International Telecommunication Union

DIGITAL CURRENCY GLOBAL INITIATIVE

TELECOMMUNICATION
STANDARDIZATION SECTOR

(05/2023)

Report of the Interoperability Workstream

Policy and Governance Working Group

DISCLAIMER

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of Digital Currency Global Initiative partners, including the International Telecommunication Union, or Stanford University. The mention of specific companies, or of certain manufacturers' products does not imply that they are endorsed nor recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. The Digital Currency Global Initiative partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the Digital Currency Global Initiative partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

About this report

This report was prepared by Vipin Bharathan Vice Team Leader of the Policy and Governance Working Group of the Digital Currency Global Initiative, as part of the activities of the Interoperability workstream. The author would like to acknowledge the contributions of the following persons below for their inputs to the report:

1. Eric Cohen
2. Justine Humansky

Table of Contents

Table of figures

1 Introduction

This document has been created to provide a systems view on interoperability of digital currencies and as a guide to standards development organisations.

The document starts with a basic definition of interoperability in digital currencies. Contributions from members on the different interpretations of interoperability is followed by a survey of the field of digital currency interoperability. Following this is a set of recommendations towards digital currency interoperability standards. The recommendations have been crafted by combining many sources: the interpretations of interoperability by members, industry use cases contributed to the work-stream, standards documents on interoperability published by banks, international organisations, the industry and experts. The document ends with a set of references.

Interoperability is a crucial component of the technical and non-technical aspects of the creation of national and international systems for the exchange of value. These cover remittances, as well as payments for services and goods across multiple networks in the service of an economy that affects all people. The concept of interoperability covered in this document is across all forms of digital currency. The need for and value of interoperability for blockchain and distributed ledger technologies goes beyond its relevance for digital currencies, and this document is relevant to the larger discussion as well.

1.1 Definition

Digital currencies under the purview of the DCGI include cryptocurrencies, stablecoins, e-money and central bank digital currencies (CBDCs).

The ISO Definition of Interoperability[1] (based on ISO 19941:2017), states that interoperability is the ability for two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

There are numerous definitions of interoperability. Most of them refer to interoperability systems which exist independent of each other. In the most generic sense, these concern systems which may include analog systems and processes. This document addresses only a subset of this definition of interoperability. The interoperability between digital currency systems.

The basic definition of interoperability for the purposes of this document is the ability of two or more systems to exchange information and mutually use this information, at least one of these systems should be a Digital Currency System (DCS). In this sense, an interface to read(or query) a DCS is a part of the interoperability section.

A DCS is a system that implements one of the types of digital currencies noted in the first paragraph of this section. The definition of interoperability can be further refined as the ability of two or more digital currency systems to exchange their currencies.

The definition is broad enough to include meta-data including proof of verification (eg. consensus proof), legal underpinnings, liquidity, regulatory compliance, proof of audit, reporting and any other information that facilitates interoperability.

[1] Kosanke, Kurt. (2006). ISO Standards for Interoperability: a Comparison. 10.1007/1-84628-152-0_6

1.2 Motivation For Interoperability

All digital currencies are not implemented in a single DCS. Protocols and infrastructure used to implement these DCS can also be different. Even if they are implemented on a single instance of a protocol, such as the different tokens implemented in Ethereum MainNet, they are in effect isolated from each other in currency islands without mechanisms to swap between them, which is an interoperability construct. Not only that, these DCS are at various stages of development and maturity. Wildly disparate value, scale and digital currency characteristics distinguish the individual currencies in different DCS.

The aim of interoperability is to create bridges between these DCS, to be able to use a digital currency in multiple venues, to make payments or store value in multiple systems.This is especially true if the behaviour and the economic characteristics of these DCS are heterogeneous. Interoperability is a unifying concept, creating liquidity and a marketplace for the exchange of currency between systems, which is amplified by the ease of converting between currencies. Paradoxically, this increase in the ease of transfer allows for an individual DCS to be more specialised and competitive by increasing diversity without causing undue fragmentation and marooning of a currency. Interoperability can increase **Scalability and Privacy**, by offloading transactions and by being able to transact in different systems with different privacy guarantees.

1.3 Current State

As the number of DCS have increased, especially cryptocurrency systems, the number of papers dealing with interoperability have increased. Most of these papers deal with blockchain based crypto-currency as well as stablecoin systems, whose rates of growth are correlated. There are several comprehensive surveys or systemization of knowledge papers. Many are descriptions of solutions that have been implemented. However, most of the papers remain at the technical level, rarely venturing beyond the semantic layer and technical implementations[2].

2 Perspectives on Interoperability

Several different ways of viewing interoperability are examined in this section. These are ways of looking at interoperability from different perspectives. These views serve as a guide to suggesting standards for interoperability as well as for implementation. Some of these are from existing practice in Interoperability. Others from similar analyses in related fields. When creating recommendations for standards, each view is taken in turn to express the recommendation.

2.1 Layered approach

The lower layers of the model make the other layers possible, building capability through the layers. The implementation of any layer can be changed without affecting the other layers. The actual pace of change can be independent as well. There are limits to such independence, since the higher layers

[2] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. 1, 1 (March 2021), 63 pages. https://arxiv.org/abs/2005.14282v3 p 2.

depend on the content conveyed by lower layers. One way to achieve this independence is through the use of registries.

2.1.1 Structural Layering

In Figure 1 the layering technique separates the purely technical layers from the behavioural and policy layers. Technical implementers usually speak of the bottom three layers. Complete interoperability standards should address all the layers. These layers are present in any non-trivial digital currency system and in many legacy systems.

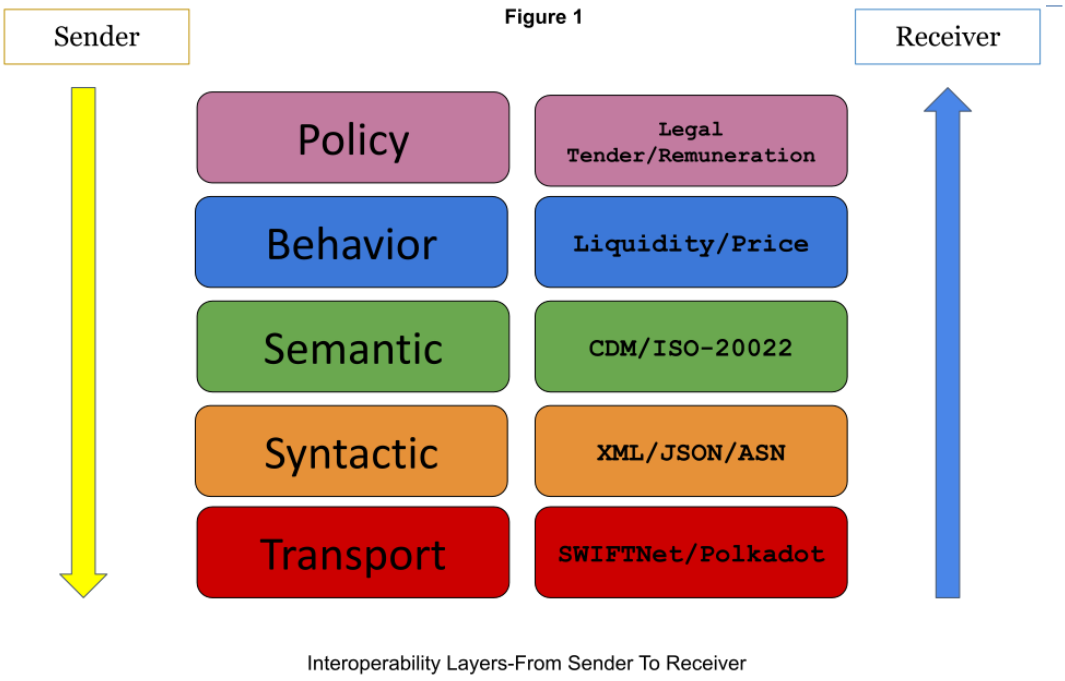


Figure 1

Interoperability implementations also have these layers. NIFO (National Interoperability Framework Observatory) suggests that such layers function within an interoperability governance framework which cross-cuts all the layers.

Interoperability standards should provide clarity on what, if any, of the policies or behavioural aspects of the source and destination DCS are enforced. Even if technically possible using the lower layers, Policy layer limitations should be transparently enforceable. For example, the FATF directives for Digital Currency (implemented through VASPs or Virtual Asset Service Providers) called the travel rule[3] needs to be implemented for the originating jurisdiction and the destination jurisdiction. Even in a borderless digital currency, this means collecting data on senders and

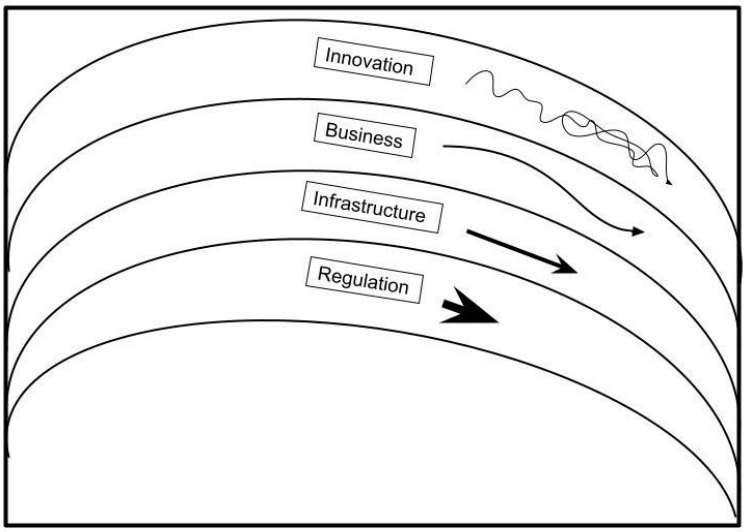
[3] International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, FATF 2012, Amended 2022, pp 71-75 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

recipients for transactions greater than $1000 (USD). This applies to any intermediary such as an exchange.

In Figure 1 the sender and receiver operate the layers in reverse order. Any layers that do not map due to different standards being used, need adaptors to convert from the sender's layer to the receiver's layer. Sometimes, these conversions are not possible, especially in the Policy or Behavior layers. In this case the guarantees have to be dialled down to the intersection of the capabilities between the sender and the receiver, to the more stringent of the two.

2.1.2 Pace Layering

Figure 2



Pace Layering in Software

Figure 2

The term pace layering refers to the difference in pace or speed of change in the various layers that make up any system. A system made up of layers that differ in the speed of response to stress and rapid demands is more stable and resilient. The dynamism of the upper layers is undergird by the stability and slowness of the lower layers. In addition to speed the layers are characterised by differences in scale and size. Stewart Brand[4], first proposed this name for such a complex system pattern, which he used to analyse and explain the stability of civilizations. However, there have been many other references to the pattern in software structures, in built architecture and and . A modified diagram applied to software and regulation can be seen in figure 2. Brand asserts that all

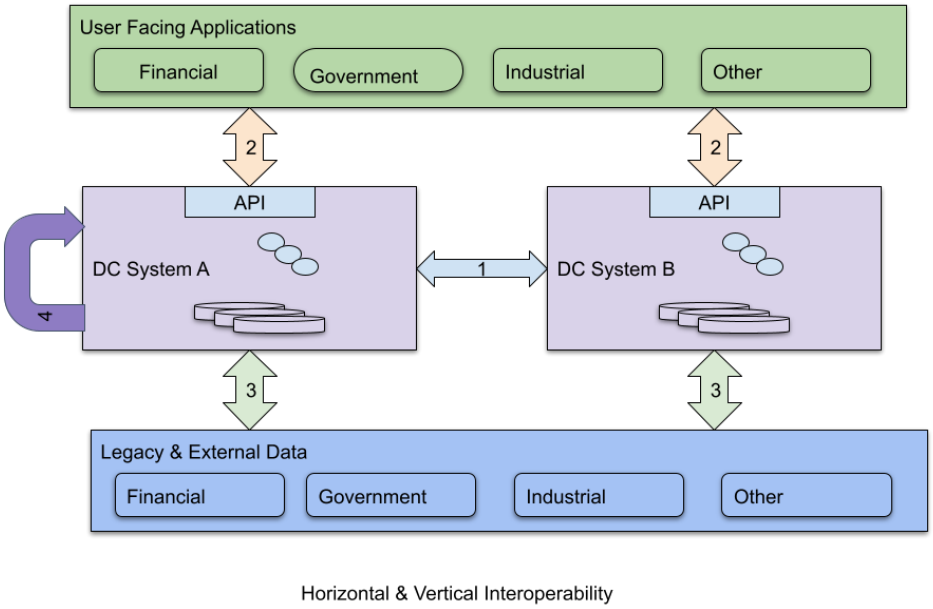
[4] Brand, S. (2018). Pace Layering: How Complex Systems Learn and Keep Learning. Journal of Design and Science. https://doi.org/10.21428/7f2e5f08

durable dynamic systems share this structure. Gartner[5] proposed this layering to govern software applications through their life-cycle, they propose three layers: systems of innovation, systems of differentiation and systems of record. The aim was to create a strategy to govern a firm where all three layers co-exist. One of the key takeaways from Gartner was the creation of glue elements that maintain the friction, yet integrate the governance of the layers. These include standards and regulations in addition to Identity and Access Management and master reference data to increase interoperability between the layers. The initial papers are from 2012. If updated for the current landscape, the suite of glue tools includes Blockchain, Payment rails and other infrastructure that creates collaboration between firms to mutualize the source of truth as well as to cross inter firm, national and jurisdictional boundaries.

Durable dynamic complex currency systems have a pace-layering structure. Interoperability pace-layers consist of the innovation layer, the business layer, the infrastructure layer and the regulation and standards layer. Standards creators have to be aware of this and address it in the standards. The fact that standards lag innovation can be explained by pace-layering. Slower lower layers change more slowly, however this pace can be increased if the challenges from the higher layers are more intense. DeFi, which is one way of implementing interoperability, the pace and intensity of higher layers such as innovation in the AMM algorithms, the new businesses being built on top, have increased the calls for regulation and associated standards to adapt.

2.2 Horizontal and Vertical

Figure 3



Horizontal & Vertical Interoperability

Figure 3

[5] Genovese, Y. (2012, January 9). *Accelerating Innovation by Adopting a Pace-Layered Application Strategy*. Gartner. https://www.gartner.com/en/documents/1890915/accelerating-innovation-by-adopting-a-pace-layered-appli

This view takes the perspective of whether the interoperability is between an external system and a digital currency system or directly between two DCSs. This model is from ITU SG 16, and a very common way of modelling interoperability.

The initial case is labelled 1, which is the direct interoperability between two DCS. In practice, an implementation of 1 involves intermediaries, purely decentralised exchanges are not possible[6]. The distinction between user facing apps and back end systems are labelled 2 and 3, respectively. Another class of vertical applications are querying applications that extract data in order to do subsequent analysis, either for interoperability or for analysis. The results of the analysis can be used in various applications built on top of the interoperability stack.

2.3 Digital currency interoperability capability maturity model (DCICMM)

The DCICMM is based on the capability maturity model integration (CMMI[7]). The initial idea was suggested by Eric Cohen, a member of the ISO/TC 307 as well as one of the leaders of the XBRL community. A capability maturity model is not a process model. It is an assessment technique for measurable progress across the various levels. DICMM recognizes that the final state is not static, it is a *continuous quest for perfection* that allows for evolution. Certain tools and metrics can be used to assess the capabilities of interoperability for any DCS and can be placed in the maturity model. When two DCS interoperate, the capability of the interoperation is limited by the DCS with the lower capability.

[6] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. 1, 1 (March 2021), 63 pages. https://arxiv.org/abs/2005.14282v3

[7] Capability Maturity Model Integration. (2021, October 1). In *Wikipedia*. https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

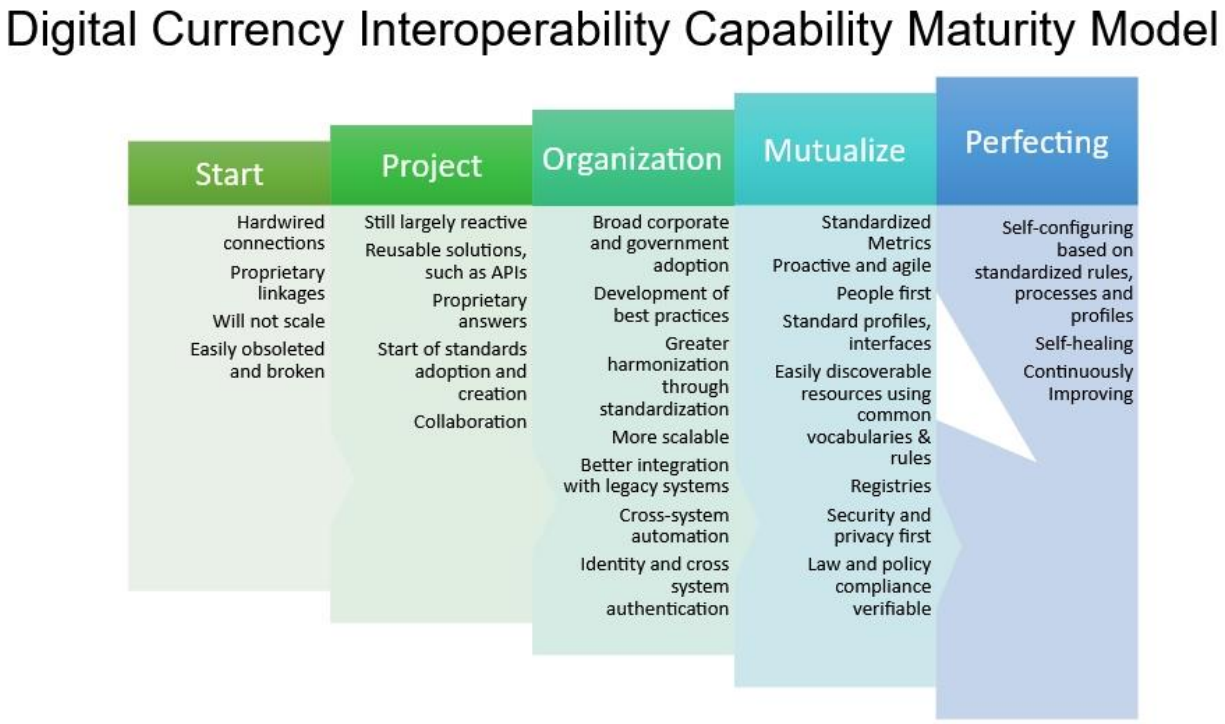


Figure 4

2.4 Monetary Policy & Market Considerations

As currencies, monetary policy considerations such as money supply, velocity of money, remuneration(interest) have a great bearing on convertibility and fungibility of currencies. Additionally systemic stability, global contagion and capital market controls may operate at the higher levels of theInteroperability stack (Figure 1). Related, but not entirely separate are fiscal policy controls such as taxation covering swapping of currencies, especially as it applies to fiat swaps. These considerations impinge on the interoperability between different DCS. The structure and dynamics of the market for exchange between different digital currencies depends on liquidity, price and market clearing. Market clearing mechanisms are also regulated in terms of participants, limits, concentration risks and so on. Standards for DCS interoperability have to address these topics, either by referring to existing standards, regulations, measurement and reporting techniques and also by ensuring a path forward for updating the standards to handle emerging interoperability use cases based on observations during periods of stress.

Moneyness is defined by Merriam Webster as the quality or state of being convertible to cash, in other words liquidity. Another definition of moneyness has to do with derivatives, the closeness of the price of a derivative with respect to the price of an underlying. In this section the basic definition of money is used to examine moneyness. The three functions of money viz. store of value, unit of account, and medium of exchange and how the currency in a DCS embodies these functions can create a measure of moneyness. Convertibility to cash is thus a short-hand for such a measure, as cash approaches perfect moneyness.

Unit of account and medium of exchange functions depend on the store of value function. Monetary stability is the measure of this, severe inflation or deflation threaten the other two functions. If there is deflation, there would be a tendency to hoard money, and the opposite for inflation. Digital currencies are meant to function in these three capacities. In practice, they have different degrees of moneyness. At any instant, the interoperability between two digital currencies might be at a

premium or a discount depending on the perceived relative moneyness of the currencies. In extreme cases of stress this exchange can cease to function. Moneyness is a dynamic property, changing constantly and evolving over time.

This spectrum of moneyness can range from NFTs, at the low end, through crypto-currencies to stable-coins to CDBDCs. A properly implemented CBDC should be convertible at par to cash. As far as moneyness goes, it is highly liquid.

In conventional markets, Liquidity Coverage Ratios (LCR) and Net Stable Funding Ratios (NSFR) have been developed to implement controls on liquidity. LCR deals with the liquidity of the current backing asset mix and NSFR with assured liquidity for a set time into the future. When there are identifiable intermediaries, like in the case of non-algorithmic stablecoins these requirements can be mandated[8]. For interoperability between stablecoins and fiat currencies, transparency of these ratios through standards may affect the price and stability of the interoperability system.

It is bound to be a challenge to implement similar metrics for a fully decentralised automated system that operates an autonomous interoperability venue. These AMMs (automated market makers) have been liquidity starved at crucial points when the price of one of the pair of assets starts to drop precipitously.

As the scale and volume of interoperability solutions increase, the risk of contagion, or threat to the wider economy beckons. An example is the reported $30 billion of corporate bonds backing USDT, a popular stablecoin; if there is a run on USDT, a forced liquidation of corporate bonds can cause contagion in the corporate bond market, which can spread to other markets due to leveraged derivative positions.

3 Interoperability Solutions

Short technical notes are presented on interoperability structures, use cases and concepts. These notes describe the structure and taxonomy and then contribute to recommendations for standards, which join the list in 4.1. General principles and recommendations for Interoperability standards are drawn from the patterns of usage and vulnerabilities are drawn from historical data and from a resilient approach to emergent effects, never seen before. Many of the challenges are due to the fact that most public crypto-currencies are global in reach and scope whereas most laws are confined to nations, in cases where the law reaches beyond a nation, it is often not easily enforceable or is in the realm of recommendations, similar to FATF guidance.

The first portion of this appendix is on ***Stablecoins*** as they are the most important vector of interoperability through which DeFi itself becomes possible. Stablecoins purport to put fiat on-chain. Stablecoin adoption is the main reason for the growth of the DeFi ecosystem which in turn stimulates more Stablecoin issuance and newer projects to come on line.

Layer 2 (L2) constructs help escape the scalability constraints, high fees,lack of privacy and low transaction speed of public blockchains like Bitcoin or Etherum. Analogous protocols can be implemented in Enterprise or permissioned blockchains. However, they may not be as necessary in these contexts as permissioned blockchains are not challenged in the same manner as public

[8] Prudential treatment of cryptoasset exposures Issued for comment by 10 September 2021

Bank of International Settlements. https://www.bis.org/bcbs/publ/d519.pdf

blockchains which are highly decentralised as far as validators and creators of new blocks enforcing the sequence of events. **Lightning Network** as a representative of L2 is examined next.

Another construct that allows Interoperability are ***Blockchain Bridges***. We will look at the basic ideas behind Blockchain Bridges. Blockchain Bridges are in the news for hacks and exploits as being some of the most vulnerable constructs. Further we go into why and whether any guidance for standards can be extracted from the past with thoughts to the future.

The next topic is ***DeFi***, concentrating on DEXs like AMMs first and Yield Farming second. AMMs allow swapping one coin for another, an interoperability capability. In this pairwise universe, one of the pairs is a stablecoin, most of the time. More complex AMMs are also known, that swap between different coins. We will put that in context.

Various protocols and frameworks that create secure Interoperability capabilities are discussed next, standardisation at all levels of the Interoperability stack (Figure 1). The constructs include Data Semantics, Proof of Reserves, Dynamic Market Metrics such as measures of liquidity. Since space is limited, a subset of such possible constructs are discussed. The main idea is that Interoperability, like most complex concepts, is a systemic complex, emerging from the actual protocols for raw Interoperability strengthened by these constructs. Interoperability spans a spectrum from weak to strong.

3.1 A.1 Stablecoins

Stablecoins are an interoperability mechanism. A Stablecoin, as the name promises, represents relative stability on-chain. This stability is in contrast to the volatility of crypto-currencies. Stablecoins are meant to achieve stability by being pegged to an off chain index or reference which is relatively stable. A particular Stablecoin achieves interoperability between its peg and the wide world of unstable crypto-currencies and digital assets. The most widely used peg is the USD, the current global currency. Thus, a Stablecoin, which is a crypto-currency itself, can be seen as a bridge between fiat currencies and volatile crypto-currencies. Stablecoins are also being touted as a payment rail.

Money has three major functions, a store of value, a unit of account and a medium of exchange. They are all based on stability, without stable value, prices for goods and services cannot be stable and hence exchange for quoted goods or services is not practicable. This is why high inflation or deflation is a challenge for any instrument used as money. Stablecoins, with this promise of stability, allow the rapid switching between crypto-currencies which are volatile and the stablecoin itself. The reason participants want to be exposed to the volatility of crypto-currencies is to participate in the trading and holding of volatility, to be able to speculate on price appreciation, and also participate in the rich ecosystem of Decentralised finance. The switching or interoperability rails usually reside in exchanges. These exchanges can be centralised or decentralised. Decentralised exchanges are examined in the section below dealing with DeFi.

The taxonomy of Stablecoins can be seen in the following diagram. The diagram is adopted from Moin et al[9]. This taxonomy does not cover all possible cases. The peg and the mechanism are the most important drivers of the stability of any stable coin. The biggest stablecoins that constitute 95%

[9] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. 2020. SoK: A classification framework for stablecoin designs. https://doi.org/10.48550/arXiv.1910.10098

or more of the total value are pegged to USD today. These are centralised, issued by a single intermediary and often custodied by the same entity. These axes are not completely orthogonal. Many stablecoins use combinations for mechanisms, price discovery and reserves. HQLA are high quality liquid assets.

Another way of looking at Reserves which back the stablecoins is to segment them into custodial and non-custodial stablecoins[10]. In custodial stablecoins, entities that resemble traditional intermediaries custody the reserves and holders of the Stablecoin have a claim against the reserves. In a non-custodial setting, the reserves are reachable by smart contracts and backed by economic models for participation through a dual coin or a hybrid reserve approach where there are no conventional reserves, and no traditional custodians. These are usually referred to as algorithmic stablecoins. Even though these are called non-custodial, custody still happens in some of these coins, namely the custody of crypto-currencies or other assets through the medium of smart contracts.

3.2

Peg	**Fiat**	**Commodity**	**Index**	
Mechanism	**Reserve**	**Algorithmic**		
Reserve	**Fiat**	**HQLA**	**Commodity**	**Liquid Crypto**
Reserve ratio	**Full**	**<100%**	**>100%**	**None**
Market Info	**Oracle**	**Market**	**Voting**	

The graph given below gives an idea of the current market value of stablecoins[11]. As can be seen, the majority of the value is concentrated in three custodial stablecoins (Tether, USDC and BUSD), the only non-custodial stablecoin of note is DAI. Also noteworthy in this graph is the collapse of Terra (TUSD) due to deleveraging spirals, which were foretold and studied in depth[12]. In the case of TUSD,

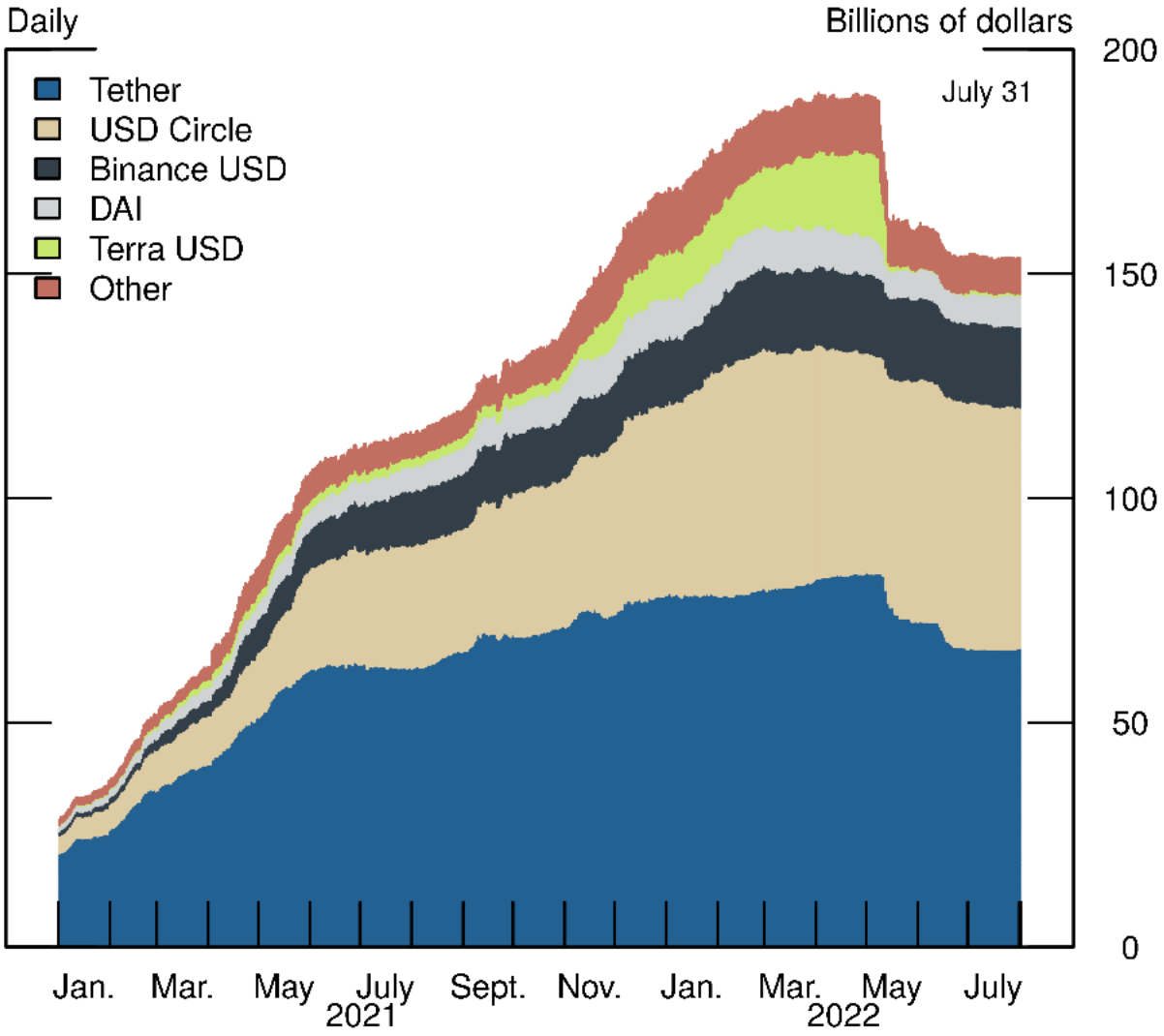
[10] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic Foundations and Risk-based Models. In 2nd ACM Conference on Advances in Financial Technologies (AFT'20), October 21–23, 2020, New York, NY, USA. ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3419614.3423261

[11] Azar, Pablo D., Garth Baughman, Francesca Carapella, Jacob Gerszten, Arazi Lubis, JP Perez-Sangimino, David E. Rappoport, Chiara Scotti, Nathan Swem, Alexandros Vardoulakis, and Aurite Werman (2022). \The Financial Stability Implications of Digital Assets," Finance and Economics Discussion Series 2022-058. Washington: Board of Governors

of the Federal Reserve System, https://doi.org/10.17016/FEDS.2022.058.

[12] Ariah Klages-Mundt, and Andreea Minca (In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. https://doi.org/10.48550/arXiv.1906.02152

the contagion was limited to just the crypto-currency universe which lost 1-2 Trillion USD due to the collapse of TUSD coupled with the correlation risk with conventional markets in May/June 2022. We close this section with recommendations for standards for stablecoins in particular, based on the taxonomy and observation of the history and literature surrounding the economic models or the capital risk associated with these stablecoins.



3.2.1 A.1.2 Stablecoin Risks

These risks can be assessed by conducting two types of stress tests[13]. Can the stablecoin withstand a redemption run? In this stress test, a redemption of 100% of the stablecoin should be tested to show whether it can withstand such an event. In an existing stablecoin, this can only be a thought experiment. However, a good test to see whether a coin can survive such a run is the proof of the existence of a highly liquid reserve that covers 100% of the collateral. The second test asks the question whether there could be events that cause the peg to break and for the stable coin to move a certain % in each direction, bigger than a normal variation (say .1%). Many stablecoins rely on arbitrageurs to revert the stablecoin to peg. If these participants disappear from the market due to

[13] Two thought experiments to evaluate automated stablecoins, Vitalik Buterin, May 25 2022

stress, the stablecoin can lose its peg by huge amounts. Both of these types of events were observed in Terra/Luna collapse, and several other algorithmic stablecoin collapses.[14]

For custodial stablecoins, there are counterparty risks coupled with capital risk for the Reserves. Counterparty risks can be further split into the risk of counterparty collapsing and censorship risk, if the counterparty decides to censor the coins held by a user or a group of users. Capital risk is due to the quality of assets held in the Reserves. If the assets themselves cause contagion in conventional markets due to stress and cause the reserve value to plunge. This can happen if a stablecoin holds a significant portion of a type of asset whose market does not have the liquidity to support extreme events. For example, reserves are held in corporate bonds or even Treasury or other sovereign bonds.

For non-custodial stablecoins, the risk is mostly in the economic model and capital. It is counterintuitive to back a stablecoin with an unstable asset, especially a crypto-currency. Usually the protection to stability is in the form of over-collateralization, which is equivalent to a haircut in traditional finance. In addition, these stablecoins have risks related to smart contracts, due to bugs, weaknesses or backdoors in the code. There is a dizzying array of risks associated with stablecoins, including ways to manipulate the price through multiple means.

3.2.2 Risk Protection through standards

In addition to standards for introspecting or querying a token, standards are needed for the contracts that define the rights and obligations of participants. ISDA standards developed for Common Domain Model(CDM) and risk specific interchanges based on Common Risk Interchange Format (CRIF) [15]can be repurposed and reused in the Stablecoin ecosystem and other contexts. In addition, these should be accessible at cost to all who wish to trade the Stablecoin, through a query function call embedded in the token itself. Included in this capability should be a way to view the dynamically changing risk landscape, through easy access to a continuous audit of the system. These ideas may seem like a reach at the moment, but it continues on the path toward the adoption of certain practices from the traditional asset markets, especially those that are highly leveraged. CDM and CRIF arose from the financial crisis of 2007-2008. Several participants are eyeing proof of reserve for Stablecoins and other backed crypto-assets such as wrapped tokens, primarily used in DeFi protocols. Proof of Reserve has to be as close to real time attestation as possible. A standard for cross network transfer of value is presented the section on Secure Asset Transfer Protocol.

3.2.3 Proof of Reserve

Since the high profile failure of FTX and several other exchanges, Proof of Reserve(POR) has regained ground as an automated way of restoring trust in the system. POR automatically and continuously links off-chain or cross-chain collateral reserves to claims made about the solvency of an on-chain system.

---

[14] Austin Adams and Markus Ibert (2022)https://www.isda.org/a/aBzTE/The-Future-of-Risk-Capital-and-Margin.pdf, “Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel,”

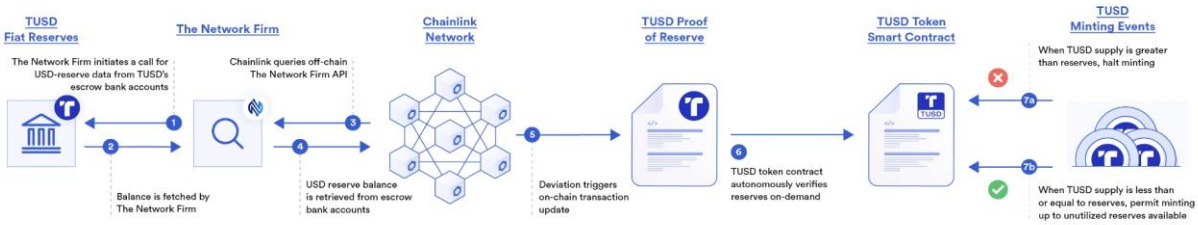
FEDS Notes (Washington: Board of Governors of the Federal Reserve System, June 2).

[15] Whitepaper: The Future of Risk, Capital and Margin Reporting, ISDA, May 2021

Non-Algorithmic stablecoins, stablecoins backed by collateral, either fiat based stablecoins or commodity based stablecoins depend on this guarantee for increased trust. For the biggest stablecoins as of this writing, such as Tether and USDC, this collateral is supposedly held in safe assets. Safe assets are usually a combination of actual dollar reserves, a pool of treasuries, in the case of USD based stablecoins, or corporate bonds. This collateral is held in commercial banks. The collateral can be locked up cross-chain assets such as Bitcoin or Ethereum. They are also subject to a periodic audit by centralised auditors, as can be seen in this example[16].

These periodic audits are slow, costly and manual. The sample above is for a January audit, released in March 2023. They are perennially late, as a lag of at least two weeks is built into the very process of auditing. In order to improve the timeliness, accuracy and trust of these audits, Proof of Reserve was proposed as an automated auditing system. The Chainlink POR, for example, is touted as a solution for this problem. A combination of decentralised attestations, integrated into smart contracts brings decentralised trust and timeliness to these audits. The pegged stablecoin is 1:1 exchangeable to fiat, the embedded optionally can cause an immediate demand for conversion to fiat, and hence prone to a run, a feature of such a system as discussed elsewhere in this document.

A diagram taken from the Chainlink website[17] shows the main components of the system for TUSD, a stablecoin. **The Reserve** which is held in a commercial bank, a network api for fetching the balances called **The Network Firm**, intermediated by the **Chainlink Network,** which feeds the **TUSD Proof of Reserve.** The Proof of Reserve(POR) feeds the **TUSD Token Smart Contract** curtailing **TUSD Minting Events,** allowing TUSD to be minted only when the amount to reserves exceeds the coin supply.



Such a system can be generalised for any digital asset backed by collateral, including tokenized Real World Assets (RWA). The prices of such tokens can be determined more accurately through POR. Price discovery in thinly traded assets is a challenge even for POR.

This system is much more timely than a manual audit conducted by human auditors. Instability in the system consists of the fact that the price of the collateral can vary independent of the token as there is an uncorrelated market for the liquid collateral. Nothing is mentioned about the scenario in which the collateral loses value and extant stablecoin supply becomes under-collateralised, in reality, this should trigger a burn of the stablecoin supply, which can only be done if there is a buffer to be burned. Counterparty risk associated with the commercial bank or any institution still exists. This is a feature, not a bug, of stablecoins.

[16] 2023 USDC Circle Examination Report January 2023, Deloitte and Touche, March 2, 2023

[17] What Are Proof of Reserves?, Chainlink, retrieved March 28, 2023

Exogenous factors such as interest rate risk, triggered by actions of external actors such as central Banks can cause collateral prices to fall. In addition, duration mismatch as the collateral is usually of longer duration than the stablecoin itself can cause an unsustainable run. The triggering of a run causes a negative feedback loop on the price of the underlying collateral, as selling pressure mounts on the collateral, depressing prices further.

An occasion to observe these supposedly black swan events was afforded by the collapse of the Silicon Valley Bank(SVB) where $3 Billion of USDC reserves were held, the ensuing depegging event brought the value of USDC down to much less than a dollar. The collapse was a result of a rapid bank run on SVB. The rescue came from fiscal authorities who guaranteed all deposits, even those worth much more than $250K. A deposit held in a banking institution, including a Globally Systemically Important Bank (GSIB), is only insured to a certain modest amount, $250K for the US and similar amounts in other jurisdictions. The collapse of a GSIB whilst not a normal occurrence, have been observed in the last 20 years. Banks, the way they are constructed today are prone to runs, especially if the deposit base is skittish or concentrated in certain industries.

A Federal Reserve account with no counterparty risk would be the best way of holding the collateral in fiat. However, the income from such a scheme will be limited by the interest rate offered on reserves. Today, in a high interest rate environment, such income from other people's money is what propels stablecoin operators. A narrow bank[18] has been proposed as the reserve for stablecoins.

A brief discussion of the way in which value changes observed through cryptographic structures depends on Merkle Trees and Zero Knowledge Proofs. A Merkle Tree constructed from the reserve balances, even from individual accounts can be used as a useful cryptographic accumulator and commitment scheme, since any change in value of individual accounts can be observed by monitoring the hash of the root of the sub-tree holding the balance. Coupled with zero knowledge methods, a proof constructed from these accounts can be provided even to the individual user without revealing the details of the other users in the subtree. Technical details have been published by stablecoin operators such as Binance[19].

3.3 Layer 2 (Lightning Network)

Blockchain protocols are said to be Layer 1. Layer 2 or L2 protocols, whilst relying on the security provided by the Layer 1 protocols, create a private scalable P2P network with low transaction fees for micropayments. This is an alternative to using a trusted third party (TTP), a centralised solution, which brings with it counterparty risk and may increase transaction costs due to monopoly. We present the Lightning Network as an example of the innovation and power of the L2 concept.

The Lightning network, proposed for Bitcoin, bootstraps secure channels of liquidity that operate independently, into a network, which can be used to make micro-payments. Lightning works with the limited scripting capability of the Bitcoin network. Each channel is secured by a 2 of 2 multi-sig contract. In combination with the Hash Time Lock Contract(HTLC) this set of bi-lateral secure channels can be turned into a network, where the payor and the payee can be connected through a series of hops. The funds are secure without a TTP and hence no counterparty risk. The transactions

[18] Narrow Banking, Wikipedia, retrieved April 2, 2023

[19] Proof of Reserves, Binance, retrieved April 2, 2023

in these channels are actual blockchain transactions, but are deferred until the channel closure. Channels can be left open for a long time as long as both participants agree.

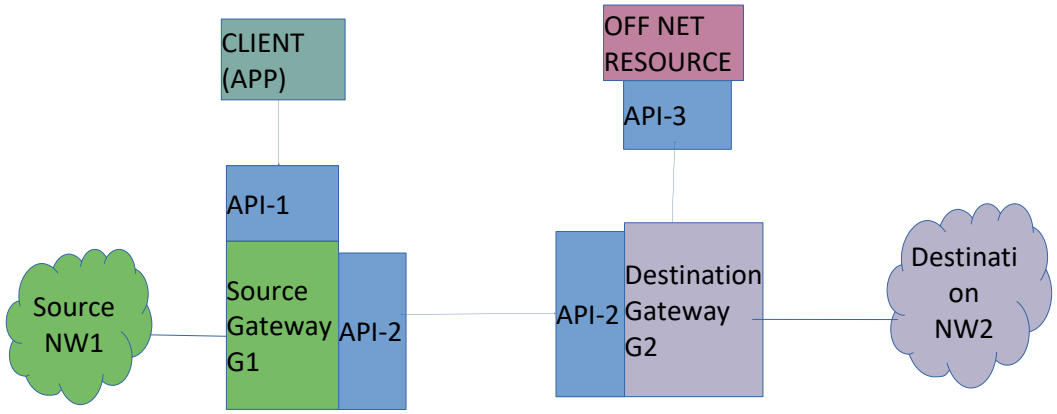
As the Lightning implementation proceeded apace, more innovation followed, in the creation and management of the network itself, separate from Bitcoin with its own mechanisms for Liquidity discovery, gossip protocols for path discovery between payers and payees and in the creation of bearer tokens and protocols for assets called Taro, which could host Stablecoins on Lightning. Taro itself came about through a rethink of the Bitcoin scripting ecosystem in Taproot and its variants including scriptless scripts. The total Bitcoin liquidity available in the Lightning Network is around 5,000 as of October 2022 (around $100 million). The Lightning Labs is a very active site of innovation and of interoperability.

3.4 Secure Asset Transfer Protocol (SATP)

The secure asset transfer protocol[20] proposes a way to transfer a digital asset in one direction between two gateways which are portals to underlying networks of value. These networks map neatly on to our concept of DCS (Digital Currency System). The digital asset is securely transferred from the source network to the destination network. The source and destination network are opaque to all entities except those who are authorised to perform reads/writes on those networks. The gateways enforces

The security of SATP enforces ACID, or Atomicity, Consistency, Isolation and Durability on the operation. ACID is a set of properties of a transaction, a single logical operation, that might involve multiple sub-operations. ACID is a key concept in database systems. SATP uses the asset-burn-mint paradigm, burning or destroying the asset in the source network and minting an equivalent asset in the destination. These operations are done through the coordinated actions of the peer gateways. Atomicity governs the success or failure of the entire transaction. Either the transfer succeeds or fails, which ensures that any half-baked results due to the failure of a part of the operation are rolled back. Consistency implies that the asset is either in the source or destination network at any time during the transfer. Isolation ensures that the asset being transferred does not participate in any other operation while in flight. Durability ensures that the effects of the transaction persist on both networks.

Given below is a schematic of the SATP setup for transfer of assets from source to destination.



The Client (application) connects with its local gateway (G1) over a REST Interface (API -1) in order to notify G1 about actions on assets in network (NW1). G1 and G2 interact with each other over a

[20] SATP Core IETF Draft, M. Hargreaves, T. Hardjono, R. Belchior April 2023

gateway REST interface (API - 2). A gateway may be required to access resources that are not located in network NW1 or network NW2 to perform its actions. Access to these types of resources are performed over an off-network REST interface (API-3). API-3 in effect is an oracle interface.

REST which stands for Representational State Transfer, is a lightweight architectural standard, usually implementable over HTTP, the basic web protocol. The information can be transferred using JSON (Javascript Object Notation), HTML, text etc. The SATP uses JSON with JWT where appropriate, JWT is a variant of JSON, augmenting its cryptographic capabilities. JSON although machine readable, can be also read by a human, usually contains a field name and a value. Example (address: 12 Sunny Field Crescent, Missoula, MI 11876).

The SAT protocol defines three flows:

Transfer Initiation flow: This flow deals with starting a transfer from one gateway to another. Several tasks are involved, including (but not limited to): (i) gateway identification and mutual authentication; (ii) exchange of asset type (definition) information; (iii) verification of the asset definition, and others. Consists of discovery using standard names or Fully Qualified Domain Names and naming of assets in an unambiguous manner.

Lock-Assertion flow: This flow deals with the conveyance of signed assertions from G1 to G2 about the locked status of an asset at NW1.

Commitment Establishment flow: This flow deals with the asset transfer and commitment establishment between two gateways.

In depth analysis of the message content and protocol itself is beyond the scope of this document; those interested can read the details of the protocol in the IETF proposal. This proposal addresses a one way transfer of assets from one network to another, employing gateways, using a burn-mint paradigm conforming to the ACID requirements. The proposal addresses a multitude of details, from discovery, asset naming, credentialling, authorisation and the protocol itself with the order and content of the messages.

3.5 Central Bank Digital Currencies and Interoperability

With the rapid innovation taking place in digital currencies and payment systems; Central Banks all over the world (9 out of 10 in the latest count by BIS) are working on creating Central Bank Digital Currencies as a public alternative and utility supporting payment systems. They are meant to be a digital form of cash and a liability of the Central Bank. As an alternative form of fiat, they are in M0, or the basic monetary supply and convertible at par with other forms of fiat; namely commercial bank money, cash and reserves on the wholesale end.

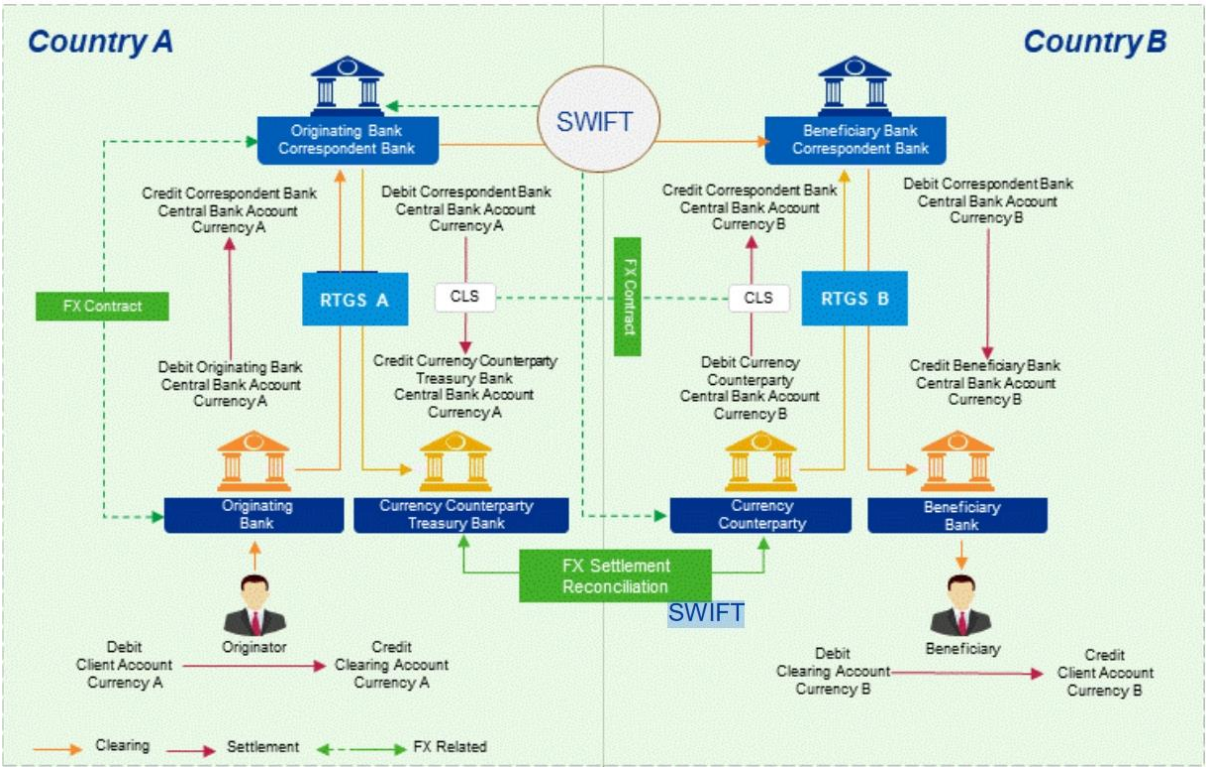
CBDCs will thus enable higher interoperability since they are a digital and frictionless form of fiat, fulfilling and exceeding many of the qualities of Stablecoins, especially since they are the direct liability of a Central Bank.

Many of the Central Bank experiments in CBDCs are in the form of pilots or research, however some have already been released into production. The CBDCTracker [21]website provides details of the current state of CBDC development all over the world.

With the advent of CBDCs it is thought that one of the most intractable problems in payments, namely cross border payments may be solvable. Today's cross border payments are error prone,

[21] The CBDC Tracker, retrieved May 19, 2023

costly and slow. The diagram[22] below illustrates the complexity. Although the diagram is from 2018 the state of the system remains similar in 2023. The complexities are due to the interaction between the clearing, settlement and FX Related portions of the cross-border payment where an originator, or payor, and the beneficiary ,or payee, reside in two different countries with different currencies. These flows and complexities are illustrated in the diagram below.



This inefficient system, cumbersome at best, is ripe for innovation. The BIS along with central banks have been conducting a series of pilots to improve the efficiency of cross border payments. Some of these pilots involve CBDCs, some do not. The other often overlooked aspects are the interoperability of CBDCs with well developed payment rails including the EMV interfaces, as well as offline payments with CBDCs. The experiments and pilots as well as their findings are examined below, starting with m-Bridge.

3.5.1 mBridge

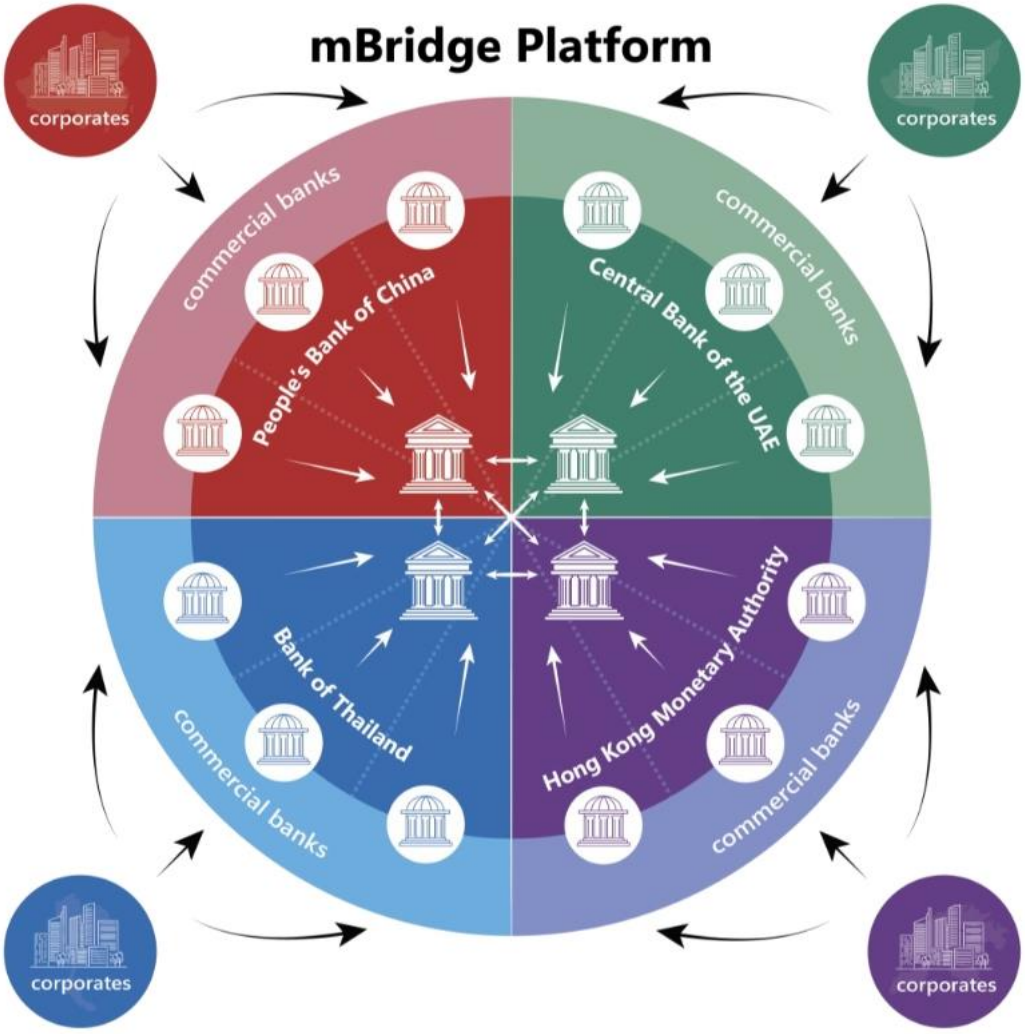
The aims of the project continue to be efficiency improvements in cross-border payments. The project mBridge report released in October 2022[23] says, “due to duplicated processes and steps in the correspondent banking chain, cross-border payments exhibit high costs, low speed, operational complexities, limited access and low transparency. These inefficiencies also introduce settlement risk into the system, to the detriment of both financial intermediaries and end users”. This statement is resonates with existing studies conducted on the subject.

Project mBridge is a natural progression of the experiments orchestrated by the BIS starting with Inthanon-LionRock. mBridge can be seen as Phase III of Inthanon-LionRock, which started out in 2019 with a single multi-currency system, with peer-to-peer settlement and a Liquidity Saving Mechanism(LSM). The LSM is a netting mechanism. Netting mechanisms reduce liquidity needs by as much as 90% . Inthanon-Lionrock(ILR) which involved the Bank of Thailand and Hong Kong Monetary Authority and the BIS Innovation Hub (BISIH). ILR was continued to the second phase with ILR2 in

[22] November 2018, Cross Border Inter-bank Payments and Settlement, Bank of Canada, Bank of England and Monetary Authority of Singapore
[23]October 2022, Connecting Economies Through CBDC BIS, BoT, HKMA, PBOC, CBUAE

Sept 2021. All of these were concentrated on wCBDC or wholesale CBDC, not accessible to retail customers. By mBridge, the target was improvement of international trade through such setups

ILR1 used Corda and ILR2 used Hyperledger Besu. mBridge with added participants, Peoples Bank of China and Central Bank of the UAE built a new native blockchain "mBridge" with all central banks. The diagram demonstrates these Added to the aims of the project were the following principles: do no harm, enhancing efficiency, increasing resilience, assuring coexistence and interoperability with non-CBDC systems and enhancing financial inclusion. These principles resonated with the participant banks since they are concerned with capital flight to a universal currency like the USD, as well as protection from sanctions, recognized to be an instrument of economic warfare.



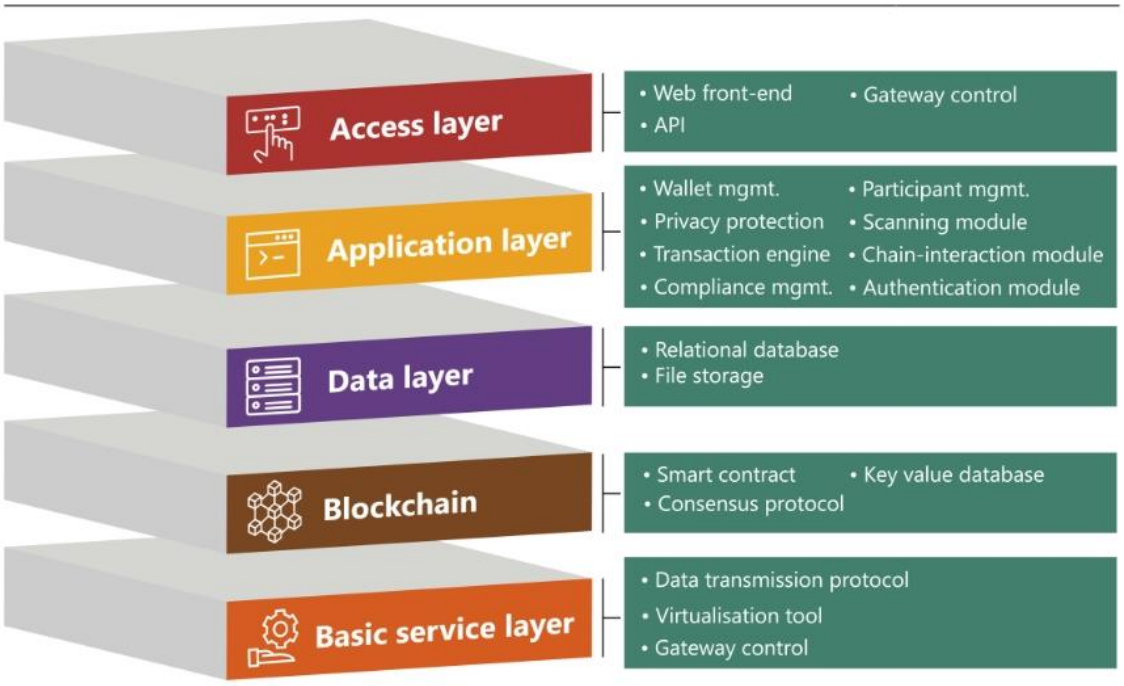
The diagram shows corporates accessing the system through commercial banks in each country. At the center is the connectivity between the respective central banks reached through the mBridge ledger, custom created for the purpose. Although intermediated through two layers in each country, the corporates experienced virtual direct peer-to-peer connections across countries. The project resulted in faster settlements, in seconds rather than days and the corresponding decrease in counterparty risk. It also afforded privacy and security of transactions.

Governance and deployment of the platform were enhanced; including three legal documents drawn up and executed by the participants. i) Pilot participation agreement: outlined central banks' role and the rights and responsibilities of the commercial bank participants. ii) Platform operating terms: provided overarching principles and procedures for commercial banks on the use of mBridge;

including settlement finality on the platform iii) Terms and conditions: outlined currency-specific rules governing the use of local CBDCs by foreign commercial banks.

These agreements were executable using click-trough digital means on the platform itself. All interactions with the platform were through modern web User Interfaces. The technical layered approach can be seen in the diagram below.

Attention to operational detail is evident in the detailed functional and technical design put forth in the main reference document from BISIH. This shows that a multi-lateral CBDC utility allowing resilient, secure and private exchange across borders is a complex multi-disciplinary undertaking.



4 Recommendations for Interoperability Standards

A mind map of the Digital Currency Interoperation space is given in Figure 5. The initial idea for this mind-map originated with Eric Cohen (private communication) identified in a prior section(2.3) as a XBRL guru and a national participant of ISO/TC 307. Any interoperability standard has to address most of the attributes noted in Figure 5.

Standards are often born from existing implementations, industry leadership and use, sometimes they are born of reinterpretation of older standards, see “Travel Rule” cited in section 2.1.1. Market strength can force adoption as a de facto standard. An example are the ERC standards such as ERC-20, ERC-721 and ERC-1155 in Ethereum. These standards are explored further in Appendix B. Token taxonomy and frameworks are published in IWA (InterWorkAlliance[24]) which can be used to implement the ERCs mentioned above, the implementation can be independent of the platform

and can guide the implementation of interoperability.

[24] https://github.com/InterWorkAlliance/TokenTaxonomyFramework

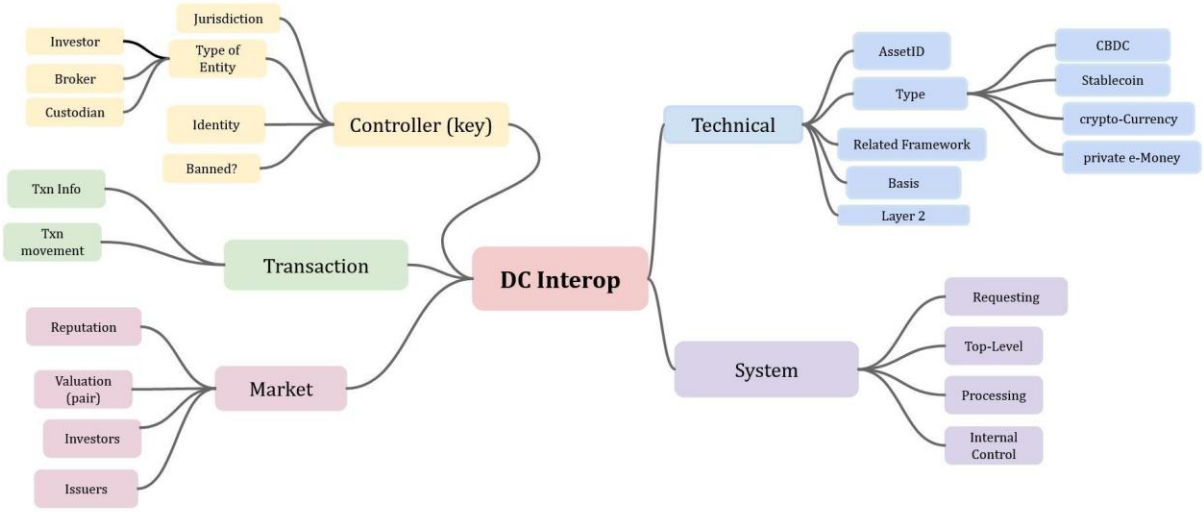


Figure 5

4.1 4.1 A Bullet List of Recommendations for Standards for Interoperability.

A. Digital Currencies Participating In the Exchange

a. Digital currency definitions and standards have to be clear before they interoperate. This can be because there is a lot of literature around them and de facto standards have been created, there is a large community around them and currencies are being developed in the open or they are well defined before they are in production. However, divergence in naming has been noticed in many areas, where different terminology is used for the same concept or operation. Appendix C provides a table of the mapping between certain systems.

b. For two digital currencies to interoperate, it is best if the currencies are supported by whitepapers which define their characteristics clearly. This is the approach followed by the European proposal for Markets in Crypto-Assets (MiCA).

c. For flexibility, standards for interoperability should use multiple parallel pathways (also based on standards) to discover and convey data crucial to interoperability. For example, there are multiple standard ways to identify securities (ISIN, CUSIP, FIGI etc.), it should be possible to use any of these means to identify digital currency in an interoperability standard.

d. Use existing, commonly used standards to refer to attributes - for example ISO 4217 for CBDC currency codes, draft standard ISO 24165 for Digital Token Identifiers(DTI).

e. Standards need pathways for discovery of registries, usually a registration authority maintains the registry.

f. Use IWA (Inter Work Alliance) authored Token Taxonomy Framework or other token standards to identify digital currencies. This can help standardise apis for interacting with the digital currency system.

g. Use existing Identity Standards, LEI for Legal Entities and the evolving SSI or legacy identifier standards to address the question of Identity in interoperability between DCS. In the case of certain crypto-currencies, this notion can just be a Public Key.

B. Layers

a. Static layers(2.1.1): Standards on the lower layers, including schemas need to be expressed with multiple pathways for an interoperability standard to have meaning across multiple digital currencies and multiple DCS. A DCS may use web APIs, program APIs, message based systems, or open or closed networks to facilitate

interoperability. It is best to refer to existing standards for such transports and formats, such as JSON.

b. Dynamic layering or pace-layering: Interoperability Standards have to take into account the difference in pace between the various layers. The creation of Standards usually has a 7-10 year lead-time. The speed of innovation outpaces standard creation. Updating standards is difficult, it helps to set the governance such that standards are updated in a 3-7 year period in keeping with trends. This means
    i. support backward compatibility
    ii. there has to be a guide within the standards for a graduated conformance, that is a basic set of standards, with a step by step or multi-faceted approach to greater conformance
    iii. use of versioning in standards should allow simultaneous support of multiple versions
    iv. use pull techniques, rather than just push for a Registration Authority RA, the RA should not be just a read-only site
    v. use of monitoring or active engagement to see whether certain elements of old standards could be dropped
    vi. the dynamism of the upper layers should be encouraged and the data and methods fed-back into the standards, with this provision embedded inside the response (if any) of communication protocols to gather this information
    vii. the RA of the standard should be charged with gathering conformance and or deviation from standards, this cost should be built into the funding of the RA.

C. Horizontal and Vertical Interoperability

a. Fiat to crypto-currency exchanges are the best examples of Interoperability between DCS. These exist outside the DCS, with connections to both worlds. Standards for Interoperability with exchanges being the intermediary is exemplified by the Rossetta proposal by Coinbase.
b. Standards for the trustworthiness, the sources and other details of oracles should be included in the Standard. Oracles are those components that gather data from the outside world (prices of currency pairs, transaction volume and other key data) for interoperability.
c. Wallets which are human interfaces to most if not all DCS need standardisation, they belong in the vertical interoperability axis.

D. Digital currency interoperability capability maturity model (DCICMM)

a. The concept of DCICMM is related to that of pace-layering. As the layers mature they migrate into lower layers.
b. Interoperability standards have to create standard methods of measuring the capability of Interoperability between two DCS so that two different pairs can be compared using metrics arrived at by similar methods.
c. Standards have to suggest a path forward for maturity, this is by addressing the measurement and criteria for the measurement. Changes to be made, either in the currency model or the interoperability solution and corresponding capabilities are thus explicitly or implicitly suggested by the standard.

E. Monetary Policy & Market Considerations

a. Standards should address how liquidity parameters can be extracted from an exchange or a DeFi site. Liquidity parameters include bid-ask spreads and trading volume in the market. Are there lenders of last resort for times of stress?
b. It is imperative to standardise the equivalent of LCR (Liquidity Coverage Ratio), NSFR(Net Stable Funding Ratio) for a purely decentralised, automated market-

maker. They do not have to follow the same principles as LCR or NSFR, but have to measure and guard against liquidity starvation in times of crisis. These measures have to be adopted, not just for protection against individual AMM failures, but contagion of the global financial system causing systemic risk.

c. In the case of widely used crypto-currencies that have evolved, interoperability solutions are implemented by third parties such as with wBTC, which is implemented as a Decentralised Autonomous Organisation (DAO). However, there are identifiable parties who function as Merchants and Custodians and the DAO is administered by the creator of the wBTC. Standards should address the structure, capital requirements and other qualities of these intermediaries.

F. Security Considerations

a. Standards for deploying automation into the interoperability solution should include audits of code for best practices (not for coding style but for bugs) as well as good deployment practices including stress testing.

5 Bibliography

1. Kosanke, Kurt. (2006). ISO Standards for Interoperability: a Comparison. 10.1007/1-84628-152-0_6.
2. National Interoperability Framework Observatory. 2020. European Interoperability Framework. https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/3-interoperability-layers
3. International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, FATF 2012, Amended 2022, pp 71-75 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
4. Catalini, Christian and de Gortari, Alonso, On the Economic Design of Stablecoins (August 5, 2021). Available at SSRN: https://ssrn.com/abstract=3899499 or http://dx.doi.org/10.2139/ssrn.3899499
5. Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. 1, 1 (March 2021), 63 pages. https://arxiv.org/abs/2005.14282v3
6. Gorton, Gary B. and Zhang, Jeffery, Taming Wildcat Stablecoins (July 17, 2021). Available at SSRN: https://ssrn.com/abstract=3888752 or http://dx.doi.org/10.2139/ssrn.3888752
7. Vitalik Buterin. 2016. R3 Report - Chain Interoperability. Technical Report. R3 Corda. https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf
8. Vitalik Buterin. 2021. An Incomplete Guide to Rollups. https://vitalik.ca/general/2021/01/05/rollup.html
9. Brand, S. (2018). Pace Layering: How Complex Systems Learn and Keep Learning. Journal of Design and Science. https://doi.org/10.21428/7f2e5f08
10. Prudential treatment of cryptoasset exposures Issued for comment by 10 September 2021 Bank of International Settlements. https://www.bis.org/bcbs/publ/d519.pdf
11. *Comments received on the consultative document "Prudential treatment of cryptoasset exposures."* (2021, September 10). Bank of International Settlements. https://www.bis.org/bcbs/publ/comments/d519/overview.htm
12. Genovese, Y. (2012, January 9). *Accelerating Innovation by Adopting a Pace-Layered Application Strategy*. Gartner. https://www.gartner.com/en/documents/1890915/accelerating-innovation-by-adopting-a-pace-layered-appli
13. Bank of International Settlements, 2018 https://www.bis.org/fsi/fsisummaries/nsfr.htm
14. https://github.com/InterWorkAlliance/TokenTaxonomyFramework, last retrieved March 21, 2022
15. Blockchain Bridges https://ethereum.org/en/bridges/
16. New experiments pave way for international payments using CBDCs | SWIFT - The global provider of secure financial messaging services
17. SWIFT INSTITUTE BRIEFING PAPER
18. Pedreira, Catarina; Belchior, Rafael; Matos, Miguel; Vasconcelos, André (2022): Trustable Blockchain Interoperability: Securing Asset Transfers on Permissioned Blockchains. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.19651248.v1

19. Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic Foundations and Risk-based Models. In 2nd ACM Conference on Advances in Financial Technologies (AFT'20), October 21–23, 2020, New York, NY, USA. ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3419614.3423261
20. Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. 2020. SoK: A classification framework for stablecoin designs. https://doi.org/10.48550/arXiv.1910.10098
21. Ariah Klages-Mundt, and Andreea Minca (In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. https://doi.org/10.48550/arXiv.1906.02152
22. Azar, Pablo D., Garth Baughman, Francesca Carapella, Jacob Gerszten, Arazi Lubis, JP Perez-Sangimino, David E. Rappoport, Chiara Scotti, Nathan Swem, Alexandros Vardoulakis, and Aurite Werman (2022). \The Financial Stability Implications of Digital Assets," Finance and Economics Discussion Series 2022-058. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2022.058.
23. Two thought experiments to evaluate automated stablecoins, Vitalik Buterin, May 25 2022
24. Austin Adams and Markus Ibert (2022), "Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel," FEDS Notes (Washington: Board of Governors of the Federal Reserve System, June 2)
25. Whitepaper: The Future of Risk, Capital and Margin Reporting, ISDA, May 2021
26. SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols Jiahua Xu, Krzysztof Paruch, Simon Cousaert, Yebo Feng arXiv:2103.12732
27. Paul Knowles , Philippe Page and Robert Mitwicki Decentralised semantics in distributed data ecosystems: Ensuring the structural, definitional, and contextual harmonisation and integrity of deterministic objects and objectual relationships

Appendix B: Terminology Mapping

This appendix is an interoperation of terminology, mapping between terminology used in different official documents. When the terms are not exact analogs, the differences are spelled out. Although there are many jurisdictions around the world, we start by looking at documents from the United States (the FED and other agencies), the EU, and FATF. We will add China and India, and supra-national institutions like the World Bank, the IMF, and WEF.

Primary Meaning	FATF	EU	US	Comments
Any asset controlled by cryptography	Virtual Asset	Crypto Asset	Digital Asset	Even basic terminology is divergent
Any identifiable entity enabling or assisting digital value transfer	Virtual Asset Service Provider (VASP)	Crypto Asset Service Provider (CASP)	Digital asset Service Provider (DASP)	Definition is broad, drawing many firms and individuals into the same set.

6 Glossary & Acronyms

AI Artificial Intelligence

ACID atomicity, consistency, isolation, and durability

AML Anti-Money Laundering

AMM Automatic Market Making

APAC Asia Pacific

API Application Program Interface

BAFT Bankers Association for Finance & Trade

CBDC Central Bank Digital Currency

CDM Common Domain Model (ISDA)

CRIF Common Risk Interchange Framework

DLT Distributed Ledger Technology

DEX Decentralised Exchange

EBA Euro Banking Association

EMDE Emerging Markets and Developing Economy

FATF Financial Action Task Force (also known by its French Initials: GAFI)

FCA Financial Conduct Authority

FSA Financial Services Agency (Japan)

FSB Financial Stability Board

FX Foreign Exchange

GAFI Groupe d'Action Financ**i**ère (same as FATF)

GDPR General Data Protection Regulation

GPFI Global Partnership for Financial Inclusion

ICC International Chamber of Commerce

ICCR International Committee on Credit Reporting

IOT Internet of Things

ISDA International Swaps and Derivatives Association

KYC Know-Your-Customer

LEI Legal Entity Identifier

MENA Middle East and North Africa

Merkle Tree A cryptographic commitment scheme structured as an upside down tree invented and patented by Ralph Merkle. The root hash is obtained from a trusted source, the data blocks are

hashed into the leaf nodes. A subtree has the same properties as long as the root of the subtree is stored in an unalterable location or broadcast as a global witness. There are some attacks, but there are protections that have to be coded into the constructor and checker. Hashing is comparatively hardened against quantum computing

ML Machine Learning

MNO Mobile Network Operator

OECD Organisation for Economic Cooperation and Development

P2P Person-to-Person (or Peer to Peer)

PE Private Equity

POR Proof of Reserve

QR Code Quick Response Code

RSMC Revocable Sequence Maturity Contract

SCF Supply-Chain Finance

SDG Sustainable Development Goal (UN)

SEC Securities and Exchange Commission

SME Small and Medium Enterprise

SWIFT Society for Worldwide Interbank Financial Transfers

UNDP United Nations Development Program

VC Venture Capital

WEF World Economic Forum

******