# Governments Planning Worldwide Regulation of Bitcoin [October 2021]

**The worlds' wealthiest nations are aiming for cryptos, restricting, amongst others, the following:**

- ✓ Peer-to-Peer Transactions;
- ✓ Stablecoins;
- ✓ Private wallets (cold storage, phone and desktop apps);
- ✓ Privacy (privacy coins, mixers, Decentralized exchanges, use of TOR and I2P);
- ✓ Former ICOs and Future Projects (DeFi, NFT, smart contacts, second layer solutions, and much more).

**In addition, these new regulations intend to:**

- ✓ Force those active in crypto to be licensed and regulated as banks (responsible for KYC and transaction tracking);
- ✓ Create full transparency for ALL transactions;
- ✓ Exclude and freeze assets of persons, activities, and countries labeled a "risk;"
- ✓ Force the inclusion of user information with all transactions;
- ✓ Revoke the license of those who don't comply.

In short: they want to change the way the space can operate. As you'll discover, the regulation rolled out aim to create a system of complete transparency and control. At the same time, regulatory clarity could pave the way for the next stage of adoption.

This report explains exactly what to expect and how you can prepare yourself...

## <What Can You Get from This Report_

For years, we wondered if governments would “ban Bitcoin.” As it turns out, they will not. Instead, they intent to simply absorb cryptos into the existing regulated financial system.

What you’re about to read is a report based on new official international regulations. This report reveals exactly what the coming regulations mean for cryptos, who is behind them, and how they will be implemented. Next, this report highlights the most revealing and stunning clauses. And finally, it summarizes which activities are likely to thrive and which are bound to suffer so that you can protect yourself.

If you work in the crypto-space, are invested in crypto-currencies, or are interested in decentralized technologies and how they shape our future world, you should read every letter in this report. A lot of activities that are currently considered normal will be so tightly regulated that the use of cryptos will change forever!

A regulatory minefield is about to be laid out for those active in the crypto space. By reading this report you know what is coming and will have the advantage.

This information is crucial for anyone in cryptos. Study this report without delay, and do not hesitate to share it with anyone you think can benefit from it.

# <What Is Going On?_

In 2018, the news that Facebook was creating a crypto, shocked international regulators. Until then, they didn't see cryptos as a risk to the stability of the global financial system. However, Libra, the coin Facebook proposed, was a so-called stablecoin; it maintains its value relative to the USD. They quickly realized what would happen when a company with a billion users creates an instant payment system that is cheaper, faster and more user-friendly than the current financial system.

This topic was discussed at the highest levels of government; the G20, an international forum for the governments and central bank governors from 19 countries and the European Union. They engaged an organization called the Financial Action Task Force (**FATF**), whose goal it is to protect *"the integrity of the global financial system."* (GVA, p6)

This organization has passed similar legislation for banking and financial service providers around the world. They are responsible for the fact that all crypto-currency exchanges where fiat is exchanged for cryptos have the same KYC and anti-money laundering requirements as banks. Now, they are going to use this framework to focus on the elements of the industry currently outside their control, and declare what is, and isn't acceptable.

In their original guidance,[1] issued in July of 2018, FATF set out to combat the perceived money laundering and terrorist financing threat of virtual assets. Since then, they made a lot of progress.

### New Guidance on Cryptos

The latest draft guidance of the FATF, to be implemented in October 2021, is called *"Guidance for a risk-based approach to virtual assets and VASPs"* (**GVA**).[2] In the remainder of this report, the GVA is often quoted, and page numbers are added for easy reference.

As you will see, they have a deep understanding of what is happening in the space. Moreover, they take the expansive view that *"most arrangements currently in operation,"* including *"self-categorized P2P platforms"* may have a *"party involved at some stage of the product's development and launch"* who will be covered by this new legislation. (GVA, p29)

## Why does the FATF have global power?

Since FATF isn't an official government agency of any country, they cannot create law. They issue what is known as "soft-laws": recommendations and guidance. Only when this guidance is implemented in the laws of the countries, they become "hard-laws" with real power. In theory, they are thus subjected to the formal law-making process of law-giving countries. However, countries that don't participate are placed on a list of "non-cooperative jurisdictions."[3] They then face restricted access to the financial system and ostracism from the international community. For this reason, almost all nations, implement these recommendations. It also must be said that national governments, especially in the Western world, highly value this kind of international cooperation and the power it gives them. Many such treaties are passed into law with little opposition or delay.

Once these treaties are accepted, they become part of a body of law called international law, a type of law in many cases superseding national laws. Unknown to the general public, international law is increasingly being used as a backdoor for passing invasive regulations such as these.

And in case anyone doubts on how the FATF sees their relationship with national laws: *"The Guidance is intended to help national authorities in understanding and developing regulatory responses* [...] *including by amending national laws, where applicable, in their respective jurisdictions."* (GVA, p7)

It must be noted that people working for this Paris-based organization are faceless bureaucrats who have not been elected, their procedures and budget are not subjected to democratic

oversight, and they are almost impossible to remove from power. Like most international organizations, they fall under the Vienna Conference on Diplomatic Intercourse and Immunities.[4] As such, they enjoy immunity for their actions, are exempt from administrative burdens in the countries they are active, such as taxes, and free from most COVID travel restrictions.

## When will this "Guidance" be implemented?

The GVA was published in March to be subjected to public consultation.[5] This gives it the appearance of the public having a say in the implementation of it, but when you read it carefully they will consider feedback only on "relevant issues" they themselves selected. Other feedback might be considered in the next review in 12 months (by then, most current recommendations will likely have been passed into law). In other words, this will be it, with minor adjustments.

In June 2021 FATF processed all feedback. Then these new "recommendations" were supposed to become official in July. However, they issued a statement[6] that this was postponed to October 2021, to give countries time to comply. From October 2021 onwards we can expect these recommendations to start being implemented with priority in national legal systems, and as such, start affecting our lives.

This process has been successfully used in the banking system and tax systems—it is now coming for crypto. It is worth noting that individual countries might decide on even more specific or explicit prohibitions on top of this. It is worth noting that these regulations do not apply to central bank-issued digital currencies. (GVA, p9)

## <How Will Cryptos Be Regulated?_

Before we can understand how FATF proposes to regulate cryptos, we must learn what they mean when they talk about a Virtual Asset:

> *"A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."* (GVA, p98)

Cryptos will not be outright banned. They will be regulated via an indirect method; those who facilitate crypto transactions, are designated as a Virtual Asset Service Provider (**VASP**). Next, all VASPs will be subjected to similar regulation as banks. The definition of VASP is so wide that most current projects in the crypto space are covered by it.

**Definition of a VASP:**

*"VASP: Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

i. *exchange between virtual assets and fiat currencies;*
ii. *exchange between one or more forms of virtual assets;*
iii. *transfer of virtual assets (In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.);*
iv. *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
v. *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."* (GVA, p18)

**Many organizations and individuals are VASPs:**

A VASP is **any natural or legal person**, and *"the obligations in the FATF Standards stem from the underlying financial services offered without regard to an entity's operational model, technological tools, ledger design, or any other operating feature."* (GVA, p21)

As you can see, they are casting a wide net. The expansiveness of these definitions represents a conscious choice by the FATF. *"Despite changing terminology and innovative business models developed in this sector, the FATF envisions very few VA arrangements will form and operate without a VASP involved at some stage."* (GVA, p29)

*"A VASP does not have to provide every element of the exchange or transfer in order to qualify as a VASP."* (GVA, p22) As such, it includes those who facilitate Decentralized Apps (DAPPS); *"...entities involved with the DApp may be VASPs under the FATF definition. For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer."* (GVA, p23)

For those wondering if they are a VASP, the following general questions can help guide the answer:

- *"who profits from the use of the service or asset;*
- *who established and can change the rules;*
- *who can make decisions affecting operations;*
- *who generated and drove the creation and launch of a product or service;*
- *who possesses and controls the data on its operations; and*
- *who could shut down the product or service.*

*Individual situations will vary and this list offers only some examples."* (GVA, p30)

## What Are VASPs Obliged to Do?

All VASPs will be forced to implement KYC legislation and monitor transactions. They become fully regulated entities who need to obtain a license. Individuals can also be labeled a VASP.

The real kicker is that all activities not part of the regulated system are labeled as "high-risk." And as such, those performing such activities become high-risk individuals, which could have repercussions in the wider financial system, since financial institutions should as well *"apply a risk-based approach when considering establishing or continuing relationships with VASPs or customers involved in VA activities."* (GVA, p10)

It is important to understand that most peer-to-peer activities themselves will not be banned (although countries may do so on their own accord). However, transactions with a "high-risk" background will be tainted and scrutinized. Exchanges risk losing their license if they deal with them, and many will simply choose not to allow them. It might get to a point where proceeds from certain peer-to-peer transactions or private wallets are no longer usable in the financial system, at least not without extensive due diligence.

## Competent Authorities

Every country should assign a "competent authority" to monitor the crypto space and communicate with competent authorities in other countries: *"VASPs should be supervised or monitored by a competent authority, not a self-regulatory body (SRB), which should conduct risk-based supervision or monitoring."* (GVA, p45) This can be an existing regulatory body, such as a central bank or a tax authority, or a specialist VASP supervisor. (GVA, p91)

# <What Activities Will Be Regulated_

This chapter highlights crypto activities, currently considered completely normal, and details how they are to be regulated.

**Peer-to-Peer Transactions:**

*"'Peer-to-peer' (P2P) transactions are VA transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets."* (GVA, p14) These transactions themselves are outside of the scope of these recommendations, because: *"the FATF Recommendations generally place obligations on intermediaries between individuals and the financial system, rather than on individuals themselves."* (GVA, p14)

However, *"the FATF recognises that P2P transactions could pose heightened Money laundering and terrorist financing risk."* (GVA, p14) Moreover, *"if P2P transactions gain widespread and mainstream traction"* this could lead to *"systemic vulnerabilities"* and could *"foreshadow a future without financial intermediaries, potentially challenging the effectiveness of the FATF Recommendations."* (GVA, p15)

To combat the *"risk"* of a peer-to-peer payment system, FATF recommends competent authorities to use *"public-private sector co-operation"* (GVA, p35) to achieve the following summarized points (GVA, p37, author notes in brackets):

a) Enhanced visibility [chain-analysis];
b) Enhanced supervision of exchanges allowing private transactions;
c) Denying licensing to VASPs if they allow P2P transactions;
d) Additional AML/CFT requirements;
e) Encouraging risk analysis of clients.

In addition, countries may wish to consider:

a) Outreach to representatives from the P2P sector [making offers they can't refuse];

b) Issuing public guidance [propaganda and FUD on the use of crypto currencies];
c) Training of supervisory, FIU, and law enforcement personnel.

Jurisdictions may even prohibit or limit *"VA activities carried out by non-obliged entities"* altogether. But when they do so, they are still obliged to perform *"outreach and enforcement actions"* to prevent people from transacting in crypto currencies *"illegally"* and in addition, *"Co-operate internationally."* (GVA, p37-38)

**Stablecoins are considered a major risk:**

FATF first explains why the main focus is on stablecoins: *"As discussed in the FATF report to the G20, so-called stablecoins may also be more likely to reach mass adoption by the public as compared to some VAs, which could potentially greatly increase the risks they pose if realized."* (GVA, p44)

Stablecoins may be targeted at the level of the central developer or governance body; *"A governance body consists of one or more natural or legal persons who establish or participate in the establishment of the rules governing the stablecoin arrangement"* and *"each natural or legal person constituting the governance body could also be a VASP depending on the extent of the influence it may have."* (GVA, p27) Moreover, they can be *"held accountable for the implementation of AML/CFT controls"* across the ecosystem. (GVA, p28)

Regulating stablecoins has a high priority; *"It is important that ML/TF risks of so-called stablecoins, particularly those with potential for mass-adoption and can be used for P2P transactions, are analysed in an ongoing and forward-looking manner and are mitigated before such arrangements are launched. It will be more difficult to mitigate risks of these products once they are launched."* (GVA, p36)

**Unhosted Wallets:**

Commonly used private wallets are naturally outside the control of any VASPs. FATF calls these: "unhosted wallets." As mentioned,

the FATF suggests denying licensing VASPs *"if they allow transactions to/from non-obliged entities (i.e., private / unhosted wallets)."* (GVA, p37)

The FATF recognizes that *"not every VA transfer may involve (or be bookended by) two obliged entities."* However, the obliged entity that is part of a transaction should still *"obtain the required originator and beneficiary information from their customer."* They should also *"treat such VA transfers as higher risk transactions that require enhanced scrutiny and limitations."* (GVA, p60)

**Client Information to Collect by VASPs:**

FATF recommends that all VASPS collect information on their clients: *"Typically, required customer identification information includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number)."* (GVA, p74)

*"Depending upon the requirements of their national legal frameworks, VASPs are also encouraged to collect additional information to assist them in verifying the customer's identity when establishing the business relationship (i.e., at onboarding); authenticate the identity of customers for account access; help determine the customer's business and risk profile and conduct ongoing due diligence on the business relationship; and mitigate the ML/TF risks associated with the customer and the customer's financial activities."* (GVA, p74)

*"Such additional, non-core identity information, which some VASPs currently collect, could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; VA wallet addresses; and transaction hashes."* (GVA, p74)

**Travel Rule:**

FATF recommends applying traditional bank wire transfer requirements on crypto currency transactions; this is called the travel rule.

It *"includes the obligation to obtain, hold, and transmit submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities."* (GVA, p77)

Information accompanying all qualifying wire transfers should always contain:

a) *"the name of the originator;*
b) *the originator account number where such an account is used to process the transaction;*
c) *the originator's address, or national identity number, or customer identification number, or date and place of birth;*
d) *the name of the beneficiary; and*
e) *the beneficiary account number where such an account is used to process the transaction."* (GVA, p53)

**Instant transfer of transaction information**

VASPs should make use of *"technological solutions"* and *"carry out the following main actions"*:

a) *"enable a VASP to locate counterparty VASPs for VA transfers;*
b) *enable the submission of required and accurate originator and required beneficiary information immediately when a VA transfer is conducted on a DLT platform;*
c) *enable VASPs to submit a reasonably large volume of transactions to multiple destinations in an effectively stable manner;*
d) *enable a VASP to securely transmit data, i.e. protect the integrity and availability of the required information to facilitate record-keeping;*

e) *protect the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure in line with national privacy and data protection laws;*
f) *provide a VASP with a communication channel to support further follow-up with a counterparty VASP for the purpose of:*
    - *due diligence against counterparty VASP; and*
    - *requesting information on a certain transaction to determine if the transaction is involving high risk or prohibited activities.”* (GVA, p77)

*“Obliged entities should submit the required information simultaneously with the batch VA transfer itself”* although the required information need not be recorded *“on the blockchain or other Distributed Ledged Technology (DLT) platform itself.”* (GVA, p55)

**Risk Based Approach:**

VA and VASP activity will be subject to a *“Risk-Based Approach.”* (GVA, p55) In practice, this means that each client and activity is categorized by their risk level. Persons or activities considered a risk can see enhanced due diligence and even their ability to use VASPs reduced.

*“VAs and VASPs in general may be regarded as higher ML/TF risks that may potentially require the application of monitoring and enhanced due diligence measures, where appropriate, depending on the jurisdiction’s context.”* (GVA, p35)

This might include *“obtaining additional information on the customer and intended nature of the business relationship, obtaining information on the source of funds of the customer, obtaining information on the reasons for intended or performed transactions, and conducting enhanced monitoring of the relationship and transactions.”* (GVA, p48)

**Risk Assessment Factors**

A wide variety of information could be used to assess the level of a risk, including, but not limited to:

- *"The AML/CFT laws and regulations of the home country or the host country where the respondent institution is doing business and how they apply;*
- *Public databases of legal decisions and/or regulatory or enforcement actions;*
- *Annual reports that have been filed with a stock exchange;*
- *Country assessment reports or other information published by international bodies which measure compliance and address ML/TF risks (including the FATF, FSRBs, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Co-operation Review Group process;*
- *Reputable newspapers, journals or other open source electronic media;*
- *Third party databases;*
- *National or supranational risk assessments;*
- *Information from the respondent institution's management and compliance officer(s); and*
- *Public information from the regulator and supervisor."* (GVA, p79)

VASPs are also ordered to differentiate between activity involving normal and high-risk jurisdictions based on credible sources such as: *"the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units."* (GVA, p47)

Existing traditional banks and other financial institutions also will monitor your crypto activity. They should *"consider establishing or continuing relationships with VASPs or customers involved in VA activities"* and *"evaluate the ML/TF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed."* (GVA, p10)

**Ongoing Transaction Monitoring:**

As mentioned, every customer is to be assigned a risk profile. Based on this profile, customer transactions will be monitored: *"Ongoing monitoring on a risk basis means scrutinizing transactions to determine whether those transactions are consistent with the VASP's (or other obliged entity's) information about the customer and the nature and purpose of the business relationship, wherever appropriate."* (GVA, p75)

*"A customer's profile will determine the level and type of ongoing monitoring potentially necessary and support the VASP's' decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (e.g., nature and volume of trading activity, origin of virtual funds deposited, etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (e.g., clients conducting similar types of VA transactions or involving the same VA)."* (GVA, p74)

This ongoing monitoring will result in the creation and sharing of "blacklists of addresses," (GVA, p75) and the silent submission of *"Suspicious Transaction Reports (STRs)"* to the authorities. (GVA, p63) In addition, there will be *"automatic flagging and subsequent inspection,"* (GVA, p75) based on *"red-flag indicators,"* such as:

a) *"Technological features that increase anonymity – such as the mixers, tumblers or AECs;*
b) *Geographical risks – criminals can exploit countries with weak, or absent, national measures for VAs;*
c) *Transaction patterns – including transactions which are structured to avoid reporting or appear irregular, unusual or uncommon which can suggest criminal activity;*
d) *Transaction size – if the amount and frequency has no logical business explanation;*
e) *Sender or recipient profiles – unusual behaviour can suggest criminal activity; and*
f) *Source of funds or wealth – which can relate to criminal activity."* (GVA, p81)

**Digital IDs:**

In the future, VA transactions might need to be subject to digital identity regulations,[7] also being developed by the FATF: *"the absence of face-to-face contact or the lack of involvement of a regulated VASP or FI in VA financial activities or operations may indicate higher ML/TF risks, and thus may require appropriate risk mitigating measures to identify or combat relevant illicit activities or frauds, such as the use of strong digital identity solutions."* (GVA, p13)

**Freezing of Assets:**

A major part of the teeth of this regulation will come from the freezing of assets. VAs can be frozen when the holder is suspect of a crime, as part of other investigations, when the VA is related to terrorist financing, and when related to financial sanctions. (GVA, p39)

The freezing of VAs will happen regardless of the property laws of national legal frameworks, and it will not be necessary that a person be convicted of a predicate offence[8] (GVA, p39).

**Anonymity-Enhanced Cryptocurrencies (AECs) and Privacy Tools:**

The GVA specifically targets tools intended to improve privacy: *"the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows."* (GVA, p6)

As well as the way of accessing crypto applications through: "*Internet Protocol (IP) anonymizers such as The Onion Router (TOR), the Invisible Internet Project (I2P) and other darknets, which may further obfuscate transactions or activities.*" (GVA, p16)

In addition, FATF is well aware of crypto projects to enhance privacy and decentralization; "*new illicit financing typologies continue to emerge*" [Author: DeFI?], "*including the increasing use*

*of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner"* [Author: Lighting, Schnorr, Taproot?]. (GVA, p6)

The goal is for VASPs to be identified and made responsible for such activities: *"Conversely, AML/CFT regulations will apply to covered VA activities and VASPs, regardless of the type of VA involved in the financial activity* [...] *the underlying technology, or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation)."* (GVA, p26)

And if a VASP *"cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities."* (GVA, p51)

**Licensing Obligations for all VASPs:**

The GVA intends to subject all VASPs to a licensing scheme: *"at a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created."* (GVA, p40)

Moreover, each jurisdiction might require licensing for those servicing clients in their jurisdiction: *"Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction."* (GVA, p41)

It bears repeating that a natural person can also be designated as being a VASP and be required to obtain a license to work on a crypto project; *"in cases where the VASP is a natural person, it should be required to be licensed or registered in the jurisdiction where its place of business is located."* (GVA, p41)

Moreover, the competent authorities get to determine who can and cannot become a VASP: *"In the licensing or registration process, competent authorities should take the necessary legal or regulatory measures to prevent criminals, non-fit and proper persons or their associates from holding, or being the beneficial*

*owner of, a significant or controlling interest, or holding a management function in, a VASP.”* (GVA, p43)

The competent authorities are obliged to monitor the Internet for unlicensed activities by engaging in *“chain analysis, webscraping for advertising and solicitations, feedback from the general public, information from reporting institutions (STRs), non public information such as applications, law enforcement and intelligence reports”* (GVA, p41); as well as engage in propaganda against such activities: *“Countries may also consider the incentive effect of publicity of enforcement actions against unregistered or unlisensed VASPs;”* or designate activities from specific countries *“which do not effectively implement licensing or registration requirements”* as *“high risk”* with *“additional reporting requirements.” (GVA, p43)* And thus discourage VASPs from engaging in them.

**Bitcoin ATMS:**

“Providers of kiosks—often called “ATMs,” bitcoin teller machines,” “bitcoin ATMs,” or “vending machines”—may also fall into the above definitions because they provide or facilitate covered VA activities via physical electronic terminals (the kiosks) that enable the owner/operator to facilitate the exchange of VAs for fiat currency or other VAs and/or the exchange of fiat currency for VAs.” (GVA, p24)

**Decentralize Exchanges:**

According to the GVA, the concept of a decentralized exchange doesn’t exist: *“For self-described P2P platforms, jurisdictions should focus on the underlying activity, not the label or business model. Where the platform facilitates the exchange, transfer, safekeeping or other financial activity involving VAs [...] then the platform is necessarily a VASP.”* (GVA, p29)

Moreover, those running the exchange can be held liable: *“Launching a service as a business that offers a qualifying function, such as transfer of assets, may qualify an entity as a*

*VASP even if that entity gives up control after launching it;"* and *"automating a process that has been designed to provide covered services does not relieve the controlling party of obligations."* (GVA, p29)

**Multisig contracts:**

In case of partial control of keys, like a multisig or any kind of shared transaction, the providers of such services could be subjected to this regulation as well. (GVA, p24)

**Regulation of Future Developments:**

According to the GVA, countries should *"identify and assess the ML/TF risks relating to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products."* (GVA, p51)

This includes projects currently considered decentralized by the community: *"The use of an automated process such as a smart contract to carry out VASP functions does not relieve the controlling party of responsibility for VASP obligations."* (GVA, p30)

**International Cooperation of Competent authorities:**

The FATF Recommendations encourage providing the fullest range of international co-operation: *"countries should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to VAs."* (GVA, p87)

*"The FATF Standards make clear that supervisors should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs."* (GVA, p92)

## <What Will Not Be Regulated?_

Some good news is that what makes crypto, crypto, remains unregulated; peer-to-peer transactions themselves, small transactions and ecommerce, open source development, and cold storage will remain lawful.

Specifically exempt are persons facilitating the technical process, such as miners and nodes (called validators), and those that facilitate and develop the network.

**Developers:**

*"A person that develops or sells either a software application or a VA platform (i.e., a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform"* [...] *"It is the provision of financial services associated with that software application or platform, and not the writing or development of the software itself, which is in scope of the VASP definition."* (GVA, p26)

**Producers of Hardware Wallets:**

*"The FATF also does not seek to regulate as VASPs natural or legal persons that provide ancillary services or products to a VA network. This includes the provision of ancillary services to hardware wallet manufacturers or to non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned covered VA activities or operations on behalf of their customers."* (GVA, p26)

**Infrastructure:**

*"...Natural or legal persons that solely engage in the operation of a VA network and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers (e.g., internet service providers that offer the network infrastructure, cloud service providers that offer the computing resources, and miners and validators that validate, create and*

*broadcast blocks of transactions) are not VASPs under the FATF Standards, even if they conduct those activities as a business.”* (GVA, p26)

**Small transactions:**

These regulations are not set-out to micromanage the space: *“the occasional transaction designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.”* (GVA, p45)

However, for payments under the threshold done through VASPs, the VASPs should still collect:

*“(1) the name of the originator and the beneficiary; and*

*(2) the VA wallet address for each or a unique transaction reference number.”* (GVA, p26)

It must be said that due to the potential difficulty of accessing the financial system with untracked crypto in the future, stores might be forced to demand a certain level of transparency from their clients by their service providers.

## <What Will Be the Outcome of These Regulations?_

This regulation, like many of its kind, will have (un)intended consequences. The stated goal of increased transparency in the space might be achieved, revealing the proceeds of certain crimes.

However, a secondary goal is clear for those understanding these kinds of open-ended legislation; controlling what can and cannot be done with crypto in the real world by labeling certain activities and undesired persons as “high risk.”

It will be increasingly difficult to deal with proceeds from the “wrong” activities, especially for people from high-risk countries, engaged in high-risk activities, or just being considered a high-risk person. Why this is a problem, can already be seen in the Netherlands, where those who are protesting the government are labeled a security risk, and subsequently cut off from financial service providers.[9]

In addition, it will become expensive and technologically challenging to comply with these legislations. Small companies with unique business models might find it impossible to survive. Only the large regulated entities might remain in existence. This is a common result of regulation that is welcomed by regulators; a few large companies are easier to regulate than one thousand small ones. In some cases, the large participants welcome regulations as well, as it reduces competition. The same happened in the banking sector, for example.

Other downsides are that such regulations smother many otherwise beneficial technological projects in the crib and criminalize perfectly legal activities and the innocent citizen performing them. The loss of privacy will also increase security risks, especially for those living in dangerous countries.

There is no denying that these regulations will see the light of day. As such, the crypto space is going to be fully regulated, controlled, monitored, and subject to freezing and asset

confiscation. Transaction speed will no longer be determined by technology, but by the approval and infrastructure of third parties.

**The Crypto World at a Crossroads:**

These regulations will have consequences for participants and investors in the crypto space. The question is: how will this effect current and future projects?

It is hard to determine how specific projects and the crypto space in general are going to be affected; especially since this is not the final guidance. Each national government will have a slightly different interpretation of these regulations, as well as existing laws and precedent in their own country. In addition, individual VASPs will interpret these regulations according to the viewpoint of their legal departments, as well. Cryptos will become a regulatory minefield.

A natural consequence of these regulations is that projects and participants in the crypto space will be divided into two categories: those who do/can meet these regulations, and those who do/cannot.

Cryptos were developed to be decentralized and peer-to-peer financial systems. At this stage, however, the future and short-term attractiveness of individual projects unfortunately depend on their relationship to these, and similar, regulations.

**Winners and Losers:**

First will be those that will fully comply with these regulations. In terms of participants, these will be the big exchanges and onramps, banks, and institutional investors. A lot of participants exclusively use VASPs already for their coins anyway, and for them nothing changes. In fact, institutional adoption might increase, an idea supported by the fact that the Bank of International Settlements issued new guidance for banks on the prudential treatment of crypto assets.[10] Assets which might succeed in such an environment are projects that have focused on

transparency and KYC from the start, or are already too decentralized and operate without any VASPs.

Next, there are the activities that are specifically targeted by this regulation; privacy coins, decentralized exchanges, decentralized finance, and other peer-to-peer systems. It appears that such projects have only one option and that is to go fully decentralized. It is not unlikely that for a select group of participants these regulations will fuel the idea of creating a parallel system of people freely interacting outside the regulated financial system. It is worth repeating that in principle, peer-to-peer systems are not against the law. Those participating in them should however accept that part of their assets and proceeds exist outside the regulated financial system, and that by engaging in them they might be labeled a “risk.”

Finally, there will be projects that fall in between: they are either too centralized to become fully decentralized and considered too “high-risk” to be licensed. Such projects will experience significant headwind. Think about the aforementioned stablecoins, certain decentralized finance applications, certain self-hosted wallets (especially when facilitating exchange functions), decentralized exchanges, future ICOs, and privacy coins.

Current projects that are still too centralized are a big question mark. Especially those who have leading individuals still in control of “road-maps,” or those relying on “governing councils.” Those persons might suddenly be designated a VASP and forced to monitor the individuals and transactions on their network (a big downside as compared to the projects already decentralized).

## <What to Do Next?_

The moment is now. Action is being taken on various levels of government to regulate cryptos. Now it is time to review your activities in the crypto space.

If you are an investor, review your portfolio to see if there are any projects that might be adversely affected by these regulations.

If you are an entrepreneur, analyze if your activities designate you as a VASP, and as such, if you risk being subjected to costly and cumbersome regulatory obligations.

Every crypto-enthusiast should decide which road he is going to take with his investments and efforts: accept and support the full integration of cryptos into the financial system or focus on more decentralized systems.

In case you aren’t sure yet what these regulations will mean for your investments or project, do not hesitate to contact the author of this report.

# <About the Author_

## Wesley Thysse MSc

Wesley started his career in finance. He worked as a project controller at Multi Real Estate, a large developer of iconic shopping malls in Europe. He later settled in Dubai where, as a corporate service provider, he assisted entrepreneurs and high net worth individuals with international tax planning and legal structuring.

In 2014, he moved to Asia and started a small consultancy firm. He has since helped hundreds of SMEs, digital nomads, crypto investors and HNW-individuals with international tax and regulatory challenges.

In 2016, together with a partner he launched a website focusing on explaining specific international tax regulations to a wide audience. Their blog on transfer pricing is now likely the world's most visited on this topic. He also co-wrote a textbook for students, a training course, and legal templates on the topic. The website and educational materials are published by the boutique tax law firm Thysse de Lange Limited, registered in Hong Kong, of which he is the Managing Partner.

In 2017, he started researching blockchain legal projects, and realized that most of them lacked real-world frameworks. He created the decentralized legal system, a first framework of its kind for Decentralized Law.

Early 2021, he published the The Crypto Sovereign, a unique book on using geo-tax-arbitrage to optimize your taxes, protect your assets, and increase your liberty by moving across borders.

Wesley holds a Master's degree in Management from the University of Greenwich, London.

### Contact me:

If you are worried about what FATF regulations mean for you or your project, wish to discuss this topic on your blog or podcast, or need the opinion of someone who is at the forefront of crypto regulations, feel free to contact me:

**Email:** info@decentralizedlegalsystem.com **Twitter:** @Decentral_Law

# <Endnotes_


1 FATF, *"FATF Report to G20 Finance Ministers and Central Bank Governors,"* (FATF, Paris, July 2018), https://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html

2 FATF, *"Draft updated Guidance for a risk-based approach to virtual assets and VASPs,"* (Paris, March 2021), http://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf

3 *"Topic: High-risk and other monitored jurisdictions,"* (FATF), accessed on 9 June 2021, https://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/

4 UN, *"United Nations Conference on Diplomatic Intercourse and Immunities,"* (Vienna, 2 March – 14 April 1961), accessed on June 10, 2021, https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

5 *"Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers,"* (FATF, Paris, March 2021), accessed on June 10, 2021, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html

6 *"Outcomes FATF Plenary, 20-25 June 2021,"* (FATF, Paris, June 25, 2021), accessed on June 26, 2021: https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2021.html

7 *"Guidance on Digital ID,"* (FATF, Paris, March 6, 2020), accessed on June 10, 2021, http://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html

8 *"Designated categories of offences,"* (FATF), accessed on June 9, 2021, http://www.fatf-gafi.org/glossary/d-i/

9 *"Machtsmisbruik van de overheid om critici de mond te snoeren,"* (Artsen voor Vrijheid, May 7, 2021), accessed on June 9, 2021, https://www.artsenvoorvrijheid.be/blog/2021/05/07/machtsmisbruik-van-de-overheid-om-critici-de-mond-te-snoeren/

10 BIS, *"Consultative Document – Prudential treatment of cryptoasset exposures,"* (Basel Committee on Banking Supervision, Basel, June 2021), https://www.bis.org/bcbs/publ/d519.pdf