CRYPTOCURRENCIES — LATEST DEVELOPMENTS ON EITHER SIDE OF THE ATLANTIC AND BEYOND

Author
Beate Erwin

Tags
Compliance
Cryptocurrency
F.A.T.F.

BACKGROUND

> What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud. . . . The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.[1]

This is how the developer(s), person(s) known under the pseudonym of Satoshi Nakamoto, described the aspirations that were embedded into the creation of cryptocurrency. The issues raised by virtual currency and, in the majority of cases, the underlying blockchain technology are manifold, including tax law, transfer pricing, regulatory rules, civil law accounting rules, and valuation. Notwithstanding their diversity, all legal, regulatory, and administrative areas affected by crypto-related technology share one common goal: protection of users and investors through the prevention of fraud and abuse. No matter which area is addressed, protection mostly involves application of rules designed for assets and related business models pre-dating the new technology. Because loopholes exist, cryptocurrency has become a refuge for tech-savvy criminals that have evaded regulators by choosing particular jurisdictions having little, no, or lenient regulatory oversight. This article provides an overview of recent initiatives globally and in the U.S. that are designed to counteract the dark side of crypto-related technology.

NEW ANTI-MONEY LAUNDERING RULES

In the common view of regulators, a balance must be drawn between personal and financial privacy and prevention of money laundering. The Financial Action Task Force ("F.A.T.F.") has taken the lead in this area. Established in 1989, F.A.T.F. is an intergovernmental organization consisting currently of 37 member countries[2] and two regional organizations.[3] It was created to set international anti-money laundering standards. Since July 1, 2019, F.A.T.F. is headed by a representative from China, who succeeded a representative from the U.S.[4] Some commentators call F.A.T.F. the "United Nations for fighting financial crimes." Since its inception, F.A.T.F. has

1 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Nakamoto Institute, October 31, 2008.

2 For a full list see F.A.T.F. Members and Observers.

3 The European Commission and the Gulf Co-operation Council.

4 The F.A.T.F. President is a senior official appointed by the F.A.T.F. Plenary from among its members for a term of one year.

developed a series of recommendations. Before June 2019, the most recent set of recommendations was published in 2012.[5] While regulatory recommendations of F.A.T.F. are not legally binding, member states are obligated to implement F.A.T.F. regulatory recommendations into enforceable local law. Including fully accredited members, over 200 jurisdictions are committed to carry out F.A.T.F. recommendations through a global network of F.A.T.F.-style regional bodies according to F.A.T.F.[6]

F.A.T.F. put forth highly anticipated new guidance in June of this year (the "Guidance"). It clarified 40 recommendations for national regulators overseeing virtual asset ("V.A.") and virtual asset service provider ("V.A.S.P.") activities.[7] Notably, it introduced a so-called travel rule calling for countries to require V.A.S.P.'s to comply with the same anti-money laundering and anti-terrorism standards generally applied to traditional financial institutions.

CRYPTOCURRENCY AND PRIVACY – THE ISSUE

Compared with traditional markets trading in stock and bonds, the cryptocurrency market is small and immature. However, the criminals trying to profit from it are among the most sophisticated in the world – reaping rewards at an estimated $4.26 billion from cryptocurrency exchanges, investors, and users just in the first six months of 2019.[8] Of great appeal to criminals is the capacity for anonymous, peer-to-peer value transfer of cryptocurrency. Technically, most cryptocurrency systems are pseudonymous, *i.e.*, users are identified publicly but only by a string of random numbers and letters. Since every transaction is recorded on a public ledger, criminals resort to a range of tactics, including using multiple addresses and exchanges, to cover their tracks.

In regulated jurisdictions like the U.S., Japan, and the E.U., exchanges that constitute bridges between the traditional financial system and the world of cryptocurrency include requirements to verify the identities users as part of a process commonly referred to as know your customer ("K.Y.C."). In other jurisdictions, exchanges may have less stringent policies in place that make it possible to move money or cash out without identification of their users. These may be referred to as T.B.E. jurisdictions, allowing exchanges to "turn a blind eye" on their customers.

RECOMMENDATION 16 – THE TRAVEL RULE

In applying Recommendation 16 under the Guidance, whenever a user of one exchange sends cryptocurrency worth more than $1,000 or €1,000 to a user of a

---

5 The 2012 version of recommendations introduced Recommendation 15, "New Technologies." Inter alia, this recommendation provides that "countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products." At that time, Recommendation 15 did not refer to virtual currencies per se.

6 See F.A.T.F. table of regional bodies and members.

7 F.A.T.F., *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, (F.A.T.F.: Paris, 2019).

8 "Ciphertrace Q2 2019 Cryptocurrency Anti-Money Laundering Report: Thefts, Scams and Fraud May Exceed $4.26 Billion for the Year," Ciphertrace, 2019.

different exchange, the originating exchange must "immediately and securely" share identifying information about both the sender and the intended recipient with the beneficiary exchange (commonly referred to as the travel rule). That information should also be made available to "appropriate authorities upon request."

According to the F.A.T.F. Interpretive Note to Recommendation 16, originator and beneficiary information should include the following identifying information:

- Name and account number of the originator
- Originator's (physical) address, national identity number, customer identification number, or date and place of birth
- Name and account number of the beneficiary[9]

Cross-border transfers below the foregoing threshold also should include the names and account numbers of the originator and beneficiary. However, the identifying information need not be verified for accuracy in the absence of suspicion of money laundering or terrorist financing.

The rules that call upon exchanges of personal information are somewhat controversial. While some fear that restrictions affecting data privacy will tarnish the attraction of exchange traded cryptocurrencies for some customers, others see it as a chance to attract financial institutions as new investors.

Verified information exchange serves several purposes in addition to the deterrence of money laundering schemes. It removes an avenue for liquidity that might otherwise be enjoyed by individuals and organizations on global sanction lists. While this may function as a trust building measure for regulators, it adversely affects high-profit operations where yields on dark markets can be much higher for operators. However, the elimination of dark markets could, in the view of some commentators, result in an increase in prices for cryptocurrencies.

BINDING OR NOT BINDING?

As mentioned above, the Guidance does not rise to the level of law unless rules in line with the recommendations are implemented into domestic law by a country. Nonetheless, the effect of the Guidance is real. As witnessed recently at its June summit held in Osaka, Japan, the G-7 and influential members of the G-20 strongly expressed their commitment to the implementation of F.A.T.F. policy. In turn, this move pressures other countries to follow suit. Some pressure may be subtle. Other pressure is less subtle, as evidenced by a statement of U.S. Treasury Secretary Steve Mnuchin in which he called F.A.T.F.'s standards binding to all countries.[10]

Further developments point in the direction of enhanced safety standards in the crypto-related technology environment. In July, F.A.T.F. reportedly supported Japan's efforts to create an international cryptocurrency payments network. This new system would be similar to the global banking network known as S.W.I.F.T., which

---

[9] F.A.T.F., International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, (F.A.T.F.: Paris, June 2019), p 79 *et seq*.

[10] Steven T. Mnuchin, "Remarks of Secretary Steven T. Mnuchin FATF Plenary Session," June 21, 3019, Orlando, Florida.

employs an international messaging protocol used to prevent money laundering for bank-to-bank payments. A separate report released by Nikkei Asian Review in August indicates that 15 governments are planning to create a system for collecting and sharing personal data on cryptocurrency users.[11]

However, some commentators see the developments in a less shining light. They doubt that a government-led global cryptocurrency surveillance system currently is in the works and further doubt the effectiveness of any system that may emerge.

NOT NEW FROM A U.S. PERSPECTIVE

In some respects, the Guidance published by the F.A.T.F. is not unprecedented. Conceptually, it is the ”crypto version” of a U.S. banking regulation also called the travel rule. It imposes a similar requirement on traditional financial institutions – albeit at the higher threshold of $3,000. Crypto exchanges in the U.S. are already been subject to this rule, according to recent pronouncements from the Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”). Plans to enforce the rule are expected to be implemented later this year. In May, FinCEN issued guidance on the application of its existing regulations to business models involving convertible virtual currencies (“C.V.C.’s”).[12] For financial institutions subject to the Bank Secrecy Act (“B.S.A.”), FinCEN guidance indicated that regulations relating to money services businesses apply to business models that involve money transmission in C.V.C.’s.

“Institutions that handle C.V.C.’s are on notice that the travel rule will be enforced.”

The FinCEN guidance does not establish any new regulatory expectations or requirements. All rules have been in effect since 2013 and are unchanged. However, it provides important regulatory clarity that seeks to remove ambiguity ahead of enforcement actions. In particular, FinCEN reiterates that the travel rule applies to cryptocurrencies. Institutions that handle C.V.C.’s are on notice that the travel rule will be enforced.

The risk for these financial institutions is material as the list of cryptocurrency addresses on FinCEN’s list of Specially Designated Nationals has grown significantly in recent months. Many of these addresses are marked as being possibly associated with the global drug trade.[13] According to the Kingpin Act,[14] U.S. companies and individuals are banned from any type of commercial relationship with addresses on the list as well as people connected to listed addresses.

In addition, the I.R.S. has begun to send letters to taxpayers with virtual currency transactions that may have failed to report income and gain from cryptocurrency transactions or did not report their transactions properly. In this context, I.R.S. Commissioner Chuck Rettig confirmed that the I.R.S. is determined to monitor compliance through tax examinations of identified traders on cryptocurrency exchanges. According to Mr. Rettig, the I.R.S. is expanding its examination efforts through

---

11 “New Global Cryptocurrency System Set to Fight Money Laundering,” *Nikkei Asian Review*, August 9, 2019.

12 FinCEN, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies, (FinCEN, 2019).

13 See the Office of Foreign Assets Control’s sanctions list.

14 Foreign Narcotics Kingpin Designation Act, P.L. 106-20, enacted December 3, 1999.

increased use of data analytics to enforce U.S. tax law on trading profits and gains.[15] While this is in line with a Virtual Currency Compliance campaign announced by the I.R.S. on July 2, 2018, taxpayers and practitioners are still awaiting further guidance on interpretation of tax rules beyond the only explicit statement in this respect so far, I.R.S. Notice 2014-21. The latter states that virtual currency is property for Federal tax purposes.

CONCLUSION

According to a public statement released in conjunction with the Guidance, F.A.T.F. will conduct a 12-month review of implementation efforts of its member countries. It is expected that member countries will revise national laws and regulations to align with the Guidance. It remains to be seen whether this ambitious initiative will be implemented by countries, and if so, the speed of the implementation. Exchanges are still early in the process of identifying systems and technologies to securely handle sensitive data in a way that complies with a range of local privacy rules. F.A.T.F. seems to be juggling many balls at the same time when it comes to those involved in cryptocurrency trading.

In the U.S., taxpayers should be aware that once the I.R.S. begins a "campaign" directed to certain income or activity, its agents use the campaigns as a roadmap to conduct examinations. A campaign on virtual currencies was announced in 2018. It is anticipated that I.R.S. examiners will focus on virtual currency transactions when examining tax returns identified as potential campaign targets. The stakes for the I.R.S. are expected to be high, matching profits reportedly by those having taken long or short positions relating to cryptocurrency.

---

[15] I.R.S., "IRS Has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency's Larger Efforts," news release, July 26, 2019.