Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations

Introduction

With the advent of decentralized finance, which generally refers to “DeFi”, regulatory authorities are paying increasing attention to the privacy, traceability, and identity aspects of DeFi systems to address regulatory challenges that the development of the decentralized financial technologies bring. While the rapid development of scaling and privacy enhancing technologies (PETs) by open-source blockchain communities could enhance scalability and privacy protection, lack of robust monitoring tools could adversely impact the ability of enforcement officers to trace financial transactions for financial crime prevention. As each stakeholder has different goals and objectives, there needs to be a venue for constructive dialogue to take place.

With this in mind, this document created under the current workstream, with contributions from diverse stakeholders including engineers, regulators, financial institutions and industry, aims to provide a source of reference especially for regulators and policy makers to have a collective understanding by, for example, analyzing recent development of major DeFi projects and technical advancements.

Disclaimer: The views expressed in the document are personal views of the participating members of the BGIN community and should not be seen as the official views or recommendations of the institutions with which they are affiliated.

otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this document, and the entire risk as to implementing this document is assumed by the implementer. The BGIN Intellectual Property Rights policy requires contributors to offer a patent promise not to assert certain patent claims against other contributors and against implementers. BGIN invites any interested party to bring to its attention any copyrights, patents, patent applications, or other proprietary rights that may cover technology that may be required to practice this document.

Table of contents

1. Scope

The major intended audiences of this document are regulators, lawyers, and policy makers exploring effective regulatory approaches in the new ecosystem. It is intended to provide a solid perspective on how the decentralized financial ecosystem has developed to date, where it stands today, and what the prospects are for its future development. The document assesses the degree of decentralization of many major projects and discusses the regulatory implications in consideration of privacy, identity, and traceability of the technologies underpinning these platforms.

This document includes the following subjects.

- Background and issues to be addressed
- General overview of the functioning of the current DeFi ecosystem Goal/motivation
    - Technologies in place (e.g., Privacy Enhancing Technologies (PETs), Automated Market Maker (AMM))
    - Governance mechanism (based on case study analysis of specific communities such as Dash and MakerDAO)
    - Degree of decentralization
- Analysis of how DeFi ecosystem is likely to evolve
    - Further decentralization and/or re-centralization
- High-level recommendations on technical and policy solutions covering diverse issues including privacy, business confidentiality, and regulatory needs

This document does not focus on the following items.

- Cyber-security analysis of decentralized financial technologies and application

2. Normative reference

This document has no normative reference.

3. Terms and definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the term.

3.1
decentralized financial technologies
technologies that may reduce or eliminate the need for one or more intermediaries or centralised processes in the provision of financial services
[SOURCE: FSB (2019)]

3.2
decentralized financial system
new financial system that could be the result of decentralized financial technology
[SOURCE: FSB (2019)]

3.3
privacy enhancing technologies (PETs)

technologies that covers the broader range of technologies that are designed for supporting privacy and data protection
[SOURCE: ENISA - The European Union Agency for Cybersecurity]

3.4
Decentralized Finance (DeFi)
financial application that could consist of a part of a decentralized financial system
[Source: Ushida and James (2021)]

3.5
Decentralized Autonomous Organization (DAO)
organization created by developers that is run through rules encoded as computer programs called “smart contracts” to automate decisions and facilitate crypto-assets transactions
[Source: Cohan(2017)]

3.6
Smart contract
a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain
[Source: NIST (NISTIR 8202)]

4. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

AML	Anti Money Laundering
AMM	Automated Market Maker
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CPMI	Committee on Payments and Market Infrastructures
CVC	Convertible Virtual Currency
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DLT	Distributed Ledger Technology
FATF	Financial Action Task Force

FSB	Financial Stability Board
JFSA	Japan Financial Services Agency
LTDA	Legal Tender Status
KYC	Know Your Customer
ML	Money Laundering
PETs	Privacy Enhancing Technologies
TF	Terrorist Financing
VASP	Virtual Asset Service Provider

5. How decentralized finance (DeFi) ecosystem currently works

5.1 Goals/Motivation of DeFi community

It could be misleading to identify common goals/motivation of the DeFi community with a variety of DeFi projects currently being launched with different functions and objectives. However, one of the key value propositions would be its contribution to financial inclusion. For example, decentralized stablecoin, lending platforms and exchanges could provide access to remittances, payments, and savings for those who had no access to traditional financial services such as banking. To ensure fair treatment among users, most of the projects do not require KYC or AML, as many communities believe that identity verification could lead to privacy violation and discrimination. In addition, innovative solutions based on decentralized financial technology could bring greater customer convenience in such areas as cross-border payment where conventional financial infrastructure does not necessarily work effectively.

Another important aspect is open innovation. Since most source code is open to the public, developers are free to combine existing protocols to launch new DeFi projects. As typically referred to as "Money Lego", multiple protocols are intricately interconnected and innovative products are being developed, such as automated asset management protocols that incorporate multiple DEX and lending platforms to obtain the optimal financial return.

It goes without saying that the intention of the DeFi community could cause conflicts with regulators as each stakeholder has different goals in their mind. The major regulatory goals for regulators such as financial stability, consumer protection, and financial crime prevention, could negatively affect some aspects that the DeFi community values such as privacy. What at least matters is to precisely understand each goal and the motivation behind it to have a constructive discussion and reach a middle ground that balances both objectives.

5.2 Definition of DeFi and ambiguously used terms

Decentralized Finance (DeFi), which generally refers to a decentralized form of financial products executed by smart contracts on public blockchain, is growing rapidly from $660M in TVL (Total Value Locked) in early 2020 to $14.5B at the end of December 2020. A wide range of financial services are available without KYC (Know Your Customers) including crypto-asset exchange, lending, derivatives, insurance and decentralized stablecoins.

In 2019, the Financial Stability Board [1] defined decentralized financial technology as "Technologies that have the potential to reduce or eliminate the need for one or more intermediaries or centralised processes in the provision of financial services" and defined financial systems as “new financial system that decentralized financial technology could bring”. Although there is no widely-accepted definition of DeFi, this paper refers to it as “financial application that could consist of a part of a decentralized financial system”. While underlying blockchain platforms such as Bitcoin and Ethereum themselves could be categorized as DeFi in a broad sense, our analysis focuses on smart contract-based applications on such platforms.

Those DeFi protocols are often developed and managed by so-called DAOs , Decentralized Autonomous Organizations. Although the DAO is also not strictly defined, we use Chohan's [2] definition that is "an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members and not influenced by a centralized entity". Typical DAOs include The DAO (2016), MakerDAO, and KyberDAO.

The degree of decentralization varies from one DeFi project to another and many of them are quite centralized, especially early in their life. As an example, specific individuals or groups typically have the authority to change the protocol or freeze locked assets. In order to mitigate the Single Point of Failure (SPoF) risk caused by dependence on such trusted parties, many communities are heading for bottom-up decentralized governance by transferring management authority of the protocol to the DAO through on-chain voting. Given the risk of hacking and increasing attention from regulatory authorities, the sound development of governance of the entire ecosystem is important as we look ahead to mass adoption beyond niche use cases, irrespective of the form and degree of centralization the governance takes.

5.3 Key technologies in place

5.3.1 Emerging decentralized financial technologies

Automated market maker (AMM)

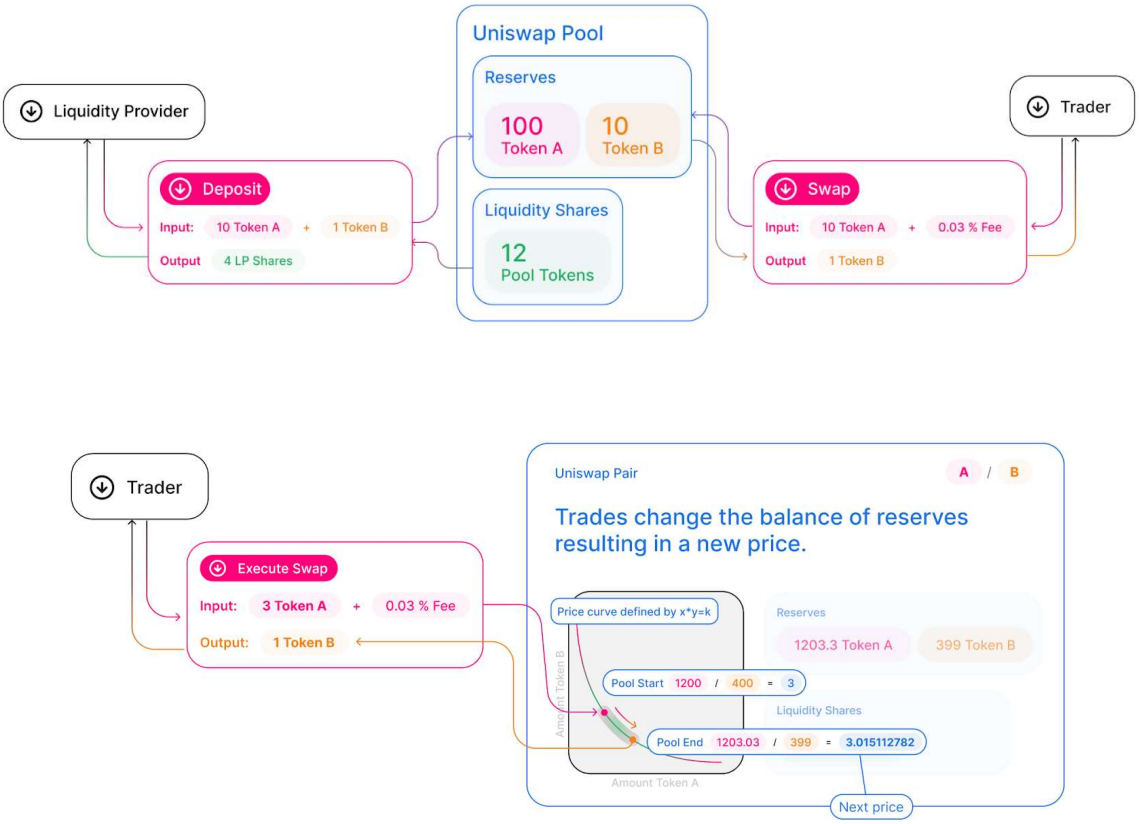
Automated market maker generally refers to a smart contract that provides liquidity to specific markets through automated algorithmic trading rules. Users add a pair of tokens to the smart contract, or liquidity pool, and the exchange rate is determined by a given mathematical formula. Those who want to exchange the tokens trade against the pool. At the moment, AMM based decentralized exchanges

(DEXs) such as Uniswap[1] or AAVE[2] have a dominant position in terms of TVL (Total Value Locked) against conventional DEXs with order books.

The diagram below shows how Uniswap's AMM practically works. Liquidity provider (LP) deposits an equivalent value of each underlying token (10 Token A and 1 Token B in this case) in return for Liquidity tokens (a.k.a pool tokens or liquidity pool tokens). Liquidity tokens represent a given liquidity provider's contribution to a pool. The proportion of the pool's liquidity provided determines the number of liquidity tokens the provider receives. These tokens can be redeemed for the underlying assets at any time.

The mathematical formula to determine the exchange rate is expressed as $x * y = k$, which states that trades must not change the product (k) of a pair's reserve balances (x and y). Hence, trades (exchange of 3 Token A and 1 Token B in this case) changes the x and y resulting in a new exchange rate.

[1] https://uniswap.org/
[2] https://aave.com/



(Source: Uniswap)

Flash loans/swaps

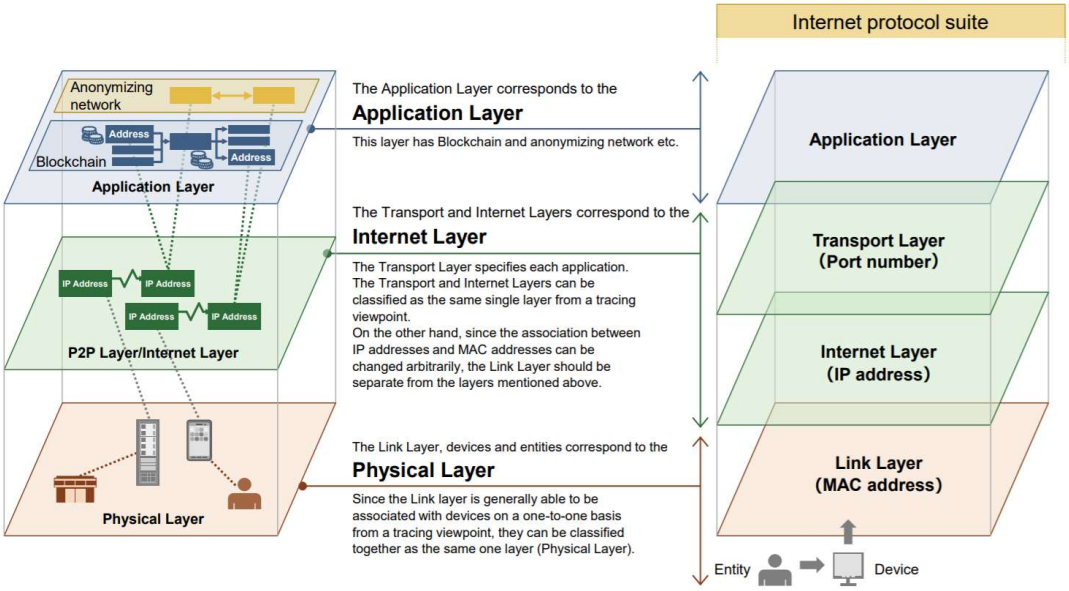
Flash loans allow users to borrow assets (tokens) without collaterals, as long as the liquidity is returned to the pool within one block transaction. To do a Flash Loan, users need to build a contract that requests a flash loan. The contract will then need to execute the instructed steps and pay back the loan + interest and fees all within the same transaction.

Likewise, Uniswap provide flash swaps, which allow users to withdraw up to the full reserves of any token on Uniswap and execute arbitrary logic at no upfront cost, provided that by the end of the transaction you either pay for the withdrawn ERC20 tokens with the corresponding pair tokens, or return the withdrawn ERC20

tokens along with a small fee. Flash swaps are useful because they obviate upfront capital requirements and unnecessary order-of-operations constraints for multi-step transactions.

5.3.2 Privacy Enhancing Technologies (PETs)

According to privacy and traceability report [3] , scaling and privacy enhancing technologies (PETs) can be classified into three layers: the "Application Layer", "Internet Layer", and "Physical Layer".



(Figure * – Overview of the relevant technologies - Comparison with Internet Protocol Suite source:JFSA)

In this paper, we focus on PETs on the application (blockchain) layer that are often used for crypto-assets trading and transactions with the DeFi protocols. In addition to already established techniques such as mixing and ring signatures, new technologies or approaches such as lightning networks, atomic cross-chain swaps, zero knowledge proofs and Mimblewimble are being proactively developed on this layer.

In early mixing services, the information on who sent crypto assets to whom was anonymized by delegating trusted intermediaries to rewrite them. Now new technologies can hide not only which intermediaries are used, but also transaction amounts and even the existence of the transaction itself. These techniques are developed with scalability, reduction of custody risk and reduction of blockchain data in mind, in addition to ensuring fungibility and protecting privacy. They are evolving according to the prerequisites specific to the public blockchain.

Off-chain transactions:

These transactions are not recorded on the public blockchain, but instead

transacted in a different means, examples of which are p2p payment channels and side-chains. Transactions are not only difficult for blockchain analytics companies and law enforcement, and those not involved in the transactions to trace, but also there is no means for the servers actually routing the transactions to monitor the number or volume of transactions on the network, nor can the routing servers determine the origin or destination of funds they route, as communications are encrypted and channel balances are not published.

Examples: Bitcoin Lightning Network, Ethereum Raiden Network, Litecoin Lightning Network

S*hielding addresses or amounts, or zero-knowledge proofs*:
These techniques mask the addresses (inputs and outputs) and/or amounts of transactions without using mixing services. Both sending addresses and receiving addresses can be shielded from third party observers.

Examples: Monero and private Zcash transactions

Burn-and-Redeem : Users are able to destroy coins and redeem them for new coins to eliminate previous transaction history or linkages by destroying all "digital trails".

Example: Firo (previously known as Zcoin)

***Mimblewimble*:**
The Mimblewimble protocol aggregates inputs and outputs of multiple transactions into one unified set, and eliminates addresses accessible to third-parties. These features make it impossible to trace transaction histories via third-party observation of the blockchain.

Examples: Grin, Beam, Litecoin (plans to launch mimblewimble in Q2 2021)

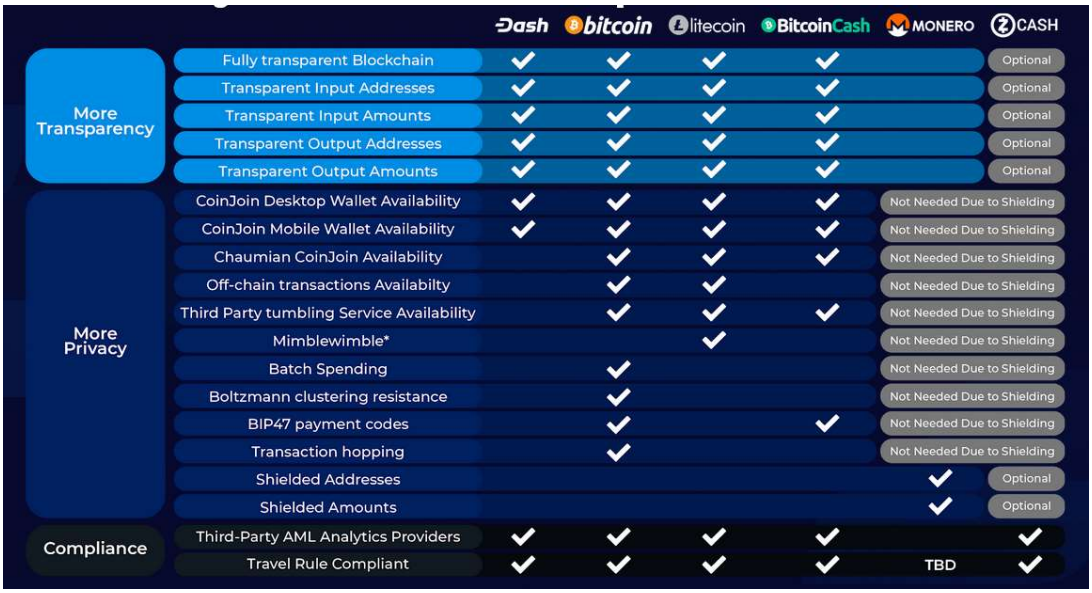
Tumbling / Mixers:
Tumblers and mixers are services operated by providers that typically require users to transmit crypto-assets to them for mixing and exchange. The centralized entity then sends back crypto-assets originating from other customers, thus eliminating the ability of third-party observers to trace the user's true source of funds. This technique is custodial, which means that users are actually transferring value to a centralized entity prior to receiving the same value back. Centralized tumbling/mixing entities have been categorized as Money Services Businesses (MSBs).

CoinJoin / Shuffling:

This privacy feature is similar to tumbling / mixing, with two distinct differences: (1) users never lose control of their coins, and (2) third-party observers can link a user's balances and transactions to an originating address (although the originating address may be difficult to attribute with 100% certainty). This is a non-custodial solution. Users simply send from one address to another within the same wallet contemporaneously with other users. All transaction details including input addresses, input amounts, output addresses, and output amounts are published to a public ledger, enabling any third-party observer to analyze these transactions.

Examples: Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Dash, and most transparent BTC-based blockchains.[3]

Table demonstrating the various implementations of privacy techniques among 6 different blockchains:



* Litecoin's Mimblewimble is expected to be released in 2021

As can be seen from the table above, regulating or blacklisting specific crypto-assets does not prevent third party developers from introducing more advanced forms of privacy to "green-listed" crypto-assets deemed public and not a compliance risk by regulators. The number of privacy enhancements on the Bitcoin network far exceed those on the many others such as Dash network.

To further illustrate the complexity of privacy on public blockchains, we can explore just various CoinJoin implementations on the Bitcoin network. Many enhancements to plain vanilla CoinJoin have been introduced over the years.

[3] https://news.bitcoin.com/how-to-mix-your-bitcoins-using-coinjoin

Chaumian CoinJoin: Typically, CoinJoin transactions leverage a coordinating server that collects information from each of the participants wishing to enter into a CoinJoin transaction with other users. The users need to know the full set of input addresses, amounts, and output addresses which other users wish to include in the transaction. In the process of collecting and disseminating this information, the coordinating server is aware of which inputs and outputs belong to the same participant.

Chaumian CoinJoin was introduced in 2017 as an improvement meant to address this problem. Chaumian CoinJoin obscures transaction details from the coordinating server so that even the coordinator is not able to definitively link the inputs and outputs produced by a Chaumian CoinJoin transaction. This means the coordinating server gathers no greater data on the transaction than is available to any other third-party observer of the public blockchain.

BIP-47: Bitcoin Improvement Proposal 47 or "BIP-47" allows for reusable Payment Codes for Hierarchical Deterministic Wallets. This proposal introduced the notion of "stealth addresses" on the Bitcoin network. BIP-47 addresses the public and transparent nature of Bitcoin transactions by providing users with reusable Payment Codes tied to unique Bitcoin addresses, instead of users reusing identifiable Bitcoin addresses. Payments conducted through Payment Codes are indistinguishable from regular Bitcoin payments and are therefore unidentifiable.

Batch transactions: Batched transactions in crypto-assets have traditionally been used to group transactions in order to save on miner costs, because the size of one large transaction is smaller than the sum of many smaller transactions. However, because aggregated inputs and outputs produce more complexity, batched transactions are naturally more difficult to analyze as well, so they infer some privacy advantage over separate transactions. A few different forms of batched transactions are implemented in privacy-oriented Bitcoin wallets, including batching between different users.

Boltzmann Clustering Resistance: While this is technically not a CoinJoin transaction type, transactions can be made to look like CoinJoin was used. In essence, it is an imitation of a CoinJoin conducted by a single user. A Boltzmann score is used to measure the entropy of a transaction, or put another way, measures the resistance a transaction has to being identified through identity clustering tools typically used by blockchain analysis companies.. Tools that use Boltzmann scores within their privacy features attempt to lower the confidence of blockchain analysis tools and introduce doubt of ownership of addresses within a cluster. This allows an identified user plausible deniability. A Boltzmann score is determined by identifying the number of feasible links or mappings of inputs to outputs in a transaction.

Transaction hopping: Transaction hopping adds a number of additional "hops" to a transaction. Hops refer to moving crypto-assets from one address to another address. Since chain analysis companies typically scan the history of the last four transactions associated with the incoming transaction, transaction-hopping

introduces extra hops of history in order to further "distance" an exchange deposit from any previous history, in effect attempting to stump chain analysis forensic tools. This technique is often used in conjunction with – and in the same wallet as – CoinJoin. This could prevent an exchange's analytics from determining that CoinJoin was used, for example.
Receiver Mix-ins: Receiver mix-ins are CoinJoin transactions in which the receiver provides one or more of the inputs to the transaction. This obscures and complicates analyzing a transaction because it counters an assumption that underpins the structure of typical Bitcoin transactions. Specifically, it violates the assumption that all inputs into a valid, cryptographically signed transaction are from the same entity. This approach may trick observers into concluding that the transaction was simply a consolidation of UTXOs within the user's own wallet, and that a transaction between two parties had not even taken place.

All of these enhancements have been introduced to CoinJoin wallets on the Bitcoin network.

Here is a link to a video providing a presentation of the various CoinJoin technologies for those more visually inclined:
https://www.youtube.com/watch?v=iRhFrXD84Og

In addition to existing privacy techniques, Bitcoin developers plan to further enhance its privacy features through its Taproot upgrade, expected to be released within the Fall 2021. This upgrade will allow for the following features to be deployed on the Bitcoin network:

CoinSwap: Typical CoinJoin transactions are relatively easy to spot, even without analytics software. There are usually many inputs and outputs of the same size within the same transaction. CoinSwap essentially fixes this by enabling coin mixing to take place without being detected. Essentially, these will be CoinJoins that appear to be regular transactions. They work by breaking CoinJoins into many separate transactions using scripts that are indistinguishable from any other Taproot single signature transaction. In essence, this creates stealth mixing sessions, rendering coin mixing undetectable to blockchain analytics.

Point Time Lock Contracts: This is one of the innovations that makes CoinSwap possible. This improves the types of scripts possible and keeps the contents of the scripts private so that third parties cannot determine that a CoinSwap was used.

Ring Signatures: Taproot will also provide users the ability to use "ring signatures" in order to cryptographically prove that they own a certain number of coins without revealing exactly which coins they own. For example, if you need to prove that you own over 100 BTC, you would be able to do so by performing a ring signature over all the Taproot UTXOs worth more than 100 BTC. This improves Lightning network node operator privacy who now have the opportunity to prove ownership of a payment channel without compromising privacy.

MuSig2: From a privacy perspective an outside observer will no longer be able to tell whether a single signature transaction or a multisig transaction took place on the

blockchain because of so-called “scriptless scripts”, since all Taproot transactions have the same digital footprint when broadcast to the network.

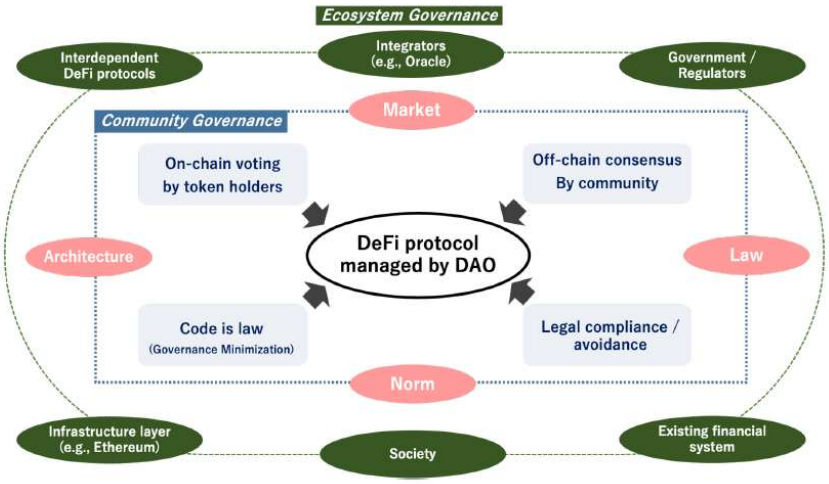
All of these enhancements represent a significant step in enhancing the privacy of the Bitcoin network. Most of these specific enhancements do not exist on any other public blockchains and represent innovative technological solutions to enhance user safety and privacy.

5.4 Governance mechanism

5.4.1 Overview of the ecosystem

According to Ushida and James [4], overall DeFi ecosystem is a complex structure composed of several elements and stakeholders including:

- Individual DeFi projects managed by DAOs
- Public blockchain including scaling solutions as an underlying platform
- DeFi integrators such as oracle providers and custody solution providers
- DeFi aggregators and curators
- DAO software as a service such as Aragon DAO and OpenLaw
- Centralized financial service providers such as centralized crypto-asset exchangers
- Other blockchains (i.e. Ethereum, EOS, Polkadot etc.)



A DeFi project typically consists of protocols (i.e., single or a set of smart contracts on the underlying public blockchain), foundation/developer team, initial investors, token holders, and a variety of types of users such as liquidity providers, lenders and borrowers. There is no "one-size-fits-all" solution as each DeFi project varies greatly in many ways such as decision-making mechanism, protocol

upgradability, attributes of tokens and types of financial applications. A couple of factors likely influence the governance of many DeFi projects with DAOs. In this section, we elaborate on governance factors that would constrain the activities in the projects.

On-chain voting by governance token holders: In order to promote decentralized decision-making, more and more projects are adopting on-chain voting using tokens. This community-driven bottom-up, decentralized mechanism could eliminate or mitigate the concentration risk of control by certain parties such as the developer team. Tokens can be designed in a variety of ways. Some tokens have not only voting rights and rights to create and submit proposals, but also the rights to receive a portion of the cash flow generated by the protocol. Some can be also used for specific purposes as utility tokens. In this paper, we define a governance token as a token that has a voting right for decision-making which influences the project, regardless of whether it has other rights/functions or not. Hacker [5] argues that token-based systems provide a clear designation of competences and procedures that breaks up the informal power structures and presents an opportunity to distribute power in a fairer and more transparent way.

Off-chain consensus by community: In the case of the Bitcoin ecosystem, Nabilou [6] describes that "various actors such as mining pools, node operators, users, developers, exchanges, custodians and wallet providers, and eventually the media and advocacy groups have their say and they ultimately decide over critical governance issues either by reaching a consensus or by forking". While some researchers like Nabilou acclaim that their existing governance arrangements have been largely successful in dealing with Bitcoin's major crises, others including Hacker criticize the lack of proper governance mechanism, especially for protocol update for dispute resolution. As an example, he points out that the Github repository is maintained by a small group of developers and unpredictability in changes to the protocol result from the lack of an institutionalized process to accommodate dissent from a wide range of stakeholders. The Etherum community, which also does not have a formal governance process such as an on-chain voting mechanism, resorted to an off-chain consensus when they decided to undo the mess caused by "The DAO" hack via a controversial hard fork. Many researchers question the transparency of the undocumented decision-making process and the validity of the judgment. Conversely, Zamfir is opposed to excessively institutionalized governance such as on-chain voting as it could force the community to choose what is against the social norm of the community captured by specific governing forces such as governments, corporates or cartel of specific groups of the community. It is worth noting that law and its potential enforcement could primarily affect the community's decision against the rule of code, as some of the community members would notice the increased attention from authorities.

Code is law: Blockchain and smart contract code is written in a formalized language and, unlike law and regulations that leave room for discretion, only actions that follow the rules set in the code are allowed. When the code is adopted as the primary constraint tool, little changes are made to the blockchain protocol except for technical maintenance. The ecosystem is built by relying solely on the original code to minimize human intervention via an on-chain or off-chain governance process. As mentioned in the previous section, the institutionalization of a specific governance

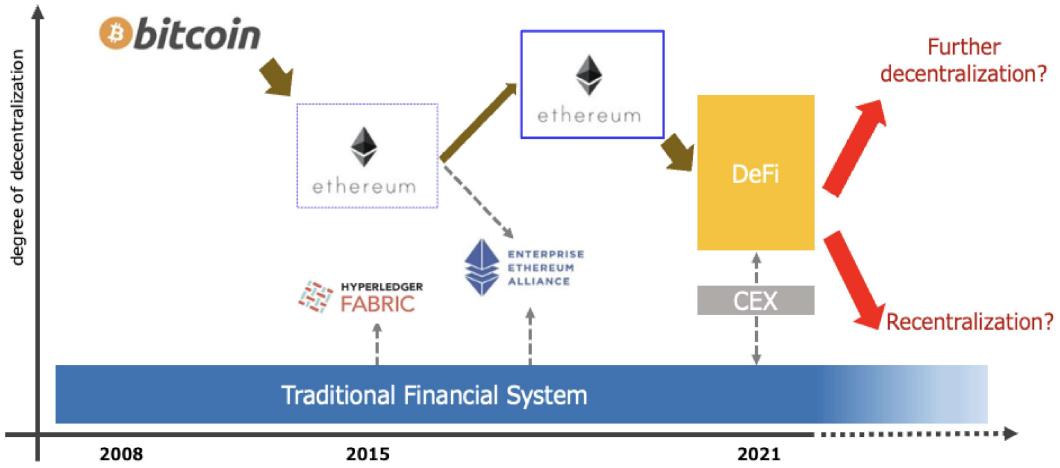
process has the risk that the ecosystem could be captured by certain groups such as governance token holders. The ecosystem could be damaged by token holders' behavior that does not align with the incentive of others. In this regard, relying solely on the code could assure certain neutrality that mitigates the risks of SPoFs of specific entities. In a community with a norm that values this neutrality, a code-centric ecosystem will be created, and De Filippi and Loveluck [7] discuss that many in the blockchain community tend to believe that individuals and organizations cannot be trusted and social interactions should be managed solely by computer code.

On the other hand, as Collomb et al. [8] points out, a formalized rule is easily gamed or exploited by malicious actors. Computer code lacks the flexibility needed to respond to edge cases, such as hacking due to bugs or vulnerabilities in the code, or to comply with incessantly changing regulatory requirements. Zamfir [9] claims that the concept of governance minimization is based on a naive interpretation of how the code interacts with the existing legal system and stands by off-chain governance to intervene to resolve disputes. While computer code is certainly one of the powerful constraints, it is important to position it appropriately in interactions with other constraints such as law and social norms.

Legal compliance/avoidance: One of the differentiating factors among DeFi projects could be the willingness of the community to comply or circumvent the existing legal framework applied to financial services in each jurisdiction. At present, it seems that the primary value proposition of many DeFi is not complying with regulatory requirements such as KYC/AML (Know Your Customer/Anti Money Laundering rules). This purportedly "democratizes" the financial services for financial inclusion while protecting users from the threat of government actions such as taxation and expropriation. In light of growing concerns and scrutiny from regulatory authorities, some of the DeFi projects might choose to further decentralize the project by, for example, dispersing the governance token ownership, anonymizing the developer and community members, or voiding administrative functions to lessen the control points that could be captured by regulators.

6. How DeFi ecosystem is likely to advance

6.1 Advancement of DeFi ecosystem to date and future direction



6.2 Further decentralization

One of the differentiating factors among DeFi projects could be the willingness of the community to comply or circumvent the existing legal framework applied to financial services in each jurisdiction. At present, it seems that the primary value proposition of many DeFi is not complying with regulatory requirements such as KYC/AML. This purportedly "democratizes" the financial services for financial inclusion while protecting users from the threat of government actions such as taxation and expropriation. In light of growing concerns and scrutiny from regulatory authorities, some of the DeFi projects might choose to further decentralize the project by, for example, dispersing the governance token ownership, anonymizing the developer and community members, or avoiding administrative functions to lessen the control points that could be captured by regulators.

As a concrete example, the Maker Foundation announced it is turning over operations entirely to MakerDAO to achieve full decentralization as the founder Rune Christensen has long promised. Going forward, community decisions will be made through on-chain governance by voting on the governance token MKR. If token holders are highly dispersed, decentralization of decision-making may be highly achieved, making it difficult for authorities to identify specific responsible entities.

6.3 Recentralization

On the contrary, others might choose to closely work with regulators and other stakeholders outside of the blockchain ecosystem to ensure legal certainty. For that

sake, whether or not it should be called "DeFi", they could choose to increase the centralized aspects of the DeFi project to be able to meet regulatory requirements in an effective manner as traditional organizations usually do. One example is Nexus Mutual, a P2P discretionary mutual on Ethereum offering a blockchain-based solution to cover against smart contract failure such as "The DAO" hack. It was established as a company limited in the UK and has received approval by the Financial Conduct Authority. KYC/AML requirements must be fulfilled to become a member of the community and the membership gives legal rights to the assets of the mutual. Residents in some jurisdictions are not able to become a member due to relevant local regulations. Another eye-catching initiative is OpenLaw's LAO, a Limited Liability Autonomous Organization that enables its members to invest in Ethereum ventures projects and generate a profit in a legally compliant manner. The LAO is an LLC (Limited Liability Company) set up in Delaware and it harnesses smart contracts to handle mechanics related to voting, funding, and allocation of collected funds. It intends to ensure legal certainty, limit the members' liability, and streamline complex tax issues. Similar example is the Flamingo, an NFT (Non fungible token)-focused DAO organized as a Delaware LLC that aims to explore emerging investment opportunities for ownable, blockchain-based assets.

In general, there exists a trade-off between regulatory compliance and openness of the project. In the case of the LAO, the maximum number of members is limited to 99, the minimum investment is 120 ETH, and the membership is limited to 9\% or for 1,080 ETH. The Flamingo also limits its membership to accredited investors capped at a maximum of 100. Such limitations could curve some of the key value propositions of DeFi, such as composability upheld by its permissionless nature, while paving the way to mass adoption in complying with social requirements. It should be noted that they might need to meet not only securities regulation but also other regulatory requirements regarding AML/KYC and financial stability, which could further increase compliance costs.

7. Regulatory implications

7.1 Regulatory and Supervisory Challenges

With the development of decentralised financial technologies leading to emergence of decentralised financial systems, existing regulatory and supervisory models may need to adapt significantly. While decentralisation of financial markets is likely to benefit financial stability by reducing the systemic importance of some existing entities, a new form of ownership concentration led by the operation of key decentralised infrastructures and technologies might lead to the emergence of new and different kinds of risks to financial stability.[4] The existing supervisory architecture, built over the years, for the underlying structure of centralised financial systems, may not be fit in all aspects for the monitoring of decentralised financial systems. Some of the key components of supervisory architecture, like data collection and monitoring, would have a direct impact on issues concerning privacy[5], identity, and traceability, with further potential of conflicts or harmonization, depending upon the future evolution of technological tools. Further, new uncertainties concerning the determination of legal liability,consumer protection and AML/CFT, along with recovery and resolution of decentralised structures add further complexity in regulatory and supervisory considerations for decentralised financial systems.

Though decentralised financial systems have reinforced the importance of an activity-based approach to regulation and supervision, such an approach may not be feasible in the absence of a supervisory infrastructure capable of responding to the issues and challenges at the basic transaction-level of financial activity. The current supervisory infrastructures operate and respond with a centralised interface of a financial entity, and hence any change in approach to regulation and supervision would need to be supported by significant changes in infrastructure capabilities. Designing such a supervisory infrastructure, with a proper consideration of issues like privacy, identity and traceability is going to remain challenging. Regulators and supervisors may wish to engage with a wider group of stakeholders, including technology providers, to influence platform and system design to avoid unintended consequences of supervisory policy.

One of the key-considerations for regulators and supervisors could be how to leverage the element of transparency, that is one of the foundational structures of decentralised financial technologies, in building a robust system of data reporting and monitoring that can serve as one of the important tools for supervisors. It may need to be considered how far such a system is capable of supporting privacy, with due consideration for user rights and responsibilities. At the very least, the inherent privacy of decentralised systems or the requirement for sharing information, in-comparison to the privacy available in centralised systems or information sharing requirements, should not lead to supervisory arbitrage.

---

[4] FSB. (2019). Decentralised financial technologies-Report on financial stability.

[5] In this context, privacy concerns generally refer to the concern that individual privacy protection rights might be infringed by those who collect identity, transaction and other personal data for supervisory purposes (e.g., regulatory authorities).

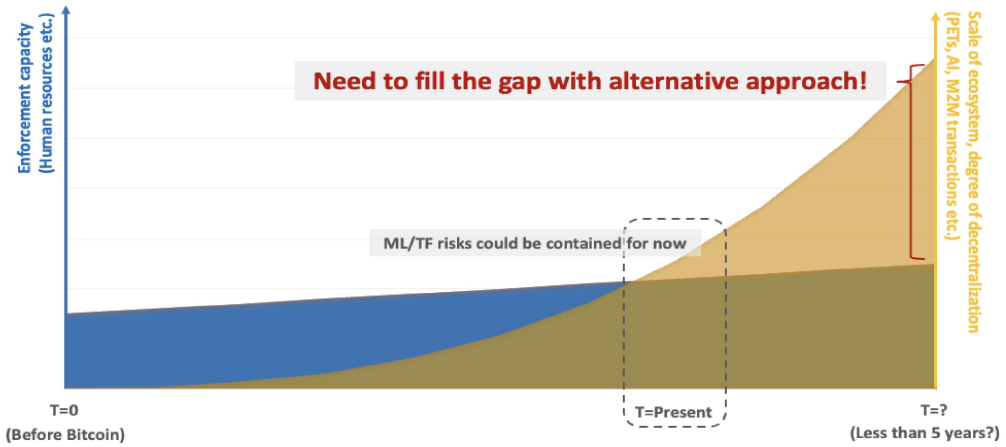
Ownership of data, along with governance of data-flows for regulatory and supervisory purposes can be another important consideration for regulators and supervisors. As rules for the data governance, including the ownership and access rights across different jurisdictions are still evolving, creating a supervisory architecture for decentralised financial systems is going to be challenging. In the absence of uniform standards, the rules are likely-to vary, from jurisdictions-to jurisdictions, often creating a perception of disproportionate or harsh obligations for the market participants in certain jurisdictions.

Further, designing a supervisory architecture is going to be affected by several unique characteristics of a decentralised financial system, that are at a stark variance with a centralised system. For instance, the supervisors mostly leverage the three lines of defence system, in a centralised financial system with a well established compliance function, which is responsible for understanding, implementing and ensuring compliance of supervisory rules. However, in a decentralised system, rule-making may not itself be sufficient to trigger compliance. The supervisory architecture must be capable of talking with the decentralised systems in their own language, without depending on the compliance function like architecture of a centralised financial system. This would often imply converting the existing rules or framing new rules in machine-readable and executable format, without any manual intervention. Such a new architecture would require significant investment in new regulatory and supervisory infrastructure. It would need to be seen how far the machine-readable and executable architecture is able to support considerations relating to privacy, identity and traceability.

In-addition to financial stability considerations, the regulators and supervisors must also take into account issues relating to KYC and AML/CFT. Supervision of decentralised financial systems, particularly due-to lack of clarity on regulatory perimeter, continue to remain in the nascent stage. In respect of crypto-assets, one of the studies[6] notes that while AML/CFT international standards are in place, most jurisdictions have just begun to implement and enforce them. The key question remains as to who and which activities fall within the regulatory perimeter. Though the basic principle could be “same business, same risks, same rules”, at the most basic level of implementation, supervisory authority must consider~~must need to consider~~ how and to what degree they need to use the ‘same-tools’ against both centralised and decentralised financial systems. The designing of these tools is ultimately going to dictate how supervisors are able to maintain the same level of parity in various aspects including privacy, identity and traceability to prevent information arbitrage between decentralised and centralised financial systems.

[6] FSI Insights on policy implementation No-31, Supervising Crypto Assets for anti-money laundering (BIS, April 2021)

7.2 Linear vs Exponential



There are reasonable possibilities and risks that the decentralized finance system (i.e. financial services that do not rely on intermediaries), which is currently marginal, will rapidly become mainstream in the future. Conventional regulatory approach taken by the FATF and national regulators, which focuses on intermediaries, will become obsolete or dysfunctional. Note that It would be too late to take action after the risks materialized.

7.3 Takeaways from multi-stakeholder roundtable

In our open discussion with regard to AML/KYC and privacy issues, a number of participants expressed concerns about the proposed AML/KYC regulations in terms of privacy, level playing fields, financial inclusion, and regulatory enforceability. On the other hand, the need to achieve regulatory objectives such as financial crime prevention was also discussed. Most of the participants agreed to find a middle ground through multi-stakeholder dialogues to strike a balance between privacy and regulatory compliance.

Key discussion points include:

- Privacy/anonymity is not binary. AECs (Anonymity Enhanced Cryptocurrency) are not well-defined and could be misleading to label specific crypto-assets as AECs.
- Traceability is not a mandatory requirement to comply with regulations such as the Travel Rule. What matters is to assess the risks and take necessary measures to mitigate the risks in collaboration with stakeholders (e.g., developers, service providers, exchanges, regulators) involved in the ecosystem.
- The disconnection between regulation and underlying technologies: technology-enabled alternative solutions are expected rather than just criticizing the proposed regulation.

- It's not only about technologies but also about processes. For example, proper processes should be in place at the exchange level.
- Regulators still need more inputs from engineers and industry sides to understand the risks of particular transactions, technologies, etc.
- The engineering community might seek for further decentralization to avoid the regulatory capture if the regulatory framework is poorly designed.
- Authorities could find a choke point to regulate DeFi (e.g., centralized exchange listing DeFi tokens, not truly decentralized DeFi), but the protocol itself is unstoppable.

7.4 Applicability and limitation of existing/proposed regulatory framework

Existing entity-based regulatory approaches could work due to the centralized aspects that many DeFi projects have at the moment. Ushida and James [4] pinpoints some of the multifaceted centralized aspects of existing DeFi projects and analyzes its impact on regulatory enforceability as follows.

Admin keys

Some DeFi projects have a specific party with administrative authorities to modify the protocol by its discretion via private keys called admin keys. The existence of such centralized power might be accepted by its community members in its bootstrapping stage as it could help facilitate the growth of the community through swift and justifiable updates by the administrators who are strongly committed to the project, such as the initial developer team. Indeed, we saw cases, such as Compound, which issued governance tokens to transfer the authority from admin key holders to token holders as the community grows. Taking as an example of the bZx hack[7], it could be argued that the bZx developer team was able to fix the bug in a relatively timely manner because they had an admin key.

From a regulatory enforceability perspective, the fact that someone is holding an admin key could make it easier to identify those responsible for the protocol and operation to demand regulatory compliance. The EtherDelta is one of the proof that regulatory bodies take the existence of the admin keys seriously to assess whether the developer is liable for the unlawful financial service provision via smart contracts. If regulators are able to identify the admin key holders, the regulators might ask them to take necessary actions such as freezing of stolen tokens in case of theft or money laundering. For instance, when crypto assets were stolen from the hot wallet of a centralized exchange KuCoin, some ERC-20 token issuers such as USDT and Ocean (government tokens) restricted token movement by administrator's judgement. Though it is not clear whether there was an order or request from the authorities, it is conceivable that the authorities will take similar enforcement actions against future incidents. Moreover, depending on the type of financial product

[7] https://www.theblockcrypto.com/post/77656/defi-protocol-bzx-attacked-lost-8-million-faulty-code

offered, authorities might require the admin key holders to comply with the same regulations that existing financial institutions providing comparable services are required to abide by.

Governance token holders

One of the major regulatory issues is the applicability of governance tokens as securities. While the holders of some governance tokens are entitled to receive a part of the fee income generated by the protocol, others have only voting rights and do not have the right to the treasury of the protocol directly. However, in many protocols, a portion of the tokens is burned as the cash flow to the protocol increases, which is equivalent to a share buyback in the case of ordinary stocks, and can be considered to have the same economic function as dividend. Collomb et al. argue that regulators should assess not only the original nature or function of the tokens being issued but also the underlying motivations of both token issuers and investors, as well as the risks that investors may incur in purchasing these tokens. Given the assumptions that token holders' primary motivation is capital and income gains that would be realized from the growth of the DeFi projects, it is conceivable that some of them are regarded as a kind of securities or investment contracts, especially for those that have specific centralized party to manage the protocol, though it needs to be examined in the context of the legal framework of relevant jurisdictions. As an example, the SEC has concluded that The DAO token was a security at the time of the issuance, and charged Ripple Labs Inc. and two of its executives alleging that they raised over $1.3 billion through an unregistered, ongoing digital asset securities.

Given the similarities between governance tokens and securities, disclosure requirements should be well considered, particularly for minority token holder protection. In corporate governance, many jurisdictions have put various institutional frameworks in place, such as a requirement to submit statements of large-volume holdings to mitigate the dominance by large investors, and regulations to protect minority shareholders interests. While such regulatory frameworks are not in place as of now, some projects such as Nexus Mutual implement specific voting rules to curb the strong voting power of large holders by, as an example, limiting the maximum voting rights to 5% of the total voting rights. However, this kind of arrangement could also raise concerns about fairness among shareholders.

Another consideration is concerning the possibility of token-based voting mechanisms being captured by authorities. It is conceivable that the authorities could hold a large number of tokens and intervene in the DeFi community's decision-making.

Other centralized factors: centralized collateral, oracle, aggregator etc.

8. Conclusion

The DeFi ecosystem and relevant technologies are rapidly developing and each project seems to be exploring various directions toward further decentralization or re-centralization, which would affect the enforceability of regulation. What is critical for regulators is to keep up with the significant change and develop

foundational knowledge about decentralized financial systems to have a constructive dialogue with the DeFi community. Whereas this paper provides an overview of the technologies, governance mechanisms and regulatory implications, an in-depth analysis should be done in consideration of complicated elements such as jurisdictional regulatory gaps.

9. Informative reference

[1] Financial Stability Board, "Decentralised financial technologies" (2019)
[2] Usman W WChohan. "The decentralized autonomous organization and governance issues. Journal of Cyber Policy", pages 1–7 (2017)
[3] JFSA, "Research on privacy and traceability of emerging blockchain based financial transactions" (2019)
[4] Ryosuke Ushida and James Angel, "Regulatory Considerations on Centralized Aspects of DeFi managed by DAOs" (2021)
[5] Philipp Hacker. "Corporate governance for complex cryptocurrencies? a framework for stability and decision making in blockchain-based organizations." Oxford University Press, pages 140–166 (2017)
[6] Hossein Nabilou. "Bitcoin governance as a decentralized financial market infrastructure." (2020)
[7] Primavera De Filippi and Benjamin Loveluck. "The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure." Internet Policy Review (2016)
[8] Alexis Collomb, Primavera De Filippi, and Klara Sok. Blockchain tech- nology and financial regulation: A risk-based approach to the regulation of icos. European Journal of Risk Regulation, 10(2):263–314 (2019)
[9] Vlad Zamfir. "Against szabo's law, for a new crypto legal system." https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827 (2019)
[10] FATF, Guidance for Risk Based Approach for virtual assets (2019)
[11] FATF, Guidance on Digital Identities (2019)
[12] FATF, 12-month Review Virtual Assets and VASPs (2019)
[13] ConsenSys, "New Ethereum DeFi Report: The Rise of Wrapped Bitcoin, ETH Insurance, and Yield Farming", July 15, 2020.
[14] Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, Arthur Gervais, "The Decentralized Financial Crisis", 2020 Crypto Valley Conference on Blockchain Technology (CVCBT), 2020.
[15] Kaihua Qin, Liyi Zhou, Benjamin Livshits, Arthur Gervais, "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit", 2020.
[16] Lewis Gudgeon, Sam M. Werner, Daniel Perez, William J. Knottenbelt, "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency", 2020.
[17] IOSCO, Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, 2020

[18] Aaron Wright and Sachin Meier, “Analyzing the United States Financial Crimes Enforcement Network’s Proposed Regulation Relating to Anti Money Laundering and Know Your Customer Compliance”, 2021
[19] Yuta Takanashi, Shin’ichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, and Hirotoshi Sato, “Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem (Part 1) (Part 2)”, 2020
[20] Economic Research at the St. Louis Fed, “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets”, 2021

Appendix A – Acknowledgement

(Informative)

A.1 Editors and Co-editors *alphabetical order

- Jacek Czarnecki (Maker Foundation)
- Jack Gavigan (ZCash Foundation)
- Omar Hamwi (Dash Core Group)
- Yuji Kawada(JFSA)
- Masa ‘Senshi’ Kikuchi (Secured Finance)
- Manoj Kumar Singh (Reserve Bank of India)
- Roman Danziger Pavlov (BGIN)
- Yuta Takanashi (JFSA)
- Ryosuke Ushida (Georgetown University)
-

A.2 Contributors

- Justin Goldstein (Georgetown University)