Can Blockchain be the Key to Overcoming the AML Challenge with Cryptocurrencies?

In this guest opinion piece, Special Counsel Roy Keidar and Associate Netanella Treistman of law firm Yigal Arnon & Co examine how blockchain could provide the answer to the anti-money laundering issues that crypto-currencies face.

In what some are coining a landmark case, an Israeli District Court recently ruled that Israeli banks are not obligated to provide financial services to companies whose primary business is trading in crypto-currencies, such as Bitcoin or Ethereum. The Court reasoned that banks should not have to assume the risks associated with providing a financial

platform to these digital currency businesses when the leading Israeli authorities on the subject, namely the Central Bank, the Securities Authority and the Anti-Money Laundering and Terror Financing Authority, themselves have been struggling to delineate clear measures to minimize them.

One of the primary risks noted by the Israeli authorities, along with regulators around the globe, is the pseudo-anonymous nature of crypto-currency. Regulators view the digital token transfer method as a “black box”, low in accountability and virtually impossible to subject to existing anti-money laundering (AML) and anti-terror financing regulations. However, inflexibility may be clouding judgment: built-in features of crypto-currency, particularly Blockchain technology, have the potential to improve, not harm, AML efforts, even surpassing mechanisms already in place today.

AML in the Crypto-Industry

The growing tension between the fast-growing crypto-currency industry and AML guidelines is fueled by several factors, beyond Bitcoin’s somewhat misguided reputation as a favorite of hackers and criminals, the primary of which is its structure. The current AML system was originally tailored to address existing centralized financial services systems. By default, these guidelines cannot account for a finance system based on intrinsic anonymity. Rather, AML relies on the ability to monitor and exploit the Know Your Client (KYC) process, identifying information which every financial institution is required to account for by law.

The AML monitoring mechanisms currently in place attributes every transaction to a pre-identified legal entity. Data tracked in a fiat money paper-trail includes: (a) the financial system entry point, i.e. opening bank account (b) any transaction within the system, for example, sending money from one bank account to another or use of swift platforms. The

systems then monitor the financial activity, evaluate the AML risks associated with such transactions, and follow up with any relevant notifications and reports. Use of the financial proceeds of a crime, when identified, can be easily attributed to a particular person, and legal measures applied accordingly.

Critics of crypto-currency point to the lack of identifying information throughout digital transactions as a substantial obstacle to existing AML surveillance and enforcement capabilities. However, all of these essential regulatory and enforcement elements—identifying parties and information, a record of the transaction and even enforcement—can all exist in the crypto-currency system. It's all a matter of adjusting perspective.

Firstly, crypto-currency accounts for the identity of its users both at the beginning and end of transactions through digital wallets. Tokens are stored in electronic wallets instead of bank accounts. Only the wallet-owner has access to their wallet. The owner can send and accept tokens from one wallet to another by providing the identification code of their wallet to the other side of the transaction. The code itself acts as a key, eliminating the need for names or other types of identification. As such, the transaction itself is seemingly anonymous. However, in most countries today, one needs to undergo the process of KYC in order to open a new digital wallet. Hence, by virtue of owning an electronic wallet, even without necessarily using it, anonymity is compromised. Nevertheless, in some places, wallets can still be opened without a proper identification process, which potentially may allow "dirty money" into the system. "Dirty money" and other issues like coin-join and "smurfing", make it difficult to attribute a financial transaction to a specific legal entity, presenting a problem still in need of a solution.

Blockchain can Reduce Risks

One possibility is the expansion of KYC as a worldwide pre-requisite to issue global e-wallets by setting designated wallet standards, thereby prohibiting token transfer to a wallet which does not meet those same standards. Considering there is only one type of entry and exit point, unlike the multiple exchange platforms available in the fiat system, crypto-currency could conceivably enhance identity tracking capability. Evidently, such specifications would require consensus by key players in the industry and complimentary regulation. The recent upswing in new KYC requirements for new *and* existing wallet owners internationally suggests that such standardization could be crucial for ensuring the proper functioning of the growing future crypto-currency industry as it nears sovereign recognition.

Additionally, thanks to blockchain technology, crypto-currencies inherently possess the potential to actually *reduce* AML risks when compared with fiat currencies. The blockchain is an online public ledger, where each transaction is supervised, validated and recorded as a complete transaction history. Public ledger viewers and crypto-miners are immediately notified of *any* transfer from one holder to another. Furthermore, unlike counterfeit hard-currency, which governments spend significant sums trying to combat, crypto-currencies are almost impossible to forge as each carry their own unique characteristics, which are verified from end-to-end by miners. Without verification of all transaction phases, including the departure wallet, the destination wallet, the currency type and amount, the transaction is blocked instantaneously without any human supervision. In this sense, the digital trail could better serve AML regulations than existing fiat paper trail. The structure of Blockchain is not the only characteristic of the crypto-currency system which benefits AML efforts. Crypto-miners, who act as de facto enforcement, are integral to the system as well. Miners oversee the implementation of the protocol attached to the blockchain code, and validation of transactions vis-à-vis solving the encryption algorithm. Once a validation is announced to the network, other miners “check the math”, and a block is added to the ledger only when the required number of miners has verified the transaction. Similarly, the blockchain protocol could be revised to limit transactions to KYC-verified wallets only. All

transactions could be traced back to an identified e-wallet. Moreover, AML risk analysis and alert and report-generating mechanisms could be integrated within the crypto-system, instead of monitoring only the entry and exit points.

As crypto-currencies gain mainstream public attention, and more individuals are putting their skin in the game, addressing AML challenges has become crucial. At the core of the crypto-system, blockchain technology's inherent characteristics offer a platform to address, if not overcome these challenges altogether. Evidently, there will be a price associated with in the form of higher transaction costs and less anonymity. But, it's a price worth paying for the purpose of allowing for crypto-currency to carry onward and change the face of money as we know it. With the cost of global AML measures currently estimated at over $10 billion annually, the Israeli authorities as well as law and policymakers worldwide would be prudent to look before they leap, ensuring their good intentions to protect financial intuitions and citizens don't end up blocking a technology which could provide a return on investment that far surpasses the price of transitional uncertainty.
Disclaimer: The views expressed in the article are solely that of the author(s) and do not represent those of, nor should they be attributed to CCN.

The online version appears **here**