# Self-hosted wallets: the elephant in the crypto room?

BY NADIA POCHER - 11 MARCH 2021

*While all-time highs of the crypto market continue to grab headlines in the first weeks of 2021, delicate questions remain unanswered as to the application of laws and regulations to cryptoassets. Besides sketching the rationale behind self-hosted cryptocurrency wallets, this blogpost explores the clash between the risks they pose in terms of money laundering and the impacts of possible bans or limitations.*

Over the first weeks of 2021, dramatic surges and sizeable investments have once again thrust the controversies of the crypto world into the limelight. Understandably, when stakes are on the rise everyone tries to secure their share of winnings. But are we sure we know the rules of the game? Indeed, while the media is echoing long-lasting debates on the volatility of cryptocurrencies, uncertainties as to some crucial aspects of their regulation linger on.

**Anti-money laundering compliance**

Ever since the advent of Bitcoin, the regulatory approach to cryptocurrencies has primarily focused on mitigating risks to financial integrity. This has largely meant addressing their misuse for illicit purposes. Following in the footsteps of the Financial Action Task Force (FATF), law and policymakers have started extending the scope of anti-money laundering (AML) and counter-terrorist financing (CFT) rules to the crypto sphere.

AML compliance is traditionally imposed on selected entities, such as banks, so that suspicious money laundering cases are detected and reported. Duties placed on these gatekeepers encompass, among others, a scrutiny of the clientele known as Know-Your-Customer (KYC) and monitoring financial flows.

The efficacy of this approach within DLT/blockchain-based ecosystems is up for debate, but the EU Fifth AML Directive included 'fiat-to-crypto exchanges' and 'custodian service providers' in its scope. Parallelly, FATF's 'crypto' travel rule lays down obligations of information collection and exchange concerning beneficiaries and originators of crypto transactions.

But what if the funds are kept out of the reach of regulated (and regulatable) intermediaries?

**Cryptocurrency wallets**

Cryptocurrencies are not held in one's (physical) pocket. On the contrary, their value never leaves the network. A user accesses and spends funds associated with a given address through the corresponding private key, a sort of authentication code. Private keys are stored in crypto wallets, more similar to keychains than to traditional wallets.

According to their preferences and expertise, users can choose among different types of crypto wallets. To name a few, *hardware* wallets are similar to USB drives, while desktop, mobile and web wallets are all *software* applications running on computers, smartphones or provided as a web service.

Because private keys grant access to funds, the choice among wallets comes with strings attached in terms of privacy and security. Often wallets are *custodial*, which means storage and custody are offered as a service by a third party. This is the case of custodial exchanges, such as Coinbase.

Alternatively, more skilled users want to retain sole custody of their private keys and use *non-custodial* wallets, also known as *self-hosted* or *unhosted* wallets. To do this, they can use hardware wallets or a selection of their software counterparts.

**Issues of self-hosting**

Self-hosted wallets have a significant impact on the efficacy of AML rules, as they allow peer-to-peer (P2P) transactions. In principle, intermediaries can be thoroughly bypassed, with the exception of transfers originating from self-hosted wallets but received by custodial wallets, or vice versa.

If regulated entities are involved, they may be required to collect information from the customer. On the contrary, in *self-hosted wallet to self-hosted wallet* transactions no third party can be held accountable for AML oversight. The FATF addressed the issue in its June 2019 Guidance and the relevant June 2020 12-Month Review.

Because illicit activities could possibly thrive in this blind corner of regulation, authorities are proposing restrictions on the use of non-custodial wallets. This could happen either in the form of bans or by imposing transactional/volume restrictions or thresholds above which specific rules apply.

The U.S. Financial Crimes Enforcement Network (FinCEN)'s Notice of Proposed Rulemaking, released in December 2020, would introduce duties to report transactions and collect counterparty data, such as beneficial owners, when regulated entities have certain interactions with self-hosted wallets. The initiative has fueled a lively controversy, but more onerous provisions are in force in Switzerland and the Netherlands.

**A controversial debate**

Disintermediation and individual freedom were at the core of the onset of DLT/blockchain-based monetary applications. From this viewpoint, imposing limitations on self-hosted wallets would hamper their adoption as non-monetary value holders and the use of cryptocurrencies as digital cash.

Advocacy groups have challenged restrictions as they could give way to total surveillance, which is at odds with fundamental civil liberties such as privacy and autonomy, and with financial inclusivity. Besides, experts have outlined drawbacks of restrictions and service providers have stressed how the application

of existing requirements, especially the travel rule, is already over-burdening the industry.

If a daring parallel is allowed, however, projects of central bank digital currencies (CBDCs) are currently exploring the trade-offs between transparency and privacy in digital cash. Namely, there is general agreement that full anonymity is out of the question.

Additionally, objections to restricting digital-cash payments seem to assume regulatory frameworks for (physical) cash inherently permit unlimited anonymous transactions. And yet, most European countries provide for strict thresholds in this regard.

**Open questions**

That of self-hosted wallets is neither the first nor the last regulatory dilemma troubling the crypto sphere. AML-wise, there seems to be little room for bargaining. In September 2020 the FATF underlined how P2P transactions and self-hosting pose risks of misuse for illicit purposes.

Against this backdrop, the growing popularity of complex crypto-related laundering schemes worsens these dangers. A combination of obfuscation methods may include *privacy coins* such as Monero and advanced services that reduce transaction transparency.

Nonetheless, P2P *self-hosted wallet to self-hosted wallet* transactions are the full realization of the crypto dream. Are we sure we want to shatter it? And what if we don't? Insights are provided by analytics companies such as CipherTrace, Chainalysis and Elliptic. In any case, under the current regime it would be impossible to enforce restrictions outside the scope of regulated (and regulatable) entities. Instead, they could run the risk of driving a part of the dissenting crypto ecosystem towards the underworld.

**ABOUT THE AUTHOR — NADIA POCHER**

**Nadia Pocher is a doctoral researcher in the Law, Science and Technology Joint Doctorate - Rights of Internet of Everything (LAST-JD-RIoE), funded by the EU Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie International Training Network European Joint Doctorate Grant Agreement No 814177. Her research takes place at the Institute of Law and Technology of the Autonomous University of Barcelona (UAB), in collaboration with the University of Bologna (UNIBO) and the KU Leuven Centre for IT & IP Law (CiTiP).**