August 2024

PREPARING FOR WEB3

BitOasis CoinDCX

Download the Report

TABLE OF CONTENTS

TABLE OF CONTENTS

AUGUST 2024

AUGUST 2024

FOREWORD

In recent years, the landscape of Web3, digital assets and blockchain technology has undergone significant transformation. As pioneers in the field, CoinDCX and BitOasis have collaborated to present this comprehensive report, aimed at providing a thorough understanding of the evolving world of Virtual Digital Assets (VDAs) and their far-reaching implications.

This compendium serves as a fundamental guide to demystify the complexities surrounding crypto assets, and blockchain technology. It covers a wide spectrum of topics, from the basic concepts of blockchain and consensus mechanisms to the diverse applications and regulatory challenges that shape this dynamic industry.

Our primary objective is to provide readers with a holistic view of the VDA ecosystem. We delve into the interconnected roles of VDAs and blockchain technology, the significance of intermediaries, and the importance of trading in the VDA economy. By examining various market players, including exchanges, wallet service providers, and custodial solutions, we aim to offer a comprehensive understanding of the ecosystem's intricacies.

Moreover, this report highlights the pivotal role of stablecoins, decentralized finance (DeFi), and the associated risks and safeguards. We explore the global regulatory landscape, focusing on how different jurisdictions are approaching the regulation of VDAs and blockchain technology. Special attention is given to the regulatory frameworks in the UAE, showcasing the proactive steps taken to foster innovation while ensuring compliance and consumer protection.

As we stand at the cusp of a new era in digital finance, our commitment at CoinDCX and BitOasis is to lead with integrity, transparency, and a forward-thinking approach. We believe in the transformative power of Web3 and its potential to revolutionize various sectors, including finance, supply chain, healthcare, and governance.

We hope this compendium serves as a valuable resource, providing clarity and fostering a deeper understanding of the VDA ecosystem. Together, let us embrace the opportunities presented by Web3 and work towards a more decentralized and inclusive digital future.

Sumit Gupta

Co- Founder
CoinDCX Group

AUGUST 2024

1.BASIC CONCEPTS

Key Themes:

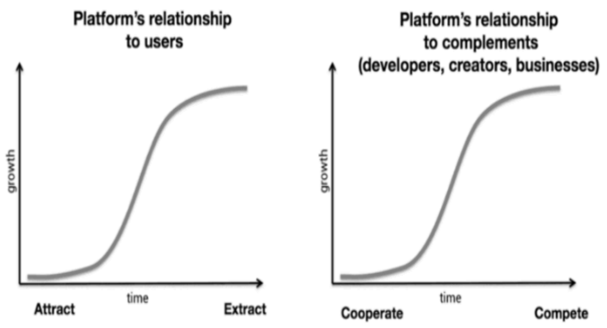
This section traces the internet's evolution from Web 1.0's open protocols to Web 2.0's centralized systems, culminating in the decentralized, blockchain-based Web3. Web3 combines openness with sophisticated solutions, enabling users to read, write, and own on the internet. Key components include blockchain for secure interactions, crypto mining for transaction verification, VDAs for incentivizing participation, smart contracts for automated transactions, and DeFi for open financial services. The Web3 Stakeholders Stack outlines the technological layers and participants driving this innovative, user-empowering internet paradigm.

1. Web3: The future of the internet

The internet's lifespan so far, can be broadly divided into three eras. The first era - from the 1980s through the early 2000s - popularly referred to as Web 1.0, saw the creation of several protocols such as http, smtp, ftp, etc. These protocols were developed such that anyone could build solutions on top of them, without anyone's permission and they still form the foundation of the internet.[1]

Given that open source is, by definition, free for anyone to use, it is difficult to monetise[2]. Over time, therefore, Web 1.0 protocols stagnated as they lacked the ability to incentivise ongoing development and further investment[3]. Instead, they became the neutral, and level playing field on top of which the ecosystem of the internet began to be built, ushering in Web 2.0.

Web 2.0 is often referred to as the "interactive and social" web. Its protocols are proprietary, closed, and are built on top of Web 1.0's open ones. This second era of the internet gave birth to some of today's most valuable companies which leveraged their protocols to offer sophisticated tech-based solutions. On the one hand, the advent of these companies and the consequent access to technology positively impacted our lives. However, this has also led to people trusting profit-driven, often opaque, centralised companies, acting as intermediaries. As a result, these companies have a considerable degree of control and oversight over a wide variety of interactions.



Source: "Why decentralization Matters, Dixon Chris

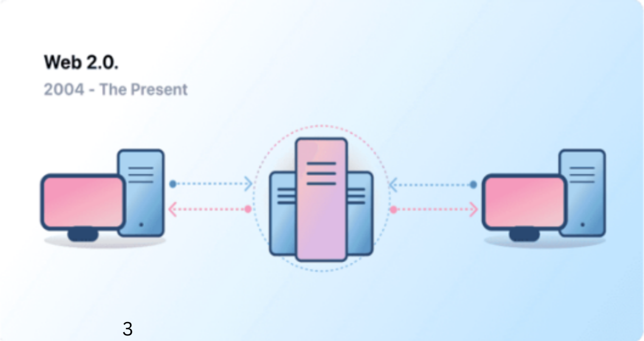
Web 1.0.
1990 - 2004

This also stifles innovation.[4] and competition, making it harder for third-parties using these platforms to grow their internet presence, without the fear of these centralised platforms arbitrarily changing the rules, taking away their audiences and profits. These problems will only become more pronounced in the future.

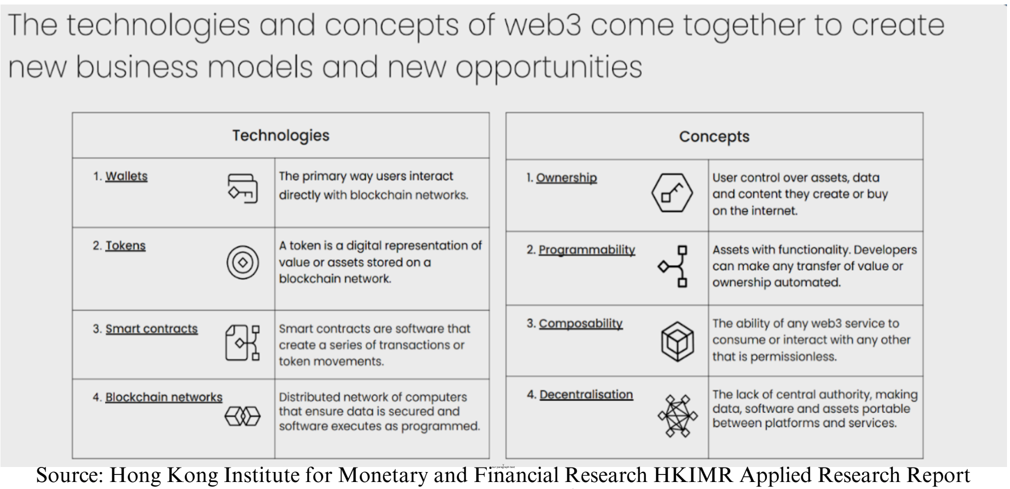
Web3 offers a tech-based solution to these challenges. Web3 is an open and decentralised internet that leverages blockchain technology and virtual digital assets. It addresses the core challenges of Web 1.0 and Web 2.0, and combines their best features, empowering users to read-write-own on the internet. It is based on Web 1.0's defining features of openness and community ownership, while addressing its challenge of lack of incentives. Like Web 2.0, it promises to deliver secure and sophisticated solutions, but it addresses the challenges associated with centralisation.

The architecture of Web3 is substantially different from that of Web 1.0 and Web 2.0, which renders the former decentralised. In both Web 1.0 and Web 2.0, users access a web browser installed on their computers to connect to hosting servers, retrieve information from webpages, and display content on their computers. Web3 leverages a blockchain-based, "peer-to-peer" architecture.

In this architecture, application code and data is hosted across participants in a distributed network rather than on servers operated by a company providing web applications or services.[5] As the next iteration of the internet, Web3 promises to serve as the basis for new forms of economic and social interaction arising from platforms that allow people to collaborate, create, exchange, and take ownership of their digital identity and assets.



[3]



The technologies and concepts of web3 come together to create new business models and new opportunities

Technologies		Concepts	
1. Wallets	The primary way users interact directly with blockchain networks.	1. Ownership	User control over assets, data and content they create or buy on the internet.
2. Tokens	A token is a digital representation of value or assets stored on a blockchain network.	2. Programmability	Assets with functionality. Developers can make any transfer of value or ownership automated.
3. Smart contracts	Smart contracts are software that create a series of transactions or token movements.	3. Composability	The ability of any web3 service to consume or interact with any other that is permissionless.
4. Blockchain networks	Distributed network of computers that ensure data is secured and software executes as programmed.	4. Decentralisation	The lack of central authority, making data, software and assets portable between platforms and services.

Source: Hong Kong Institute for Monetary and Financial Research HKIMR Applied Research Report No.1/2024 [6]

2. Key Components of Web3

Web3 is a group of technologies that encompasses several components including blockchain, virtual digital assets including NFTs, decentralised finance ('DeFi') and social platforms. [7]

2.1. Blockchain Technology

Blockchain is a distributed ledger that records transactions in a secure and tamper-proof manner. One can think of it as a network of participants who transact with one an[9]other in the 'native token' of the network and all of their transactions are recorded on a distributed database by each node in the network

Blockchain stores data in groups or blocks. Then every time a new block is created, it is interlinked to the old block. Each Block has a certain storage limit set. Since the data stored in blocks is linked together, the database is called a blockchain . This distributed database is openly accessible to all participants for adding and viewing the recorded data at any time. The same is secured using a scientific technique called cryptography. While all the VDAs are built on blockchain technology, not all of them are the same.

Blocks are self-correcting in nature. For example, if one user tampers with Bitcoin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This system helps to establish an exact and transparent order of events. For Bitcoin, this information is a list of transactions, but it also is possible for a blockchain to hold a variety of information like legal contracts, state identifications, or a company's product inventory.

i. **Blockchains enable direct peer-to-peer interactions**

Public blockchains enable a system where A and B can interact directly with one another, without the involvement of any intermediary. One can think of such blockchains as digital ledgers, similar to online spreadsheets, shared across a network of participants who can view the stored data at any time. [8]

It enables participants to transact with one another on the network without the involvement of a central server and all these transactions are recorded on the database in a distributed manner by multiple network computers. These computers are called nodes.They can initiate transactions on the request of network participants, and verify transactions initiated by other nodes. Transactions get added to the blockchain in the form of blocks, once the participating nodes consent to its authenticity. Public blockchains are append-only, time-stamped databases and subsequent changes can only be made after achieving nodes' consensus, which offers imm[4]utability. Anyone with the right infrastructure can become a node on a public blockchain, rendering such blockchains permissionless. These nodes do not know one another, which makes it difficult for them to collude rendering [5]such blockchains truly decentralised. The Bitcoin blockchain for instance is reported to have over forty thousand nodes across nearly hundred countries.

Public blockchains' decentralised nature eliminates users' vulnerability to targeted cyber-attacks as the data is duplicated and stored with a large number of nodes. Given that there is no single person or entity behind blockchains – just pre-written, open-source technology – they create a level playing field for all participants and allow equal opportunity encouraging innovation and competition. It also excludes the need for users to trust any third party intermediaries with data or[6] be subjected to algorithms and codes developed by said third party, that may be arbitrarily altered. Users and third party compliments are now no longer co[7]mpeting with centralised platforms for profits, so the system is also more economically efficient.

The immutability and transparency of blockchains also allows strangers to interact directly without the need for any trust, or intermediary. This is a significant feat which was previously considered to be impossible in the digital space.

ii. Crypto Mining:

Mining is the process of creating new blocks and verifying transactions on the blockchain. Crypto assets are based on the blockchain network; it utilizes publicly distributed ledgers to keep a record of all transactions.[2] The copies of these ledgers are also available on the systems of other network participants, ensuring the security and transparency of the Bitcoin network.

When users proceed with transactions, it is verified and validated through the mining process before being recorded on the blockchain ledgers. This method of generating new blocks is referred to as "mining" as it involves high power utilization, just like energy required in natural resources mining. Mining requires people to employ high computational resources, known as "miners". These miner nodes compete with each other to guess the answers to complex cryptographic hash problems. The first miner node who guesses the answer correctly gets to select a group of transactions for verification, generate a new block and receive an incentive of the newly created Bitcoin.

There are several ways to mine tokens depending upon the number of participants and hardware resources employed. A few types of mining methods are as follows:

- **CPU Mining:** In earlier days, when Bitcoin was introduced, it was mined using a normal computer CPU(central processing unit). So, anyone could mine Bitcoin with their laptops and PCs. This increased the number of miners and the complexity of hash problems, resulting in Bitcoin CPU mining becoming a less viable option.

- **GPU Mining:** Later, miners started employing GPU(graphical processing unit) along with CPUs to increase their chances of guessing the right answers to complex computational problems. Some miners even used to combine multiple GPUs for better hash rate output.

- **ASIC Mining:** Introduced in 2012, ASIC technology is specifically designed for mining crypto assets. ASIC, Application Specific Integrated Circuit, provides improved efficiency and performance than other mining hardware. However, ASIC-based mining[4] hardware is costlier and could quickly become older with advancing technology, resulting in unprofitable mining.

- **FPGA Mining:** Unlike ASIC hardware, which is designed[5] specifically for a single purpose, Field Programmable Gate Array (FPGA) serve better as they can be programmed and reprogrammed according to different algorithms and mining complexities of crypto assets. Furthermore, these hardware are cost-efficient and provide more speed than CPUs and ASIC mining.

- **Cloud Mining:** This mining method allows anyone to become a miner and earn mining rewards without purchasing costly hardware, softwares, or worrying about maintenance. In cloud mining, one pays cloud mining service providers a rent for utilizing their[6] computational resources virtually. This also offers miners a convenient exit option in case mining difficulty rises or becomes unprofitable.

2.1.1. How does Mining work?

The mining process begins with broadcasting new transactions to all network nodes. When new transactions are processed, they are added to a mempool or memory pool. Next, a miner node collects pending transactions from the mempool, checks their validity, and passes them through a hash function to group them into a block. The Bitcoin network hashing algorithm is SHA-256 or Secure Hashing Algorithm 256. It is a one-way cryptographic function that encrypts the transaction data into a 256-bit string[2], which can not be used to retrieve original data by decryption.

These hashed transactions are then organized into a Merkel tree and passed through a hash function until a single hash is generated. In simple words, the Merkel tree is a data structure used for the verification and organization of blockchain transactions, we are not going to discuss this further as this article then might become a technical paper.

In the next step, miners combine the hash of the previously generated block, the hash of the candidate block, along with a nonce(an arbitrary number) to form a unique hash identifier of the block. This process links the new block to the previous one, creating a chronological chain of blocks, what we know as blockchain. The first miner node to complete Proof of Work, and create a valid block identifier, broadcasts the block on the network for other nodes to validate.

2.1.2. Proof of work

It is the consensus algorithm of the crypto asset network in which miner nodes use their computational resources to solve a difficult cryptographic hash puzzle, as we discussed earlier. This PoW consensus ensures the integrity of the Bitcoin network by eliminating double-spending.

Once the network nodes validate the block and confirm if the block hash adheres to the protocol. It is updated on blockchain public ledgers, and block miner nodes are rewarded.

But what if there are two miners to solve the hash problem simultaneously? In case two blocks are mined at the same time, the block which forms the longest chain and continues the next block mined on top of it is considered the most valid block. The block that is left is referred to as the “orphan block.”

2.1.3 Block Rewards & Bitcoin Halving

Miners receive incentives to validate transactions and solve difficult computational puzzles using their processing energy. This reward includes free Bitcoins and a share of the transaction fee associated with the candidate block. As of 2023, Bitcoin miners receive 6.25 BTC as a block reward for every block added to the blockchain. However, this Bitcoin block reward is decreased to 3.125 BTC due to the Bitcoin halving event on 20th April 2024.

Bitcoin[4] supply was capped at 21 million during its creation of scarcity and value of BTC coins. Bitcoin halving is the process of reducing the rate at which new Bitcoins are mined and miner block reward to half. This process is programmed in the Bitcoin mining algorithm[1] to reduce coin inflation and maintain the value of BTC as currency over time. However, Bitcoin halving can reduce network security since there will be less miner participation due to reduced block reward. For this reason, Bitcoin miners will continue to receive transaction fee rewards for maintaining the network even after the last BTC is mined(approximately in 2041).

2.2. Virtual Digital Assets

The sanctity of a blockchain depends heavily on the nodes or the connected computers participating in the network. As noted, they have the power to initiate and validate transactions, enabling direct peer-to-peer interactions. Virtual digital Assets ('VDA') play a fundamental role in incentivising participants to honestly engage with the network.

VDAs are a medium of exchange or a store of value that secure, validate, and record transactions made on a public blockchains, serving a critical function that enables the whole system to function in the absence of a third[2]-party service. In absence of VDAs, blockchains are essentially shared platforms for storage. VDAs are rewards offered to miners who validate transactions.

For instance, nodes are awarded with tokens for recording and validating transactions correctly on the blockchain. In Bitcoin's case, miners who write a new block have permission to give themselves a reward of new bitcoins. That reward started at 50 bitcoins per block and every four years the protocol is adjusted, reducing the reward by half. Currently, this reward is limited to 3.125 blocks after the recent halving activity in April 2024. To discourage malpractices, blockchain networks leverage mechanisms such as "proof of stake". Nodes who validate a transaction need to "stake" their VDAs and risk losing some or all of them if they conduct fraud. Many blockchains actually destroy one's stake as a penalty for some provable attempt at corrupting consensus data.

Given these incentives and disincentives, blockchain networks achieve a game-theoretical equilibrium where rational participants will always choose honest participation rather than fraud, in order to receive rewards and avoid penalties.

2.2.1. How VDAs and blockchain are inter-linked

Blockchain innovation is almost entirely fueled by VDAs which form the incentive for miners and nodes to participate and perform validation tasks in the network.

For example, imagine a blockchain network that interconnects un-utilized data storage space from all our phones and aggregates them for sale on a token-based blockchain network. Any consumer who wants to host an online business or service can purchase tokens of this network and use them against storage space requirements. The incentive for network participants — in this case, all those who are sharing their storage space — is that they can now earn in the form of tokens from the network. Each sale is established via smart contract interactions in the native token and all earnings are cryptographically verified and credited to participants in the form of tokens automatically without the need for a third party.

These earnings and token holdings form a core part of the blockchain as it incentivizes participants to join the network. The more developed the use-cases and network effects of a particular blockchain, the higher the resulting earnings from the token[5]. Such a system ensures that both businesses that power the network and users benefit from it. If participants do not see any value, there is no reason for them to be part of the blockchain and this network could cease to exist.

While a centralized system running such a network is also possible, the difference is that unlike a decentralized network where all participants accrue value over time as the network grows, in a centrally driven network all the value and resulting wealth only accrue to a central entity/owner.

2.2.2. What would a blockchain without VDAs look like

A decentralised (public) blockchain cannot function without VDAs. As noted previously, the primary value proposition of such blockchains, over any other ordinary database, is the elimination of the challenges associated with trusting a centralised intermediary. This is only possible when a wide variety of participants including nodes choose to engage with the network. VDAs effectively align incentives of all parties involved to build a truly[2] decentralised, transparent, and robust blockchain. For instance, the grant of valuable VDAs as rewards (and their destruction as penalties) brings onboard a wide variety of unrelated participants to engage honestly on the network. These features of public blockchains are in turn fundamental to addressing the concerns stemming from the current reliance on "trusted" intermediaries.

In theory, a centralised agency like a company may designate nodes and incentivise them through more traditional mechanisms like salary, providing infrastructure to run the node etc. In doing so, they may even dilute the system enough to avoid a single point of failure. There may even be specific use cases for such a permissioned blockchain (not permissionless as not anyone can become a node), but it will fail to address other challenges associated with centralisation. For instance, users will still be trusting a centralised agency with their data; they will still be subject to changes in their algorithm and codes. Moreover, such a system will be grossly inefficient from an economic standpoint. This centralised agency will spend substantial resources in the form of salary for the employees running nodes, infrastructure cost etc. while instead, they can leverage VDAs to provide an inbuilt incentive mechanism to draw participants to either an existing or a new blockchain.

2.2.3 Consensus Mechanisms and why they are important

Consensus mechanisms are a key component of the effective operation of blockchains, as well as other decentralized systems. In a decentralized system where users have asymmetric information and trust about one another, some mechanism is needed to guarantee that a state, value, or piece of information is correct and agreed on by all participants validating the network. Different consensus mechanisms have vastly different requirements,deliver different outcomes, and may require different regulatory considerations. For example, some consensus mechanisms might prioritize speed and efficiency, while others might prioritize security. Quicker methods of forming consensus might be suited for situations where there are fewer participants or they can trust each other, i.e. CBDC, whereas a more decentralized, secure mechanism is more suited for cross border remittances, like Bitcoin.

i. Typical Profile of Network Participant in Public Blockchains

Regardless of the platform, or the consensus mechanism, the participants in public VDAs can be broadly categorized up into asset holders – those who hold assets in a wallet, private or custodial –, nodes – participants maintaining the historical ledger and looking for fraudulent transactions based on the agreed upon state of the network at the time –, and miners, or validators – nodes or special participants that change the agreed upon state of the ledger.

ii. Types of Consensus Mechanisms

Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated PoS (DPoS) are some of the more popular consensus mechanisms in public blockchains like Bitcoin or Ethereum, while practical Byzantine Fault Tolerance (pBFT), Istanbul BFT (iBFT), and federated BFT (fBFT) are popular in private blockchains. Several larger technology entities are actively developing or have created consensus mechanisms that have the potential to be used in products and services that could become systemic[2] quickly—for example, DiemBFT.

Proof-of-Work, or PoW was the consensus mechanism developed for Bitcoin, was the first broadly successful consensus mechanism for digital assets developed, that solves the consensus problem through an activity dubbed ‘mining’. Transactions are organized into ‘blocks’ , with the entire history of transactions forming a ‘blockchain’. Some network participants participate in a race to add new transactions to the Bitcoin ledger (i.e. a new ‘block’ of transactions) by solving a complicated mathematical problem. In the simplest terms, this math problem is finding a number associated with a new block based on all of the previ- ous blocks – meaning that if fraud had to occur, a dishonest participant would have to rewrite the entire chain of transactions and add a new block before anyone else does (known as a 51% attack). PoW has proven incredibly robust and successful, but does have a few significant drawbacks – primarily its limited throughput and high sunk cost associated with mining operations.

3.Deep-dive into the Proof-of-Stake consensus mechanisms

In a PoS consensus mechanism, an algorithm randomly selects validators (analogous to miners for PoW) for block creation based on the amount that holders ‘stake’, or lock in the network, from their own assets. First a proposer is selected, then a proposed block, and then validation of the proposed block. Individuals or entities with larger staked amounts of the native token have a greater chance of being selected. A commonly used analogy is to lotteries – even though everyone who buys a ticket has a chance of winning and selection is random, those with the most tickets have the greatest odds of winning (note, that this is only for which validator gets selected to validate a block).

PoS improves on some perceived weaknesses in PoW consensus mechanisms, such as low throughput and the need for increasingly intensive computation power, while preserving network security. This relatively lower cost of maintaining the ledger (the equivalent of mining in Bitcoin) also means a lower need to issue many new coins to incentivize participation in validation of the network. It also limits the risks of a 51 percent attack (as described above, where an entirely new chain of transactions is created). Although it is prohibitively difficult and expensive for anyone to carry out a successful 51 percent attack in a large[5] PoW-based platform like Bitcoin, it is even more expensive to do it in a large PoS-based one.

The superior throughput makes the PoS model much more useful in certain financial services contexts, like facilitating payments or running complex contracts as is the case on platforms like Ethereum or Solana. However, to increase the chances of being selected, validators might vote on multiple blocks — even those whose underlying information might be incorrect, creating risks around broader market integrity.

\While voting on multiple blocks maximizes the chances of nodes receiving a reward through transaction fees, it also increases the risks of multiple forks, which can create uncertainty with settlement finality; the infamous “Nothing at Stake” problem. Newer models of PoS seek to solve it by creating monetary penalties for the work validators do on blocks that do not get included in the chain – the latest version of Ethereum uses a mechanism called ‘slashing’ that is similar to this.

Because ownership has a direct correlation to the amount that can be staked and consequently receiving rewards for validating the network, PoS consensus mechanisms can theoretically create a community which continuously results in a concentration of wealth and governance. This scenario can lead to those participants with smaller holdings exiting the network if they aren’t able to generate rewards. In effect, PoS consensus mechanisms could create conditions where the network isn’t inclusive, as certain members (that is, those with larger holdings) are more likely to be favored over others, increasing the potential for centralization.

Even in larger PoS networks, the potential for validators to form cartels can lead to concerns around centralization, while exchanges and wallet providers could also theoretically exercise disproportionate control given their large holdings. PoS is also inefficient in its use of network native resources. Given that VDAs might be locked up for staking purposes, PoS removes the ability to transfer or spend a proportion of the total number of VDAs in circulation. A liquidity shortage could arise if token holders hoard their tokens to increase their chance of being selected as validators; this act would lower the speespeed of transaction rates, and the network could suffer from the lack of circulation.

2.3. Smart Contracts[9]

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met. For instance, smart contracts can allow the functionality to make conditional payments, contingent upon the completion of a task. A party can be required to escrow a deposit as a condition of participating in some process, and the return of that deposit, in part or in whole, can be conditioned on the party performing certain required steps, as long as compliance can be checked by a computation.
Coupled with the other components of Web3, smart contracts promise transformative potential
. They enable parties to define the behavior of a virtual actor in code, and have the VDA based consensus system enforce that the virtual actor behaves according to its code[10] Therefore, such contracts exclude human intervention from the equation. Once a condition[5] is met, the contract is executed immediately, automatically. Since these contracts exclude intermediaries, they are cost efficient and secure as well.

2.4. DeFi (Decentralised Finance)

Building on the foundations laid by blockchains, VDAs, and smart contracts, DeFi allows open access to services such as saving, lending, borrowing, and exchange of VDAs. Given that DeFI applications are based on the core concept of decentralisation, they are typically permanent and cannot be changed or manipulated by malicious actors.[11] They are also open, so any computer can participate in the network, and[6] access is not limited to a single or pre-defined group. [12]

Another core feature of DeFi is that it allows users to always retain complete control over their assets. Further, DeFI platforms are inherently auditable. The software is always source-available or open source, all underlying code is perpetually available for review, and all associated capital is open for audit. [13]
DeFi allows the potential for low cost, nearly instantaneous, borderless, peer-to-peer transfers of actual value. Access to DeFi is not subject to the business hours of mainstream financial institutions and has low barriers to entry.[14] This opens extraordinary opportunities to help underserved communities to access secure financial services. The details of this section are discussed in **Chapter 6.**

3. The Web3 Stakeholders StacK

The Web3 Stakeholders' Stack is a framework for understanding the various layers of technology and participants involved in the development and implementation of Web3. The stack consists of seven layers, each of which plays a unique role in the ecosystem.

3.1. Infrastructure

The infrastructure or protocol layer is the foundation of the Web3 Stakeholders' stack. It consists of the underlying technological infrastructure that enables the functioning of decentralized networks and applications. This layer includes various components such as distributed ledgers, peer-to-peer networking protocols, and consensus algorithms, among others. The infrastructure layer is critical for the success of Web3 technologies because it provides the necessary trust, security, and scalability required for decentralized applications to operate.

Decentralized networks rely on a distributed infrastructure to ensure that data is stored securely and\can be accessed by users in a timely and reliable manner. Some of the popular infrastructure technologies used in Web3 include blockchain networks such as Bitcoin, Ethereum, Polkadot, and Cardano, which provide the necessary smart contract functionality for decentralized applications. Other alternative technologies in this layer include InterPlanetary File System (IPFS), a distributed file system that allows for the storage and retrieval of data across a decentralized network, and Whisper, a peer-to-peer messaging protocol that enables secure
communication between decentralized applications.

3.2. Wallets & Other 2nd Level Infrastructure

The platform layer of the Web3 Stakeholders' stack is where the actual building blocks of Web3 are developed. This layer includes the platforms that are necessary to facilitate communication, transactions, and interactions within the Web3 ecosystem. Platforms in this layer are the tools and frameworks that are built on top of these protocols. These platforms enable developers to build decentralized applications (dApps) that interact with the blockchain and other Web3 protocols. Metamask [5]is a good example of an entity in this category. The platform layer of the Web3 Stakeholders' stack is crucial for the development of Web3 as it provides the foundation upon which all other layers can be built.

3.3. Middleware

The middleware layer is the third layer of the Web3 Stakeholders' stack. It consists of software tools and services that facilitate the interaction between applications and protocols. The middleware layer provides developers with APIs, SDKs, and other tools to build dApps that can interact with various blockchain networks[6] Middleware services include functions such as user authentication, identity management, data storage, and messaging services. They also offer tools for integrating with multiple blockchains, simplifying the development process for dApps.

Middleware is important for Web3 development because it provides a layer of abstraction between applications and the underlying blockchain protocols. This allows developers to focus on building applications without having to worry about the intricacies of blockchain technology. Middleware is also crucial for creating interoperability between different blockchain networks. By providing tools for cross-chain communication, middleware can help to build a more connected and interoperable Web3 ecosystem.

3.4. Applications and Services

The Applications and Services layer is arguably the most significant layer of the Web3 Stakeholders' stack. It consists of the actual end-user applications and services that utilize the underlying infrastructure, protocols, and middleware layers to provide decentralized and blockchain-based solutions. This layer includes various types of dApps, such as finance, gaming, social media, and other innovative applications. This layer includes applications like Uniswamp and DYDX.

DApps are built on blockchain platforms and use smart contracts to enable trustless, decentralized transactions between users. They offer various benefits such as decentralization, security, privacy, and transparency to users. These applications and services are designed to enable users to interact with the blockchain and the Web3 ecosystem in a user-friendly and intuitive manner. The Applications and Services layer is critical to the success of Web3 as it is the layer that interacts with end-users and solves their problems, or provides the actual service. This layer is expected to revolutionize the way we use technology, and it holds immense potential for disrupting traditional business models and creating new ones.

3.5. Users and Communities

The Users and Commodities layer is one of the bottom layers of the Web3 Stakeholders' stack, and it represents the actual users and commodities that are being used in the Web3 ecosystem. This layer includes individuals, organizations, and other entities that are participating in the Web3 ecosystem as well as the assets and commodities that are being traded or used.

The Users and Commodities layer plays a crucial role in the Web3 ecosystem as it drives demand and usage for the underlying infrastructure, protocols, middleware, and applications. Without users and commodities, the Web3 ecosystem would not exist, and it is the responsibility of the other layers to provide services and applications that cater to the needs of the users. The Users and Commodities layer represents a significant shift from the traditional centralized systems, where users had to rely on centralized authorities and intermediaries for their transactions.In the Web3 ecosystem, users have more control over their assets, data, and identities, and they can transact directly with other users without rel5ying on intermediaries.

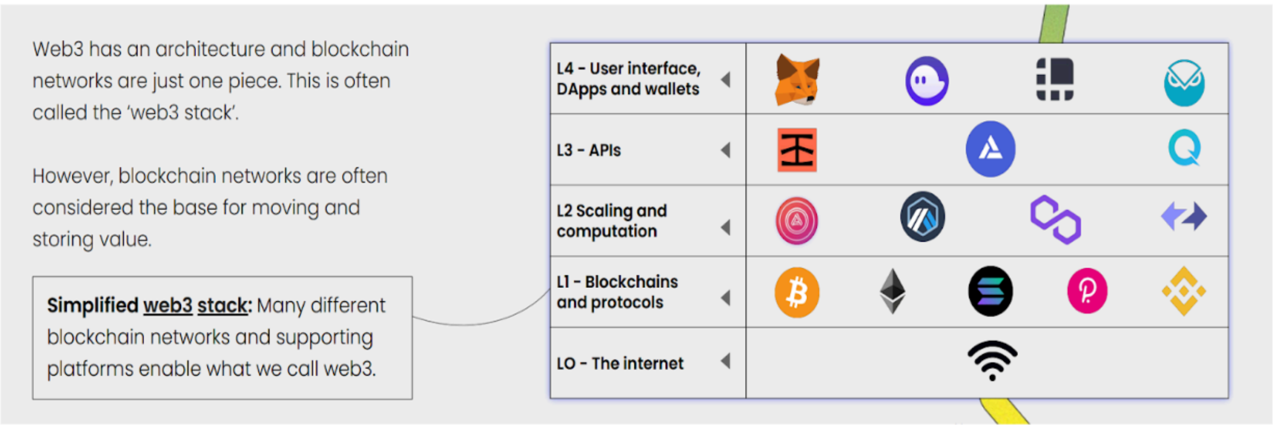
3.6. Governance and Coordination

The Governance and Coordination layer is another bottom layer of the Web3 Stakeholders' stack. This layer is responsible for creating and managing decentralized governance models for Web3 networks and applications. It consists of organizations, individuals, and communities who oversee and govern the use of Web3 technologies and ensure that they align with the goals and values of the ecosystem. This layer includes decentralized autonomous organizations (DAOs) that use blockchain-based governance models to make decisions collectively, without relying on6 centralized authorities. They use smart contracts and voting mechanisms to ensure transparency, accountability, and fairness in decision-making.

The Governance and Coordination layer is crucial to the success of Web3, as it ensures that the ecosystem evolves in a decentralized and democratic manner, with the interests of all stakeholders taken into account. It promotes open participation and collaboration, enabling a diverse set of voices to contribute to the development of Web3 technologies and applications.

3.7. Legal and Regulatory

The Legal and Regulatory layer is the bottommost layer of the Web3 Stakeholders' stack. It is a critical layer that ensures the legality and compliance of the Web3 ecosystem with existing laws and regulations. As the Web3 ecosystem evolves, it is likely to face various legal and regulatory challenges, such as issues related to privacy, security, consumer protection, and intellectual property. The Legal and Regulatory layer seeks to address these challenges by developing legal frameworks, policies, and guidelines that enable the responsible and ethical use of blockchain technology. The layer includes legal and regulatory experts, policymakers, and industry associations working together to shape the legal landscape of Web3. These stakeholders create a supportive environment for blockchain and Web3 innovation while ensuring that it aligns with existing legal and regulatory frameworks. This Web3 Stakeholders' Stack provides a useful framework for understanding the various layers of technology and participants involved in the development and implementation of Web3. By understanding each layer and the interactions between them, we can gain a deeper understanding of the ecosystem and the potential impact of Web3 on various industries and communities.



Web3 has an architecture and blockchain networks are just one piece. This is often called the 'web3 stack'.

However, blockchain networks are often considered the base for moving and storing value.

Simplified web3 stack: Many different blockchain networks and supporting platforms enable what we call web3.

L4 - User interface, DApps and wallets

L3 - APIs

L2 Scaling and computation

L1 - Blockchains and protocols

LO - The internet

Source: Hong Kong Institute for Monetary and Financial Research HKIMR Applied Research Report No.1/2024 [15]

2.THE VDA ECOSYSTEM

Key Themes:

This section examines some fundamental concepts relating to the larger VDA ecosystem. In particular, it discusses the importance of VDA trading in creating value and fostering the growth of blockchain projects.

1. The role of intermediaries in today's digital era

Today, nearly all digital transactions are conducted through intermediaries. For instance, if A wishes to relay a message to B, they may do so through email hosted by the likes of Gmail and Yahoo; or speak over the phone using platforms like Whatsapp and Facetime; or communicate over social media through platforms like Facebook or Twitter. The state of play leads users to place heavy reliance on the proprietary solutions offered by these mostly opaque, profit-driven intermediaries. This reliance raises several fundamental challenges. Users give up privacy and valuable data. These platforms that benefit from multi-sided network effects, also exercise a large degree of power over users and third-party complements like developers. They are involved in a zero-sum game. Since they leverage proprietary algorithms and codes, they create the rules and hold the power to change them. These changes may often be detrimental to users and third-parties, while benefiting the platform's own pursuit of profits. The existing degree of centralisation therefore is not only economically inefficient, but it also hampers innovation and competition.

2. Fundamentals of the VDA industry

Just the way public companies have tradable assets which are offered to retail investors in the form of equity in the company, which allows them to partake in the company's governance decisions, en public blockchains have tradable assets in the form of VDAs, which are at the core of every public blockchain ecosystem.

Similar to public companies, public blockchain ecosystems too solve real world problems for users.
For example, the Ethereum blockchain enabled millions of participants access to collateralized lending in the form of Decentralized Finance (DeFi) by simply locking their ETH holdings in smart contracts. Once they provide their ETH as collateral, they receive liquidity in native tokens, which could be used in various dApps for gaming, trading, minting NFT's, etc. Just as stock market listed companies have underlying fundamentals, ETH too has fundamentals like daily transaction volumes, total value locked in DeFi, number of nodes running the network (which is a sign of its health), number of active wallets (transacting users) on the network, and so on.
Each of these fundamentals are verifiable on-chain records available publicly in real-time. As these fundamental indicators keep growing in strength, the price of the token also increases.

3. The importance of trading in the VDA economy

Let’s first break down VDAs into broad categories that have been adopted by many financial regulators globally.

The categories of such tokens can be distinguished are as follows:

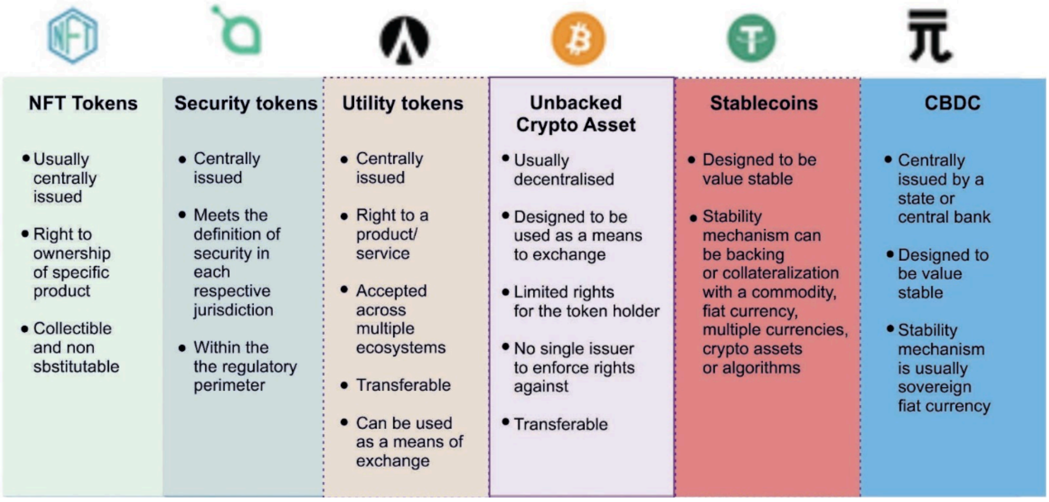
- NFTs issued with utility and participating rights in the network
- Security tokens represent securities, as defined by the relevant jurisdiction (e.g. a share in a company).
- Utility tokens provide digital access to an application or a service (e.g. a software license or a voucher).
- Unbacked Crypto Asset like Bitcoin that is completely decentralised and works as an unbiased and trustless settlement mechanism and works as a payment token is a complementary currency for a specific service, for example a blockchain-based distributed network for computing power: The only way to access the network is by using the token.
- Stablecoins are VDAs backed 1:1 by fiat currencies
- CBDC central bank digital currency issued by sovereign states

The most common use of issuing tokens for companies is to do token sales as an alternative means to raise capital. This process is known as an initial coin offering (ICO) in the case of utility tokens.

Similar to initial public offerings, token issuance theoretically offer a number of advantages:

- Tokens are immediately transferable and can be traded 24/7 on secondary markets.
- Clearing and settlement is a matter of a few minutes at most.
- Tokens can be held personally, i.e. brokers and custody accounts are no longer required.
- The underlying blockchain ensures the transparency of all transactions.

The end users gain only if there is sufficient distribution and activity in liquid and efficient secondary markets. Without trading activity and effects of the secondary markets on prices the upside for project creators and early supporters gets severely restrict- ed. Similar to speculation in existing capital markets, secondary markets in VDAs too are fueled by speculation, however, contrary to popular belief there are several key factors that drive prices of these tokens in the secondary prices and not just plain speculation.



NFT Tokens	Security tokens	Utility tokens	Unbacked Crypto Asset	Stablecoins	CBDC
• Usually centrally issued • Right to ownership of specific product • Collectible and non sbstitutable	• Centrally issued • Meets the definition of security in each respective jurisdiction • Within the the regulatory perimeter	• Centrally issued • Right to a product/ service • Accepted across multiple ecosystems • Transferable • Can be used as a means of exchange	• Usually decentralised • Designed to be used as a means to exchange • Limited rights for the token holder • No single issuer to enforce rights against • Transferable	• Designed to be value stable • Stability mechanism can be backing or collateralization with a commodity, fiat currency, multiple currencies, crypto assets or algorithms	• Centrally issued by a state or central bank • Designed to be value stable • Stability mechanism is usually sovereign fiat currency

Some of the key parameters that drive prices of tokens in secondary markets are:

- No of unique wallets
- DAUs, MAUs and other active user metrics
- Network effects in the form of growth in wallet addresses
- Market Cap of the token
- Tokenomics or token distribution mechanics (how many will be reserved for founders, marketing, airdrops, etc)
- Tech and product roadmap
- Partnerships with other ecosystem players that adds value to the network i.e. Partnership with a wallet product that makes token usage easier and can further increase mass adoption
- Founding team credentials
-

In the absence of exchanges and marketplaces that build and drive the secondary markets, some of the mechanisms token issuers use to distribute tokens are airdrops or the free distribution of tokens among users. There are more like promotional events that seek to incentivise the early supporters of token projects.

Outside of exchanges and marketplaces, these secondary markets primarily exist within OTC trading systems.

Furthermore, nation states are racing to become the most sought after destinations for Web3 projects - as is demonstrated by the US, UAE, Australia, and the UK. Post the initial phase of ICOs or Initial Coin Offerings in 2017, which offered new issuance of tokens directly to end users, a new paradigm that sought support from CEXs or Centralised Exchanges emerged, whereby new tokens would only get launched on exchanges - with this format, exchanges would whet the tokens being issued and would co-assume the responsibility of launching quality projects only.

Notable developments in regulation are observed in the case of the UK's FCA, where they look at web3 as opportunities. The Bennett Institute has discussed the possibility of looking at token sales as adapted versions of the Seed Enterprise Investment Scheme (SEIS), Enterprise Investment Scheme (EIS), and Enterprise Management Incentives scheme (EMI) which can in turn serve as a means of increasing the supply of capital and talent available to early-stage web3 ventures. Furthermore, FCA encourages DeFi projects to apply for the FCA’s Regulatory Sandbox to help the UK consolidate its position as a global fintech centre. Meanwhile artists, musicians, and video content creators would benefit from clearer guidance on and revisions to the tax treatment of NFTs.

Therefore, it is clear that in the absence of a highly liquid and efficient secondary market for tokens, most token projects will fail to sustain growth after raising funds from investors. Furthermore, the early investors who took high risks to back the project will not be incentivised to take risks to drive the use cases driven by these token projects and the flywheel of innovation from Web3 that looks to solve complex challenges will lose momentum and in turn accelerate the P2P economy driven by decentralised exchanges for achieving the same purpose. It is legitimate businesses, regulators and law enforcement agencies that will lose out on the critical pieces of information, which are enabled by Centralised Exchanges (CEXs), that can help build a win-win situation for all.

3.MARKET PLAYERS IN THE VDA ECOSYSTEM

Key Themes:

This section takes a deep dive into the market players within the VDA ecosystem. In particular, it examines the anatomy of VDA exchanges and discusses how they enable VDA trades. It goes on to examine the market players who perform custodial functions in the VDA ecosystem by discussing the different kinds of wallet service providers.

1. Exchanges and trading venues

1.1. Background

In any VDA ecosystem there are multiple participants that perform different functions. For instance in the Bitcoin network the participants are:

- **Developers:** a collective of open source contributors who write, audit and evolve the source code for how the network operates and engages with the backbone of the network being the Blockchain Ledger - the core encrypted database that stores all the transactions taking place within the network in a time-ordered manner since day zero till date.
- **Nodes:** a collection of network enthusiasts who secure the network by running machines connected to the network at all times with the primary task of maintaining one copy of the updated ledger each
- **Miners:** a set of incentive driven individuals who invest in ASIC machines to perform the PoW algorithm that forms the final leg of processing a Bitcoin transaction on the Bitcoin network and thereby receiving freshly minted Bitcoin as reward from the network.
- **End Users:** Represented by wallet addresses on the Bitcoin network, these users hold the private keys to their public wallet addresses and can use them to sign and broadcast trans- actions they want, to the blockchain network onto the ledger. In the case of the Bitcoin network the native token for all transactions is Bitcoin (BTC). End users send and receive BTC, and Miners get incentivised by freshly minted BTC upon successfully validating, processing and appending a legitimate transaction onto the Bitcoin blockchain ledger.

Once the VDA network is set into motion by generating the first set of tokens the system runs as follows:

- End User A, signs his wallet with his private key and makes a SEND transaction to End User B’s wallet
- Miners pick up these transactions and start validating them for their own incentive (newly issued Bitcoin tokens)
- Once the transaction is successfully validated all the nodes update their copies of the ledger reflecting the new finality within the system post settlement

Which means that users can pseudonymously transact with each other using VDAs, simply by participating in the above network as an End User (wallet address holder). All users require are an internet connection and a mobile device. No user authentication, no KYC, no identity information is required. Now, based on the above explanation, Virtual Digital Assets were designed to disintermediate financial services, however participating in these networks also turns out to be fairly complex for the masses.

1.2. The role of exchanges

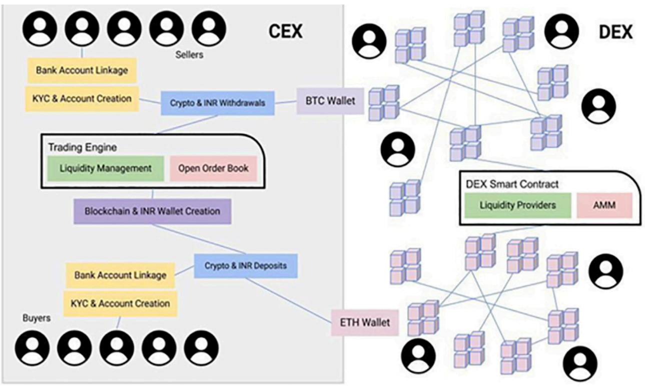
The inherent complexity in dealing directly with VDA networks, made it imminent that new types of centralized entities, such as exchanges (CEXs) and wallet providers would have to emerge in order to abstract out these complexities. Such entities, on one end would themselves plug into the VDA networks as Nodes, and/or End Users and on the other end facilitate users to create user accounts with them. Within these accounts the CEXs would plug into the VDA network on behalf of their users - create, manage and maintain the wallets required for holding and transacting various VDAs, allow the users on their platforms to transact with each other off-chain and then eventually settle the transaction on-chain. They became hugely successful across the globe as they were a sort of aggregator of hundreds of VDA blockchain networks which allowed end users a simple and familiar onboarding interface of creating an online user account.

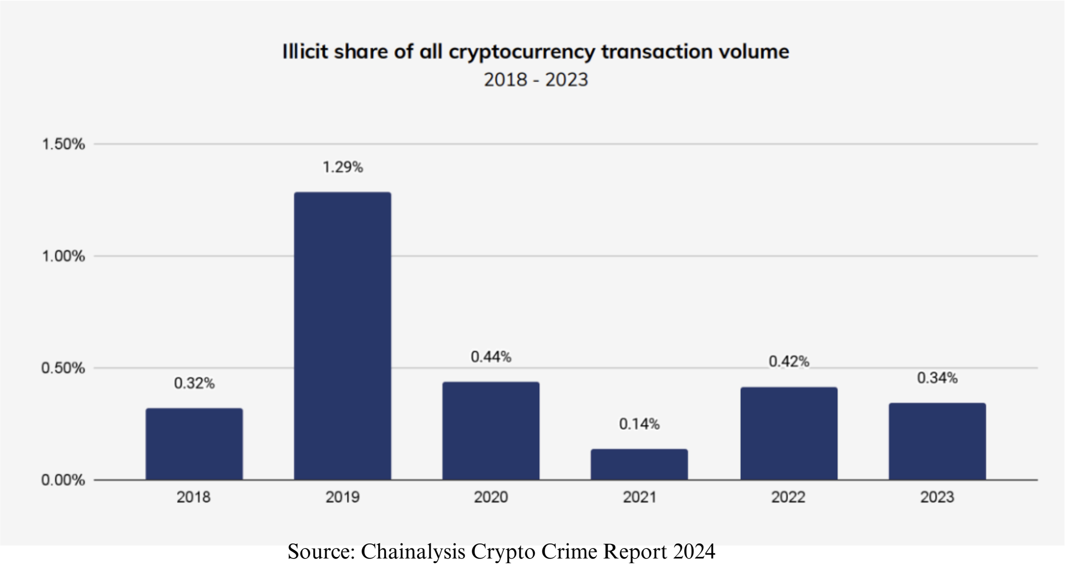
In the absence of a CEX, the user could directly engage with the VDA network and even find means to exchange one VDA to another without creating an account, thereby making absolutely untraceable P2P transactions.

By creating user accounts, the CEX ensures that when they plug a user into the VDA network, they also have his/her identity related information attached to the end user.

Thus, if the user were now to perform any kind of illicit transaction on a VDA network in a P2P manner, the VDA network can be analysed to create a linkage between wallet addresses indulging in illicit transactions and the identity information collected by CEXs. In this manner any movement from the FIAT economy to the VDA economy or back can be traced all the way down to each and every single interaction.

This was corroborated by the August 2016, Bitfinex VDA exchange hack. It announced it had suffered a security breach in 2016 and forensic investigations were initiated. In 2017 small amounts of money began to move out of the single wallet in early 2017 through darknet marketplaces. Finally in February 2022, a New York couple, Ilya Lichtenstein (age 34) and his wife Heather R. Morgan (age 31), were traced using VDA transactions and linkages with centralised exchanges (CEXs) where the missing piece of their identities were facilitated. Both were charged by US federal authorities with conspiring to launder the bitcoin, which was by then worth US$3.6 billion.





Source: Chainalysis Crypto Crime Report 2024

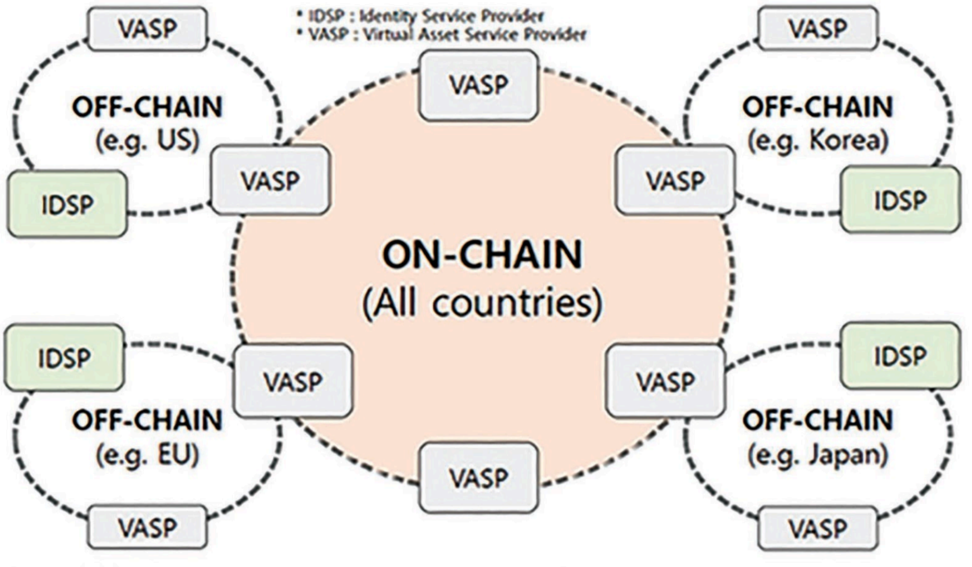
This system of CEX for identity management and on-chain transactions for end-to-end surveillance has ensured that across the world, illicit usage of VDAs continues to reduce, even as the overall volume of VDA usage increases over time. On the basis of forensic analysis and blockchain surveillance tools, Chainalysis in their Crypto Crime Report 2024 revealed that this was indeed a fact and the share of illicit transactions in the overall volume of VDA transactions had fallen, to 0.34% in 2023 from 0.42% in 2022.[16]

Even the FATF explicitly defines exchanges as VASPs, as exchanges are the only source of user KYC data within the VDA ecosystem.
In particular, in October 2018, the FATF adopted two new Glossary definitions—"virtual asset" (VA) and "virtual asset service provider" (VASP)—and updated Recommendation 15 (R. 15)(see Annex A). The objectives of those changes were to further clarify the application of the FATF Standards to VA activities and VASPs in order to ensure a level regulatory playing field for VASPs globally and to assist jurisdictions in mitigating the ML/TF risks associated with VA activities and in protecting the integrity of the global financial system.

The FATF also clarified that the Standards apply to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs.
Therefore, globally it is understood that only exchanges can help in achieving the objective of KYT or Know Your Transaction across cross-border transactions.

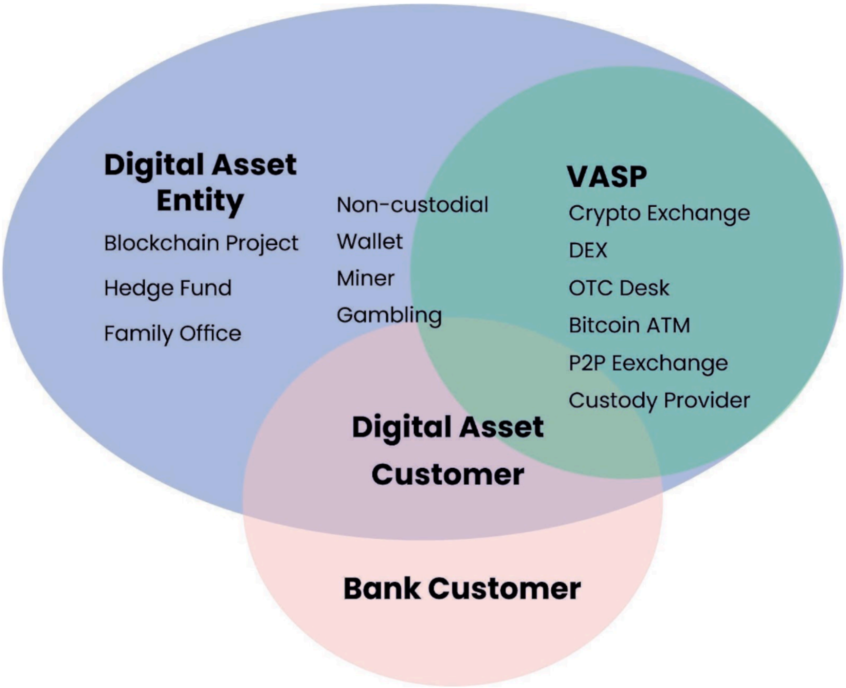
With leaps in technology VASPs can ensure KYC by complying with the Travel Rule with the following objectives:

- Identify counterparty VASPs
- Get accurate originator & beneficiary data with consent
- Ensure this is done with minimal cost and high efficiency using technology
- Perform these in a fully secured, transparent and auditable manner



• OFF-CHAIN : register, update and remove customer identity information only in the same jurisdiction
• ON-CHAIN : share customer identity information with virtual asset service providers in all countries

For a truly successful globally co-operative model, the VASPs in multiple countries will be required to share their massive customer identity information including personal data before cross-border VA transfers. In addition, it is very important for them to prevent tampering with customer identity information, along with ensuring transmission of data in real-time to enable interventions.



On a closing note, within the entire universe of VDAs it is evident that any systems of regulating and surveilling are made possible by building a global collaborative framework between CEXs, the Digital Asset Customer and the Bank Customer. The intersection of these three represent a safe and compliance movement of funds into and out of the traditional economy and the VDA economy. However there needs to be deliberation on data sharing, disclosures and transaction rules to enable enforceability and to build frameworks with dos & donts for cross-border VDA transactions.

2. Wallet service providers

The importance of self-custody wallets has grown tremendously as users explore ways to safeguard their digital assets. The fallout of FTX, the world's second-largest VDA exchange has made self-custody wallets more relevant than ever before. In the case of FTX or any centralized exchange, the private keys of the users are held by centralized entities and as a result, the users risk losing their funds in the case of hacks and bankruptcy threats.

Understanding the difference between custodial (centralized) and non-custodial (decentralized) wallets is crucial as it defines who controls the private keys or passwords to your wallet. To understand private keys, we must first understand what public keys are: Think of a public key as an email address that you give to send and receive emails. The private key is like a password to your email address that is needed to verify the transfer of your digital assets. There is a unique private key associated with every public key also known as the wallet address. The public key and the private key are both required in unison to conduct transactions on the blockchain. One must never share their private keys with others as anyone with a private key can have full control of the funds associated with the public key.

2.1. Custodial wallets

Custodial wallets are run by a centralized organization, such as a VDA exchange. These have some advantages, such as less user responsibility for managing your private keys. However, when a user outsources wallet custody to a centralized company, they are essentially handing over their private keys to that company.

The individual user is not responsible for safeguarding the private key to the wallet and thus relies on the centralized entity to keep the private key secure.

If a user wants to transfer VDA from a custodial wallet, they simply log in with a username and password, enter the public key of the location to which they want to send VDA, and the centralized company enters the private key to complete the transaction.

This results in a very simple solution for the user to perform VDA transactions, but it also introduces an additional layer of risk to user funds as the company has complete control over user assets.

2.2 Non-custodial wallets

Non-custodial or self-custody wallets are the ones where the user maintains full control of their assets. As a user, you control the private keys to your wallet and retain complete ownership at all times. You do not require any permission to send, store and receive your VDA as no central entity can prevent you from conducting transactions using self-custody wallets.With non-custodial wallets, no central party can prevent you from undertaking a transaction. The user controls the private key, and hence these transactions are essentially censorship-resistant. Some central entities in custodial wallets can freeze your VDA holdings, set limits on the amount you can transact and even use your assets for their personal gain as was witnessed in the FTX case.

Security is another important aspect one should consider. With self-custody, there is no single point of failure, and thus provides multiple layers of security to your funds. Self-custody not only provides users with ownership rights but also protects powerful actors from corrupting the network and its participants.

4.CENTRAL BANK DIGITAL CURRENCY

Key Themes:

This section provides a concise overview of Central Bank Digital Currencies (CBDCs), emphasizing their distinction from traditional digital money. CBDCs are a central bank liability used for payments and settlements, with retail CBDCs for public transactions and wholesale CBDCs for interbank use. It highlights the global momentum, with 134 countries exploring CBDCs and several in advanced stages. The section addresses the costs, management, and security challenges of CBDC implementation, their potential to disrupt banking, finance, and payments sectors, and their regulatory requirements. It also discusses economic risks, including privacy concerns and potential impacts on financial stability.

1. What is Digital Currency?

While electronic or digitized money has existed for close to 40 years in various forms, 'digital currency' as it is being discussed today refers to one of the latest iterations. Specifically, digital currency refers to Central Bank Digital Currencies (CBDC) which are a digital form of central bank monies that can be used for payments and settlements. CBDC is also different from digital money held in bank accounts or payment apps. Digital forms of money held in these apps or accounts are a liability of the commercial bank; CBDC is a liability of the central bank. CBDC is usually intermediated, meaning that it is distributed through banks, payment service providers, and digital wallets. Even in this case, CBDC is still a liability of the central bank. Broadly, we can categorize CBDCs into two types retail CBDC (rCBDC) and wholesale CBDC (wCBDC). rCBDC is used by the general public for commercial and peer-to-peer transactions. rCBDC would be used to buy a cup of coffee, for example. wCBDC is used by financial institutions to settle interbank and securities transactions. Its use is comparable to that of interbank transactions with central bank reserves. [17]

1.1 Key Facts on CBDC Market [18]

- 134 countries and currency unions, representing 98% of global GDP, are exploring Central Bank Digital Currencies (CBDCs). This number increased from 35 in May 2020. Currently, 68 countries are in advanced phases of exploration—development, pilot, or launch.
- 19 of the G20 countries are in advanced stages of CBDC development, with 11 in the pilot stage, including Brazil, Japan, India, Australia, South Korea, South Africa, Russia, and Turkey.
- The Bahamas, Jamaica, and Nigeria have fully launched a CBDC. The Eastern Caribbean Currency Union halted DCash due to technical issues and is developing a new pilot.
- There are 36 ongoing CBDC pilots, including the digital euro. The European Central Bank (ECB) is in a 2-year preparation phase, ending in 2025.
- Retail CBDC progress has stalled in the US, with a widening gap between the US and other G7 banks. CBDC development is a topic in the ongoing US presidential campaign.

- There are several multinational or SSB level efforts at interoperable CBDCs, for example, Project Agorá,[19] launched by the Bank for International Settlements (BIS), a group of leading central banks and the Institute of International Finance (IIF), is inviting the private sector to join its exploration of how tokenisation can enhance the functioning of the wholesale cross-border payments.
- Brazil, Russia, India, China, and South Africa are in the pilot phase. New BRICS members like Saudi Arabia, Iran, and the UAE are exploring cross-border wholesale CBDCs. BRICS promotes developing an alternate payment system to the dollar.
- China's digital yuan (e-CNY) reaches 260 million wallets across 25 cities as of 2024. It has been used in various settings since 2022. In 2024, the focus is on optimizing overseas tourist use and expanding cross-border applications.

Other countries[20] have not been as successful, for example the e-Naira was not successful after launching in October 2022,[21] despite being released in Nigeria; a country full of crypto-curious investors and with paper Naira notes in short supply. In fact, even in China multiple media reports suggest that adoption has actually been low. [22] [23]

2. What Will Be Its Cost of Implementation?

The cost of implementing a CBDC can be substantial, involving the development of technology infrastructure, cybersecurity measures, legal frameworks, and public awareness campaigns. Specific costs vary by country and complexity of the system. The exact cost depends on the scale and underlying model. In their seminal research on the topic, the Central Banks of Canada (BOC), England[25] (BOE), and Singapore (MAS) lay out three separate models for CBDCs in 2018, the first two are based on enhancing existing domestic interbank payment systems, while the third specifically involves tokenized forms of central bank liabilities, which is the model that typically represents CBDCs today.

The cost of implementing tokenized central bank liabilities can be considerable; for example the World Bank suggested in 2021 that the third model could be prohibitively expensive for countries with less developed financial markets and digital infrastructure.[26] This view is echoed by other organizations, for example, the BIS found in a 2022 working paper[27] that the cost of implementing a CBDC would likely be considerable, not including additional costs like labor, external software, cyber security, support costs etc. it would take to create an adequate CBDC

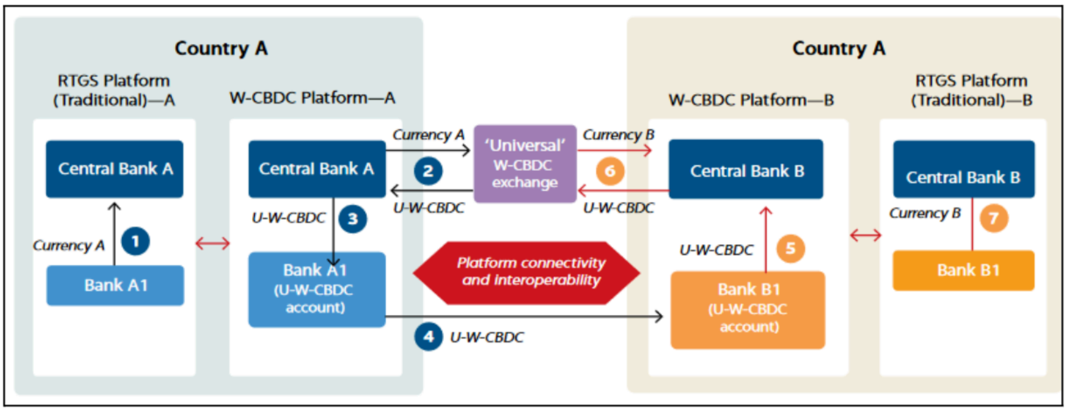
Cross Border CBDC Projects[24]

Project Jura	Project Icebreaker	Digital Euro
D-Cash	Project Agorá	Project Mariana
Project Cedar x /Ubin+	Venus Initiative	Project Helvetia
Project Polaris	Project Rosalind	Project Dunbar
Project Aurum	Project mBridge	Project Mandala
Project Sela	Project Tourbillon	e-CNY

3. How Will It Be Managed at the Back End?

As they represent liabilities of the central bank directly, CBDCs are typically managed by the Central Bank with appropriate technology partners, although distribution takes place through bank/fintech applications. This is different from tokenized deposits,[28] which are based on the liabilities of the bank in questionThe usage and access depends on the model, i.e. rCBDC or wCBDC. In the same vein, various models are being explored to enable interoperability between CBDCs of various countries are being explored (which would require some middleware or independent platform to bridge the two CBDCs). Unlike public blockchains, governance of CBDCs are entirely centralized.

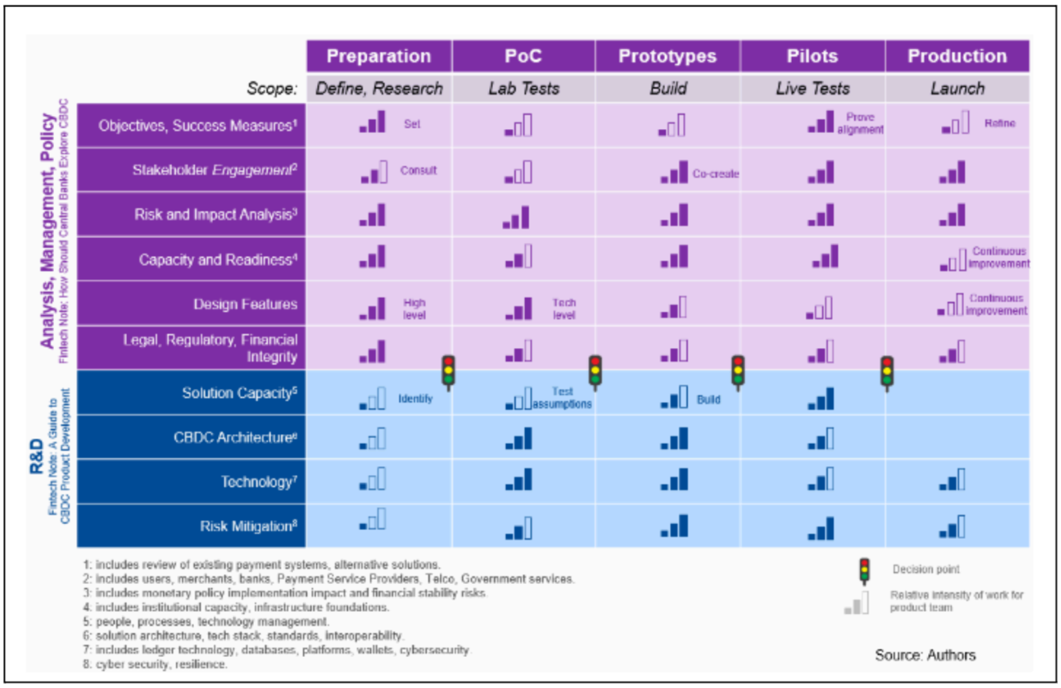
Cross Border CBDC Implementation[29]



In terms of rollout, the IMF, in their CBDC handbook, outline 5 key phases in CBDC development that need to be undertaken by a central bank:

1. **Preparation:** Research trends, monitor technology, and understand implications. Key questions: What do new technologies offer? What are the tradeoffs and risks? What capacity is needed? What are the business impacts?
2. **Proof-of-Concepts:** Lab test assumptions and key features. Key questions: What assumptions need validation? How to test architectures? What technologies support requirements?
3. **Prototypes:** Build CBDC and ecosystem. Key questions: How to integrate architecture and technology? What skills and processes are needed?
4. **Pilots:** Live test with real use cases. Key questions: Does the system work as expected? How to test risk mitigation? Were adoption assumptions correct?
5. **Production:** Launch and operate CBDC. Key questions: How to promote adoption and mitigate risks? How to monitor and implement innovations? How to maintain stability and security?

Overview of CBDC Implementation [30]



		Preparation	PoC	Prototypes	Pilots	Production
	Scope:	*Define, Research*	*Lab Tests*	*Build*	*Live Tests*	*Launch*
Analysis, Management, Policy Fintech Note: How Should Central Banks Explore CBDC	Objectives, Success Measures[1]	▂▄█ Set	▂▯▯	▂▯▯	▂▄█ Prove alignment	▂▯▯ Refine
	Stakeholder *Engagement*[2]	▂▄▯ Consult	▂▯▯	▂▄█ Co-create	▂▄█	▂▄█
	Risk and Impact Analysis[3]	▂▄█	▂▄█	▂▄█	▂▄█	▂▄█
	Capacity and Readiness[4]	▂▄█	▂▄▯	▂▄█	▂▄█	▂▯▯ Continuous improvement
	Design Features	▂▄█ High level	▂▄█ Tech level	▂▄▯	▂▯▯	▂▯▯ Continuous improvement
	Legal, Regulatory, Financial Integrity	▂▄█	▂▄▯	▂▄▯	▂▄▯	▂▄▯
R&D Fintech Note: A Guide to CBDC Product Development	Solution Capacity[5]	▂▯▯ Identify	▂▯▯ Test assumptions	▂▄▯ Build	▂▄█	
	CBDC Architecture[6]	▂▯▯	▂▄█	▂▄█	▂▄▯	
	Technology[7]	▂▯▯	▂▄█	▂▄█	▂▄▯	▂▄▯
	Risk Mitigation[8]	▂▯▯	▂▄▯	▂▄█	▂▄█	▂▄▯

1: includes review of existing payment systems, alternative solutions.
2: includes users, merchants, banks, Payment Service Providers, Telco, Government services.
3: includes monetary policy implementation impact and financial stability risks.
4: includes institutional capacity, infrastructure foundations.
5: people, processes, technology management.
6: solution architecture, tech stack, standards, interoperability.
7: includes ledger technology, databases, platforms, wallets, cybersecurity.
8: cyber security, resilience.

🚦 Decision point

▂▄▯ Relative intensity of work for product team

Source: Authors

4. Security Features

As a digital currency, a CBDC could be vulnerable to the same cyber risks that threaten other digital or electronic payment means. For example, if the CBDC is account-based and authentication is weak, a cyber attack could be perpetrated to obtain profit from fraud. Similarly, if the CBDC does not have sufficient controls, e.g., to separate identity and transaction information, a data leakage could occur, and sensitive and personal data be revealed to criminals or non-authorised third parties. In both cases, the central bank might be accountable for malfunctioning, fraud, or theft. This could imply reputational risks to the central bank that could hinder the adoption of the CBDC. Likewise, a CBDC could be vulnerable to use for money laundering, terrorist financing, and other illegal activities, as has occurred with physical cash and other digital payment systems in the region.[31]

5. Sectors Which Will Be Disrupted Due to Digital Currency

- Several sectors will be impacted, including:
- **Banking and Finance:** Reduced need for physical cash, changes in traditional banking operations if deposits are shifted to CBDC presents the biggest risk.
- **Payments & Fintech:** CBDCs offer some programmability, which in turn can spur enhanced efficiency and reduced transaction costs. Additionally, CBDC is government managed infrastructure, (as opposed to a commercial bank) and has a cost advantage based on just that
- **International Remittances:** Interoperable CBDCs have the potential to reduce international remittance and settlement time by several degrees (i.e. days to minutes)

6. Role of Blockchain in Management of This Currency

Tokenization is commonly conflated with blockchain, although tokenization has always been possible through centralized means.[32] Specifically, tokenization simply refers to using technology to create digital tokens representing an asset (in this case legal tender issued by the Central Bank). While blockchain technology can provide a transparent, immutable ledger for recording transactions, enhancing security and efficiency, it can be prohibitively expensive. Having said that, several CBDC implementations do use blockchain in some way. For example, a large part of the e-naira has been developed using Hyperledger Fabric.[33] However, it is important to point out that blockchain is in no way needed for a CBDC.

7. Inherent Threats/Challenges in a Country Like India

- **Cybersecurity Risks:** Potential for cyber-attacks and data breaches.
- **Regulatory Hurdles:** Establishing comprehensive regulations and ensuring compliance.
- **Economic Impact:** Potential disruptions in the banking sector.

8. How It Would Be Regulated?[34]

The IMF lays out 4 pillars for CBDC regulation:

- **Legal Foundation:** CBDC issuance and distribution require a robust legal basis, involving experts in central banking, monetary law, payment systems law, and financial law. A sound legal framework ensures legal certainty, financial stability, and proper accountability. Legal amendments may be needed to provide CBDC private transactions with legal certainty and strengthen regulatory frameworks. Central banks must assess their legal basis for issuing CBDC and consider reforms based on the design and use cases of CBDC.
- **Financial Integrity:** CBDC arrangements must comply with AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism) standards. Legal frameworks should be updated to address risks, including those posed by new service providers or activities. Effective AML/CFT measures should include customer due diligence, transaction monitoring, record-keeping, and reporting suspicious transactions.
- **Supervisory Considerations:** CBDC systems must adhere to Principles for Financial Market Infrastructures. Clear legal relationships between CBDC holders and the central bank are necessary to reduce risks. Supervisors need adequate capacity and expertise to monitor compliance, and new supervisory models may be required, especially for cross-border usage. Law enforcement and judicial capacity to handle CBDC-related cases is critical, necessitating potential amendments to criminal law frameworks.
- **Technological and Regulatory Adaptations:** CBDC design should consider data security, privacy protection, and compliance with national capital flow management measures. Jurisdictions should assess their private laws to ensure legal certainty and trust in CBDC, facilitating cross-border transactions and informing regulatory considerations. New technologies may enhance the efficiency of AML/CFT measures.

5.STABLECOINS

Key Themes:

This section offers a detailed examination of stablecoins within the Web3 framework. It discusses the definition and the types of stablecoins, emphasizing their role in maintaining value stability in digital transactions.. Additionally, the chapter considers the regulatory landscape, discussing various international regulatory approaches for stablecoins.

1. Stablecoin and its Characteristics

1.1. Definition

Stablecoins are digital tokens designed to maintain a stable value relative to a specific asset or a pool of assets, most often including cash reserves, government securities (T-bills), and other assets and commodities including VDAs, depending on the model implemented. They are often pegged to a currency like the US dollar or to a commodity like gold, and in some cases they are backed by neither but supported through algorithms.[35]The primary purpose of stablecoins is to provide stability in the volatile crypto-asset markets. They enable users to store value, make transactions, develop applications, and leverage the benefits of blockchain technology without experiencing significant price fluctuations. They aim to combine the benefits of digital tokens(such as speed, security, and decentralisation) with the stability of traditional financial assets.

Key aspects of stablecoins include their programmability, operational flexibility, and their potential to complement Central Bank Digital Currencies (CBDCs). Stablecoins can play a crucial role in remittances, and fostering financial innovation.Moreover, stablecoins can revolutionise sectors like peer-to-peer lending, digital asset trading, asset tokenisation, and government disbursement systems.

1.2. Characteristics of Stablecoin :

1.Pegging Mechanism:

- **Fiat-Collateralised Stablecoins**: These are backed by reserves of fiat currency in a bank account. Each coin is typically pegged 1:1 to a fiat currency, such as USD. Examples include Tether (USDT) and USD Coin (USDC).
- **Crypto-Collateralised Stablecoins**: These are backed by reserves of other crypto-assets. They often require over-collateralisation due to the volatility of the collateral. An example is DAI, which is backed by Ethereum and other crypto-assets.
- **Algorithmic Stablecoins**: These are not backed by any collateral but use algorithms and smart contracts to control the supply of the stablecoin, aiming to maintain its peg. Examples include TerraUSD (UST) and Ampleforth (AMPL).

2. Stability:

- **Value Stability:** The primary characteristic is the stable value, often achieved through mechanisms like collateralisation, algorithmic adjustments, or backing by physical assets.

- **Value Stability:** The primary characteristic is the stable value, often achieved through mechanisms like collateralisation, algorithmic adjustments, or backing by physical assets.

3. Transparency:

- **Reserve Audits:** Reputable stablecoins often undergo regular audits to verify the backing reserves, enhancing trust and transparency.
- Smart Contracts: For algorithmic and crypto-collateralised stablecoins, smart contracts on the blockchain provide transparency in the issuance and redemption processes.

4. Liquidity:

- **Ease of Conversion:** Stablecoins should be easily convertible to the pegged asset or other crypto assets, ensuring liquidity in the market.
- **High Trading Volumes:** Frequently traded on multiple exchanges to maintain liquidity and ease of access.

5. Utility:

- **Payments and Remittances:** Used for quick and low-cost cross-border transactions, providing a stable medium of exchange.
- **DeFi Integration:** Widely used in decentralized finance (DeFi) applications for lending, borrowing, and yield farming due to their stability.
- **Store of Value:** Serves as a stable store of value in volatile crypto-asset markets.

Examples of Stablecoins:[36]

1. **Tether (USDT):** Fiat-collateralised, pegged to the US Dollar.
2. **USD Coin (USDC):** Fiat-collateralised, issued by Circle and Coinbase.
3. **DAI:** Crypto-collateralised, pegged to the US Dollar, and managed by the MakerDAO protocol.
4. **TUSD:** is a stablecoin fully backed by the US dollar and developed by Trust Token.
5. **BUSD:** is a 1:1 USD-backed stablecoin approved by the New York State Department of Financial Services (NYDFS).
6. **Paxos Standard (PAX):** Fiat-collateralised, regulated by the New York State Department of Financial Services (NYDFS).

Stablecoins play a crucial role in the crypto-asset ecosystem by providing stability and reliability, enabling broader adoption and integration into various financial services and applications.

2. Benefits of Stablecoin

1. **Reduced Volatility:**
   - **Stable Value:** Stablecoins are designed to maintain a stable value relative to a fiat currency or another asset. This stability reduces the price volatility commonly associated with other crypto-assets like Bitcoin or Ethereum.
   - **Predictability:** Users and businesses can transact with confidence, knowing that the value of stablecoins will not fluctuate drastically over short periods, which is crucial for everyday transactions and financial planning.

2. Enhanced Liquidity:

- **Market Accessibility:** Stablecoins are widely traded on crypto-assets exchanges, providing high liquidity compared to many traditional crypto-assets.
- **24/7 Availability:** Unlike fiat currencies that are subject to banking hours and holidays, stablecoins facilitate continuous trading and transactions globally, enhancing liquidity and accessibility.

3. Easier Integration into Digital Economies:

- **Cross-Border Transactions:** Stablecoins facilitate fast, low-cost cross-border transactions without the need for traditional banking intermediaries. This capability is particularly beneficial in regions with limited banking infrastructure.
- **Digital Payments:** They serve as efficient mediums of exchange within digital ecosystems, such as decentralized finance (DeFi) applications, where speed and cost-effectiveness are critical.
- **Smart Contract Use:** Stablecoins can be integrated into smart contracts on blockchain platforms like Ethereum, enabling programmable transactions such as automated payments and complex financial agreements.

4. Financial Inclusion:

- **Access to Banking Services:** Stablecoins provide access to financial services for individuals and businesses in underserved or unbanked regions, where traditional banking services may be inaccessible or costly.
- **Lower Transaction Costs:** Compared to traditional banking systems, stablecoins often offer lower transaction fees, making them more affordable for small-scale transactions and remittances.

- **Regulatory Transparency:**
  - **Audits and Transparency:** Reputable stablecoins undergo regular audits of their reserves and operations, providing transparency to users and regulators alike, which is essential for maintaining trust and stability.

5. Hedging and Risk Management:

- **Risk Mitigation:** Businesses and individuals can use stablecoins to hedge against volatility in other crypto-assets or traditional assets, reducing overall portfolio risk.
- **Stable Investment Vehicles:** Some stablecoins offer yield-generating opportunities through lending protocols in DeFi, providing additional income streams while maintaining stability.

Overall, stablecoins play a pivotal role in bridging the gap between traditional financial systems and blockchain-based innovations, offering stability, liquidity, and regulatory compliance essential for broader adoption and integration into digital economies worldwide.

3. Global Regulatory Landscape of Stablecoins

The regulation of stablecoins varies significantly across jurisdictions, reflecting different approaches to addressing the risks and benefits associated with these digital assets.

3.1.United States

In the U.S., the regulatory landscape for stablecoins remains fragmented and uncertain. Currently, there is no comprehensive federal framework specifically for stablecoins, leading to a patchwork of state regulations.

- **State-Level Regulation:** States, like New York, have implemented specific regulations for stablecoin issuers. The New York Department of Financial Services (NYDFS) has issued guidance requiring stablecoin issuers to maintain adequate reserves and provide transparency regarding their operations.
- **Federal Legislative Efforts:** There are ongoing discussions in Congress regarding potential federal regulations for stablecoins. The Clarity for Payment Stablecoins Act aims to create a regulatory framework similar to traditional financial services. However, progress has been slow due to political gridlock.
- **Regulatory Oversight:** Non-bank stablecoin issuers may be classified as commodities or securities, depending on their structure and function. The Financial Stability Oversight Council (FSOC) may also intervene if stablecoins are deemed a systemic risk.

3.2.United Kingdom

The UK is in the process of developing a regulatory framework for stablecoins, with the Bank of England and the Financial Conduct Authority (FCA) taking the lead.

- **Regulatory Framework:** The UK government has proposed regulations that would classify stablecoins as a form of electronic money (e-money). This framework would require issuers to obtain licenses and adhere to strict consumer protection and financial stability standards.
- **Systemic Risk Assessment:** The Bank of England is particularly focused on assessing the risks posed by large stablecoins that could impact the broader financial system. This includes evaluating their potential to disrupt payment systems.

3.3. Singapore

Singapore has established a clear regulatory framework for stablecoins under its Payment Services Act (PSA).

- **Licensing Requirements:** Stablecoin issuers must obtain a license to operate, ensuring compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.
- The Monetary Authority of Singapore (MAS) announced a regulatory framework for single-currency stablecoins (SCS) pegged to the Singapore Dollar or any G10 currency, issued in Singapore. This framework mandates requirements for value stability, capital maintenance, redemption at par, and disclosures, ensuring stablecoins serve as a reliable medium of exchange. Only compliant issuers can label their stablecoins as "MAS-regulated stablecoins," distinguishing them from unregulated tokens.[37]

3.4. Hong Kong

Hong Kong is also moving towards a regulatory framework for stablecoins, with the Hong Kong Monetary Authority (HKMA) leading the charge.

- **Consultation and Guidelines:** The HKMA has conducted consultations on the regulatory treatment of stablecoins, focusing on issues such as consumer protection, risk management, and the potential for systemic risk.
- **Licensing Framework:** Similar to Singapore, Hong Kong is expected to implement licensing requirements for stablecoin issuers, ensuring they meet regulatory standards.

3.5. United Arab Emirates

The UAE has taken proactive steps to regulate stablecoins through its Financial Services Regulatory Authority (FSRA), Central Bank of UAE (CBUAE), Dubai International Financial Corporation (DIFC) and Abu Dhabi Global Market (ADGM).

- **Comprehensive Framework:** The FSRA has established a comprehensive regulatory framework for digital assets, including stablecoins. This framework includes licensing requirements, AML/CTF obligations, and consumer protection measures.
- **Innovation and Growth:** The UAE aims to position itself as a global hub for digital assets, encouraging innovation while ensuring regulatory compliance.

3.6.European Union

- The EU is implementing the Markets in Crypto-Assets (MiCA) regulation, which will significantly impact the regulation of stablecoins.
- **Comprehensive Regulation:** MiCA will provide a comprehensive regulatory framework for all crypto-assets, including stablecoins. It requires issuers to maintain adequate reserves, ensure the redemption rights of token holders, and safeguard assets.
- **Implementation Timeline:** The MiCA regulation is expected to come into force in July 2024, marking a significant step towards harmonising the regulatory landscape for stablecoins across EU member states.

The regulation of stablecoins is evolving rapidly across the globe, with different jurisdictions adopting varying approaches. While the U.S. continues to grapple with a fragmented regulatory landscape, countries like Singapore and the UAE are leading with clear frameworks that promote innovation while ensuring consumer protection. The EU's MiCA regulation represents a significant step towards harmonising regulations across member states. As stablecoins continue to gain traction, the need for comprehensive and coherent regulatory frameworks will be paramount to address the associated risks and foster a secure environment for their use.

6.DECENTRALISED FINANCE (DEFI)

Key Themes:

This section provides a comprehensive overview of decentralized finance (DeFi) within the Web3 landscape. It explores DeFi's definition, applications, and benefits, such as decentralized decision-making, open innovation, and financial inclusion. It also addresses the regulatory challenges and international approaches to DeFi regulation

1. DeFi and its Applications

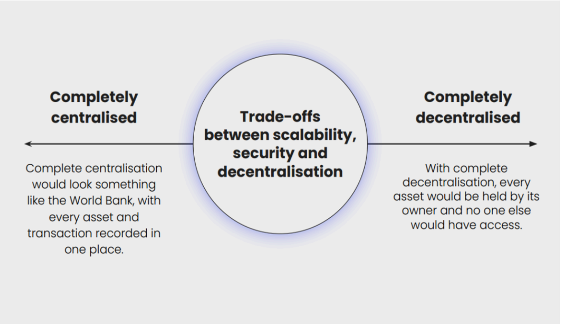
1.1. Definition and Relevance

DeFi is an ecosystem of decentralized applications (dApps) with financial functionalities built on blockchain technology. It enables peer-to-peer interactions without intermediaries through smart contracts, which are self-executing contracts where the terms are directly written into code. DeFi operates on decentralized networks, allowing users to access financial services in an open, transparent, and efficient manner.

DeFi represents a fundamental shift from traditional finance (TradFi) by removing the need for centralized entities such as banks, brokers, and exchanges. Instead, financial transactions are executed and recorded on a blockchain, which is a distributed ledger technology. This decentralization ensures that no single entity has control over the entire system, reducing the risk of fraud and increasing transparency.

The ethos of DeFi is rooted in decentralization across three main dimensions:

- **Decentralized Record-Keeping:** Every node in the network keeps a copy of the ledger, eliminating the risk of inaccurate or fraudulent records at a single point.
- **Decentralized Governance:** Decision-making is transferred from centralized institutions to a broader group of stakeholders, often through DAOs.
- **Decentralized Risk-Taking:** Financial risks are distributed among users rather than being concentrated in a single institution.


Completely centralised
Complete centralisation would look something like the World Bank, with every asset and transaction recorded in one place.
Trade-offs between scalability, security and decentralisation
Completely decentralised
With complete decentralisation, every asset would be held by its owner and no one else would have access.

Source: Hong Kong Institute for Monetary and Financial Research HKIMR Applied Research Report No.1/2024[38]

1.2. Potential Benefits

The innovative features of DeFi offer several potential benefits:

- **Decentralized Decision-Making and Control:** Governance through Decentralized Autonomous Organizations (DAOs) allows token holders to participate in management decisions. DAOs democratize the control of financial services, enabling a more equitable and transparent decision-making process.

- **Open Innovation:** The interoperability of smart contracts enables the rapid development of new products and solutions. Composability allows developers to combine different DeFi protocols like building blocks to create novel financial products and services tailored to specific market needs.
- **Reduced Transaction Time:** Tokenized securities can achieve instant settlement, enhancing operational efficiency and reducing counterparty risk. Traditional financial systems often require several days to settle transactions (T+1 or T+2), whereas DeFi can offer near-instantaneous atomic settlement.
- **Greater Financial Inclusion:** Permissionless access allows any consumer to use DeFi protocols without restriction. This accessibility can help underbanked and unbanked populations gain access to financial services that were previously unavailable to them.
- **Monitorable Financial Activity:** The transparency of blockchain transactions allows all stakeholders to understand the risks and mechanisms of DeFi protocols. This transparency can help mitigate fraud and build trust among users.
- **Cost Efficiency:** By eliminating intermediaries, DeFi can reduce the costs associated with financial transactions. Lower transaction fees can make financial services more affordable for users.

.3. Main Applications

DeFi replicates many traditional financial activities and introduces novel features. Key categories include:

- Exchanges: Decentralized exchanges (DEX) allow trading of crypto-assets without central counterparts. DEXs like Uniswap and SushiSwap enable users to trade directly from their wallets without the need for a centralized exchange, reducing the risk of hacks and improving privacy.
- **Borrowing and Lending:** DeFi protocols enable interest-earning deposits and borrowing without credit assessments. Platforms like Aave and Compound allow users to lend their crypto-assets to earn interest or borrow assets by providing collateral, often with more favorable terms than traditional financial institutions.
- **Derivatives:** Users can create and trade crypto-asset derivatives. DeFi platforms like Synthetix facilitate the creation of synthetic assets that track the value of real-world assets, providing new opportunities for hedging and speculation.
- **Insurance:** DeFi insurance protocols allow hedging against risks related to crypto-assets. Nexus Mutual, for example, provides insurance against smart contract failures, exchange hacks, and other risks specific to the crypto ecosystem.
- **Asset Management:** Protocols offer automated investment strategies and reallocation to optimize returns. DeFi asset management platforms like Yearn.finance automatically move users' funds between different DeFi protocols to maximize yields.
- **Payments:** DeFi can facilitate cross-border payments with lower fees and faster settlement times compared to traditional payment systems. Stablecoins, such as USDC and DAI, are often used in DeFi for their price stability and ease of transfer.

1.4. Innovations in DeFi

Innovative features unique to DeFi include:

- **Automated Market Makers (AMMs)**: AMMs maintain liquidity in exchanges through liquidity pools and algorithmically determined exchange rates. Liquidity providers deposit pairs of tokens into pools, and the AMM uses a mathematical formula to price trades, ensuring continuous liquidity without the need for a traditional order book.

- **Flash Loans:** Instant loans that require repayment within the same transaction, facilitating arbitrage opportunities without collateral. Flash loans allow users to borrow large amounts of funds for short periods to exploit price discrepancies across markets, provided they can repay the loan within the same transaction block.
- **Liquid Staking:** Enables earning rewards from staking while retaining liquidity through staked tokens. Liquid staking protocols issue staked tokens that represent a claim on the underlying staked assets, allowing users to trade or use these tokens in other DeFi applications while still earning staking rewards.

2. Regulatory Challenges and International Approaches

The rapid evolution and international nature of DeFi present several regulatory challenges that require a nuanced and coordinated response from financial authorities around the world. This section explores the primary regulatory challenges associated with DeFi, as well as various international approaches to addressing these challenges.

2.1. Regulatory Challenges

1. **Accountability:** One of the foremost regulatory challenges is identifying accountable parties within DeFi systems. Traditional regulatory frameworks rely on the presence of centralized entities that can be held responsible for compliance and oversight. However, DeFi protocols often operate on decentralized governance structures, such as Decentralized Autonomous Organizations (DAOs), where decision-making is distributed among token holders. This decentralization complicates the identification of responsible parties, making it difficult for regulators to enforce compliance and accountability.

2. **Legal Enforceability:** Smart contracts, the backbone of DeFi transactions, present unique challenges in terms of legal enforceability. Unlike traditional contracts, smart contracts are executed automatically by code, without the need for intermediaries. While this automation provides efficiency, it also raises questions about the applicability of existing legal frameworks. The pseudonymous nature of blockchain transactions, coupled with their immutable and irreversible qualities, complicates the identification of contracting parties and the adjudication of disputes. Ensuring that smart contracts are legally enforceable and that parties have recourse in the event of fraud or error remains a significant challenge.

3.**Regulatory Fragmentation:** The borderless nature of DeFi and the varying regulatory approaches across jurisdictions create opportunities for regulatory arbitrage. Some jurisdictions may adopt a light-touch regulatory approach to attract innovation, while others may impose stringent regulations or outright bans on certain DeFi activities. This fragmentation can lead to inconsistencies in regulatory oversight and enforcement, making it difficult for authorities to achieve effective supervision and compliance. Coordinating regulatory efforts globally is essential to address these disparities and ensure a coherent regulatory environment for DeFi.

2.2. International Approaches

1. **Guiding Principles:** International organizations and financial authorities have advocated for the principle of "same activity, same risk, same regulation" to ensure consistent regulatory treatment of DeFi activities. This principle emphasizes that similar financial activities should be subject to equivalent regulatory standards, regardless of whether they occur within traditional or decentralized systems. Applying this principle helps create a level playing field and mitigates the risk of regulatory arbitrage.
2. **High-Level Recommendations:** Several international organizations have issued high-level recommendations to guide the regulation of DeFi. These recommendations focus on enhancing international collaboration, minimizing regulatory arbitrage, and supervising entities providing crypto-asset services. For instance, the Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO) have emphasized the need for cross-border cooperation and information sharing among regulators to address the global nature of DeFi markets.

3. Jurisdictional Responses: Different jurisdictions have adopted various approaches to regulating DeFi, reflecting their unique legal, economic, and technological contexts. Some jurisdictions have clarified existing regulations to explicitly include DeFi activities, while others have extended their regulatory frameworks or introduced bespoke regulations to address the specificities of DeFi. For example, the European Union's Markets in Crypto-Assets Regulation (MiCA) aims to provide a comprehensive regulatory framework for crypto-assets, including DeFi protocols.

7.MARKET RISKS & INDUSTRY SAFEGUARDS

Key Themes:

Having discussed the fundamentals of the VDA ecosystem, and introduced the market players therein, this section looks at the ecosystem more holistically and identifies the key risks and vulnerabilities therein. It also discusses industry best practices to address risks, and regulatory directives in the form of the FATF travel rule. Lastly, it views the ecosystem from an Indian perspective and discusses the threat of dollarisation, particularly in the trade of digital goods and services.

1. Overview of VDA functioning and vulnerabilities

Public, (such as Bitcoin, Ethereum etc.), as well as private (Corda, Hyperledger Fabric) blockchains have no specific norm, but are thus far largely a variant of the 'initial' blockchain system developed for Bitcoin. Although consensus mechanisms have begun to diverge between platforms (Proof of Work vs. Proof of Stake), by and large VDAs rely on Public Key Cryptography used widely across internet and digital applications.

A 'public key' can be thought of as an address of ID that allows users to receive tokens. Each public key is associated with a private key – and in conjunction the two allow a user to send funds by broadcasting a transaction along with a digital signature derived from both keys and the transaction details.

The most common attack vector in data breaches has always been via users of a system, rather than the system itself – attackers have found it easier to leverage human error and poor judgment rather than bringing down systems themselves, although this can still happen.

In this context it is easy to see the vulnerability that is intrinsic to funds and data stored in VDAs, users themselves must be incredibly careful to not accidentally expose their private key online, as well as to keep it in a safe and accessible place so that it may be used for a long period of time. A natural consequence of this is the emergence of 3rd party VDA custodians, including 'hot' or online wallet providers, exchanges and other financial platforms, and pure custodians.

This however, creates a counterparty risk – if the 3rd party is hacked, all users could lose funds even if they did nothing wrong. It also means that users would have to trust 3rd party providers to not misappropriate their funds, something that has occurred repeatedly in the space.

From a regulatory visibility perspective, a key vulnerability is posed by offshore exchanges. Given that regulations over the VDA ecosystem exist in silos, and that consensus over appropriate regulatory frameworks is still growing – offshore VDA exchanges can leverage opportunities for regulatory arbitrage. This is exemplified by entities like FTX and Binance.

2. Attack Vectors for VDAs

This section gives a brief overview of the types of attack vectors that exist for VDAs – identifying them now before illustrating how they will be tackled by the custody solution presented in this note.

2.1. Systemic Risk vs Storage Risk

Systemic Risk refers to the risk that the system itself will be hacked, i.e. a 51% attack on the Bitcoin Protocol. Storage Risk refers to loss due to negligence like losing private keys or an individual being compromised.

2.2. Storage Risk: Key Focus

Systemic Risk has proven low for large-cap VDAs; storage risk is the risk that is being mitigated through a custodial solution like the one presented here:

- **Mishandling Risk by Individuals:** Users can store their own private keys without the need for third-party storage systems, but will thus be responsible for their own security. Users can be compromised in multiple ways, i.e. through phishing, creating several attack vectors that can exploit this kind of risk
- **Counterparty Risk:** Where a trusted 3rd party may misappropriate funds by colluding with an outside attacker, defaulting (like FTX), and incompetence resulting in the loss of private keys
- **Hacking Risk via Technical Weakness:** Methods used to steal digitally-stored private keys and/or the decryption keys to access the data, such as open ports, uncomplicated passwords, unpatched operating systems, and bad encryption.
- **Hacking Risk via Impersonating a Customer:** Should a hacker obtain control of a customer's email account, it is possible to effectively impersonate the customer Furthermore, e-mails are frequently used to reset login passwords or validate requests, often giving email intruders access to somebody's VDAs by extension
- **Hacking Risk via Impersonating a Counterparty:** Should an attacker succeed in hacking the website of the counterparty, they might be able to change the bank account or address where funds are to be transmitted. In this case, a customer would unknowingly send funds to the attacker instead of the intended counterparty.
- **Hacking Risk via Intercepting Communications:** Also called a man-in-the- middle attack (MITM), if an attacker can intercept and change the address to which bitcoins are to be transferred due to an insecure transmission medium, this would be an easy manner to steal bitcoins.
- **Private Key Loss Risk:** If stored online private keys may accidentally be deleted, while there is a risk of physical loss of private key medium (piece of paper, USB drive, etc.) or physical degradation of said medium.

3. Risks and Vulnerabilities specific to DeFi

3.1. Governance

While DeFi protocols claim decentralization, many exhibit de facto centralization. Governance tokens are often concentrated among a small group of stakeholders, such as protocol developers, venture capital investors, or early adopters, leading to potential manipulation and misrepresentation.

The concentration of governance power can lead to:

- **Misaligned Incentives:** A small group of token holders may prioritize their interests over the broader community, resulting in decisions that may not benefit all users.

- **Security Risks:** Centralized control points can become targets for attacks, undermining the security of the protocol.
- **Lack of Transparency:** The opacity of governance structures can lead to a lack of accountability and oversight, increasing the risk of fraudulent activities.

3.2. Compliance and Legality

DeFi's borderless nature and pseudonymous transactions present challenges for compliance with anti-money laundering (AML) and counter-financing of terrorism (CFT) regulations. The lack of cohesive regulations across jurisdictions allows for regulatory arbitrage, where non-compliant actors can exploit regulatory gaps.

Key compliance and legality issues include:

- **Regulatory Uncertainty:** DeFi protocols often operate in legal gray areas, with unclear regulatory status in many jurisdictions.
- **AML/CFT Risks:** The anonymity of DeFi transactions can facilitate illicit activities such as money laundering and terrorist financing.
- **Legal Enforceability:** Smart contracts may not be recognized as legally binding in all jurisdictions, complicating dispute resolution and enforcement.

3.3. Economic and Technological Fragilities

DeFi protocols are susceptible to economic and technological vulnerabilities, including smart contract failures, scalability issues, and exploitation by malicious actors. The hierarchical nature of the DeFi stack means each layer's security depends on the one below it.

Economic and technological risks include:

- **Smart Contract Bugs:** Errors in code can lead to significant financial losses, as seen in various DeFi hacks and exploits.
- **Scalability Challenges:** Many blockchains face scalability issues, struggling to handle increased transaction volumes without compromising security.
- **Market Manipulation:** The transparency and reorderability of blockchain transactions can be exploited for front-running and other manipulative practices.
- **Infrastructure Vulnerabilities:** Oracles, cross-chain bridges, and Layer 2 solutions can introduce centralization risks and become points of failure.

3.4. Interconnectedness

The composability of DeFi protocols leads to high interdependence, amplifying the scope and speed of financial contagion. The interconnectedness between DeFi and centralized crypto-asset finance (CeFi) can also lead to systemic risks.

Interconnectedness risks include:

- **Protocol Dependencies:** The failure of one protocol can trigger cascading failures across multiple dependent protocols.
- **Financial Linkages:** Interactions between DeFi and CeFi platforms can create channels for contagion, spreading financial distress across markets.
- **Operational Risks:** Shared infrastructure components, such as oracles and bridges, can become single points of failure, affecting multiple protocols simultaneously.

3.5. Leverage, Liquidity, and Maturity Mismatches

High levels of leverage and collateralization, along with liquidity and maturity mismatches, pose significant risks. Over-collateralization and re-collateralization of crypto-assets can create complex and fragile systems.

Leverage and liquidity risks include:

- **High Leverage:** Excessive leverage can lead to procyclical behavior, exacerbating market volatility during downturns.
- **Liquidity Mismatches:** Promises of immediate redemption combined with illiquid investments can trigger liquidity crises.
- **Maturity Mismatches:** Mismatched asset-liability profiles can lead to redemption runs and financial instability.

3.6. Investor and Consumer Protection

The lack of comprehensive investor and consumer protection measures, combined with the immutability of blockchain transactions, increases the risk of fraud and financial loss. Regulatory responses are still developing to address these challenges.

Investor and consumer protection issues include:

- **Fraud Risks:** The ease of creating and deploying DeFi protocols without auditing increases the likelihood of scams and fraudulent schemes.
- **Information Asymmetry:** Retail investors may lack the technical knowledge to understand the risks and mechanisms of DeFi protocols.
- **Immutability of Transactions:** Once executed, blockchain transactions cannot be reversed, making it difficult to recover lost or stolen funds.

3. Travel Rule for Virtual Asset Service Providers

3.1. Background

VDAs are more vulnerable to criminal activity and money laundering since the public keys engaging in a transaction cannot be directly linked to an individual.

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. FATF's 'Travel Rule' requires financial institutions to pass along information to one another for certain electronically-facilitated transfers. The info 'travels' along with the pertinent transactions from bank to bank until the funds reach their end destination. The intent behind the Travel Rule is that sharing information* will allow participants to: (1) Block terrorist financing (2) Stop payments to sanctioned individuals, entities, and countries (3) Enable law enforcement to subpoena transaction details (4) Support reporting of suspicious activities (5) Prevent money laundering of VDAs.

The Travel Rule rule, formally known as FATF Recommendation #16, requires VASPs to communicate the information of the originators and beneficiaries of VDA transactions that exceed a certain threshold. More specifically, the regulations require VASPs to exchange information regarding the identities of the originator and beneficiary whenever the amount transacted is above $1,000.

Notably, FATF has defined a Virtual Asset Service Provider (VASP) as any person or entity who is not covered elsewhere under the Recommendations and, as a business, conducts one or more of the following activities or operations for or on behalf of another person:

1. An exchange between VAs and fiat currencies
2. An exchange between one or more forms of VAs
3. A transfer of VAs (moves a VA from one VA address or account to another)
4. The safekeeping or administration of VAs or instruments enabling control over VAs
5. Participation in and provision of financial services related to an issuer's offer or sale of a VA

The Travel Rule mandates that organizations collect and exchange personal data from transaction parties. The Rule initially only applied to banks. The FATF, however, expanded this regulation to VDA firms in 2019. In addition, the G20 and several other jurisdictions began incorporating the Travel Rule into their local anti-money laundering laws in 2020.

India amended its anti-money laundering law to include virtual digital assets, requiring KYC checks and reporting of transactions. As India continues to gain prominence in the crypto market, the government has been providing clarity on various related issues, including the application of anti-money laundering (AML) and FATF Travel Rule for crypto transactions.To bring crypto under the ambit of the Act and reign in Virtual Digital Assets Service Providers (VDASPs), the Indian government amended the PMLA 2002 (Prevention of Money Laundering Act).

Recently FATF released a fifth update on jurisdictions' compliance with FATF's Recommendation 15 and its Interpretative Note (R.15/INR.15). The report finds that while some jurisdictions have made progress in putting AML/CFT regulation in place, global implementation is still lagging.

When focusing on the countries with materially important VA sectors (who were included in the roadmap analysis published in March 2024) the picture is better, with a majority having the core measures in place. Nevertheless, despite progress made by individual countries, there is still a lot of work to do in order to complete the global system of AML/CFT regulation for the virtual asset sector, and FATF will continue to prioritise closing these gaps.

It acknowledges positive developments in the VA sector reported by the private sector, such as increases in VA transaction volume using Travel Rule compliance tools and in VASPs considering Travel Rule obligations in their operations. The report highlights that all players need to have appropriate risk identification and mitigation measures and continue to work towards fully compliant Travel Rule compliance tools.

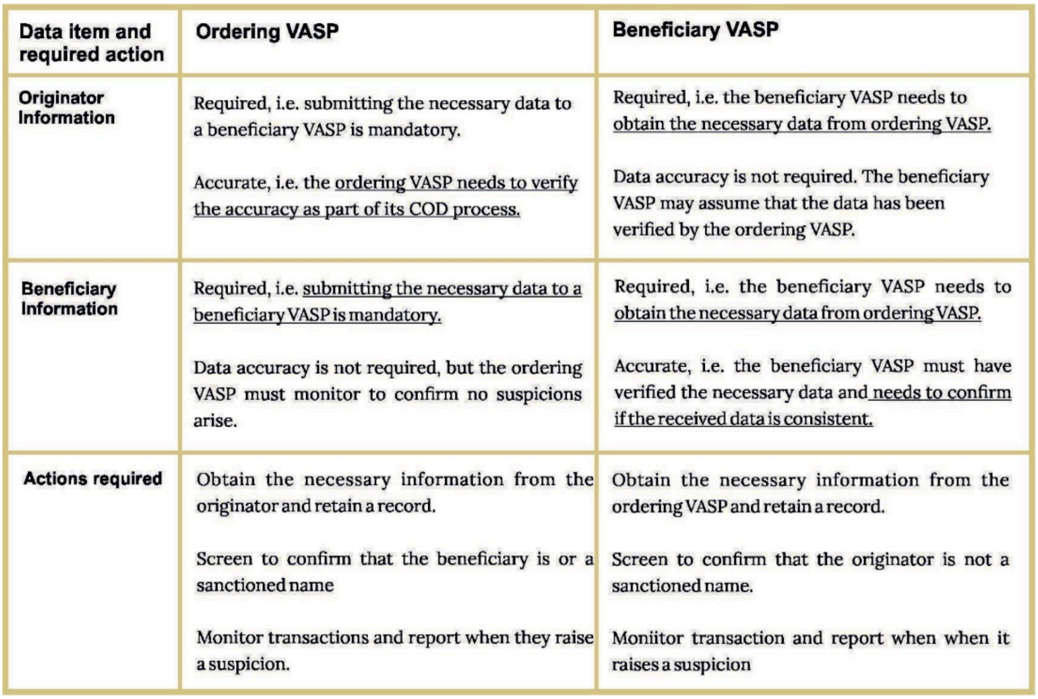
3.2. Examining FATF Recommendation #16:

VDA exchanges, custodial wallet providers, and other virtual asset service providers (VASPs) must disclose personal client data accurately during transactions under this regulation. Information such as the sender's and recipient's names, geographic addresses, account numbers, and more must be collected and submitted to the appropriate authorities. Specifically, whenever the amount transacted exceeds $1,000, the regulations oblige VASPs to share information about the originator and beneficiary's identities.

In addition to the extra information required by individual regulators, FATF recommends the following data ought to be transmitted back and forth by VASPs:

1. The names of the sender and the recipient
2. The address of the sender
3. The account number of the sender and the recipient

Many VASPs face a challenge when complying with the 'Travel Rule' and facilitating transactions across jurisdictions called the 'sunrise' challenge – or problem. This occurs when jurisdictions are at different stages of complying with or setting expectations for the travel rule. In jurisdictions where VASPs must adhere to the travel rule (aka the sun has risen), they could find it very difficult to transact and even maintain relationships with VASPs where travel rule compliance is not yet established or enforced (aka the sun is still down).



Data item and required action	Ordering VASP	Beneficiary VASP
Originator Information	Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory. Accurate, i.e. the ordering VASP needs to verify the accuracy as part of its COD process.	Required, i.e. the beneficiary VASP needs to obtain the necessary data from ordering VASP. Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP.
Beneficiary Information	Required, i.e. submitting the necessary data to a beneficiary VASP is mandatory. Data accuracy is not required, but the ordering VASP must monitor to confirm no suspicions arise.	Required, i.e. the beneficiary VASP needs to obtain the necessary data from ordering VASP. Accurate, i.e. the beneficiary VASP must have verified the necessary data and needs to confirm if the received data is consistent.
Actions required	Obtain the necessary information from the originator and retain a record. Screen to confirm that the beneficiary is or a sanctioned name Monitor transactions and report when they raise a suspicion.	Obtain the necessary information from the ordering VASP and retain a record. Screen to confirm that the originator is not a sanctioned name. Moniitor transaction and report when when it raises a suspicion

Industry Best practices to Arrest Money Laundering, Terror funding and Tax evasion

India Story

VDAs have emerged as a central facet of Web3 technologies, causing concern among policy makers. It is arguably the most widespread of these technologies. While its adoption is driven heavily by its genuine value proposition, it has partly also been fueled by aggressive endorsements. Like any emerging technology, it brings both immense potential and inherent risks.

The industry has consistently demonstrated its commitment to surpassing minimum standards and setting an exemplary model for compliance in the industry. Our proactive approach towards regulatory adherence and global best practices highlights its dedication to ensuring a compliant and secure VDA ecosystem. Many of the voluntary compliance practices adopted by the industry have transitioned into mandatory requirements following the notification of the Prevention of Money Laundering Act (PMLA). Here are the key voluntary compliances undertaken by the industry:

1.Setting up of an Industry Association:

1. The industry came together to set up the Bharat Web3 Association (BWA). Members of the association include infrastructure providers such as Polygon and Biconomy; crypto-asset exchanges such as CoinDCX, Coinbase, and Coinswich Kuber; non-fungible token based gaming platforms like Hike; other virtual asset service providers like Liminal and other Web3 players like Tax Nodes.
2. BWA maintains proactive collaboration with diverse government agencies such as law enforcement, Ministry of Electronics and Information Technology, and the Reserve Bank of India (Central Bank) fostering meaningful dialogue and cooperation.

DIGITAL · DECENTRALIZED · PEER TO PEER
BIT
ripple coin XRP
MONERO · SECURE · PRIVATE · UNTRACEABLE · PRIVATE

2. KYC is a must

1. All member (BWA) VDA exchanges in India have KYC requirements in place that are inline with those followed by banks & other financial institutions. While most platforms have both automated & manual processes for verification of user documents, some have also incorporated direct verification via government databases i.e. PAN verification via NSDL and Aadhaar verification via Digilocker. This ensures verified identity of all users on the platforms and prevents cases of spoofing.
2. This was voluntarily implemented by members prior to the release of Guildelines under PMLA for Virtual Digital Asset Service Providers.

3. VDA Exchanges have Compliance Processes

Once a user's identity has been verified and recorded, VDA platforms also perform additional due diligences like bank account verification checks involving ‘penny testing’ methods, uniqueness checks across user details to prevent duplicate accounts and alerts for suspicious transactions to ensure multiple layers of checks and balances.

4. Closed Fund Flows

Once a user deposits funds (INR) into his/her VDA exchange account, there is no way for the user to transfer his INR other than back into his/her own bank account. Further, when the users buy or sell VDA, they place their trades on open order books and a high performance matching engine, matches their orders with other KYC verified users on the platform.

5. Regtech and Suptech Integrations

Most Indian VDA exchanges have implemented regulatory technology integrations (regtech) for ensuring AML compliance with global standards. These regtech solutions help create and maintain an index of malicious VDA accounts and alerts for platforms in the event that any transaction from or to the platform comes in contact with such tainted account addresses. These solutions help Indian platforms steer clear of sanctioned lists, darknet addresses, terrorism funding and known addresses with hacked or stolen funds, thereby keeping platform user funds secure with real-time risk alerts of bad actors through their interoperable AML/CFT system.

Further, some exchange platforms have also implemented financial supervision technology (Suptech) to ensure there is no instance of market manipulation or money laundering across all transactions taking place within the platform.

These measures ensure reduced counterparty risk, investor protection, safe and transparent trading environment. Some of the monitoring tools are as follows:

- Jocata- Jocata is a transaction monitoring tool which implements pre-defined rules on the basis for which alerts are generated. It also provides a case management system for any alert that is generated.
- Coinfirm - Coinfirm provides a risk-core on the basis of which one can assess the risk associated with any VDA deposit or withdrawal.

Using these tools, the platform implements a layered set of rules to automatically flag suspicious transactions. Accounts are automatically frozen, suspended, or asked for EDD as per the guidelines followed by the case management system.

6. VDA Exchanges help with Tax Compliance

All the major Indian VDA exchanges have built Tax Deducted at Source (TDS) compliances and assist the exchequer by aggregating TDS collections on behalf of their platform users and posting them against each PAN in a systematic manner. In fact, Indian VDA platforms also worked closely with Central Board of Direct Taxes (CBDT) to build frameworks for complex transactions like VDA to VDA transactions and defined the process of TDS collection, conversion to fiat and consequent submission to the government.

7. Protection of User Funds & Data

Exchanges employ multiple procedures for ensuring user funds are safe. There is no single point of failure or access to funds held directly, in any of the exchange accounts, with multiple signatures along with other conventional security mechanisms (OTP, 2FA etc.) required. The exchanges conduct regular security audits in which regular stress, scenario, and penetration testings are conducted to mitigate any attack vector onto our platform. Additional security measures include TLS encryption on communication protocols, DDOS protection.

8. Grievance Redressal Mechanism

All exchanges maintain a 24x7 grievance mechanism via a ticket system where each ticket is addressed within 24 hours, and provides dedicated resources to help clients transact in larger volumes. Many exchanges have a dedicated Grievance Officer to oversee redressals.

9. Consumer Awareness

Indian VASPs have taken substantial strides in enhancing consumer awareness regarding this space. Through various educational initiatives, webinars, and informative content, exchanges have actively aimed to educate users about the nuances of trading, the underlying blockchain technology, and the potential risks associated with crypto investments. By providing accessible resources, explanatory videos, and guides, they have empowered users to make informed decisions and navigate the crypto landscape with greater confidence. Additionally, many exchanges have engaged in awareness campaigns to promote responsible trading practices and to caution against fraudulent schemes.

8. UNLOCKING OPPORTUNITIES IN WEB3

Key Themes:

This section delves into the transformative potential of Web3 technology, highlighting its significant growth and innovation. It begins by showcasing the remarkable expansion of the global crypto and Web3 market, emphasizing key regulatory advancements across G20 countries and the introduction of Bitcoin spot ETFs. The chapter also explores the growing interest in tokenization of Real-World Assets (RWA), DeFi, and DePIN, illustrating their impact on the financial ecosystem. Furthermore, it examines the increasing institutional investment in Web3, with major companies like Microsoft, Google, and PayPal integrating blockchain solutions. Lastly, the chapter presents various use cases of blockchain technology, including NFTs, efficient capital markets, RWA tokenization, energy trading, and governance, demonstrating how these applications are revolutionizing traditional industries and driving economic growth globally.

1.Web3: Unlocking Innovation and Growth:

- The global market cap for crypto assets and Web3 has grown from $1.37 trillion in 2021 to $2.48 trillion as of mid-2024, reflecting significant expansion.
- Approximately 400 million people are now part of the Web3 landscape. Global regulation of the crypto landscape has seen substantial advancements, with all G20 countries implementing some form of crypto regulation.
- In the U.S., a bill is being considered to establish a regulatory framework for cryptocurrencies and stablecoins, while Europe's Markets in Crypto-Assets (MiCA) regulation is being rolled out, requiring licensing for all types of VASPs.
- Additionally, the introduction of Bitcoin spot ETFs in January 2024 has provided a regulated and liquid way for investors to gain exposure, further legitimizing the crypto market, with Ethereum ETFs expected by Q3 2024. Trends in Real-World Assets (RWA), DeFi, and DePIN are also notable.
- The tokenization of RWAs, including stablecoins and U.S. Treasuries, has seen over $13.5 billion in on-chain issuances across various platforms like Ethereum and Solana. DeFi continues to grow, with significant activity in lending and credit markets, and is projected to expand at a CAGR of 9.06% from 2024 to 2030.[39]
- DePIN is emerging as a new frontier, applying blockchain to physical assets like real estate and commodities, with 106 coins in this sector totaling a market capitalization of $20.67 billion.[40]
- The highest grassroot adopters of crypto assets are often developing nations, including India, Vietnam and the Philippines.

2. Institutions Dive In: The Rise of Web3 Investment

In recent years, institutional interest in Web3 has grown significantly, with various well-known organizations and companies entering the space. Here are some examples:

1.Microsoft: Microsoft is reportedly planning to offer increased support for crypto wallets in its next generation of hardware products, according to documents revealed in the ongoing lawsuit with the US Federal Trade Commission. The documents indicate that Microsoft intends to introduce a range of new products, including consoles, phones, web browsers, PCs, and a new "cloud system" with enhanced crypto wallet functionality.Microsoft has been making notable strides in the crypto space, including partnering with blockchain protocol Aptos for AI-based blockchain products and joining forces with LeverFi to address challenges in the decentralized finance (DeFi) industry.

2. Google: As per Bloomberg reports, Google has formed a team looking into blockchain and crypto projects in January 2022. Google’s parent company Alphabet has also revealed that it invested $1.5 billion in the blockchain sector between September, 2021, and June, 2022. The companies that received this funding include digital asset custody platform Fireblocks, Web3.0 gaming company Dapper Labs, Bitcoin infrastructure tool Voltage and venture capital company Digital Currency Group. In February 2023, Google Cloud announced its partnership with the Tezos Foundation to grow its web3 application development and provide new services for its customers. Earlier this month, Google Cloud announced a tie-up with LayerZero, a crypto startup recently valued at $3 billion, wherein the cloud provider will verify data sent between blockchains on the startup’s messaging protocol.

3. Paypal: PayPal USD is designed to contribute to the opportunity stablecoins offer for payments and is 100% backed by U.S. dollar deposits, short-term U.S Treasuries and similar cash equivalents. PayPal USD is redeemable 1:1 for U.S. dollars and is issued by Paxos Trust Company. Eligible U.S. PayPal customers who purchase PayPal USD will be able to:

- Transfer PayPal USD between PayPal and compatible external wallets
- Send person-to-person payments using PYUSD
- Fund purchases with PayPal USD by selecting it at checkout
- Convert any of PayPal's supported cryptocurrencies to and from PayPal USD

PayPal's stablecoin PYUSD is also available on Venmo and will roll out fully in the coming weeks. PYUSD is already on exchanges like Crypto.com, Bitstamp, Coinbase, and Kraken. About 90% is held in wallets controlled by Paxos Trust. BitPay is also supporting PYUSD. This move is part of PayPal's ongoing expansion into the crypto space, following its acceptance of digital asset payments in 2021 and the establishment of on- and off-ramps for Web3 payments in 2023**.**

4. MicroStrategy: The business intelligence firm MicroStrategy made headlines in 2020 when it announced its intention to allocate a substantial portion of its treasury reserves to Bitcoin. The company has since acquired billions of dollars' worth of Bitcoin and continues to view it as a long-term store of value

5. Tesla: In early 2021, Tesla, led by Elon Musk, announced a $1.5 billion investment in Bitcoin and revealed plans to accept Bitcoin as a form of payment for its electric vehicles. Although Tesla later suspended Bitcoin payments due to environmental concerns, its initial investment highlighted institutional interest in the crypto.

6. Square: Square, a financial services company led by Jack Dorsey (also the CEO of Twitter), invested $50 million in Bitcoin in 2020. Square's Cash App also allows users to buy and sell Bitcoin, further integrating crypto into its services.

7. Fidelity Investments: Fidelity, one of the largest asset management firms in the world, launched its digital asset subsidiary, Fidelity Digital Assets, to provide institutional-grade crypto custody and trading services.

8. Grayscale Investments: Grayscale manages a suite of crypto investment trusts, including the Grayscale Bitcoin Trust (GBTC) and the Grayscale Ethereum Trust (ETHE). These trusts allow institutional and accredited investors to gain exposure to cryptocurrencies through traditional investment vehicles.

9. Goldman Sachs: Goldman Sachs, a prominent investment bank, relaunched its crypto trading desk in 2021 to meet increasing demand from clients interested in Bitcoin and other digital assets.

10. JPMorgan Chase: While JPMorgan's CEO, Jamie Dimon, was initially critical of Bitcoin, the bank has since adopted a more positive stance. It launched its own digital currency, JPM Coin, and provides banking services to crypto exchanges Coinbase and Gemini.

11. BlackRock: The world's largest asset manager, BlackRock, has been exploring opportunities in the crypto space. It has acknowledged the potential of Bitcoin as a store of value and has reportedly started to dabble in Bitcoin futures.

12. Traditional Asset Managers: Various traditional asset management firms, including VanEck, WisdomTree, and SkyBridge Capital, have launched or proposed crypto-related investment products, such as Bitcoin exchange-traded funds (ETFs).

13. University Endowments: Several universities, including Harvard, Yale, and Stanford, have invested in crypto-focused venture capital funds. This indirectly exposes their endowments to the crypto ecosystem.

These are just a few examples of the growing institutional interest in crypto. As the crypto market continues to mature and regulation becomes more clear, it is likely that we will see even more institutional adoption in the years to come.

3. Use Cases

3.1. NFTs & Digital Credentialing

Tokenization as a concept has been used by the Reserve Bank of India (RBI) for enabling secure credit card payments. If one were to apply the same concept to Identities, tokenization is being used with Crypto Wallets for verifiable digital credentialing. As an example, MIT created Blockcerts, an open standard where apps can be built to issue academic certificates and other documents via blockchain. Blockcerts is built to function on the Bitcoin blockchain and is also expanding to Ethereum. Development work continues for making Blockcerts to work across public chains, and to be easily extended for private chains as well. This means one can have absolute interoperability by incorporating virtual assets as the token to fetch validation requests, thereby increasing its efficacy as a global system. The Maltese government also used this standard to implement a system whereby its Ministry for Education and Employment can verify any academic credential using token based blockchains.

3.2. Efficient Capital Markets

Ongoing research projects are looking to fractionalise shares listed on stock markets in the form of tokens. Given that the tokens will be a part of the blockchain network, the tracking of share issuances and transfers can be carried out securely on a distributed ledger. Furthermore, if shares are registered on a distributed ledger, investors and issuers would be able to interact directly, 24/7 with instant settlement and guaranteed finality. Property rights will become crystal clear. Capitalization table management would become easy. Proxy voting would be transparent and always accurate. Dividends and other corporate actions (such as stock splits) would be automated and always accurate. Certificates of good standing would never again require a prerequisite forensic audit. Securities lending records would always be accurate, so accidental over-issue of securities would never happen. Also, the entry barriers for investing in stock markets can be greatly reduced. A Web3 company, Tokenfolio is working on making this possible by enabling startups to tokenize their early stage fund raise requirements and raise capital from angel investors in the form of tokens.

Another example is Interest Rate Swaps (which have a reported quadrillion dollars in notional value exchanged each year), as a traditional financial derivative that if introduced, could disrupt the DeFi market, while decentralized IRSs could have significant benefits for traditional finance. Interest rate swaps are financial derivatives that help corporations, banks, and nations manage their debt and are one of the most commonly traded derivatives in traditional finance. The potential for IRSs to make the leap to the decentralized finance (DeFi) ecosystem is significant, as they provide scalability and complexity to the global financial system. DeFi can transform IRSs by providing a decentralized platform, reducing costs and increasing accessibility, and revolutionizing traditional interest rate swaps by automating the execution and settlement of interest rate swaps. However, introducing IRSs to DeFi presents unique challenges and requires a more innovative approach to deliver the same utility in an environment with different constraints. Solutions like Tempus and the Voltz protocol aim to solve this issue, along with several other similar projects

3.3. Real World Asset (RWA) Tokenization

Real World Asset (RWA) Tokenization is transforming traditional financial markets by digitizing tangible assets like real estate, commodities, and art on blockchain platforms. This innovative process involves creating digital tokens that represent ownership of these assets, providing increased liquidity, transparency, and accessibility.

Key components of RWA tokenization include blockchain technology, tokens, and smart contracts, which collectively enhance the efficiency of transactions and ensure immutable ownership records. The global market for RWA tokenization is rapidly expanding, driven by technological advancements, growing investor interest, and the need for higher liquidity in traditional asset classes. Notable examples include Emaar Properties' real estate tokenization, the Dubai Multi Commodities Centre's commodity trading platform, and Standard Chartered’s trade finance initiatives. Additionally, Singapore’s Monetary Authority of Singapore (MAS) has launched Project Guardian, which successfully piloted the tokenization of trade finance assets, demonstrating enhanced operational efficiency and transparency in trade finance transactions.

The regulatory landscape for RWA tokenization is evolving, with proactive frameworks emerging in key regions like the US, Europe, Singapore, and the MENA region. These regulatory developments aim to support innovation while ensuring investor protection and market integrity. For instance, the UAE, with its robust regulatory environment and initiatives like the Dubai Blockchain Strategy, is positioning itself as a global leader in blockchain adoption. The market potential for RWA tokenization is substantial, with projections estimating a market size of $16 trillion by 2030.

As financial institutions, governments, and investors continue to collaborate and embrace this technology, RWA tokenization promises to democratize investment opportunities, reduce transaction costs, and drive economic growth globally.

For example, **BlackRock's BUIDL** fund provides a deployed RWA use case by leveraging tokenization to offer a diversified portfolio of real world assets. Utilizing blockchain technology, BUIDL enhances transparency, security, and efficiency in investment management, allowing for fractional ownership and increased liquidity. Each BUIDL unit trades at close to a dollar, backed by a diversified portfolio that primarily US Treasury bills, and offers daily dividends, 24/7 transferability, and automated smart contract functionality for secure transactions and compliance.

Key participants in the BUIDL fund include BlackRock as the primary asset manager, Coinbase for secure trading and management of digital assets, Circle for providing the USDC stablecoin backing, and Securitize for the tokenization process and regulatory compliance. BNY Mellon serves as the custodian, ensuring the safekeeping and interoperability between digital and traditional assets. The fund is issued on the Ethereum blockchain, utilizing its smart contract capabilities to ensure transparent, secure, and immutable transactions, thereby enhancing investor confidence and participation.

The global market for RWA tokenization has shown remarkable growth in recent years, driven by technological advancements, increased investor interest in digital assets, and the demand for higher liquidity in traditional asset classes. As of July 2024, the market has grown 25 times from 2021 to 2024. The total market value has reached around $13.5 billion in 2024.

3.3.1. Key Components of RWA Tokenization [41]

1. **Blockchain Technology:** This distributed ledger technology ensures secure and transparent recording of transactions.
2. **Tokens:** These are digital representations of ownership rights to physical or financial assets.
3. **Smart Contracts:** Self-executing contracts with terms directly written into code, facilitating automatic transactions on the blockchain.

3.3.3. Benefits of Tokenization [42]

1. **Liquidity:** Tokenization transforms traditionally illiquid assets into tradable digital tokens, enhancing market liquidity.
2. **Fractional Ownership:** By allowing the purchase of fractions of high-value assets, tokenization reduces entry barriers for investors.
3. **Transparency and Security:** Blockchain technology ensures that all transactions are recorded immutably, enhancing trust and security.
4. **Operational Efficiency:** Smart contracts automate processes, reducing the need for intermediaries and cutting operational costs.

Examples of Tokenization

- **Real Estate:** Platforms like RealT and Emaar Properties in Dubai allow fractional ownership and trading of real estate properties, increasing liquidity and accessibility for investors.
- **Commodities:** The Dubai Multi Commodities Centre (DMCC) has launched a blockchain-based platform for trading tokenized commodities like gold, enhancing efficiency and transparency.
- **Trade Finance:** Standard Chartered's Project Guardian demonstrated the enhanced operational efficiency and transparency of tokenized trade finance assets.
- **Investment Platforms:** Platforms like tZERO and Harbor offer fractional shares of real estate and other assets, broadening investor access.

3.4. NFT Based Land Records

Traditional legal-contract execution is costly to both governments and their citizens. However, smart, self-executing contracts, enabled by blockchain are improving the process of contract creation and execution. These contracts are publicly accessible and secure within the network. For example, the Swedish land registry uses a blockchain-based solution for land-title transfers. The disintermediation and removal of notarization through smart contracts has reduced the transaction time by more than 90 percent.

Some industries have tried to create consortiums that use smart, self-executing trade contracts over blockchain to improve the flow of goods between various countries. Several governments in India are also looking to enable land records on blockchains. Interestingly one of the most popular solutions comes from NFTs, which are also a subset of virtual assets based on token based blockchains. For example, the United Nations Development Programme (UNDP) has been working on a project to integrate blockchain technology into the land registry process in India as part of efforts to make it more reliable.

3.5. Agri-Commodity Financing and Supply Chain

- Whrrl is working with the Polygon blockchain to issue a line of credit to farmers on the basis of tokenization of real world assets like excess crops stored in warehouses. It achieves this by building an offline oracle bridge that relays the status of the underlying asset to a smart contract and allows lending and borrowing to DeFi participants on one side and farmers on the other side.
- Emertech Innovations is using blockchain technology to bring solutions for farmer producer organizations(FPOs) by ensuring transparency and efficiency to the farm supply chain. They have created a tamper proof easily verifiable ledger of agriculture supply chain accessible to the farmer, distributor, logistic provider, retailer and the end user.

3.6. Energy trading

Renewable energy trading and management is one of the main areas found in current blockchain projects in several countries. For instance, a project supported by the Japanese Ministry of the Environment aims at building a system for measuring and managing self-consumed renewable energy. The project utilizes the crypto assets side of the blockchain technology to build the trading system. Specifically, the self-consumed renewable energy is first converted into tradable values and sent to the blockchain network. The real-time trading prices are then calculated according to the exchange cost and demand. When the transactions are finalized, energy can be exchanged locally without having to be transmitted to a central location. EcoWatt, which is a Token backed by renewable energy and reforestation was remarked on and awarded 'Best Sustainability Blockchain Solution' at the 2nd edition of the Future Innovation Summit event held in UAE in May 2022.

3.7. Governance

Estonia was the first Nation-State in the world to deploy blockchain technology in production systems – in 2012 with the Succession Registry kept by the Ministry of Justice. The technology chosen for Estonian systems is KSI Blockchain, also used by NATO and the U.S. Department of Defense.Estonia X-Road and KSI Blockchain Zug pilot tokenized ID on ETHUAE 'Smart Dubai' Initiative.The government has been leveraging technology to efficiently deliver services with respect to record keeping, public healthcare, education and inclusion. [43]

9. STANDARD SETTING BODIES APPROACH TO VDAs

Key Themes:

This section outlines the significant role of the G20 in shaping the global regulatory landscape for crypto-assets. This section also analyses the commitment to innovation and international cooperation of contributions from the Financial Stability Board (FSB) and the International Monetary Fund (IMF), and has driven forward the agenda on creating a balanced, effective approach to crypto regulation globally. The section also entails the crypto-assets regulatory landscape of G20 nations like USA, UK, Singapore, Hong Kong, AND UAE. Furthermore the section lists down the road maps of standard setting bodies with regards to crypto assets.

G20's efforts

The G20 has significantly impacted the crypto industry by acting as a catalyst for global conversations on crypto-asset regulation and adoption. Through various summits and meetings, the G20 has encouraged member countries to develop and implement regulatory frameworks that address the risks and opportunities associated with digital assets. For instance, the Financial Stability Board (FSB) and the International Monetary Fund (IMF) have been instrumental in providing guidelines and recommendations for crypto regulation.

The G20 New Delhi Leaders' Declaration

In October 2023, theNew Delhi Leaders' Declaration, issued at the conclusion of India's G20 Presidency, was a landmark document that provided valuable insights into the G20's stance on crypto assets.. It highlighted several key points:

1. **Acknowledgment of Crypto's Impact:** The declaration recognized the growing significance of crypto assets in the global economy. It acknowledged that crypto assets had evolved beyond a niche market and had the potential to impact financial stability, monetary policy, and consumer protection.

2. **Commitment to Innovation:** The G20 leaders expressed their commitment to fostering innovation in the financial sector. They acknowledged that crypto assets and blockchain technology had the potential to improve efficiency, reduce costs, and enhance financial inclusion.

3. **Risk Mitigation:** While recognizing the potential benefits of crypto assets, the declaration also emphasized the need to mitigate risks associated with them. It called for efforts to address concerns such as money laundering, terrorist financing, and tax evasion, which had been associated with crypto assets.

4. **International Cooperation:** The G20 leaders stressed the importance of international cooperation in regulating crypto assets. They recognized that crypto assets operated in a borderless environment and required coordinated efforts to develop effective regulatory frameworks.

1. **The IMF FSB Synthesis Paper on Crypto**

In addition to the G20 New Delhi Leaders' Declaration, the International Monetary Fund (IMF) and the Financial Stability Board (FSB) published a joint Synthesis Paper on Crypto assets during India's G20 Presidency. This paper provided further insights into the global perspective on crypto regulation.

1. **Systemic Implications:** The IMF FSB Synthesis Paper highlighted the potential systemic implications of crypto assets It discussed the need for a comprehensive assessment of the risks posed by crypto assets to global financial stability.
2. **Regulatory Approaches:** The paper presented various regulatory approaches adopted by different countries, ranging from outright bans to permissive regulatory environments. It emphasized the importance of tailoring regulations to the specific characteristics and risks associated with crypto assets.
3. **Cross-Border Challenges:** Cross-border challenges posed by crypto assets were a central theme in the paper. It emphasized the need for international cooperation to address issues such as jurisdictional conflicts and money laundering.
4. **Financial Inclusion:** The IMF FSB Synthesis Paper acknowledged that crypto assets had the potential to promote financial inclusion, especially in regions with limited access to traditional banking services. It underscored the importance of striking a balance between regulation and innovation to harness this potential.

Further, several countries have taken notable steps towards regulating the crypto industry. The United States has focused on implementing stricter AML measures and ensuring investor protection. The European Union has introduced the MiCA regulation to create a harmonised framework across its member states. Japan has established a comprehensive regulatory environment, ensuring consumer protection and market integrity, while South Korea has implemented strict AML requirements and licensing systems for crypto exchanges.

1.1. Singapore’s Robust Crypto Ecosystem: Singapore enhances its crypto regulatory framework with legal trading and possession of crypto assets, enforcing strong anti-money laundering (AML) and counter-financing of terrorism (CFT) regulations, and requiring virtual asset service providers to meet licensing standards. Initiatives like Project Guardian explore blockchain potential, and the Monetary Authority of Singapore (MAS) collaborates internationally to develop global digital asset standards.

1.2. Hong Kong’s Strategic Crypto Regulation Developments: Hong Kong emphasizes transparency and investor protection through regulatory measures for virtual asset trading platforms and stablecoins. The introduction of Bitcoin and ether ETFs and the e-HKD pilot program for central bank digital currency demonstrate its commitment to a well-regulated digital asset environment.

1.3. Dubai’s Defined Regulatory Framework: Dubai’s Virtual Assets Regulatory Authority (VARA) provides a transparent framework, attracting crypto firms and fostering innovation. The Central Bank of the UAE regulates UAE dirham-backed stablecoins as part of its Financial Infrastructure Transformation Programme, promoting innovation and digitization. Various free zones also have regulatory frameworks, e.g. ADGM and DIFC.

1.4. Europe’s Unified Approach with MiCA: Europe's Markets in Crypto-Assets (MiCA) regulation creates a unified regulatory landscape across 27 EU countries, ensuring consumer protection and legal certainty. The European Securities and Markets Authority (ESMA) introduces technical standards to enhance transparency and oversight in the EU crypto-asset sector.

1.5. Progress in the United States: The Financial Innovation and Technology for the 21st Century Act (FIT21) clarifies the regulatory responsibilities of the SEC and Commodity Futures Trading Commission over digital assets, providing a structured framework to address key concerns and support bipartisan policy.

1.6. Countries Pacing Up:

1. **Turkey**: Introduced a comprehensive crypto bill for licensing crypto firms under the Capital Markets Board (CMB).
2. **South Korea**: Implemented laws to curb illicit activities in the crypto market and considers abolishing income tax on crypto gains.
3. **Taiwan**: Issued guidelines to enhance market transparency and security, with crypto exchanges forming a regulatory office to ensure compliance and risk management.

Post the G20 summit in India, significant strides have been made in shaping the global approach to crypto assets. The G20 countries have endorsed a comprehensive regulatory framework designed to enhance international cooperation and establish robust standards for crypto regulation, striving to balance innovation with the necessary oversight to ensure consumer protection and financial stability. Additionally, the implementation of the Crypto-Asset Reporting Framework (CARF) and updates to the Common Reporting Standard (CRS) have been accelerated to increase market transparency and compliance. The consensus is clear: crypto assets will not be recognized as legal tender, thus safeguarding monetary stability, yet no ban on crypto assets is contemplated. Instead, the focus is on licensing and registration for issuers to prevent illegal activities, coupled with improved data sharing and transparency measures among nations to monitor and regulate the crypto environment effectively. These developments reflect a commitment to regulate rather than restrict, aiming to harness the benefits of digital innovations while mitigating their risks.

As Brazil takes the lead in the G20 presidency, we hope to see more international cooperation, fostering a collaborative approach to crypto regulation that balances innovation with investor protection.Brazil’s leadership is expected to foster a collaborative approach, encouraging more countries to adopt consistent and effective regulatory measures, ultimately contributing to the stability and growth of the global crypto industry.

2. Roadmaps of standard setting bodies for crypto assets

Financial Stability Board (FSB)

The roadmap for crypto-assets in 2024, as detailed by the Financial Stability Board (FSB), emphasizes a comprehensive approach to maximizing the value of its initiatives to enhance global financial stability, particularly in response to digital innovation and market dynamics.

The FSB is focused on the effective implementation of global regulatory and supervisory frameworks for crypto-asset activities and markets, including global stablecoin arrangements. This effort is particularly crucial in emerging market and developing economies (EMDEs), where the use of crypto-assets is relatively more prevalent compared to advanced economies. Key activities include the completion of a crypto-assets implementation plan, analysis of financial stability implications of tokenisation, and a report on developments in artificial intelligence and their potential impacts on financial stability.

International Organization of Securities Commissions (IOSCO)

In response to the ongoing evolution and growing significance of crypto-assets, IOSCO is set to revise its 2020 report aimed at enhancing investor education for retail investors. Given the sustained priority of crypto-assets within IOSCO’s framework, this updated report will incorporate new insights into the behaviors, demographics, and experiences of retail investors across its member jurisdictions. The final report, expected in the second half of 2024, will not only detail these findings but will also showcase educational materials from Committee 8 members. These examples will serve as resources for other IOSCO members to design their own educational and protection strategies for retail investors in the crypto-asset space.

Furthermore, IOSCO is advancing its Crypto-Asset Implementation Roadmap, which received board approval in December 2023. This comprehensive initiative aims to facilitate the timely and effective implementation of the Crypto-Asset and Decentralized Finance (DeFi) Recommendations across its member base. The first phase of the roadmap, to be completed in 2024, involves a thorough stock-take of existing regulatory approaches to crypto-assets among IOSCO members.

This foundational phase sets the stage for the development and subsequent piloting of an assessment methodology for these recommendations, beginning in the latter half of 2024. This methodology will ultimately guide the comprehensive evaluation of the Crypto-Asset recommendations in subsequent phases, coordinated by IOSCO's Fintech Task Force and Assessment Committee.

Financial Action Task Force (FATF)

The FATF has been actively monitoring and implementing Recommendation 15, which focuses on virtual assets and Virtual Asset Service Providers (VASPs). This initiative stems from the inherent international and borderless nature of virtual assets, emphasizing the need for robust regulation to mitigate global risks.

Serious concerns such as the theft and laundering of virtual assets by the Democratic People’s Republic of Korea (DPRK) for weapons proliferation, and the use of virtual assets for ransomware payments and terrorist financing, underscore the urgency of this regulatory focus. The FATF has strengthened its guidelines to aid jurisdictions in effectively regulating and supervising VASPs for AML/CFT purposes.

The FATF’s approach includes a detailed evaluation of the implementation status among its members and other jurisdictions with materially important VASP activities. This assessment helps in understanding the compliance with and adoption of the FATF standards.

.

Jurisdictions are encouraged to regulate or, depending on their risk assessments, potentially ban VASPs, highlighting the critical role of global cooperation in managing the challenges posed by virtual assets. The ongoing efforts aim to support jurisdictions in enhancing their regulatory frameworks to address the risks associated with virtual assets effectively.

10. RECOMMENDATIONS: PRINCIPLE BASED REGULATION

Key Themes:

This section recommends a set of guiding principles and for a comprehensive regulatory framework over the VDA /crypto ecosystem.

Guiding Principles

While developing the model regulation, there are a few key principles we believe any policy makers should be cognizant of. These have been chosen for the specific quality of being independent of technological change, and will be (largely) invariable regardless of the type of product or direction technology is taking :

- **Protect consumers:** Ensure that appropriate safeguards are in place to protect consumers from financial loss due to fraud or market volatility.
- **Promote financial stability:** Develop regulations that address risks to the stability of the financial system, such as the potential for VDAs to be used to evade monetary policy.
- **Prevent illicit activities**: Put in place measures to prevent the use of VDAs for illicit activities such as money laundering or financing terrorism.
- **Foster innovation:** Encourage innovation in the VDA sector while also ensuring that appropriate safeguards are in place.
- **Ensure fair competition:** Develop regulations that promote fair competition among market participants.
- **Promote financial inclusion:** Consider how VDA regulation can be used to promote financial inclusion for underserved populations.
- **Protect personal privacy**: Ensure that appropriate measures are in place to protect personal privacy in relation to VDA transactions.
- **Promote investor education:** Encourage the development of investor education materials and programs to help consumers make informed decisions about VDA.
- **Foster international cooperation:** Work with other countries and international organizations to develop a coordinated approach to VDA regulation.
- **Ensure clear and consistent regulation:** Develop clear and consistent regulations that are easy to understand and follow.

2. Key Aspects of Regulation

The following list provides 10 key aspects of regulation that must be considered when developing an appropriate framework in order of priority.

2.1. Definition & Classification

- **Proposed Regulation**: Define VDAs as 'digital representations of value', rather than fitting them into existing asset categories like commodities or securities. Regulate based on specific activities or use cases, recognizing their diverse applications.

- **Rationale**: VDAs are multifaceted and cannot be easily classified into a single existing category. Tailored definitions will help balance regulation with innovation, benefiting consumers, businesses, and the economy.

2.2. Regulatory Body

- **Proposed Regulation**: Establish an inter-ministerial committee comprising finance, technology, and consumer affairs stakeholders, alongside industry representatives, to oversee and regulate the VDA economy.

- **Rationale**: The VDA ecosystem intersects multiple domains, requiring a coordinated approach. A single regulatory body can manage the diverse.

2.3. Licensing & Registration for VDA Service Providers

- **Proposed Regulation:** Introduce a licensing framework for VDA exchanges and brokers, including standards like majority domestic holding and minimum net worth requirements.

- **Rationale:** A licensing framework will facilitate enforcement, promote local businesses, and level the playing field by requiring foreign exchanges to comply with domestic regulations.

2.4. User Protection

- **Proposed Regulation:** Mandate education campaigns, responsible advertising, transparency requirements, grievance redressal mechanisms, and minimum security standards. Allow the creation of insurance products to protect customers.

- **Rationale**: A robust framework will safeguard consumer interests, ensure privacy and security, and build consumer confidence in using VDA technology.

2.5. Taxation

- **Proposed Regulation:** Develop a conducive tax framework aligned with similar assets and and create a level playing field for all the participants.

- **Rationale:** A clear and progressive tax structure will encourage the use of compliant exchanges, enhancing regulatory visibility and reducing reliance on offshore platforms.

2.6. Safe Harbor & Support

- **Proposed Regulation:** Introduce safe harbor provisions for VDA intermediaries and start-ups. Support incubation centers and establish infrastructure for token-based projects.

- **Rationale:** Encouraging the development of VDA technology can drive economic growth and innovation, positioning the country as a global leader in the Web3 ecosystem.

2.7. Harmonizing with Existing Regulatory Frameworks

- **Proposed Regulation:** Ensure VDA exchanges comply with all applicable laws, regulations, and rules in the country.

- **Rationale:** New VDA regulations should complement existing laws, particularly in areas like anti-money laundering and consumer protection, ensuring a cohesive regulatory environment.

ENDNOTES

1. Nader Dabit https://www.freecodecamp.org/news/what-is-web3/
2. Peter Levine, Jennifer Li https://future.com/open-source-community-commercialization/
3. Miles Jennings https://future.com/web3-decentralization-models-framework-principles-how-to/
4. Chris Dixon https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e
5. https://sgp.fas.org/crs/misc/IF12075.pdf
6. https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/defirep.pdf
7. https://a16z.com/wp-content/uploads/2022/01/WEB3-Policy-Handbook-PxP.pdf.pdf
8. https://bitnodes.io/nodes/all/
9. https://www.ibm.com/in-en/topics/smart contracts#:~:text=Smart%20contracts%20are%20simply%20programs,intermediary's%20involvement%20or%20time%20loss.
10. https://freedom-to-tinker.com/2018/02/26/blockchain-what-is-it-good-for/
11. https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf
12. https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf
13. https://future.com/what-is-decentralized-finance
14. https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf
15. https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/defirep.pdf
16. https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf
17. https://www.bis.org/about/bisih/topics/cbdc.htm
18. https://www.atlanticcouncil.org/cbdctracker/
19. https://www.bis.org/press/p240403.htm
20. https://business.cornell.edu/hub/2023/04/28/nigerias-enaira-cbdc-what-went-wrong/
21. https://www.bbc.com/news/world-africa-64626127
22. https://www.coindesk.com/policy/2024/05/13/chinas-digital-yuan-isnt-taking-off-despite-state-employee-salary-trial-report/
23. https://www.bloomberg.com/news/articles/2021-05-09/china-s-much-hyped-digital-yuan-fails-to-impress-early-users
24. https://www.atlanticcouncil.org/cbdctracker/
25. 25.https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf
26. 26.https://documents1.worldbank.org/curated/en/369001638871862939/pdf/Central-Bank-Digital-Currencies-for-Cross-border-Payments-A-Review-of-Current-Experiments-and-Ideas.pdf
27. https://www.bis.org/publ/work989.pdf
28. https://www.ledgerinsights.com/tokenized-deposits/
29. https://documents1.worldbank.org/curated/en/369001638871862939/pdf/Central-Bank-Digital-Currencies-for-Cross-border-Payments-A-Review-of-Current-Experiments-and-Ideas.pdf
30. https://www.imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook How Should Countries Explore CBDCs?

ENDNOTES

31. https://www.bis.org/publ/work989.pdf
32.https://www3.weforum.org/docs/WEF_Modernizing_Financial_Markets_with_Wholesale_Central_Bank_Digital_Currency_2024.pdf
33. https://enaira.gov.ng/design-paper/
34. https://www.imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook How Should Countries Explore CBDCs?
35. For example, MakerDAO and DAI, the most popular crypto based stablecoin, uses ETH as collateral, yet maintains a dollar peg.
36. This list is from Market Cap (Taken from coinmarketcap.com (As on 24/7/24)
37. https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework
38. https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/defirep.pdf
39.https://ibsintelligence.com/ibsi-news/decentralized-finance-defi-market-set-to-soar-to-48-02bn-by-2031-study shows/#:~:text=According%20to%20SkyQuest%2C%20the%20global,period%20(2024%2D2031)
40. https://www.bitget.com/price/category/distributed-computing
41. https://app.rwa.xyz/
42. https://defillama.com/protocols/RWA
43. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

AUGUST 2024