SWISS
BLOCKCHAIN
FEDERATION

Swiss Blockchain Federation | Schauplatzgasse 39 | 3011 Bern

FATF / GAFI
2, rue André Pascal
F-75775 Paris Cedex 16

Mail: fatf.publicconsultation@fatf-gafi.org

Bern, 19th April 2021

Comments of Swiss Blockchain Federation on the draft revised VASP Guidance

Dear Financial Action Task Force

We greatly appreciate the opportunity to comment on the draft guidance on virtual assets. So far, the Financial Action Task Force's (FATF) responses to crypto finance appeared to be somewhat rushed, starting with an ambiguous definition of "virtual assets"[1] and culminating with the latest ideas to stretch the scope of the term "Virtual Asset Service Providers" (VASP) beyond financial intermediation. We hope that we can help to move the discussion towards a more effective and actually risk-based approach towards money laundering and terrorist financing in Decentralized Finance (DeFi). We propose a number of principles and alternative ideas that are designed to leverage blockchain technology instead of eroding the benefits of disintermediation.[2] Finally, we also have some important inputs to the application of the travel rule.

Proportionality and Technology Neutrality

Regulations in financial markets, whether directly applicable or indirectly stated for further implementation in national laws must comply with the general principles of proportionality and technology neutrality. (i) Proportionality means that the proposed regulations are suitable to achieve the envisaged objectives, that the degree of intervention into private businesses does not go further than required for the realization of the objectives, and that the burden imposed by the regulatory intervention stands in a reasonable proportion to the prevented damage.[3] (ii) Technology neutrality attempts at implementing the released regulations in a way being not dependent upon the actual

[1] A good definition positively describes what something is. The FATF definition of virtual assets does the opposite: it says what a virtual asset is not, leading to ambiguity and causing confusion. The FATF implicitly recognizes this problem as it undertakes considerable effort in the draft recommendation to clarify the meaning of "virtual asset". In this context, we would like to point the FATF to the newly adopted article 973d of the Swiss Code of Obligations, which contains a much more workable and precise definition of crypto assets: These are assets that an owner can digitally hold and transfer without depending on the help of the issuer or a third party. Usually, crypto assets are controlled using cryptographic methods, hence the name crypto assets.

[2] The FATF itself admits that its recommendations lead to unintended, negative consequences in a recent publication, but only grasps the tip of the regulatory burden it imposes on fintech companies and the consequential harms done to the freedom to innovate and overall economic growth. (https://www.regulationtomorrow.com/eu/mitigating-the-unintended-consequences-of-the-fatf-standards)

[3] There are hints that AML regulation is at risk of violating proportionality principle. See: Ronald F. Pol (2020) Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice, 3:1, 73-94, DOI: 10.1080/25741292.2020.1725366

technology but applicable for all comparable business models irrespective of the chosen technology (no. 41). Partly, reference is also made to the notion of functional approach (nos. 22 lit. c and 48).

While money laundering is a crime of general application in many, if not most, jurisdictions, anti money laundering (AML) regulations imposing administrative and organizational obligations apply only to professional financial sector entities. They have been extended to non-financial sector actors solely with great reluctance and solely if it was proven that that sector was particularly exposed to money laundering. The reasons for this reluctance are obvious: enforcing administrative due diligence duties and obligations outside of a sector which already is subject to, and familiar with, regulations is nearly impossible. Furthermore, expanding the scope of AML regulations threatens to overload supervisory authorities and to adversely deflect regulatory resources.

So far, AML regulations were to be complied with by those financial intermediaries that had the actual and legally relevant control of and power over certain assets owned by third persons.[4] This control or power is important since thereupon the assets can be transferred to other beneficial owners. In the introduction of the latest FATF update, acting “on behalf” of someone is still a defining criterion for VASPs,[5] but later ignored in an attempt to squeeze operators of DApps and other tangentially involved parties into the definition of “VASP”.[6]

The fundamental problem the FATF faces is that blockchain-technology enables disintermediation, but its so-called recommendations[7] rest on the assumption that most financial transactions are done through financial intermediaries. Therefore, the FATF’s initial reaction of trying to expand the scope of its AML recommendations beyond financial institutions is comprehensible, but misguided. Rather the scope of application should coincide with financial markets regulations.

Open DApps only pose minimal risks

The most prominently featured piece of evidence the FATF provides for the necessity of its intentionally “expansive” regulation is the wannacry ransomware attack.[8] According to United States sources, this attack originated in North Korea and caused billions of dollars in damage.[9] While the motivation behind the authors might not have been financial, they nonetheless succeeded in collecting Bitcoins worth 86,000 USD in ransom.[10] However, as the FATF indicates, their attempt at layering the crypto assets failed. This is owed to a defining characteristic of transactions on public blockchains:

[4] See “enabling control” in nos. 47 [iv] and 60 et seq. Acting “on behalf” of a client, which implies control over the clients assets, is also a defining feature of the FATF definition of “financial institution”.
[5] The FATF writes: “In that respect, it highlights the key elements required to qualify as a VASP, namely acting as a business on behalf of the customers and facilitating VA-related activities.”
[6] See sections 75 to 79 of the draft recommendations.
[7] Member countries commit in writing to implement the FATF’s “recommendations”. Calling these regulations “non-binding” and “recommendations” appears to be misleading.
[8] https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)
[9] https://www.reuters.com/article/us-cyber-northkorea-sony-idUSKCN1LM20W
[10] The three Bitcoin addresses associated with the wannacry virus are:
https://www.blockchain.com/btc/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94,
https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw,
https://www.blockchain.com/btc/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn . As anyone can verify, they received about 54 Bitcoins in total, worth about 1,600 USD each at that time.

their transactions are anonymous, but can be publicly tracked. By definition, they are ill-suited to laundering money, at least vis-a-vis a competent observer.[11] [12]

The most economically successful example of a DApp that would be adversely affected by the proposed recommendations might be Uniswap, a decentralized exchange that currently enjoys considerable trading volume (a few billions per day) and fee revenues (about a billion per year). Imposing the contemplated rules on the team behind the project would likely destroy Uniswap and the whole ecosystem around it. It thrives on openness and accessibility. Anyone, including other DApps, can create new trading pairs, provide liquidity, and trade on it. The FATF's implicit assumption that DApps like Uniswap can somehow be transformed into a financial intermediary without destroying their business model is a misjudgment.

Due to Uniswap being based on a public blockchain, all transactions are public and every trade can be tracked. For example, consider transaction 0x22e7...d120. Here, the owner of address 0xf5e2...b2dc swapped 5000 units of the dollar-pegged stablecoin DAI into 2.9 Ether. This transaction does not obfuscate any source of funds. All it does is convert a balance denominated in DAI into a balance denominated in ETH sitting on the same address. Any competent intermediary that receives these Ether can identify their source and can use that information to verify the plausibility of the "source of funds" declaration of its client. That's why decentralized exchanges like Uniswap and other DApps will not be of much help to criminals like the author of wannacry. If any regulatory action is necessary at this point in time (which is doubtful), it should be aimed at preserving the openness and transparency of blockchain technology.

Seven Principles

We suggest that the FATF includes some guidance on how the unintended side-effects of its recommendations can be mitigated. In particular, the following principles might prove helpful in guiding national regulators:

1. **Regulation must refrain from imposing obligations on persons that cannot fulfill these obligations.**
   As a corollary, regulation should not force entities that do not engage in financial intermediation to become financial intermediaries. Forcing DApps such as Uniswap or DAI to become financial intermediaries by definition destroys the foundations of their and any other business model built on the benefits of disintermediation. The FATF unconvincingly assumes that the purpose of giving up control in disintermediated setups is to circumvent regulation, when in fact disintermediation greatly increases the security and dependability of financial services.

2. **Regulation imposed on a business should be related to its business model.**
   For example, a business that processes transaction data without having access to any client funds might be subjected to data retention rules, but it should not have any obligations to freeze or otherwise interfere with client assets if it cannot technically do so. This principle is already applied to operators of network nodes and deserves expansion. Such a rule could

[11] While the FATF does not define "money laundering" in its glossary, money laundering is commonly assumed to mean the obfuscation of the origin of illicit funds. Public blockchain-based transactions are much less suitable at achieving that aim than private transactions done through intermediaries. That's also why the existing approach towards crypto, namely regulating the gate-keepers, is effective.
[12] See also "An Analysis of Bitcoin's Use in Illicit Finance", by former CIA director Michael Morell, 2021-04-06 https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

greatly increase legal certainty and thereby reduce the legal risks of testing new business models.

3. **The issuance of securities is not intermediation.**
Box 3 in the FATF draft states that the act of issuing virtual assets makes a business a VASP. In the case of crypto assets representing securities, this is inconsistent with traditional FATF rules. The FATF should clarify that equally to the issuance of traditional securities such as bonds or shares, the issuance of virtual assets that serve an investment purpose (and not a payment purpose) does not constitute financial intermediation per se. However, third parties supporting the issuance process might qualify as financial intermediaries or VASPs, just like in case of traditional financial instruments.

4. **Regulation should not introduce analog steps into otherwise digital processes.**
For example, an exclusively digitally acting financial intermediary should be allowed to entirely rely on digital data in its know-your-customer (KYC) processes.

5. **Regulation should not introduce manual steps into otherwise automated processes.**
The introduction of manual verification steps into otherwise fully automated processes destroys the scalability of otherwise scalable business models, thereby harming economic growth.

6. **Allow financial intermediaries to collaborate when identifying clients.**
In Switzerland and other countries, the law requires every financial intermediary to repeat the whole KYC process for every client, even when other financial intermediaries have identified the same client immediately before that. So in a setup as described in Box 4 of the updated FATF draft, a user would have to complete all KYC forms multiple times as the setup involves multiple VASPs. This puts decentralized setups at an unjustifiable disadvantage compared to centralized service providers. In order to avoid this consequence, FATF should encourage national regulators to allow financial intermediaries to share client information data and to rely on third party identity proofs instead of having each intermediary repeating the same steps again for the same client.

7. **Regulation should recognize the reduced risk of public transactions and therefore aim at keeping DApp transactions easily traceable.**
The FATF claims to be strongly committed to a “risk-based approach”, even putting it into the title of its draft guidance. Recognizing that publicly visible transactions pose a much lower money-laundering risk than private transactions, the FATF should refrain from applying the same regulation to both types of transactions. Recognizing that public transactions are less suited for money laundering and that transparency and accountability are desirable public goods, regulators should embrace open and transparent systems instead of pushing them into traditional, opaque setups.

Based on these seven guiding principles, one can also answer the FATF's questions on how peer-to-peer transactions should be handled: namely by recommending that technical facilitators of financial transactions should ensure that the transactions they facilitate can be traced back when the transacted funds finally arrive at a financial intermediary. Depending on the involved parties and systems along the way, this could imply data retention obligations and legal foundations to allow better sharing of collected data among and with financial intermediaries. For initiators of DApps and other decentralized systems, this could mean that they should provide financial intermediaries and regulators with the documentation, data, and tools necessary to monitor and trace the relevant transactions.

Travel Rule

With regards to the travel rule, the recommended approach of the FATF to apply it in a technology-neutral way is the right way forward. Also, the idea of letting the client provide the missing information in case of payments from and to non-custodial wallets seems reasonable and fit for purpose. However, it would be helpful to clearly indicate the bounds of the travel rule. The travel rule has been designed for payment instructions, and not for trade instructions and other types of instructions where the payment is not the primary purpose.

For example, when executing a Bitcoin transaction, there is always also a small payment flow in the form of a transaction fee and it should be made clear that the beneficial owner of the transaction fee does not need to be identified. The deeper reason for why this makes sense is that the client cannot choose the recipient of the transaction fee, making it ill-suited for money laundering or terrorist financing even if it was large. While the risk of regulators mistakenly applying the travel rule to transaction fees appears to be marginal, there are other types of transactions where that risk is higher, in particular swaps on decentralized exchanges.

Just like traditional banks are not required to identify the beneficial owner on the other side of a trade when a client buys some IBM shares on the stock market, virtual asset service providers must not be required to identify the counterparty of a trade when they swap crypto assets through a decentralized exchange on behalf of a client. In both cases, with traditional stock markets and with decentralized exchanges, there is neither a need nor a legal basis to apply the travel rule. In both cases, the transactions are not suited for money laundering or terrorist financing as the counterparty of the trade is unknown to the client and there is no net transfer of value, only a change in denomination.

It should be made clear by the FATF that the travel rule is only to be applied for transactions that serve the purpose of transferring value to a specific beneficiary known by the client. Transactions, for which the client cannot specify the beneficiary ex ante, are by definition not suitable to funnel illicit funds to a specific counterparty. Therefore, there is no necessity to identify the counterparty for the purpose of combating money laundering or terrorist financing. This principle applies to the transaction fees of crypto assets, to swaps through decentralized exchanges, and to many other transactions facilitated by DApps.

The SBF is open to support the FATF in adopting and further refining the recommendations presented herein. We strongly believe that blockchain technology can be an enabler for building a more open, more free, and more transparent financial system: an “Internet of Finance”. The influence of the FATF on how fast such a vision can be realized and what such an Internet of Finance could finally look like cannot be understated. With great power comes great responsibility; therefore, we kindly ask you to carefully reevaluate your draft with regards to the issues we raised.

Best regards

Swiss Blockchain Federation	Swiss Blockchain Federation
Heinz Tännler President	Mathias Ruch Member & Expert Council