Outcomes of neutral multi-stakeholder discussions at Blockchain Governance Initiative Network (BGIN)

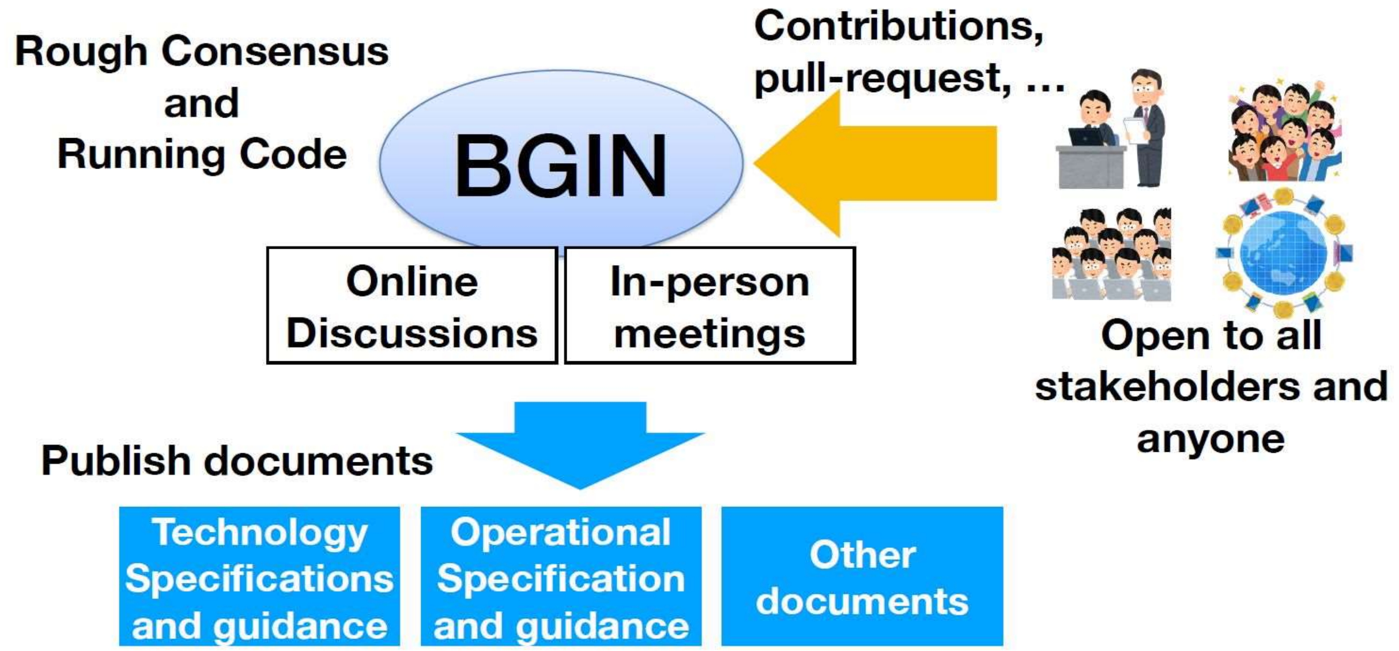
Shin’ichiro Matsuo, Acting co-chair of BGIN

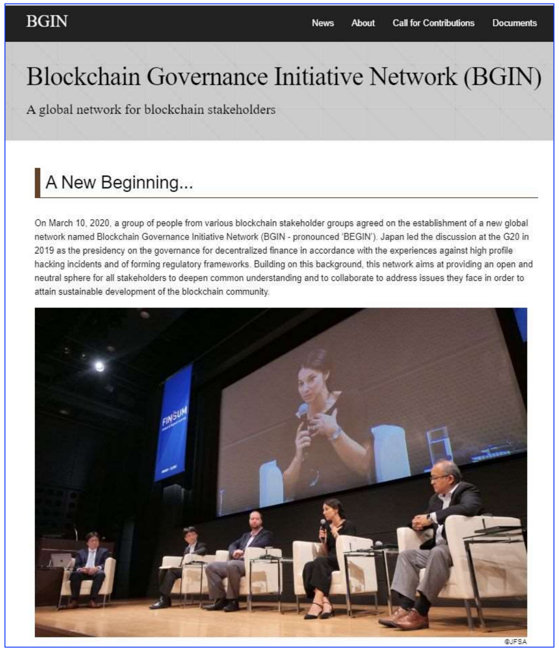
April 20, 2021

bgin-global.org

Blockchain Governance Initiative Network (BGIN)

- An open and neutral sphere for all stakeholders to deepen common understanding and to collaborate to address several competing values such as AML/CFT vs privacy and innovation to attain sustainable development of the blockchain community.
- Established in March 2020 following 2019 G20 Communique


Rough Consensus and Running Code
BGIN
Contributions, pull-request, ...
Online Discussions
In-person meetings
Open to all stakeholders and anyone
Publish documents
Technology Specifications and guidance
Operational Specification and guidance
Other documents



Blockchain Governance Initiative Network (BGIN)

A global network for blockchain stakeholders

A New Beginning...

On March 10, 2020, a group of people from various blockchain stakeholder groups agreed on the establishment of a new global network named Blockchain Governance Initiative Network (BGIN - pronounced 'BEGIN'). Japan led the discussion at the G20 in 2019 as the presidency on the governance for decentralized finance in accordance with the experiences against high profile hacking incidents and of forming regulatory frameworks. Building on this background, this network aims at providing an open and neutral sphere for all stakeholders to deepen common understanding and to collaborate to address issues they face in order to attain sustainable development of the blockchain community.

©JFSA

https://bgin-global.org

Tentative goals:

1. Creating an open, global and neutral platform for multi-stakeholder dialogue
2. Developing a common language and understandings among stakeholders with diverse perspectives
3. Building academic anchors through continuous provision of trustable documents and codes based on open source-style approach

BGIN Initial Contributors

- 23 experts with diverse backgrounds (**Engineers**, **Regulators**, **Internet Pioneers**, **Academia**, **Business**, **Standards**.)

Mai Santamaria
Head of Financial Advisory team (SFAD),
Department of Finance Ireland
Dublin, Ireland

Jumpei Miwa
Director, Fintech and Innovation Office,
Financial Services Agency, JAPAN

Yuta Takanashi
Deputy director, Office of International Affairs,
Financial Services Agency, JAPAN

Jeremy Rubin
San Fransisco, US

Danny Ryan
Ethereum Foundation

Yuji Suga
Internet Initiative Japan Inc. / CGTF
Tokyo, Japan

Julien Bringer
CEO, Kallistech
Paris, France

Nat Sakimura
Chairman, OpenID Foundation
Tokyo, Japan

Nii Quaynor
Chairman, Ghana Dot Com Ltd
Accra, Ghana

Pindar Wong
Chairman, VeriFi Limited
Hong Kong, China

David Ripley
COO, Kraken
San Francisco, US

Philip Martin
Chief Information Security Officer,
Coinbase Global Inc.

Flora Li
Director, Huobi Blockchain Academy
Beijing, China

Brad Carr
Managing Director, Digital Finance,
Institute of International Finance
Washington D.C., US

Michèle Finck
Senior Research Fellow,
Max Planck Institute for Innovation and Competition
Munich, Bavaria, Germany

Shin'ichiro Matsuo
Research Professor,
Georgetown University
Washington D.C., US

Aaron Wright
Clinical Professor of Law,
Cardozo Law School
New York, US

Katharina Pistor
Professor, Columbia Law School
New York, US

Shigeya Suzuki
Project Professor,
Graduate School of Media and Governance,
Keio University
Fujisawa, Japan

Joaquin Garcia-Alfaro
Full Professor, Institut Mines-Télécom
/ Institut Polytechnique de Paris
Paris, France

Kazue Sako
Waseda University
Tokyo, Japan

Robert Wardrop
Director,
Cambridge Centre for Alternative Finance
Cambridge, UK

Byron Gibson
Program Manager,
Stanford Center for Blockchain Research
San Francisco, US

BGIN’s contribution on the discussion of AML/CFT

BGIN has hosted several conferences for **multi-stakeholders** to discuss key issues such as AML/CFT in **a neutral setting**, including;

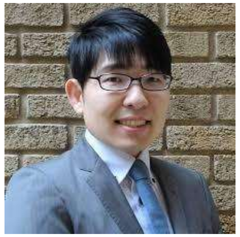
- ***Workshop on Coordination of Decentralized Finance*** (CoDecFin) @ Financial Cryptography 2021: March 5, 2021
  An academic conference based on peer-reviewed papers
  - A multi-stakeholder roundtable discussion of recent regulatory actions and technology advancements on AML/KYC and privacy.

  Website: https://fc21.ifca.ai/codecfin/program.html

- Main Panelists
  - Marta Belcher (protocol.ai)
  - Steve Christe (Kraken)
  - Taariq Lewis (UniFi DAO)
  - Sachin Meier (Georgetown Univ.)
  - Leon Molchanovsky (IOHK)
  - Yuta Takanashi (JFSA)
  - Ryan Taylor (Dash)
  - Diana Barrero Zalles (Yale Univ.)

- ***BGIN second general meeting*** *(Block #2)*: March 8-10, 2021
  - Invited Talks
    - James Angel, Georgetown University USA
    - Jack Gavigan, Executive Director at the Zcash Foundation
    - Frederic de Vaulx, Prometheus Computing LLC
  - Round Table
    - Above + Ryosuke Ushida, JFSA + all participants
  - Unconference Sessions

  Website: https://bgin-global.org/block_2/



We echo FATF's mandate and approach

From our discussion at CoDecFin and Block #2

- While many expressed **concerns about AML/KYC regulations** in terms of privacy, financial inclusion, and enforceability etc, **the need to achieve regulatory objectives was also appreciated.**

- Most of the participants agreed to **utilize a middle ground through multi-stakeholder dialogues** to strike a balance between privacy and regulatory compliance.

- The disconnection between regulation and underlying technologies: **technology-enabled alternative solutions are expected rather than just criticizing the proposed regulation**.

- BGIN supports the aim of FATF to address risks of ML/TF/PF arising from VAs and understand that FATF chose the most straight forward measures to achieve its aim.
- On top of that, BGIN makes technical comments and suggests more practical approaches that FATF may wish to consider to achieve regulatory objectives

Key arguments raised by Stakeholders

Mitigation of ML/TF/PF risks arising from virtual assets is important and urgent. To achieve this effectively without harmful unintended consequences, BGIN stakeholders have made several arguments on the proposed draft guidelines.

- **Cryptographic keys to manage for consumer protection**
- **Clearer regulatory perimeter**
- Need for evidence based approach
- Avoiding one size fits all approach
- Avoiding regulatory arbitrage
- Safety guidance for P2P transactions

See appendices

Cryptographic keys to manage for consumer protection [Para.62]

Argument:

- Cryptographic keys are distributed to multiple entities to protect consumers and attorneys often receive one for legal reasons.
- When the number of DeFi applications generating keys increase, we may face shortage of number of attorneys managing a key on behalf of consumers.
- If attorneys managing a key need to follow all regulatory requirements for VASPs, they will refuse receiving keys, which could exacerbate the shortage of number of attorneys and end up eroding consumer protection.

Potential solution:

- Evaluate pros/cons of application of regulatory treatment on specific functionalities and if needed tailor the requirements to them (avoiding one-size-fits-all approach).
- Encourage developing proper governance that defines roles and responsibilities among entities involved.

Clearer Regulatory Perimeter [Para.47, 68]

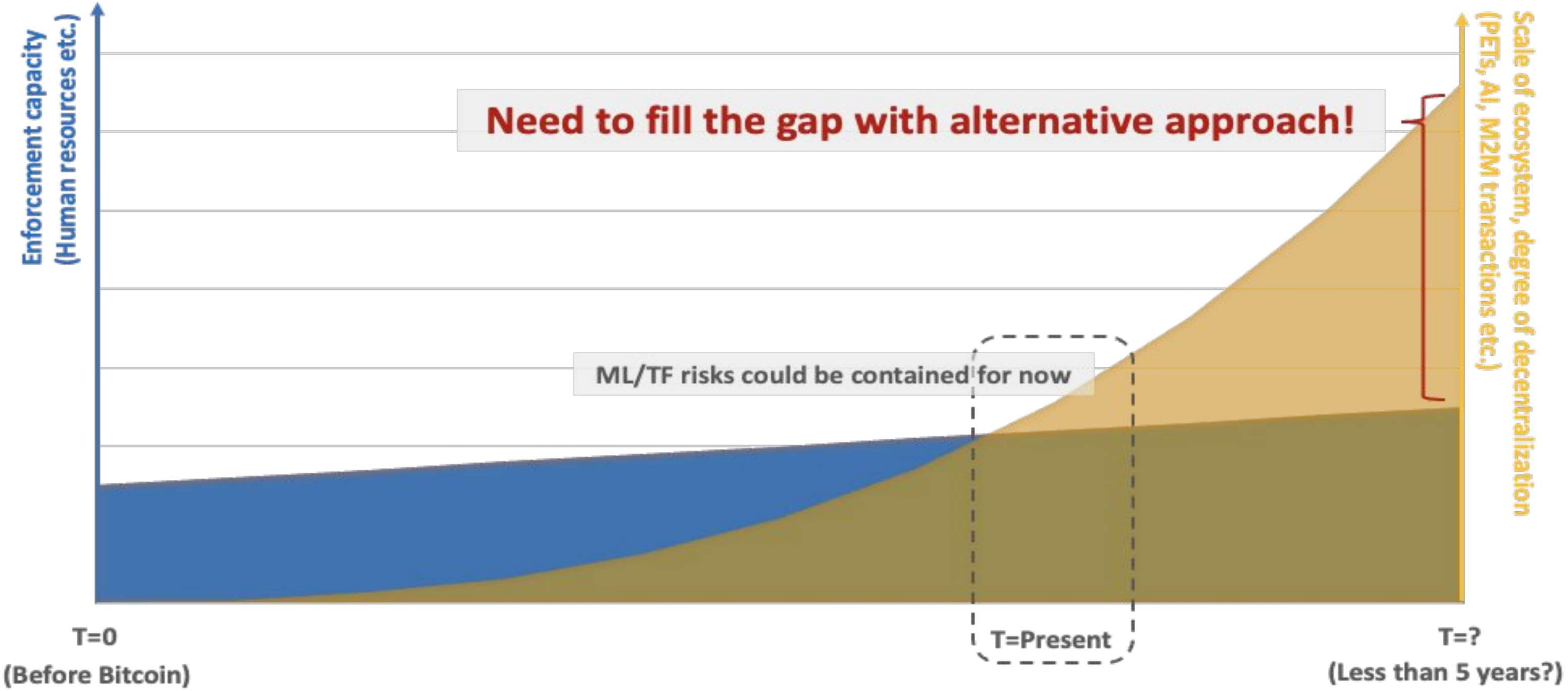
Argument:

- The guidance fails to provide clear definition of VA and VASP, which could cause significant regulatory uncertainties (i.e. large room for discretion of authorities in interpretation). This could end up causing regulatory fragmentation among member jurisdictions.
  - (e.g.) It is highly uncertain if a developer who developed a DEX protocol is a VASP or not if he does not gain direct economic interests such as fees but benefit from the community growth indirectly (e.g., appreciation of governance token).
- This also cause unintended consequences such as harmful impact on innovative activities within financial system, which, in the longer run, could reduce social welfare.

Potential solution:

- FATF should give clearer guidance on the interpretation of the definition of VA and VASP to promote consistent and coherent application of this guidance at the national level.
- FATF should provide FAQ even after the finalization of the guidance and if necessary consider updating the guidance reflecting new market/technical developments.
- FATF may also wish to clarify certain activities meeting certain conditions are not considered as a VASP or exempt from certain regulatory requirements.

Towards the future: Linear vs Exponential



- Reasonable possibilities and risks that 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 disfunctional. Note that It would be too late to take action after the risks materialized.

Challenges in the (near) future

- **Potential Regulatory Gaps raised by P2P & M2M (Machine-to-Machine transactions as P2P transactions)**
- **Risk of Underground Activities via further decentralization/anonymization**
- Common understandings on the FATF guidance (need more time)
- Collecting data for evidence-based policy making
- Analysis on unintended consequences that the guidance could cause

Potential Regulatory Gaps raised by P2P and M2M

Reality of exponential phenomenon:

- Machine to machine transactions / communications could pose ML/TF/PF risks (e.g. hacked/unattended vulnerable machines could be used as a stepping stone for illicit activities) *[Para.35]*
- AI-powered self-learning smart contracts could entirely remove the need of human intervention for the operation *[Para.56]*

Suggestion:

- Suggested VASP definition-excludes machines without operators or ultimate beneficial ownership *[Para.47]*
- FATF depends on approaches to VASP in mitigating risks of peer-to-peer transactions without directly addressing the transaction or parties participating in the transaction. *[para 91]*

Next step to fill the gap:

- FATF may need to consider M2M transactions as a potential source of ML/TF/PF risks in a forward-looking manner (beyond risk of P2P transactions), which could require reconsideration of its standards as well. Global cooperation led by FATF is essential.
- (Joint) research project with academia to deepen understanding on this issue

Risk of Underground Activities

Reality of exponential phenomenon:

- OSS community may seek further decentralization/anonymization to avoid regulatory burden, which makes it even harder and more complicated to achieve regulatory purposes in the long run
- Rapid development of PETs (e.g., payment channel, zk-SNARKs)

Suggestion:

- Too stringent regulatory treatments on decentralized financial services could incentivize such service providers to hide underground *[Para.35, 36(e)(f)]*
- Indeed, OFAC sanction on Bitcoin addresses has encouraged developers to develop more anonymization technologies.

Next step to fill the gap:

- To explore a way to calibrate regulatory treatment carefully to balance between risks of ML/TF/PF and further decentralization and anonymization.
- In so doing, FATF could rely on multi-stakeholder cooperation to develop a mid/long-term regulatory roadmap and explore alternative approaches including code based solutions, taking into account fast-moving technological advancements

How to scale toward an exponential world

Examples of ideas by individual members
(not necessarily reflect the official view of BGIN)

- Code-based approach to scale up regulatory enforcement capacity exponentially in order to keep up with exponential market developments
  - e.g., Deploy codes that automatically refuse processing high risk transactions and report it to FIUs.
- Scale the number of collaborators: Stakeholders (potentially incl. FATF) to develop open global database (e.g., smart contract platform for experimentation) in an collaborative manner
  - Accuracy and fairness of the database and protocols should be subject to review by independent evaluators comprised of academia and other experts
  - Beneficial to explore a code/evidence/risk-based approach
- Safe harbour / regulatory sandbox to incubate disruptive FI-related solutions and experiment with legislation
- Use AI/ML and other tools to evaluate risks and assign risk scores to each transactions

Keep eyes toward the future

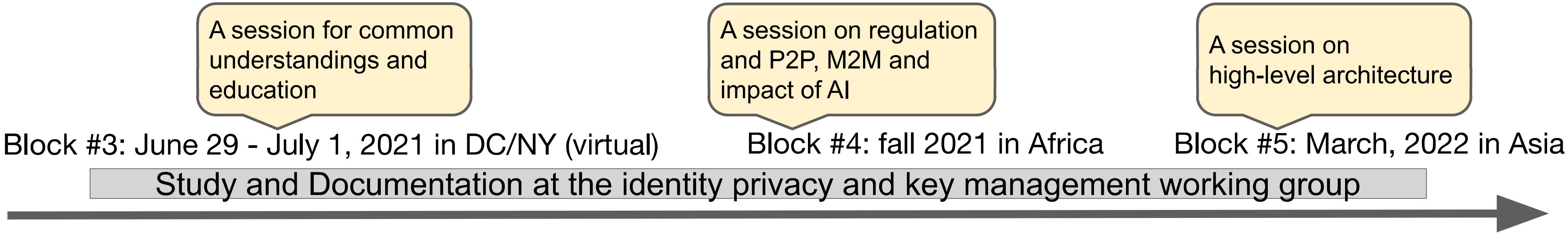
- FATF's current efforts to engage with private sector are **essential to make regulations to catch up with the rapid and disruptive developments in the market.**

  Keep going!
  - Maintain "Kaizen" loop: continue discussions on essential issues
- Reframe thinking style to keep regulations effective in the exponential world
  - Learn from the regulations on the communication industry (e.g. the Internet)

We can help to do better than the current thinking.
We must do better than the current thinking.

Call for (joint) work to improve technologies, operations and regulations

- **Information and idea sharing** over a neutral platform
  - Focus on some exact problem(s) - Examples: P2P, M2M and impact of AI
  - Explore ways to improve technologies and operations to fit regulatory goals
  - Explore ways to improve rules more workable, effective and scalable
- **Work in progress**: working on relevant themes at the Identity, Privacy and Key Management (IPKM) working group to develop several documents. (see next two slides for further details).
- **Next work**: A high-level architecture to deal with P2P, M2M and impact of AI (expecting to be referred by future FATF discussion): NFT, DeFi and Money-LEGO are coming.
- **The third general meeting (Block #3)**: June 29 - July 1, 2021 in DC/NY (virtual)
  - Hold a session to have common understandings and education regarding FATF guidance



A session for common understandings and education

A session on regulation and P2P, M2M and impact of AI

A session on high-level architecture

Block #3: June 29 - July 1, 2021 in DC/NY (virtual)

Block #4: fall 2021 in Africa

Block #5: March, 2022 in Asia

Study and Documentation at the identity privacy and key management working group

BGIN hopes for YOUR participation!

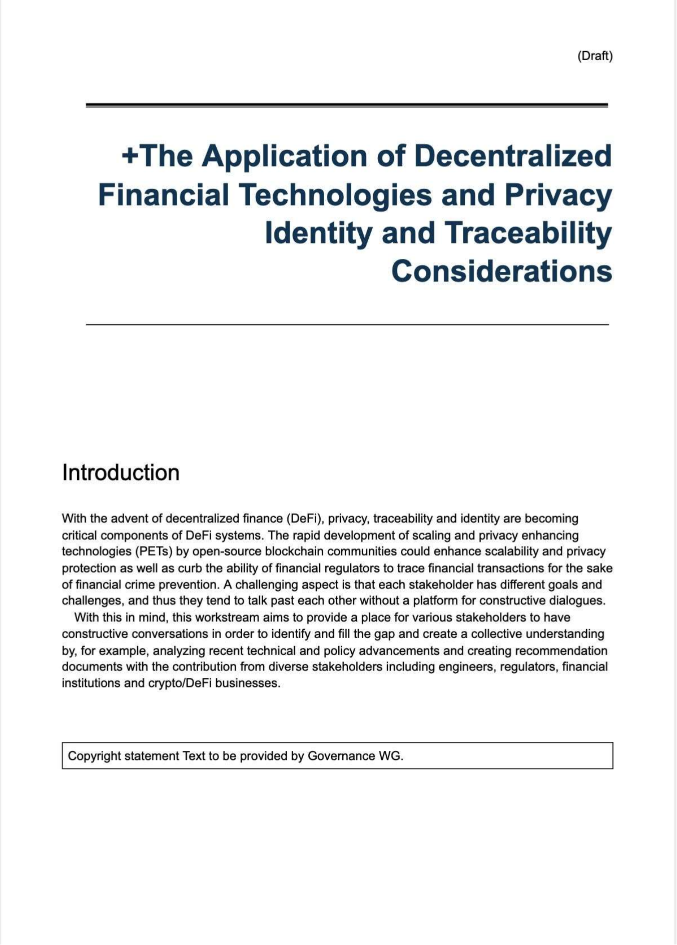
Ongoing documentation at BGIN

The Application of Decentralized Financial Technologies and Privacy Identity and Traceability Considerations

- Considerations on privacy and traceability aspects of decentralized financial technologies/system based on tangible use case analysis

- Policy recommendations for regulators strike a balance between innovation and meeting regulatory requirements (e.g., FATF Travel Rule) with inputs from key stakeholders including engineers, regulators, and businesses

- Link to the current draft



(Draft)

+The Application of Decentralized Financial Technologies and Privacy Identity and Traceability Considerations

Introduction

With the advent of decentralized finance (DeFi), privacy, traceability and identity are becoming critical components of DeFi systems. The rapid development of scaling and privacy enhancing technologies (PETs) by open-source blockchain communities could enhance scalability and privacy protection as well as curb the ability of financial regulators to trace financial transactions for the sake of financial crime prevention. A challenging aspect is that each stakeholder has different goals and challenges, and thus they tend to talk past each other without a platform for constructive dialogues.

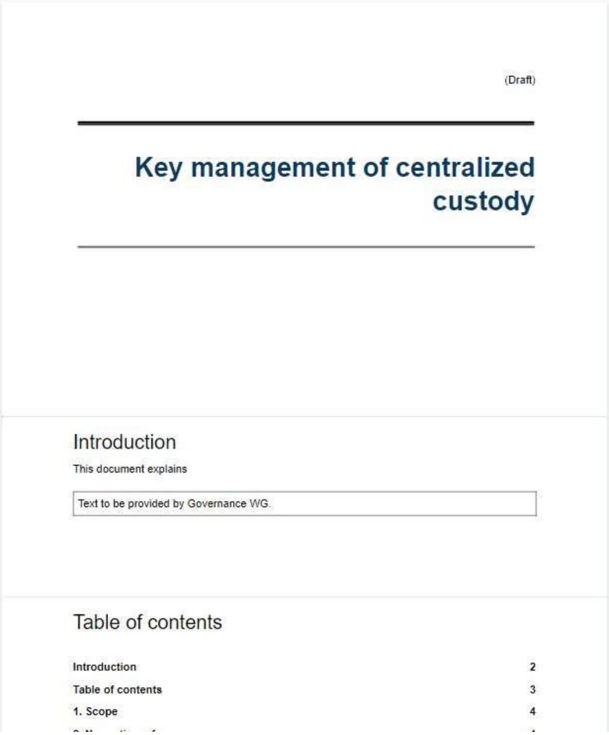
With this in mind, this workstream aims to provide a place for various stakeholders to have constructive conversations in order to identify and fill the gap and create a collective understanding by, for example, analyzing recent technical and policy advancements and creating recommendation documents with the contribution from diverse stakeholders including engineers, regulators, financial institutions and crypto/DeFi businesses.

Copyright statement Text to be provided by Governance WG.

Ongoing documentation at BGIN

Key Management of Centralized/Decentralized Custody

- Model(s) of cryptoasset custodians system that provides cryptoassets custodians work for customers (consumers and other exchanges)
- A list of information assets managed by the cryptoassets custodians system (including the signature key of the cryptoassets)
- The (social) impact which can be exerted by imperfect security measures of the cryptoassets custodians system
- Key lifecycle and its management
- Threat model
- Incident response upon data breach
- Identity management with access control (privilege management)
- AML (FATF Travel Rule)
    - Audit
    - How well current cryptographic solutions and/or protocols satisfy the requirements of FATF for cryptocurrencies, and the limitations of existing solutions to satisfy FATF
    - concern/requirements from regulators
    - inputs by engineers, including descriptions on infeasibility of regulations/requirements.
    - conflict between privacy regulations and AML, not every country is aligned in that sense, and these regulations vary widely around the world.
- Other regulatory requirements (e.g. Japanese regulation, European MiCA)
- Link to the current draft (Centralized Custody)
- Link to the current draft (Decentralized Custody)



(Draft)

Key management of centralized custody

Introduction

This document explains

Text to be provided by Governance WG.

Table of contents

Thanks and Q&A

bgin-global.org

Appendices

Additional arguments & potential solutions

Key arguments raised by Stakeholders

Mitigation of ML/TF/PF risks arising from virtual assets is important and urgent. To achieve this effectively without harmful unintended consequences, BGIN stakeholders have made several arguments on the proposed draft guidelines.

- Number of cryptographic keys to manage for consumer protection
- Clearer regulatory perimeter
- Need for evidence based approach
- Avoiding one size fits all approach
- Avoiding regulatory arbitrage
- Safety guidance for P2P transactions

Need for evidence-based approach

Argument:

- FATF fails to provide solid evidence such as data on the usage of virtual assets for ML/TF/PF that justifies changes it makes on the guidance.
- As of now, AML/CFT solution providers focusing on virtual assets have provided divergent data on the usage of virtual assets for ML/TF/PF and there are no widely accepted analysis on the risks posed by virtual assets.

Potential solutions:

- FATF should provide evidence on the ML/TF/PF risks associated with virtual assets to justify changes on the guidance.
- Or FATF should gather more relevant information before making any changes on the guidance.
- One possible approach for FATF is to work closely with industry partners to develop an open database on ML/TF/PF activities using virtual assets.

Avoiding One Size Fits All approach

Argument:

- Newly designated VASPs due to interpretative changes of the definition could pose very different risks as compared to traditional VASPs such as exchanges.
- One size fits all approach for VASPs with different risks contradicts FATF's "risk based approach".

Potential solutions:

- More tailored approach is needed reflecting actual risks posed by different types of VASPs.
- In considering appropriate regulatory requirements on VASPs, FATF should rely not just on theoretical considerations but also on firm evidence regarding risks associated with particular activities.

Not One Size Fits All Problems

Argument:

- All entities that have keys are generally regulated as VASPs.
- However, if they always sign an additional signature on transactions where AML/CFT actions have been taken by other VASPs, the ML/FT risk has already been reduced.
- When an entity that makes an additional signature on another VASP's signature follows the VASP's obligation, it creates a double VASP obligation.

Potential solutions:

- An entity that always signs an additional signature for transactions for which AML/CFT actions have been taken by other VASPs has no need for VASP obligations.

Avoiding Regulatory Arbitrage

Argument:

- Ambiguous definition of VA/VASPs could cause cross-jurisdictional regulatory fragmentation, which would drive services with higher ML/TF/PF risks to move to jurisdictions with less stricter regulatory treatments.

Potential solutions:

- FATF should provide more clarity on the guidance and publish FAQ to facilitate consistent and coherent application of the guidance.
- FATF may wish to consider conducting peer review among jurisdictions to monitor application of the guidance and its enforcement.

The Sunrise problem in Box-2

Box-2 (How to the FATF Standards apply to a new asset; page 19)

Argument:

- In Country A, VASP can handle NFT tokens? or not in Country-B. (When trading some goods with regulations, the trader can follow this guideline, but they can not follow this guidance when NOT regulated in the country.)
- The flowchart of Box-2 is dependent on the country's law. This could lead so-called sunrise problem.
- If we face on new frameworks of coins, FATF guidelines should be modified?

Potential solutions:

- Reconsideration of flaw chart (sorry for no idea in this moment)

Safety guidance for P2P transactions

Areas of focus 2 (paragraphs 91-93)

Argument:

- The risk mitigation measures are not sufficient and feasible. (paragraph 91)
- Limiting exposure to P2P transactions is not a viable approach. Since **economic freedom**, P2P activity, is constitutionally guaranteed as fundamental human rights, it is not directly enforceable.
- Establishing **best practices for P2P transactions** should help us avoid the risk of getting involved in ML/TF transactions.
- Denying licensing is not enough because VA transactions are, by nature, private using unhosted wallets. Therefore, we also need **clear guidance for non-VASP transactions** to minimize the risk of ML/TF. (paragraph 91 c)
- The public guidance should also include **the proper usage of P2P transactions** to make the right choice between P2P and non-P2P transactions. (paragraph 92 b)

Potential solutions:

- To improve the visibility of P2P activity, FATF may propose countries to facilitate **digital identity registry**. Such a system discloses selected information (country, entity kind, history) to filter out malicious actors while preserving user's privacy.
- To enhance reporting, record-keeping, and due diligence, FATF may promote the use of **public ledger** to accelerate embedded supervision for real-time monitoring and long-time traceability.
- FATF ~~should~~ may wish to study the best practices of **user verification in P2P transactions** (Know Your Counterparty). Users should be able to verify the counterparty's identity (ex. verifiable credentials).
- FATF may want to ~~should~~ establish **comprehensive guidance** (VASP, non-VASP, hosted, unhosted) and conduct information campaigns to establish the most secure and effective normative practice to mitigate the ML/TF risks in any form of VA transaction.