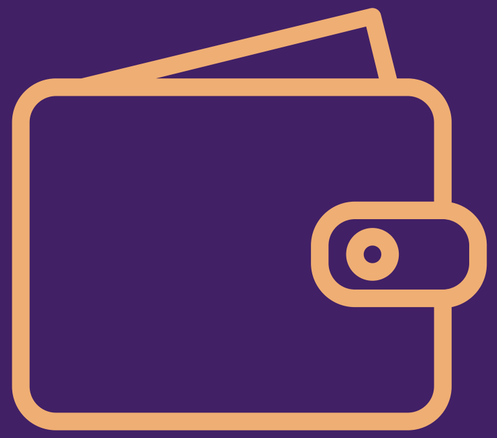
Analysis of Famous Cross-Chain Wallets Attacks

Attacks in 2022



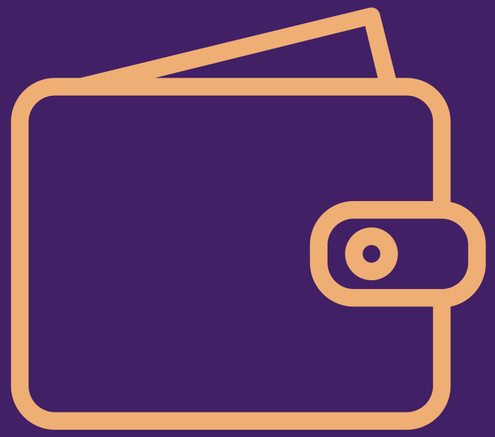
https://hub.elliptic.co/media/mdqixda0/screenshot-2022-06-24-at-10-39-37.png?anchor=center&mode=crop&width=1920&rnd=133005335974300000

Attack Causes



Compromised
Private Keys

Vulnurabilities in
Bridges Smart Contracts



Compromised Private Keys

- Ronin Attack [**$650M**]
  - 5/9 validators hacked
- Harmony Attack [**$100M**]
  - 2/5 validators hacked

Pitfalls in Bridges Smart Contracts

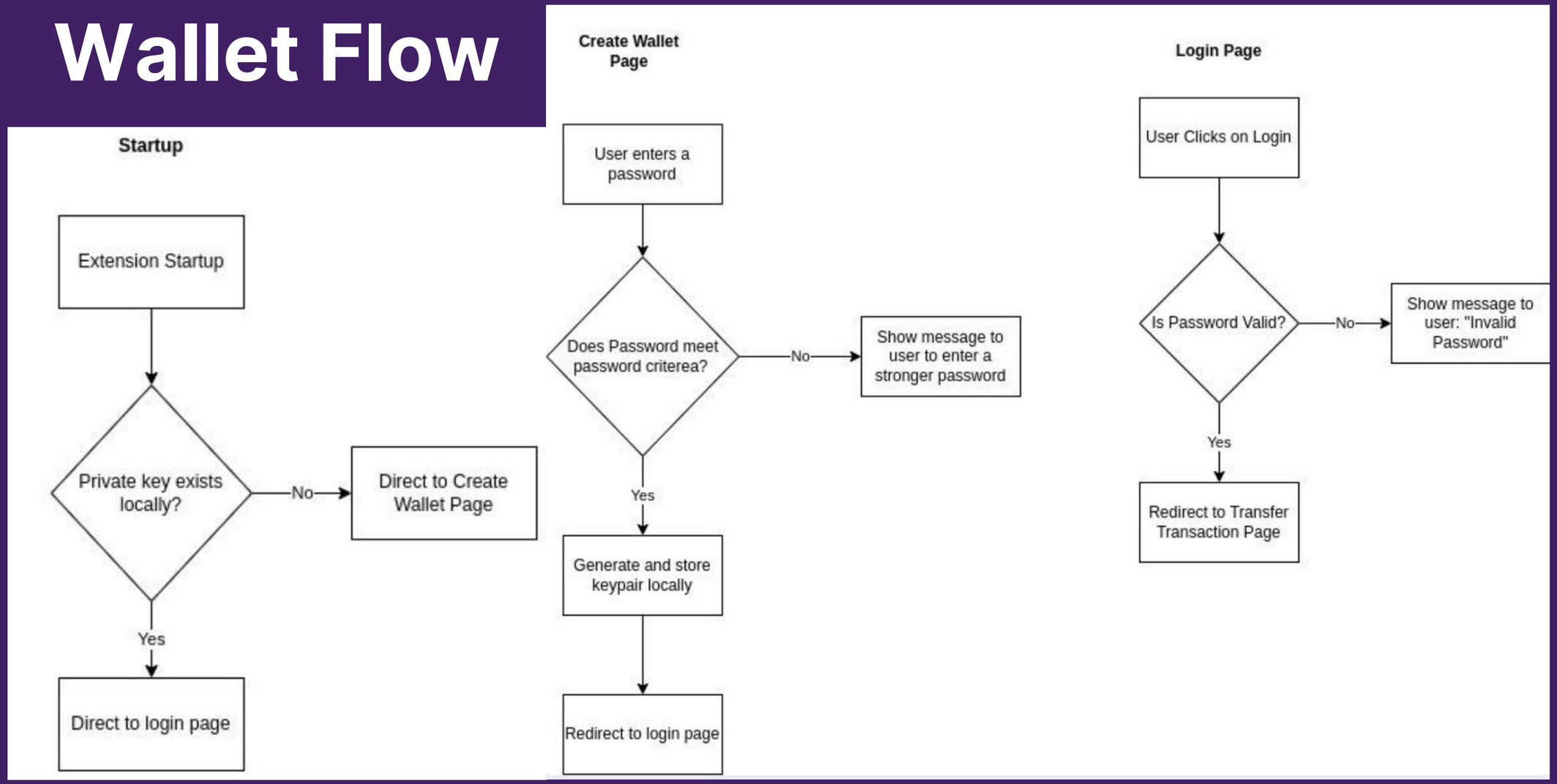
- Wormhole Attack [**$320M**]
- Nomad Attack [**$190M**]
- Qubit Attack [**$80M**]

Reflection on Attacks

Given that we will not create our own bridges, we will make the required research to choose the best bridges in the market according to the previously mentioned mechanisms to choose from them.

Demo

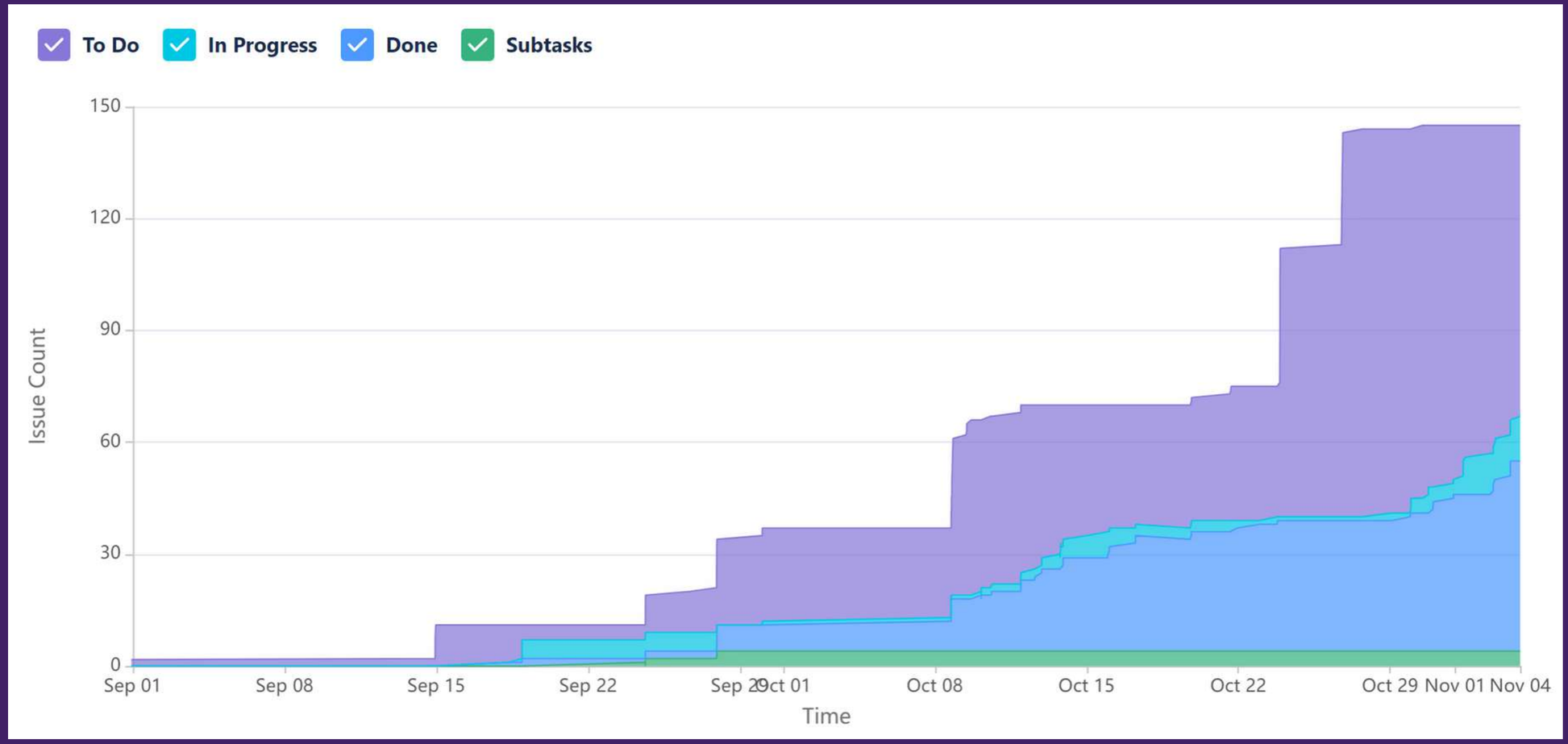
Wallet Flow


Startup
Extension Startup
Private key exists locally?
No
Direct to Create Wallet Page
Yes
Direct to login page
Create Wallet Page
User enters a password
Does Password meet password criterea?
No
Show message to user to enter a stronger password
Yes
Generate and store keypair locally
Redirect to login page
Login Page
User Clicks on Login
Is Password Valid?
No
Show message to user: "Invalid Password"
Yes
Redirect to Transfer Transaction Page

Demo Time

Implementation

Jira Report


To Do
In Progress
Done
Subtasks
150
120
90
60
30
0
Issue Count
Sep 01
Sep 08
Sep 15
Sep 22
Sep 29
Oct 01
Oct 08
Oct 15
Oct 22
Oct 29
Nov 01
Nov 04
Time

Implementation :

PM

Product Management [Agile]

- 1-week sprints
- Planning every week
- Dividing tasks into: Epics, Stories and sub-tasks
- Sub-tasks type include: Research, Scripts and GUI

Research -> Evaluate -> Apply -> Repeat

Build an MVP (Minimal Viable Product) with GUI

Attach | Add a child issue | Link issue

Description

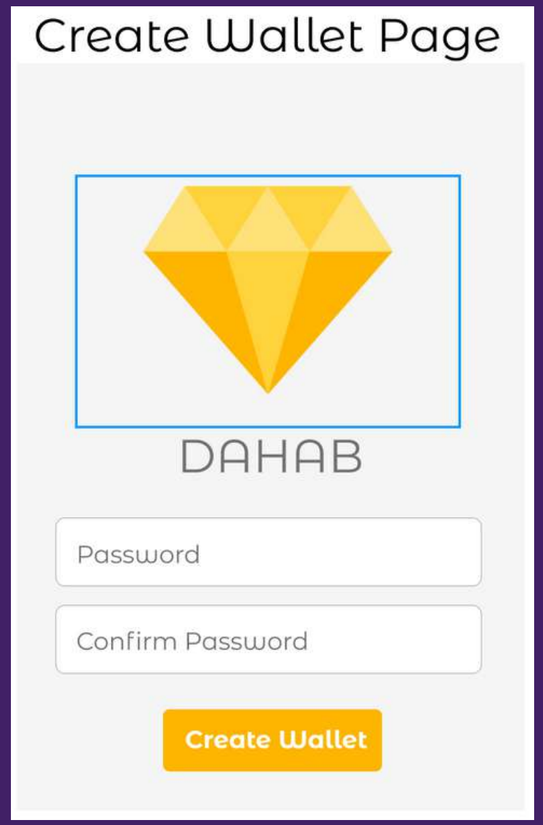
- MVP Details
  - First time open: create wallet (specifies a password) ⇒ generates a private key and stores it in a known location locally and provides mnemonics for the user (user stores them
  - Later: access your wallets using a password (access private key local)
  - **Make a transaction** ⇒ [Same-chain or Cross-chain]
    - Public key for the recepient
    - Amount

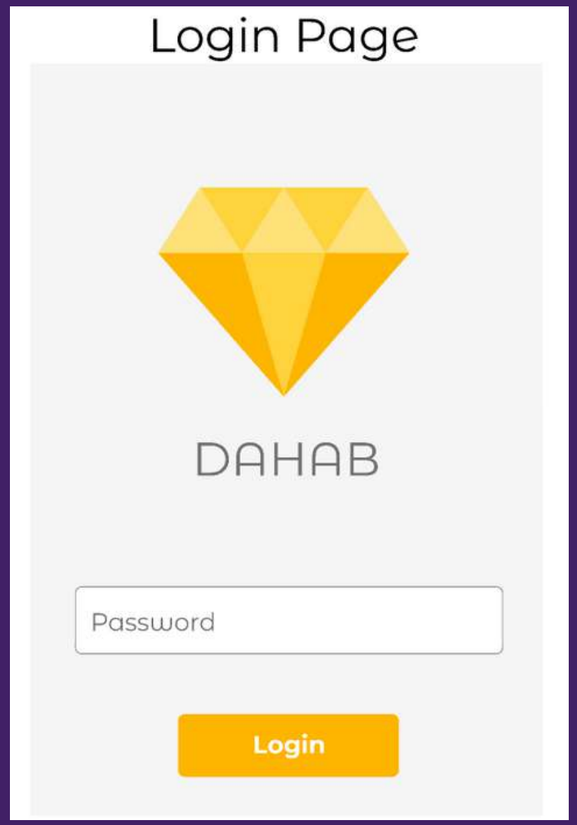
WLT-85	Create a Wallet + Login Pages		TO DO
WLT-87	Create a transfer transaction on the same chain		TO DO
WLT-88	Add Support to Cross-chain		TO DO
~~WLT-89~~	[GUI] Create Wallet Page (signup)		DONE
~~WLT-109~~	[GUI] Create Login Page		DONE
~~WLT-90~~	[CLI + spec] Create `create_wallet` function		DONE
~~WLT-91~~	[CLI +spec] Create `store_keypair` function		DONE
~~WLT-105~~	[CLI + spec] Create `meets_password_criteria` function	SR	DONE
~~WLT-92~~	[CLI + spec] Create `store_password` function	SR	DONE

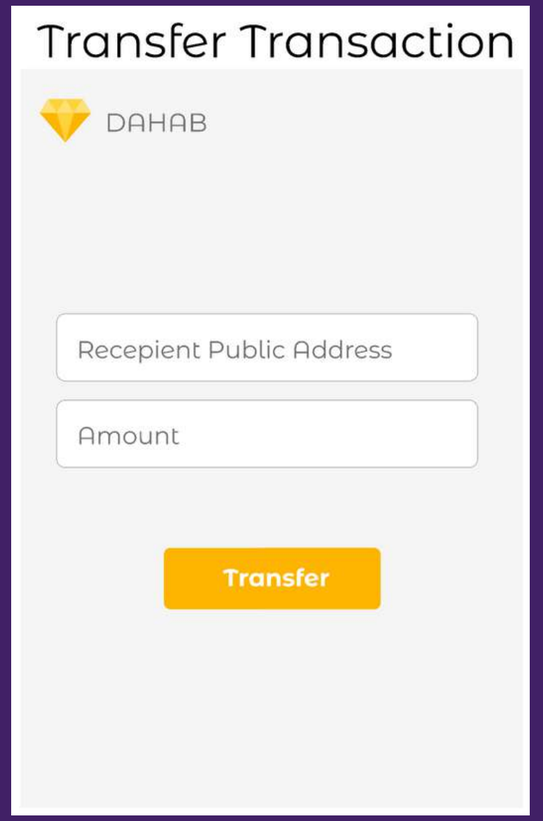
Implementation :

UI

Figma Designs







Implementation :

Password

Password

Validating Password Criteria

Storing Password

Checking if entered password is correct

Validating password criteria

We identified the criteria that represents a the ***minimum requirements of a strong level password***, and the list included:

- One lowercase letter
- One uppercase letter
- One digit
- One special character
- At least eight characters long

Storing password

1. Get password from user
2. Validate password criteria
3. Define a secret key
4. Use the validated password to encrypt the secret key
5. Save the encrypted secret key to local storage

Checking if entered password is correct

1. Get password from user
2. Retrieve the encrypted secret key from local storage
3. Decrypt the secret key using the entered password
4. Check if the decrypted word equals the secret key
5. Return true if both are equal

Better storing password algorithm after research

1. Get password from user
2. Validate password criteria
3. hash the password using SHA-256
4. Save the hashed password in local storage

Checking if entered password is correct

1. Get password from user
2. Retrieve the hashed password from local storage
3. Hash the password entered by the user using SHA-256
4. Compare the retrieved password with the newly hashed input
5. Return true if both hashes are equal

Advantages of SHA-256 over encryption

1

Since encryption is two-way, the data can be decrypted so it is readable again. Hashing, on the other hand, is one-way, meaning the plaintext is scrambled into a unique digest, through the use of a salt, that cannot be decrypted.

2

SHA-256 is still the most secure hashing algorithm out there. It has never been reverse engineered and is used by many software organizations and institutions, including the U.S. government, to protect sensitive information.

Implementation :

Key Pairs

Generate & Store Keypair

A library is used for every chain to generate keypair on this chain. Every keypair has a specific algorithm (i.e: Ed25519)

ETHEREUM	CASPER	SOLANA
ethers	casper-storage	solana

Keys are stored in the local storage for the non-custodial model and it will be stored on AWS secrets manager for the custodial model.

Implementation :

Transfer Txs

Transfer Transactions

1. Get the private key
2. **Connect to a provider**
3. **sign the transaction**
4. Fire the transaction
5. Make sure it is transferred

Libraries

1. Casper-js-sdk
2. **Ethers.js**
3. **Solana/web3.js**

Goals

Vision

”providing more convenience and accessibility without sacrificing security while giving full control through a hybrid model ”

Features

One Wallet To rule them All

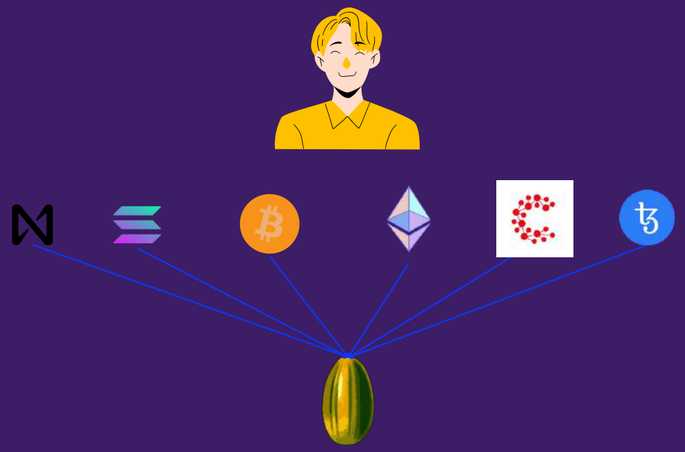
HD mnemonic generation

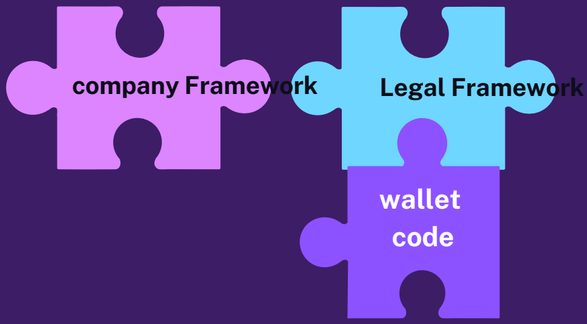
Arabic Language support

Interoperability

Security Prioritization

Security ▪ Statefulness ▪ Capital Efficiency ▪ Speed ▪ Connectivity





Legal frameworks

Hybrid custody model

Inheritance

Future Plans

Future Plans

- For the keys storage, a custodial model will be implemented to implement the hybrid custodial model

- For the non-custodial model, a more secure way will be used such as encryption before storing into local storage

- Createing one master seed for the all accounts on all chains

- Implementing the swap feature in the wallet

- Enable the user to import already made account

- Add recovery keys feature using the mnemonic

- UI enhancements

Meet the Team !

Omar Diaa

Seif Rady

Kareem Kassab

Instabug

BAIN & COMPANY

5ire

Mahmoud Elshinawy

Salaheldin Sameh

Omar Elsayed

esi

THE LINUX FOUNDATION

NETHERMIND

THANK YOU

Blockchain-Based Property Registration System

Group 8

Adham Meligy, Amr Kandil, Joseph Emad,
Maria Amgad, Mohamed Mansour

Supervised by:

Dr. Mohamed Sedky, Dr. Adel El Messiry

Outline

Problem statement

"Property registration process in Egypt is a very long process requiring many physical transactions and paperwork that could take several days. Using the blockchain technology, the transactions will be more efficient with high security and there will be less probability of fraud."

NFTs and Smart Contracts

- Two ways of registering a propertyon BC
  - writing the contract as a new block
  - NFTs

- Why NFTs?
  - NFTs are a more generic representation
  - Can easily link to an owner (public key)
  - Easily trace all properties of a certain owner (wallet)
  - No need to write our own smart contract

CEP-47 vs CEP-78

CEP-47

Implements the minimium required NFT interfaces

Matches the Ethereum ERC-721 standard

First class support on CSPR Live

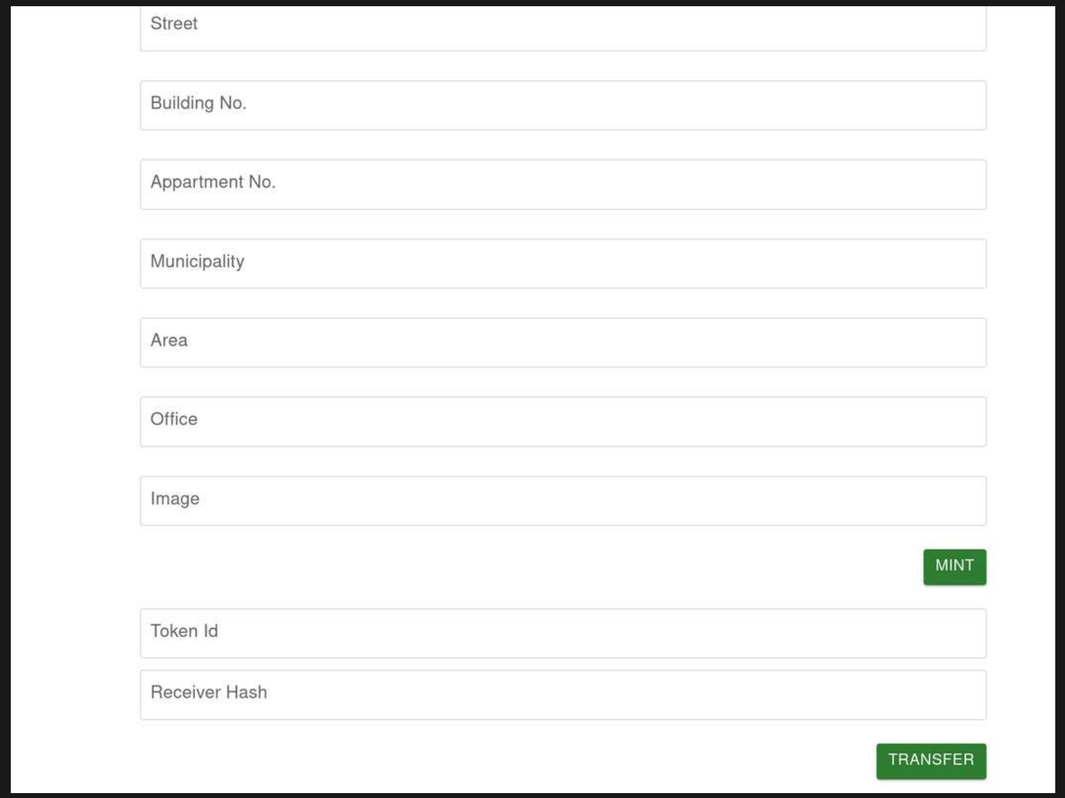
CEP-78

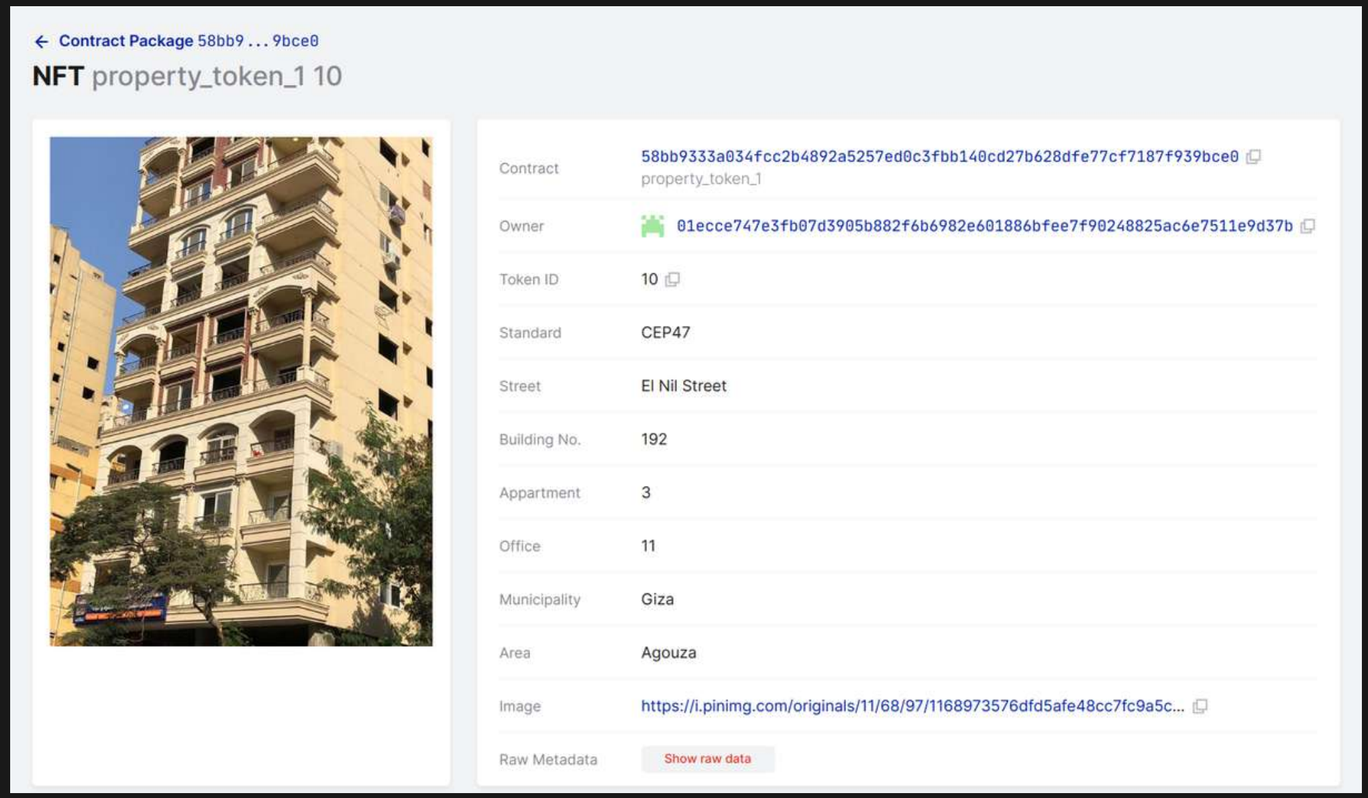
Metadata schemas

Higher lever of control over mints and transfers

Automatic hash identifiers

Initial Prototype





Initial Prototype

- Web development
  -REACT

- Backend
  -Casper
  -Node js

Initial Design

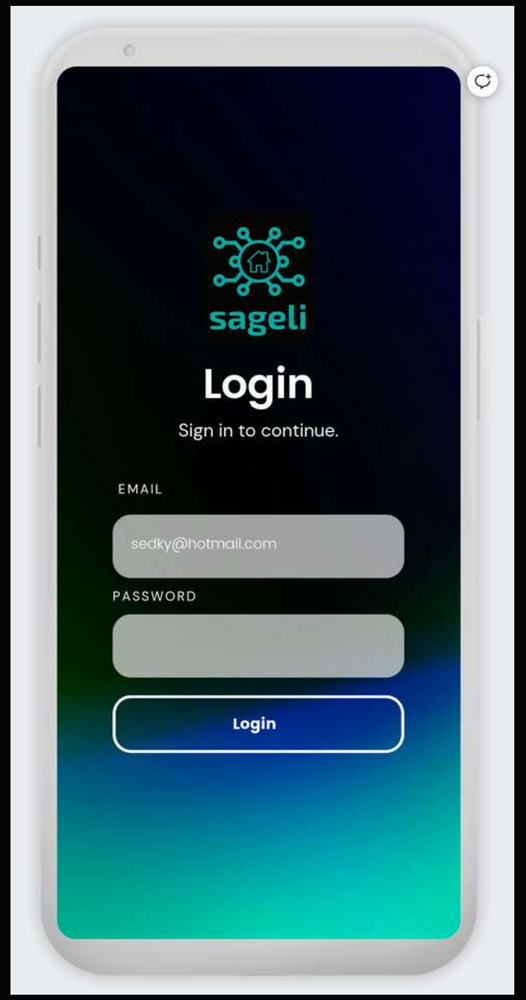
- System Name
- Target Audience
- Color Scheme

sageli

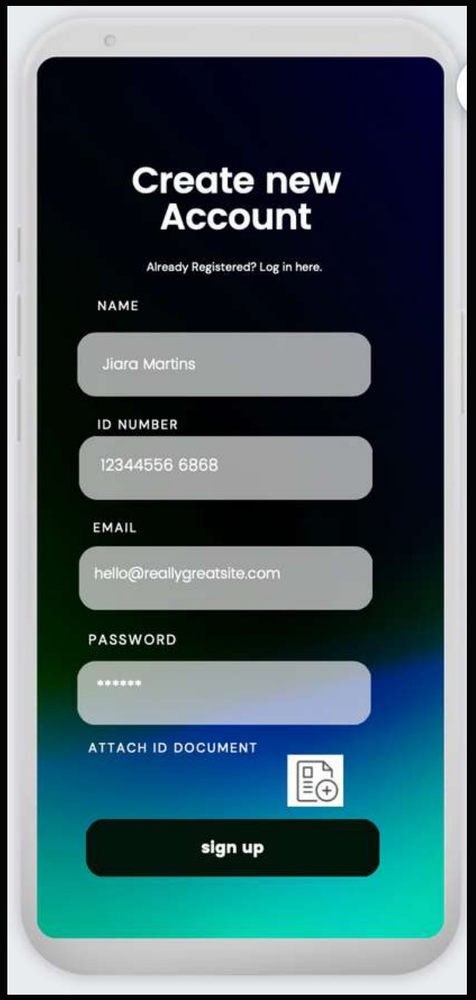
Interfaces

- Login/Create Account
- Home Page
- My Properties
- Transfer Ownership
- Request a Register

Interfaces

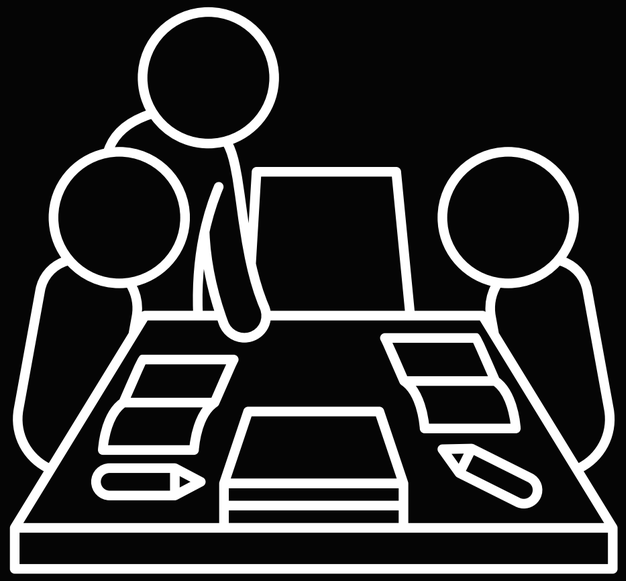


Login



Signup

Future work



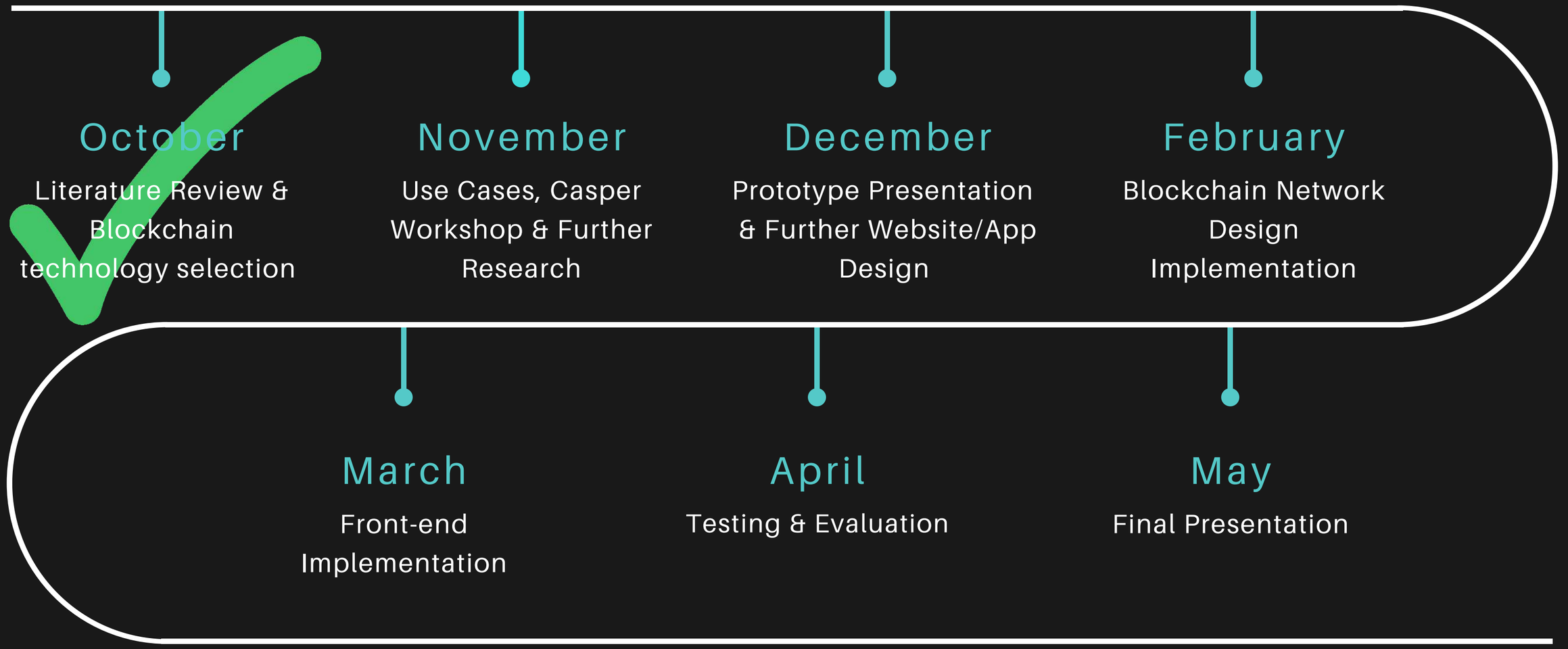
Property Regisration System Expert

Updated Use Cases

Further Website & App Development

Blockchain-Based Property Registration System

Updated Timeline



Questions?

References

- https://github.com/casper-ecosystem/cep-78-enhanced-nft
- https://github.com/casper-ecosystem/casper-nft-cep47
- https://eips.ethereum.org/EIPS/eip-721

Thank you!

Future work

Blockathons are a potent way to increase the awareness of blockchains and encourage academic adoption of blockchain in computer science departments. It is our recommendation to continue the support for codathons, with more emphasis on support from early-stage startup investment funds.