Introduction

Traditional small-to-medium financial institutions (FIs), notably in emerging markets, are facing intense competition from digital banks and fintech companies (e.g. e-wallets, digital micro loans, digital micro insurance) because d-banks and fintechs can:

- operate more efficiently, which leads to more competitive offerings
- reach a wider customer base
- innovate faster through technology

These traditional FIs must offer a digital experience, or risk losing their customers. In order to leap-frog the competition, they must leverage Web3 technology to gain access to new/global markets, lower operating costs/gain better efficiencies, improve security, scalability, availability, and reliability, lower time-to-market for new services, and innovate faster. However, all current public Web3 infrastructure lack true privacy and true compliance, which are show-stoppers for these highly regulated institutions. CRDZ is a confidential (aka privacy-first) public blockchain that features built-in KYC and compliance which was architected specifically to allow FIs (and other businesses) join the Web3 ecosystem and remain fully compliant with regulations such as AML/CTF.

CRDZ allows these FIs to offer a digital experience by creating Closed Loop or Open Loop financial systems. Specifically, they can leverage the public CRDZ blockchain and its reference wallet implementation within their IT Systems. These FIs can selectively delegate functions/business capabilities to the CRDZ chain components, for example:

1. E-wallet backend
2. E-wallet frontend
3. Transaction processing
4. Credential management such as KYC
5. Compliance management such as AML/CTF
6. Gateway to other blockchain products and services
7. Hardware infrastructure

By delegating functionality to the public CRDZ chain, FIs will reap the benefits of Web3: access to a wider, potentially global, audience for their service offerings (i.e. more revenue), lower operating costs/improved efficiencies, quicker time-to-market for new services, scalability, improved security, and the ability to innovate more quickly. FIs can fully utilize micro-incentives with their customers, which is a key feature of Web3. Finally, because CRDZ has compliance built-in at the base layer, FIs will have lower costs for compliance and reporting.

Alternatively, FIs can white-label offerings from 3rd party vendors. However, in order to leap-frog d-banks and fintechs, these 3rd party vendors must utilize public Web3 infrastructure[1]. These 3rd party vendors can reap

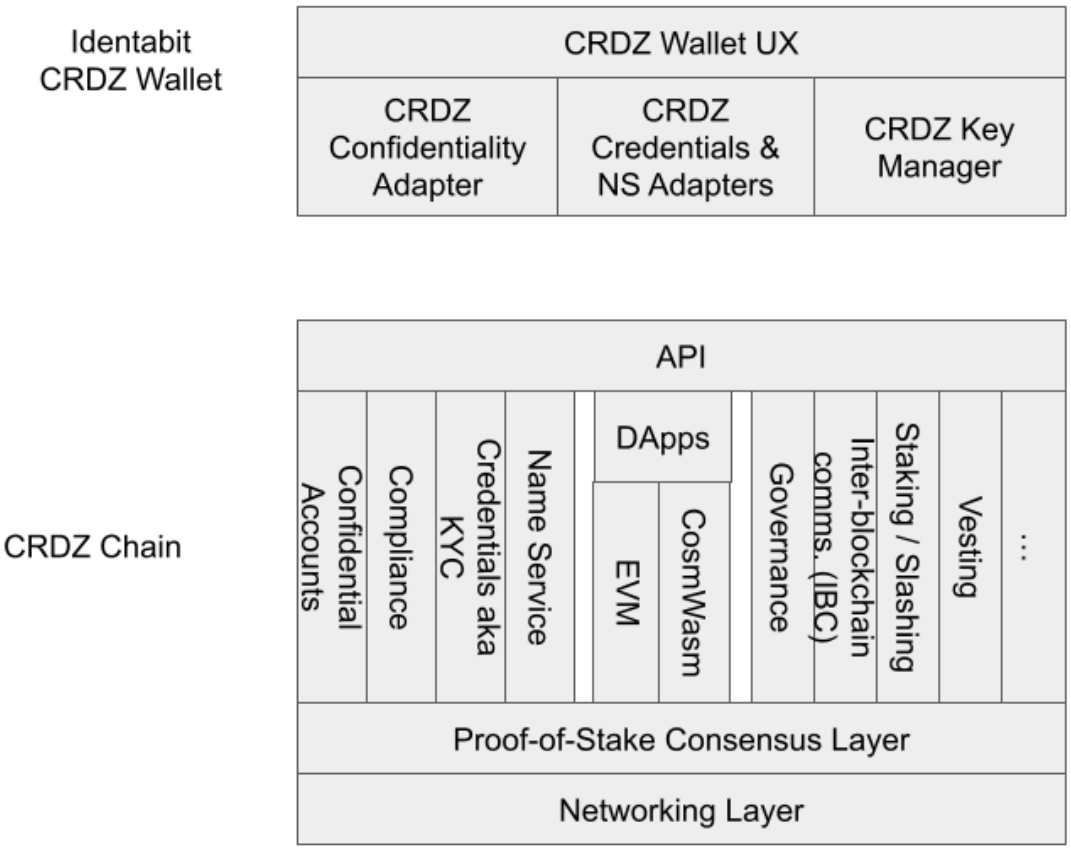
CRDZ Architecture

CRDZ consists of two major components, Identabit (CRDZ's wallet) and the CRDZ chain. FIs that need to provide a digital experience for their customers, or those that want to be ready for Web 3, can leverage one or both of these CRDZ components, or subsets thereof, depending on their requirements. Whether these FIs want an open-loop or closed-loop system, and whether they have an EMI license, MNRC accreditation, or a banking license, they can all benefit from operational efficiencies, an enhanced security posture, reduced time-to-market for service introduction, access to innovative Web 3 decentralized products and services, access to crypto currencies, and the ability to add micro-incentives to improve the business value chain.

CRDZ chain is a public permissionless chain that incorporates privacy preserving technology, self-sovereign encrypted credentials, and a unique "self regulation" compliance protocol. The compliance protocol allows Fully Private Users of the CRDZ chain to continue or cancel transactions that get flagged by the compliance module as suspicious, which provides the perfect balance between user privacy and societal protection.

Identabit is a reference implementation for a CRDZ mobile wallet that gives its users a familiar e-wallet experience, hiding any complexities and responsibilities associated with decentralized technologies. In other words, Identabit features a user experience equivalent to centralized FI alternatives, despite being non-custodial. Identabit users need not worry about maintaining/backing-up seed phrases and private keys, but will still be able to recover their accounts by just "being themselves" (i.e. re-authentication). Furthermore, Identabit users transact with other users using familiar identifiers such as phone numbers, email addresses, and user-selected handles, instead of cryptic blockchain addresses. It is important to note that this "UX equivalence" is provided while maintaining 100% privacy and compliance.

[1] Utilizing private Web3 infrastructure is costly, requires the 3rd party vendor (of FI) to run their own centralized nodes, and would need to integrate with public Web3 infra in order to provide access to global



The diagram above shows a high level architecture for Identabitt and the CRDZ Chain. Adapters/libraries are provided in both Typescript and Go for the UX to interface with the CRDZ chain.

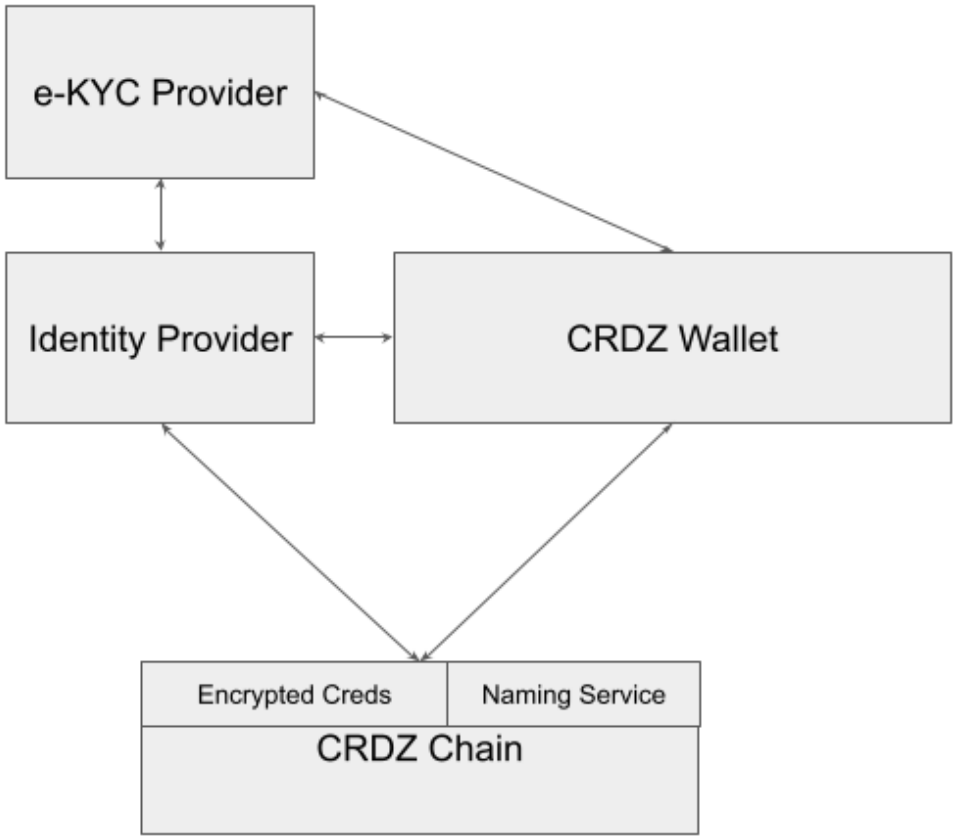
Confidentiality is a key requirement for any business or user to be able to use decentralized technologies for mainstream/real-world applications. The responsibility for maintaining on-chain confidentiality is split between a wallet and the CRDZ chain. The CRDZ Confidentiality Adapter provides a high level, developer-friendly transaction abstraction to the Wallet UX, allowing the wallet developer to focus on the UX needs of the user. The adapter supplies all the decoding/encoding, decryption/encryption, and zero-knowledge proof algorithms that are needed by the CRDZ chain.

“UX equivalence” is absolutely necessary for mainstream/mass adoption of decentralized technologies – it would be unacceptable for the majority of users to be presented with a poor UX, where they are forced to understand, and cope with, the inner workings of blockchain technology. CRDZ Credentials & NS Adapters and CRDZ Key Manager are the components within the wallet that solve this key requirement.

The CRDZ Credentials & NS Adapters provide APIs for interfacing with credential identity providers, the KYC providers used by those identity providers, and the CRDZ Naming Service. The credential identity providers are entities that are used to certify users’ credentials. CRDZ

Naming Service is used by wallets to locate other users on the network. High level, developer-friendly abstractions are exposed, while hiding the details of the confidentiality requirements of the CRDZ chain.

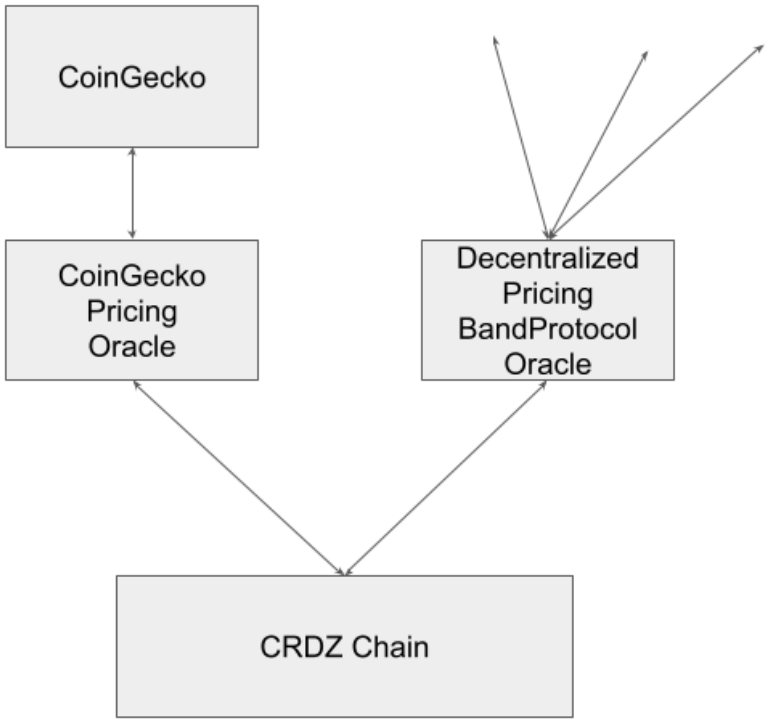
As its name implies, CRDZ Key Manager provides the abstraction needed by the wallet to manage (i.e. generate, use, back-up, recover) seed phrases and private keys. CRDZ allows phrases/keys to be spread throughout the network, and facilitates their recovery through a combination of re-authentication and partner endorsements.



The diagram above shows the external components that a wallet interfaces with in order to perform user authentication (aka KYC). A CRDZ wallet selects an Identity Provider (or more than one if needed for increased decentralization) that will authenticate and certify user credentials. These Identity Providers participate in the CRDZ ecosystem (i.e. they get

compensated for the services they provide). The Identity Providers may employ the services of 3rd party e-KYC Providers such as Passbase or may use internal e-KYC technology. In either case, the wallet uses the API/library provided by the e-KYC Provider in order to collect the necessary information from the user (e.g. full name, gender, date of birth, place of residence, and other PII), together with documents that prove their information (e.g. passport, utility bill, etc.). The Identity Provider is then responsible for encrypting the credentials and storing them on the CRDZ chain, which a CRDZ wallet can retrieve later and link/bind to the user's account. Aside from authentication credentials, there may be other credential/identity providers that can join the CRDZ ecosystem, such as education/diploma identity providers, skill certification identity providers, etc.

The CRDZ Authentication Protocol ensures that only the wallet/user will have access to the credentials, and that only the Wallet will know the binding between the Wallet and the Credentials that are stored (encrypted) on the chain. Even though the Identity Provider and/or the e-KYC Provider could in theory store credentials, none of those components will be able to map those credentials to the account/wallet that owns them.



The diagram above shows how the CRDZ chain is able to obtain virtual currency/digital asset prices through the use of various oracles. CRDZ chain needs access to reliable virtual

currency/digital asset prices in order to provide compliance services, regardless of the type of currency or digital asset.

Fully Private Users (FPU)

By default, users of the CRDZ public chain that use the CRDZ wallet (Identabit, the reference implementation) will have full privacy and compliance. This means that no other FPU, financial institution, or users belonging to a financial institution that are using the CRDZ network can view transactions of these FPUs.

For these types of users, the built-in compliance module of CRDZ will be responsible and accountable for generating suspicious transactions and routing them to the appropriate regulatory authorities. CRDZ's "self regulation" compliance protocol notifies users when their transactions are determined to be "out of norm", at which point they are offered a choice to continue with the transaction by providing a justification for the transaction, or cancel it altogether. If they choose to cancel the transaction, their privacy is fully preserved. If they choose to continue the transaction by providing justification (i.e. a note explaining the reason for the funds transfer), then the CRDZ network, through a patent-pending process, will inform the appropriate regulator of that transaction. This compliance protocol preserves privacy but also provides regulatory guard rails.

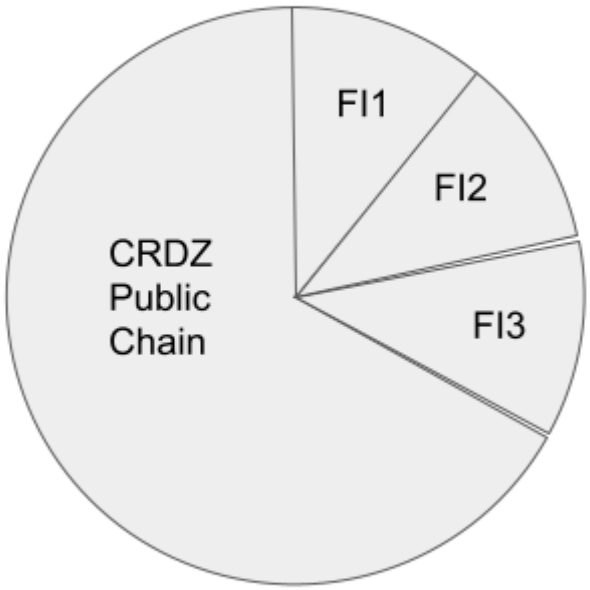
FPUs will naturally have access to open market Decentralized services. FPUs may also be granted access to Centralized services offered by FIs. It's expected FIs will want to be able to compete with open market DeFi products and that FI products that are open to FPUs will potentially reach a far wider user base as they are part of the broader ecosystem. This has the potential to increase revenue for these FIs. For instance, micro-FIs in the Philippines may be able to provide their financial offerings to similar emerging market FPUs. As mentioned earlier, FPUs attracted to institutional products may have to forgo some privacy (i.e. allow the FI access to certain credentials) as it pertains to the requirements of that particular institution's offering.

Virtual Private Decentralized Network (VPDN)

The CRDZ chain has a virtual private decentralized network (VPDN) feature, which is capable of providing its services to centralized financial institutions. Each financial institution gets a completely private (i.e. confidential) slice of the CRDZ network. This is analogous to how Virtual Private Networks (VPN) give their customers a private encrypted network overlaid on top of a public unencrypted network.

When financial institutions use the CRDZ VPDN feature, they may choose to delegate certain functions to the CRDZ chain, or may choose to implement those features centrally. The main reasons for delegating functionality to the chain ecosystem are quicker time-to-market for new services, enhanced security, and lower operational costs.

The simple diagram below shows how the CRDZ public chain can be subdivided to provide its services to centralized financial institutions, but still support public users. In the diagram, Financial Institution 1, FI2, and FI3 have a share of the CRDZ Public Chain.



Privacy & Compliance

Financial institutions that leverage the CRDZ VPDN feature may have different regulatory requirements and responsibilities. The table below shows the flexibility CRDZ offers to various types of financial institutions, ranging from those that are allowed to delegate Suspicious Transaction processing to CRDZ chain (Type A), to those that need full visibility and are responsible/accountable for generating Suspicious Transactions themselves (Type D):

	Type A	Type B	Type C	Type D
Account balance visibility		X	X	X
Credential visibility				X

Transaction visibility			X	X
CRDZ Suspicious transaction visibility	X	X	X	X
Generate suspicious transactions				X

Type A FIs are those that can rely on CRDZ to do all the regulatory scanning and suspicious activity generation. These FIs may need to be copy-furnished with the suspicious transactions that are generated by CRDZ, in order to answer questions from the regulator. These FIs are accountable for suspicious transactions, but may not be responsible for their generation.

Type B FIs may need to have account balance visibility of their customers, in case it has maximum balance restrictions. These are similar to Type A FIs, but may need to be able to monitor and report on account balances.

Compared to Type B FIs, Type C FIs may need the additional visibility of the transactions of their customers in order to have deeper visibility of the actions of their customers, for example, in order to mine the data.

As illustrated above, type A/B/C FIs do not have immediate access to the customer credential data, but could be granted access by the customers themselves. The primary reason FIs may not want to have the customer credential data is that they may not want to be responsible/accountable for storing and protecting that information, since many countries have strict data privacy rules and regulations with possibly large fines for data privacy breaches.

Type D FIs may be required to generate the suspicious transactions themselves, and hence need full visibility to accounts/credentials/transactions of their customers, because they exist in a regulatory environment that is not yet ready for Web3.

Note that these FI types are only examples. It is up to an FI to decide what information it needs visibility to, if any. It is possible that an FI could start at Type D, and as regulatory authorities embrace the more advanced way of doing compliance (i.e. “self regulation”), the FI could move towards Type A. The major advantage of being a Type A is that there is far less work for the FI in terms of security, data privacy, compliance, etc., leading to better operational efficiencies. The FI only needs to focus on the services it provides to its customers.

Services

Centralized

Financial institutions can provide centralized financial services (e.g. un/under-collateralized loans, savings, investments, etc.) to the CRDZ network. These services may need access to the credentials of the customers that wish to use them, in which case the customers will need to grant credential access when requested, for example, when the FI needs to perform a credit rating check.

FIs that provide these services may restrict access either to their customers only (i.e. part of their VPDN), to customers of other VPDNs, or to FPUs. FIs offering their services beyond their traditional boundaries will have more revenue potential.

Decentralized

DApp developers can offer decentralized services to the CRDZ network (e.g. DEX, decentralized over-collateralized loans, flash loans, etc.) that will always be available to Fully Private Users.

Financial institutions using the CRDZ VPDN feature may opt to limit access to those decentralized services for their current customers.

One user, one account

CRDZ enforces the “one user, one account” policy. All users (or businesses/entities) within CRDZ must be authenticated in order to be granted full access and use of the ecosystem. This means that a person or business/entity can only have one master account in CRDZ. This is a fundamental tenet in CRDZ compared to all the current public blockchains. There are many benefits in enforcing this policy:

1. It enables end-to-end analyses of transactions to ensure compliance guard rails are effective. Transactions are always between authenticated users/entities and there are no exits to anonymity, overcoming the stigma of potential illicit transactions. Mule accounts can also be detected.
2. It enables decentralized applications to be built that rely on, or benefit from, real-world identities. Examples include social networks, professional networks, instant messengers, e-commerce, rating networks. Applications such as a “decentralized LinkedIn" would most certainly benefit from the “one user, one account” policy because the actions/reputation of its users would be immutable. A user whose reputation deteriorates cannot just choose to abandon that account and re-create themselves with a clean slate. A “decentralized Yelp or TripAdvisor” can have more trustworthy ratings when they are tied to real-world identities.

3. It enables flexibility in on-chain voting/governance. In today's public blockchains, on-chain governance is plutocratic (i.e. purely stake-based). Those with higher stakes will have more influence. While this is sometimes desirable, there are a few arguments against this:
    a. Centralization: Stake-based governance can lead to centralization of power, where a small group of wealthy individuals can control the decisions (case in point, Do Kwon's control of Terra)
    b. Lack of expertise: Holding a large amount of cryptocurrency does not necessarily make one an expert in what's being voted upon.
    c. Short-term focus: Those with more stake may be more interested in short-term gains than the long-term viability.
    d. Manipulation: Stake-based governance can also be susceptible to manipulation, where individuals or groups buy up large amounts of stake to gain more voting power and influence the outcome of decisions.

    With CRDZ, it is now possible to support other forms of voting/governance. For example, they can now be democratic (popular vote or some form of indirect representation similar to the way elections are handled in the United States via the electoral college). Democratic governance would be especially useful for cooperatives (where each member's vote counts), certain classes of decentralized autonomous organizations, certain classes of protocol improvement proposals, etc. It is also possible to create a hybrid of stake-based and democratic governance.

4. Recovery of all of one's assets is possible since the user/entity has only one master account in CRDZ. The user/entity just has to re-authenticate themselves to recover everything that they own.
5. It enables other types of compliance
    a. Tokenized asset trading compliance - the world is moving towards tokenizing assets (e.g. equities, titles, etc.), and there are specific rules and regulations that may need to be monitored/enforced when these tokenized assets are traded
    b. Decentralized trading compliance - current decentralized exchanges, whether for fungible assets (crypto-currencies) or non-fungible assets (NFTs), are very susceptible to wash trading.

Note that it is possible and encouraged (for privacy reasons) to have many sub-accounts/wallets that belong to this master account.

Coins, Tokens, Assets

CRDZ chain has a base coin called CRDZ. As with all Layer 1 blockchains, CRDZ coins are used to drive the ecosystem. This includes:

- Pioneers (aka validators) are compensated for processing transactions and executing smart contracts
- Identity Providers are paid for their authentication services

- Users are incentivized to delegate their CRDZ to Pioneers (CRDZ is a Delegated Proof-of-Stake chain) to increase their chances of being selected to produce blocks
- Users can lock their stake to vote on governance proposals

CRDZ, being a programmable smart chain, is capable of supporting new tokens. This capability can be used to support new currencies, non-fungible tokens, tokenized equities, tokenized assets, etc.

A company can create a new token that's under their complete control in terms of issuing, transfer, exchange, etc. For instance, a micro-FI in the Philippines (for illustration purposes, it is called MFI_PH) can leverage CRDZ to create a closed-loop system - in such a scenario, it would create a new token (e.g. MFI_PH_TOKEN) which would be worth exactly 1.0 Philippine Peso, under its complete control for issuing, transfer, and exchange. Its customers would have CRDZ accounts under the MFI_PH VPDN. These accounts would be used to track the balances of their respective customers. MFI_PH could then create a centralized loan service within CRDZ that it offers to its customers. MFI_PH supplies all the liquidity for this loan service, and hence, earns all the revenues for this loan service. When a loan is approved and disbursed to an MFI_PH customer, the amount would be reflected in that customer's CRDZ account. The loan itself would be associated with the CRDZ account of the user.

In another scenario, another micro-FI, again in the Philippines (for illustration purposes, called MFI_OL_PH) may choose to participate in an open-loop system. In this case, its customers would have CRDZ accounts under the MFI_OL_PH VPDN, used to track balances of their respective customers. MFI_OL_PH would use a Philippine Peso stablecoin (e.g. PHP_SC) that was issued by an authorized FI in the Philippines. MFI_OL_PH would exchange fiat currency for PHP_SC which it could store in its treasury (a CRDZ account). MFI_OL_PH could then create a centralized loan service within CRDZ that it offers to its customers. MFI_OL_PH supplies all the liquidity from its treasury for this loan service, and hence, earns all the revenues for this loan service. When a loan is approved and disbursed to an MFI_OL_PH customer, the amount would be reflected in that customer's CRDZ account. The loan itself would be associated with the CRDZ account of the user. Users of MFI_OL_PH can use the PHP_SC stored in their CRDZ accounts to pay for goods and services at any merchant, since PHP_SC would be recognized as legal tender. They can also send/receive funds to/from other users, whether they're part of the MFI_OL_PH VPDN or not, because this is an open-loop system.

Terminology Overview

Closed Loop Systems

A closed-loop financial system is a type of payment system where transactions occur exclusively between a single issuer and a set of authorized merchants or consumers. In other words, a closed-loop financial system is a system in which all transactions are conducted within a closed network, where the parties involved are already established and predefined.

Closed-loop financial systems are commonly used in situations where a specific organization or company wants to issue its own proprietary payment instrument, such as a store credit card or a loyalty program point system. The closed nature of the system allows the issuer to closely manage and control the transaction flow and the fees charged, which can help to increase efficiency and reduce costs.

Closed-loop financial systems typically work by issuing a closed-loop payment instrument, such as a card or a digital wallet, which can be used exclusively with authorized merchants or for specific types of transactions. These payment instruments are not generally accepted outside of the closed network.

One of the main advantages of a closed-loop financial system is that it allows issuers to collect and analyze transaction data to improve their services and develop targeted marketing campaigns. Additionally, the closed nature of the system can help to reduce fraud and increase security, as transactions are only conducted within a trusted network.

However, closed-loop financial systems also have limitations, as they may not be as widely accepted as open-loop systems, which allow for transactions to be conducted with any merchant or user, regardless of affiliation with a particular issuer.

Open Loop Systems

An open-loop financial system is a type of payment system where transactions occur between a variety of issuers and acquirers, without any restriction on who can use them or with whom they can conduct transactions. In other words, an open-loop system is a system in which transactions are conducted within an open network, where parties involved are not predetermined or established but are identified.

Open-loop systems are commonly used in the form of credit cards, debit cards, and other payment instruments that are issued by financial institutions, and can be used to conduct transactions with any merchant or user that accepts the payment instrument, regardless of affiliation with a particular issuer.

In an open-loop system, the issuer of the payment instrument works with a network of merchants, acquirers, and processors, to ensure that the payment instrument can be accepted and processed by a wide range of businesses and organizations.

One of the main advantages of an open-loop financial system is that it provides greater flexibility and convenience to consumers, as they can use the same payment instrument across a wide range of merchants and services, regardless of the issuer or service provider. This makes it easier for consumers to make purchases and conduct transactions, and helps to promote financial inclusion by making it easier for consumers to access financial services.

However, open-loop systems can also be more vulnerable to fraud and security breaches, as the open nature of the system can make it easier for unauthorized parties to gain access to sensitive financial information. Additionally, the fees charged by issuers and processors in

open-loop systems can be higher than those charged in closed-loop systems, due to the greater complexity and the number of intermediaries typically involved in transactions.

EMI license (Philippines-specific)

An EMI license allows its holder to issue electronic money or e-money, which is a digital equivalent of physical cash that can be used for various financial transactions such as online purchases, bill payments, money transfers, and other similar transactions. This license is required by any company or institution that wants to offer electronic money services in the country.

To obtain an EMI license in the Philippines, the applicant must first be a corporation registered with the Securities and Exchange Commission (SEC) or a financial institution authorized by the BSP to engage in e-money operations. The applicant must then comply with various requirements and regulations set by the BSP, which include capitalization requirements, risk management, data privacy and security, and other relevant rules and regulations.

Once granted, an EMI license allows the licensee to operate as an electronic money issuer in the Philippines and offer electronic money services to consumers and businesses.

IT System Architecture

An IT system for a financial institution typically includes a range of software applications, hardware, and networking infrastructure to support the electronic money services (i.e. a digital UX) provided by the institution. Here are some of the components that could be included:

1. Electronic wallet software: This software allows customers to create and manage their electronic wallets, which can store funds and facilitate digital transactions.
2. Payment gateway software: This software is used to process electronic payments and transfers, and can interface with various payment networks and systems.
3. Anti-money laundering (AML) software: This software is used to identify and prevent financial crimes, such as money laundering and terrorism financing. It uses algorithms and machine learning to analyze transactions and flag suspicious activity.
4. KYC software: This software is used to verify the identity of customers and ensure that they meet regulatory requirements for electronic money services.
5. Compliance management software: This software helps the financial institution to manage its compliance with relevant laws and regulations, such as KYC and AML requirements.

6. Reporting and analytics software: This software provides insights into the institution's operations and financial performance, and can be used to generate reports for regulators, investors, and other stakeholders.
7. Hardware infrastructure: This includes servers, workstations, and other computing devices needed to support the software applications.
8. Networking infrastructure: This includes routers, switches, firewalls, and other components needed to connect the various hardware and software components and provide secure access to the electronic money services.

In addition to these components, an IT system for a traditional financial institution would also need to have robust security measures to protect against cyber threats, data breaches, and other risks. This could include measures such as encryption, multi-factor authentication, intrusion detection and prevention systems, and regular security audits and testing.