SUERF
The European Money and Finance Forum

SUERF Policy Brief
No 330, May 2022

How to regulate crypto currencies

By Eduard de Jong*

Keywords: Crypto currencies, financial regulation, know your customer (KYC), blockchain technology, per-transaction withholding.

The rapid growth in crypto currencies has gotten ahead of financial regulations. Regulators have limited choices: a complete ban, or historic methods of regulation that are a poor fit with crypto currencies. This paper proposes a novel approach that leverages the technology used for blockchain-based currencies to enable oversight while continuing to enable legitimate transactions with minimal impact.

*I'd like to express my gratitude to Peter Cattaneo for his critical reviews of earlier drafts and his support in editing the final version.

Many countries around the world are actively looking for ways to manage the rapid rise in crypto transactions. A large number of these transactions are funding criminal activities such as the recent wave of ransomware attacks. The U.S. Secretary of the Treasury, Janet Yellen, spoke on 7 April 2022, promoting the recent Executive Order from President Biden calling for "a coordinated and comprehensive government approach to digital asset policy."[1] A mechanism for regulators to distinguish legitimate transactions from criminal activity that works at the speed of blockchain transactions is urgently needed.

What is required to regulate crypto currencies? A key part of financial regulation is to *know your customer* "KYC". All blockchain transactions are public, with a digital identity tied to each transaction. But these identities are not always linked to real identities in the relevant jurisdiction. A mechanism is required for the appropriate authorities in each jurisdiction to get access to the KYC information when required. With the transaction information and the real identity, the existing legal framework can be used to manage fraud and criminal activity.

Crypto currencies create a virtual world in which its virtual currency value lives; regulation is part of the real world. The challenge in regulating is to identify where these two worlds meet. The first interaction point is in the so called exchanges, where users can exchange between state issued money and crypto currency. Regulation can be applied to the commercial entities that operate exchanges. Such regulation could, for instance, include reporting on anomalous transactions similar to the anti-money-laundering (AML) requirements for banks.

The primary point of engagement between the virtual and real worlds is in each of the computing nodes that generates transactions and puts them on a blockchain. These computing nodes are real and operate off of a common code base, which differs for each blockchain. Operators of the blockchain nodes are called 'miners', and miners are responsible for the code that they execute. Miners are where the mechanism for regulation must be implemented.

The code base for each blockchain is open source. Authorities can specify the change in this open source code required to add a KYC mechanism as a bridge between the virtual world and their jurisdiction. Miners using code that contains this extension can create blockchains that are legal for that jurisdiction. Miners that don't will have the same legal status as criminals who engage in high-value transactions without proper reporting. Compliance with this implementation can be seen in the distributed ledger, which is publicly visible.

Miners operate in different locations simultaneously, together computing the next record to put on the blockchain. Blockchain code includes a mechanism to move miners to code updates so that new blocks must be created by with the updated version. In the spirit of the open source software development a regulator could work with existing developers or by commissioning a commercial software developer to register as contributor and have it implement the actual code for the specified change. Any registered developer in open source project can implement a code change and then propose the change for adoption. A proposed change is first balloted by the collective developers to be incorporated in the code base and subsequently presented for adoption in running code by the miners.

Since early in the twentieth century withholding tax has been a tool in managing financial affairs in many countries. Withholding a tax can also be the basis of regulating cryptos. In this case the withholding can be applied to each crypto transaction processed. For instance, with a 35% withholding, 65% of the transaction is transferred to the target account as usual and recorded in the next block added to the chain, in the same block the balance is recorded as a transfer into the crypto account for the regulatory authority in a specific jurisdiction.

[1] https://home.treasury.gov/news/press-releases/jy0706

Withholding part of each transaction meets a key requirement for the per-miner code to implement regulatory oversight while allowing the mining process to continue to operate essentially as before. Legal niceties underpinning the withholding can be managed according to the best practices in each jurisdiction.

To realize the required code change in multiple cryptocurrencies, it would make sense for authorities from multiple jurisdictions to cooperate. This collaboration could be based on an agreed upon common design for the KYC mechanism. Collaboration on specifying the technical requirements and sharing the realization burden could be a natural extension of the long-standing international cooperation in financial management and criminal justice. Collaboration is not a requirement for this proposal to be effective. Since crypto code is dynamic, collaboration can be implemented on any schedule.

The miner code to implement per-transaction withholding is simple: each transaction is enacted as two distinct simultaneous transactions. The only visible change is a requirement for the receiving user to specify a jurisdiction for each transaction. This is, of course, already mandatory for legal transactions so it is not really a change, just cryptos catching up with basic requirements.

Each jurisdiction can then implement appropriate processes for a receiving party to register its identity using the standard KYC procedures to file a claim against withheld funds. Once a claim is filed, it can be arranged to save a link to the provided identity information for use in subsequent transactions, further reducing the friction in the system. Along these lines, friction can be further reduced, almost eliminated, by staying within the crypto currency mindset and create an autonomous, automated refund mechanism.

Every country in the world already has processes and procedures in place based on their legal system to maintain privacy and security in these systems, while providing information access to the appropriate criminal justice and tax authorities. The only groups that will be negatively affected by this will be criminal enterprises.

The proposed small change to the miner code provides regulators a simple, secure, and efficient mechanism for compliance by inspecting the ledger and verifying the provenance of each new block. Crypto-currency enthusiasts can keep enjoying the benefits of blockchain technology while complying with standard financial oversight. Individuals and organizations that fail to comply will pay a severe financial penalty. And the failure to register will flag these transactions as suspect, which is a standard requirement in anti money-laundering regulations.

The novel points presented here are:

1. Implement regulatory oversight through a code update to the blockchain.
2. Use withholding to allow transactions at speed, while providing a mechanism for compliance.

This approach provides a simple path to bring blockchain currencies into compliance. By aligning with blockchain technology it works with the community governance to keep up with transactions. Proven mechanisms like KYC and withholding fit within existing legal frameworks and compliance enforcement organizations.

While this proposal has been created for the purpose of enabling financial compliance, it should be noted that it would also be suitable for managing a Carbon Tax. ■

About the author

Eduard de Jong *has been involved in digital money, cryptography and IT security for more than 30 years. He has been directly involved in the analysis, design, development, and deployment of crypto-based digital currencies since before the current generation of blockchain-based projects. Eduard has been granted over 40 patents including one that lead to the development Java Card technology. In 2017 he received the annual smart card award from the Fraunhofer institute for Secure Information Technology (SIT) in Darmstadt (DE). His current projects include a design for the transactional management of distributed renewable energy resources (DERs) and a design for an electronic cash based comprehensive secure value transfer system that could be applicable to offline payments, and for a distributed implementation of an open digital payment infrastructure.*

SUERF Publications

Find more **SUERF Policy Briefs** and **Policy Notes** at www.suerf.org/policynotes

SUERF
The European Money and Finance Forum

SUERF is a network association of central bankers and regulators, academics, and practitioners in the financial sector. The focus of the association is on the analysis, discussion and understanding of financial markets and institutions, the monetary economy, the conduct of regulation, supervision and monetary policy.

SUERF's events and publications provide a unique European network for the analysis and discussion of these and related issues.

SUERF Policy Briefs (SPBs) serve to promote SUERF Members' economic views and research findings as well as economic policy-oriented analyses. They address topical issues and propose solutions to current economic and financial challenges. SPBs serve to increase the international visibility of SUERF Members' analyses and research.

The views expressed are those of the author(s) and not necessarily those of the institution(s) the author(s) is/are affiliated with.

SUERF Secretariat
c/o OeNB
Otto-Wagner-Platz 3
A-1090 Vienna, Austria
Phone: +43-1-40420-7206
www.suerf.org • suerf@oenb.at