# Cryptocurrency, Virtual Assets, and Open Government

By Joseph Foti

June 2024

Open Government Partnership

## Summary


- Cryptocurrencies are the most well-known type of “virtual asset.”
- Cryptocurrencies aim to facilitate anonymous but trustworthy, decentralized exchange.
- Governments are increasingly taking on oversight of these markets. For countries with adequate financial sector regulatory authority, this has not proven to be quite as complicated as expected.
- Open government can help determine whether that oversight will be democratically controlled and whether that oversight can reduce corruption without curbing civic space.


## Key definitions

**Virtual assets** (VAs) refer to any digital representation of value that can be digitally traded, transferred, or used for payment. It does not include digital representation of fiat currencies.

**Cryptocurrency** is a form of digital currency that is not sponsored by most central banks or governments, but can be traded for goods or services like traditional money. Bitcoin is the most famous.

A **virtual asset service provider** (VASP) is any natural or legal person that conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets and fiat currencies;
- Exchange between one or more forms of virtual assets;
- Transfer of virtual assets;
- Safekeeping and/or administration of virtual assets or instruments, enabling control over virtual assets; and/or
- Participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.

**Decentralized autonomous organizations (DAOs)** are both communities and protocols that allow for trustworthy exchange. They may allow for the exchange of more than just money. For example, some DAOs authorize the buying and selling of art and investments, grant-making, or exchanging media and entertainment. Once established and launched by humans, DAO may be self-operating according to its rules. The most famous example is Ethereum.

**Web3** is the term used to describe the broad set of technologies using blockchain technology to allow more secure transactions, clearer identification, and clearer contracts for exchange.

## Why VAs matter

Proponents of virtual assets assert that their technologies will benefit society. While it is still unclear whether these claims are supported by large-scale evidence, it is worth stating these claims before identifying risks.

### The argument for VAs

There are numerous cryptocurrency advocates, many with differing viewpoints. A number of the mainstream arguments for the continuing evolution of cryptocurrencies are below, according to proponents of virtual assets.

- **Allow free trade:** Many people believe that there should be fewer government controls on trade, including some goods and services that are declared contraband.
- **Avoid authoritarian tendencies in government:** Decentralized systems are, in theory at least, harder for governments to shut down. This can be good for human rights organizations in Russia or democracy activists in Iran who might need to move funds outside of state control. Even in relatively non-authoritarian contexts, people may want to move information and assets outside of excessive government surveillance. For Web3 technologies, some argue that it could also allow for encrypted communication and break down controls such as the "Great Firewall of China."
- **Counter inflation:** Some cryptocurrencies are built to run independently of or counter to inflationary cycles of reserve currencies. This would, in theory, allow individuals and even middle-tier governments to not be subject to inadequate foreign exchange balances or to hold debt in dollars or euros. Further, this would resist inflationary cycles due to government overspending.
- **Resist monopolies:** Similar to concerns of government controls on currency, a decentralized market is, in theory, resistant to "cornering the market" or other manipulations that a company or private buyer might wish to undertake to drive the cost of an asset up or down.
- **Increase trust:** As people's trust declines globally, replacing human beings with algorithms should increase the amount of trust people have in transactions and markets to be free of manipulation. (Don't ask me to explain this one.)

Of course, there are also less savory arguments for cryptocurrencies that rarely make it into public documentation. They may help break the law, avoid scrutiny of ethics, or hide reputationally damaging activities. For a small group of people, these are benefits. For the rest of us, these are costs.

## VA risks and threats

As cryptocurrencies become more popular, on the other hand, they pose a number of threats.

- **Money laundering:** First and foremost, cryptocurrencies can facilitate the movement of ill-gotten gains.
- **Corruption:** Cryptocurrencies can make bribe paying and influence peddling easier and harder to trace. For example, many open government advocates will want to make sure that virtual assets are part of both asset declarations as well as campaign finance transparency.
- **Tax avoidance:** It has been argued that cryptocurrencies can allow people and companies to avoid tax payments. This has knock-on effects of eroding the tax base and exacerbating inequality.
- **Payment for illegal activities:** Cryptocurrencies may not only be good for buying drugs; they are also good for trafficking in humans or endangered species, cultural goods, and antiquities markets. In particular, FATF notes the large-scale use of cryptocurrencies to finance terrorism.
- **Uninsured Ponzi scheme:** Numerous crypto-assets do not have the confidence of users and are in fact subject to exploitation and, in the case of failure, do not have the backing or insurance that fiat currency and the traditional banking sector do.
- **Lack of law enforcement and dispute resolution:** The UN Security Council has identified the theft of virtual assets by North Korea as a major source of revenue for the illegal nuclear program. However, under current structures, none of this stolen property is recoverable.
- **"Alegal" nature:** Some may consider this a benefit, but many of the decentralized codes do not care if they are following the law or not. Once a code is running, in theory, it cannot be stopped for certain transactions or people, even if those people are using the protocol to commit crimes.
- **Environmental impact:** Cryptocurrencies solve complicated math problems to record transactions, which drains natural resources—for example, Bitcoin uses more electricity than a mid-sized country. Newer cryptocurrencies seem to be more efficient than Bitcoin, however.

# Relevant laws and guidance

## FATF

FATF is the principal global standard on anti-money laundering efforts and anti-terrorism finance. VA and VASPs are covered by guidance under Rule 15, adopted in 2021. The FATF guidance suggests a risk-based approach, rather than an outright ban.

The FATF monitors its member states' implementation of regulations on VAs and VASPs. Its most recent report (June 23) shows that a mere quarter of its membership is fully compliant to address the issue of money laundering via VAs. In another quarter of its membership, the sector is completely unregulated.

## United States

The US is currently the largest host of VASPs operating as businesses and is the largest financial secrecy jurisdiction in the world, according to the Tax Justice Network.

Notably, existing US law already applies to cryptocurrencies and other VAs.

- The **National Defense Authorization Act for Fiscal Year 2021**, passed with a veto-overriding majority, contained the Anti-Money Laundering Act of 2020 (AMLA). The AMLA expands the Bank Secrecy Act of 1972 to include "services related to value that substitutes for currency." It also redefines "monetary instruments" under law to cover "value that substitutes for any monetary instrument." This redefinition allows federal regulators to use existing statutes to prosecute money laundering as well as predicate crimes that involve money laundering (such as terrorism finance, corruption, nature crimes, smuggling, or human trafficking). Notably, this is the same legislation that established beneficial ownership reporting through the Corporate Transparency Act.
- The **Money Laundering Control Act** and the **Bank Secrecy Act** respectively define money laundering (both domestic and international) and establish customer due diligence requirements on financial institutions to report, record-keep, and have compliance programs. FINCEN has already issued guidance on crypto-assets.
- The **Financial Crimes Enforcement Network** (FinCEN) has issued guidance defining VAs —specifically convertible virtual currencies—and defining which entities are regulated. Currently (as of late 2023), FinCEN is carrying out a participatory process on the regulation of "mixers," which anonymize transactions.
    - Of particular importance to open government advocates, such regulation covers not only terrorism finance, but also other predicate crimes such as overseas bribery, which fall under the **US Foreign Corrupt Practices Act** (FCPA). This requires accounting for crypto-transactions, transparency, and reporting on compliance only for companies publicly listed on securities exchanges, however.

Two pending pieces of legislation have been introduced in this Congress, which stand some chance of passage:

- **Crypto-Asset National Security Enhancement and Enforcement Act** (2023) would require decentralized financial services companies to meet AML requirements and sanctions compliance, just like other financial institutions, and would require conversion services to verify the identity of parties.
- The **Digital Asset Money Laundering Act** (2023) would make VA regulation subject to the same controls as fiat currency, prioritizing the role that VAs play in the fentanyl trade.

In the context of the US, subjecting decentralized finance businesses to the same oversight as traditional institutions means that the public (including shareholders, other levels of government, and law enforcement) would be able to see major transactions and monitor the enforcement of relevant laws.

## Europe

The EU has issued rules on VAs since 2014, but a 2019 report by the European Banking Authority found that only a minor proportion of the European market would be regulated by such rules. There are two major concerns: one on the exposure to risk for consumers and investors and another on money laundering.

In 2020, the European Parliament called on the European Commission to issue a plan to regulate VAs. A subsequent report laid out a plan to harmonize Customer Due Diligence reporting across the financial sector. This would include establishing a person's real identity and harmonizing reporting to regulatory agencies in each member state.

This resulted in the 2023 passage of Markets in Crypto-Assets Regulation (MiCA). MiCA establishes a list of regulated services and activities relating to any crypto-asset, including:

- providing custody and administration of crypto-assets on behalf of clients;
- operating a trading platform for crypto-assets;
- exchanging crypto-assets for funds or other crypto-assets;
- executing orders for crypto-assets on behalf of clients; or
- providing advice on crypto-assets.

Also in 2023, the Transfer of Funds Regulation established key criteria for transparency and traceability of crypto-assets. Regulated entities are to provide:

- the name of the originator;
- the originator's distributed ledger address or crypto-asset account number;
- the originator's address, including the name of the country;
- an official personal document number and customer identification number, or alternatively, the originator's date and place of birth (subject to the existence of the necessary field in the relevant message format and where provided by the originator to its crypto-asset service provider);
- the current LEI or, in its absence, any other available equivalent official identifier of the originator.

Finally, the European Parliament has adopted a raft of relevant measures, which include the following.

- The establishment of the EU's "single rulebook" regulation, with provisions on conducting due diligence of customers and establishing the transparency of beneficial owners and the use of anonymous instruments, such as crypto-assets and new entities like crowdfunding platforms.
- The 6th Anti-Money Laundering Directive, containing national provisions on supervision and Financial Intelligence Units, as well as on access for competent authorities to necessary and reliable information, e.g. beneficial ownership registers and assets stored in free zones. The text was adopted with 107 votes to 5 and 0 abstentions.
- The regulation that establishes the supervisory and investigative powers of the European Anti-Money Laundering Authority (AMLA) to ensure compliance with AML/CFT requirements. The text was adopted with 102 votes to 11 and 2 abstentions.

## Emerging case law and oversight actions

Where governments have the legal authority, they have been able to regulate cryptocurrency under existing national and global security laws, corporate governance rules, and anti-corruption laws. Currently, the majority of major actions on cryptocurrencies have been the result of US and European government action, although other major banking and fintech centers may play a growing role. Of course, the reach of enforcement actions in these financial centers is dependent upon clear jurisdictions and institutional capacity. In the case of domestic laws that are not enforced or crimes that do not cross boundaries, there remains much work to be done.

### NATIONAL SECURITY, ROGUE STATES, AND SANCTIONS

- **Paypal (2015–2022):** PayPal reached a US $7.7 million settlement for sanctions violations with the Office of Foreign Assets Control (OFAC) on Iran Sanctions. This settlement led to a shift in PayPal's actions—in 2022, when Russia invaded Ukraine, PayPal did not wait to cut off Russian PayPal accounts.
- **ShapeShift and Wanna-Cry ransomware (2021):** Shapeshift was an exchange used by Etherium that intentionally hid the identity of users. The Wall Street Journal found that North Korea's Wanna-Cry ransomware developers were using it to launder their money. In a related measure, in 2022, the US sentenced one of Ethereum's early advisors to five years in prison for assisting North Korea with using cryptocurrencies to avoid sanctions.
- **OFAC vs Tornado Cash (2022):** Tornado Cash, a "mixer," had been used to launder US $7 billion of cryptocurrency, including US $455 million stolen by the Lazarus Group, a criminal hacker organization associated with the North Korean government. OFAC "designated" TornadoCash as a sanctionable individual even though it was an automated DAO. OFAC stated that Tornado Cash could resume operations once it stopped illegal activities. Instead, Tornado Cash cut off its ties to all other cryptocurrencies that cooperated with OFAC on Russian sanctions. This has lessened Tornado Cash's access to capital from more cooperative partners, but it remains unresolved. In new charges filed in August 2023, the US DOJ has charged the at-large founders of Tornado Cash for US $1 billion equivalent and sanctions violations. As of May 2024, one cofounder of Tornado Cash received a 64-month sentence from a Dutch court, having been found criminally liable for money laundering.
- **Blender.io vs OFAC (2022):** OFAC has added mixer Blender.io to its sanctions list, as it has enabled North Korean actors to launder stolen cryptocurrency from its hacker organization, Lazarus Group.
- **Meta and Libra (2019–2021):** Faced with scrutiny by the European Central Bank, the French Government, and the US Department of Treasury, Meta shuttered its plans for a global private currency (Libra) after it was repeatedly unable to show that it had proper controls for national security.

## Emerging case law and oversight actions

### OTHER CRIMES

- **EU and TrustCom Financial (2024):** The European Union, led by authorities in Italy, Latvia, and Lithuania, froze more than €11 million in assets and arrested 18 people suspected of helping launder €2 billion. EuroJust, which coordinates enforcement actions across national borders, stated that the exchange was established by an Italian crime syndicate, which helped launder money into real estate and cars.
- **Bitzlato vs US FinCEN and French Department of Treasury (2022):** The Russian founder of Bitzlato (registered in Hong Kong) is charged with facilitating hundreds of millions of transactions for known criminals through Hydra (a part of the "Dark Web").
- **Sim Hyon Sop vs US DoJ:** Sim Hyon Sop is a representative of the North Korean Foreign Trade Bank. The US has charged him with running tobacco smuggling (owned by the North Korean military) and bringing that money back in through illegal crypto operations to pay for North Korean nuclear weapons development.

### CORPORATE GOVERNANCE

- **American CryptoFed DAO (2022):** The US Securities and Exchange Commission has brought proceedings against American CryptoFed on the grounds that it needed to register, as its tokens were securities. In order to legitimately register, it needed to present full financial reporting, which it had not done at the time.

### BRIBERY

- **Sam Bankman-Fried and FTX (2022):** In addition to being convicted of seven counts of fraud, Sam Bankman-Fried has also been indicted for bribery of a foreign officer, for bribing a Chinese official with US $40 million in cryptocurrencies.
- **M.Y. Safra Bank vs. US Department of Treasury:** Safra did not implement AML controls in its digital assets or compliance programs (under *Banking Secrecy Act* and *Sarbanes-Oxley*). The Treasury issued a compliance order, establishing that regulated banks need to establish compliance programs.

## Beyond law enforcement: Open government approaches

The changing landscape for money means that:

- There are increasing opportunities and means for corruption, money laundering, and payments for other illegal activities. However, governments with major financial markets have already shown a willingness and ability to clamp down on illegal activities *under existing laws*. More laws and controls will likely come into place soon as well.
- However, the risk of abuse in controlling crypto-markets is real, following how anti-terrorism and financial crime laws have been used to silence and harass oppositional voices. To that end, a system of democratic controls is essential to oversee such regulatory measures.

Crypto-markets need to be regulated. But it matters how those markets are regulated. It can be done in an arbitrary, ad hoc manner, or it can be done in a way that balances competing rights and favors democracy and fairness.

### Transparency

- **No secret laws:** Create clear and public rules, laws, and case law (where applicable) on when and where controls on virtual assets can be put in place. FATF Recommendation 15 provides guidance for OGP members on putting in place a legal and administrative framework. (For more guidance, see the FATF interpretative note, which develops the application of Recommendations 1 (Mitigating AML/CTF Risks), 10 (Customer Due Diligence), 16 (Travel Rule), 35 (Sanctions) and 36–40 (International Cooperation) for virtual assets.)
- **Corporate reporting standards:** Transparency reports from major companies (similar to social media platforms and other big tech) can help the public understand where enforcement and information requests come from, as well as what compliance actions companies are taking to prevent illegal activity. Governments can facilitate the development of these standards according to FATF Recommendation 20 (Suspicious Transactions Reports (STRs).
- **Agency transparency:** Publish transparency and performance reports from prosecutorial bodies.
- **Impact analysis:** Publish safeguards to ensure that rules are applied in a non-discriminatory, legal, proportional, and risk-based manner, where such rules might disproportionately affect particular groups (for example, religious organizations or credal groups).

### Participation

- **Consultative bodies:** Where possible, develop multi-stakeholder processes, including with civil society, to prioritize threats, responses, and safeguards.
- **Notice and comment:** Maintain or enhance regular administrative law in the development of regulations or crypto-market regulation.
- **Oversight:** Public oversight committees can ensure that agencies and courts continue to follow established and legal due process in carrying out crypto-market regulation.

## Public Accountability

- **Judicial forums:** Establish clear lines of judicial oversight through regular processes to ensure that agencies follow the due process of law in instituting sanctions and asset freezes, among other actions.
- **Public parliamentary oversight:** Establish standing mandates to compel testimony, carry out oversight of the executive, and prepare legislation to ensure that laws are being enforced in a legal, proportionate, and non-discriminatory fashion.
- **Remedies for rights violations:** Ensure that there is clear guidance for agencies to redress and remedy violations of rights to speech, assembly, and association. The public should also have access to channels to report violations and request redress from agencies.
- **Public interest standing and citizen suits:** In cases where there may be illegality (or extra-legality) on the part of government action, parliaments may establish a public right of action. In cases where the law enforcement fails to take action against egregious illegal activities, parliaments may choose to support a public right of enforcement.