BLOCKCHAIN:

How to combat risks associated with a new era of business transactions

Blockchain is a commercial reality and companies must become comfortable with a radical new way of working, just as they had to when the World Wide Web came along. Already, blockchain is used for items such as smart contracts, financial services, global shipping and mobile payments – all with the primary aim of saving time and cutting costs. Digital assets (cryptocurrencies) are underpinned by blockchain.

There have been a number of recent developments in the commercial use of blockchain.

> *"This year's annual meeting of G20 central bankers and finance ministers put regulation of cryptocurrencies at the top of the agenda."*

Top Silicon Valley venture firm Andreessen Horowitz has launched a $300m venture fund, called 'a16z crypto', to invest in cryptocurrency companies and protocols. The fund will be co-led by industry heavyweight Kathryn Haun, who was formerly with the US Department of Justice (DOJ) and led high-profile investigations into bitcoin-based marketplace Silk Road and bitcoin exchange Mt. Gox.

Blockchain as a service is now offered by Amazon, IBM, Microsoft, Oracle and SAP, supporting global corporations in using blockchain for their operations, to improve speed, cut costs and increase transaction security. Early adopters in financial services include Northern Trust and Santander. HSBC and JPMorgan are currently testing platforms and transactions.

A number of major companies have started to use and accept cryptocurrency in exchange for goods and services, including Expedia, Microsoft, PayPal, Reddit, Subway and Virgin Galactic.

This year's annual meeting of G20 central bankers and finance ministers put regulation of cryptocurrencies at the top of the agenda. The group has since been working on a strategy to de-risk cryptocurrency markets and build regulations that will not compromise the innovative potential of blockchain.

Despite this level of acceptance, there are still outstanding questions about the scope for fraud and money laundering, particularly with respect to cryptocurrencies. Some of the issues have been overstated, but there are some real vulnerabilities that will probably become more important in the future and must be addressed now. Exchanges, regulators, investigators and those who accept or use cryptocurrencies as payment should all take action to guard against money laundering and fraud via blockchain, rather than waiting for regulators to act first. What are the issues in the marketplace to date, and how real are they?

> *Fortunately, money laundering via blockchain should be relatively easy to detect.*

In contrast to fiat currency, cryptocurrency is decentralised and currently unregulated, and has the reputation of being used as a means for criminal activities. The value of a cryptocurrency is comparable with that of modern art: its value is purely an artefact of the market, and is highly volatile, fluctuating from one day to the next. Lack of regulation, coupled with market volatility, creates substantial opportunities for fraudsters and money launderers.

There is evidence that some of the concerns regarding criminal activities are exaggerated. Regarding money laundering, for example, the head of Europol, Europe's policing agency, estimates that currently only 3 to 4 percent of the region's criminal proceeds are laundered through crypto-assets.

Fortunately, money laundering via blockchain should be relatively easy to detect. One of the core principles of blockchain is that a transaction cannot be altered or hidden, and is traceable back to its origin if needed. When working with a digital coin exchange, it is quite possible to find out what original identifier relates to whom. It can, therefore, be relatively easy to investigate possible crimes, provided you have the right technology, algorithms and analytical skills, plus enormous computer power.

In contrast with the apparently low level of money laundering activity, fraudulent activities involving blockchain have already received widespread news coverage. Popular types of fraud include hacking into exchanges and funnelling millions of coins to illicit accounts or setting up fake exchange activities. Recent news includes the current investigation into a Vietnamese perpetrator who allegedly hired out cryptocurrency mining machines for between $100 and $5000 a day, then disappeared with $35m of investors' money. South Korean authorities are currently investigating a possible crypto scam involving locating a ship that sank 113 years ago with billions of dollars worth of gold on board: the company in question asked investors to buy into crypto that would later be reimbursed with the gold from the ship.

How to protect yourself from fraud and money laundering

It makes sense to take steps to protect your business against both fraud and money laundering via blockchain, even if you feel the dangers are currently overstated.

To eliminate risk, currency exchanges should make sure they can answer the following questions:

Are we converting coins for cash and vice versa? Is the trader a politically exposed person (PEP), and are we dealing with high-risk countries? What cryptocurrencies are we converting, and what are their characteristics? Is it possible to trace where the money is coming from and how it was obtained? Are we able to identify the customer clearly?

For regulators, the first target should be those exchanges where ordinary money is swapped for cryptocurrencies and vice versa. Exchanges should be required to obtain identification from their clients and keep a record of unusual transactions. Some countries have already implemented this requirement, including Australia and South Korea, and the EU has recently passed a directive imposing the same requirement.

> *Blockchain is here to stay. Digital assets, such as bitcoin, have already become an acceptable payment method, and they are proliferating: the number of cryptocurrencies available over the internet as of April 2018 was more than 1565, and growing.*

For investigators, it is essential to be aware of the security and anonymity features of the various currencies. Coinmarketcap.com, for example, is a good place to check on primary cryptocurrencies and gets regularly updated.

It is also important to know how to link digital identities to real-world profiles. Every blockchain user has a virtual currency wallet with a unique and anonymous account ID and all transactions from and to the wallet are accessible to all users, so as to be transparent and self-regulating.

In an investigation, the main hurdle is, therefore, not tracing transactions but identifying the wallet owner (analogous with the bank account in traditional finance). This could be an individual engaged in money laundering activities, or

an employee using blockchain to funnel money out of the organisation. The ID is recorded on the transaction within the traditional bank account and if repeated transactions go back to the wallet with the suspicious transactions, it is fairly straightforward to find the wallet owner, often with the help of the digital coin exchange used for the transaction.

Regulators and other authorities are acting, but the rest of us cannot afford to wait

Blockchain is here to stay. Digital assets, such as bitcoin, have already become an acceptable payment method, and they are proliferating: the number of cryptocurrencies available over the internet as of April 2018 was more than 1565, and growing. Yet questions about regulation, tax implications, fraud and anti-money laundering (AML) activities are still pending.

Clearly, authorities worldwide need to get this area under control, and fortunately there is plenty of evidence that they are alert to these issues. The FBI is rumoured to have 130 cryptocurrency-related investigations in process. The Trump administration has created a new task force to help with investigations including 'digital currency fraud'. The DOJ has also formed a cyber security task force whose responsibilities include cryptocurrencies. Initiatives on the ground in the UK include the launch by the City of London Police's Economic Crime Academy of a course on 'Cryptocurrencies for Investigators'.

Regulators, too, are aware, as recent G20 activity shows. Extending existing AML rules and regulations to blockchain should be their next step.

In the meantime, digital coin exchanges and organisations that accept cryptocurrency as a form of payment for goods and services should self-regulate so as to be compliant once regulations come into force. For example, it is always advisable to know where your customers and their funds originate from, and that should be extended to crypto payments.

This article was first published in *Financier Worldwide Magazine September 2018:* www.financierworldwide.com

Rob Brunner
Senior Managing Director
FTI Consulting
T: +1 (415) 283 4204
robert.brunner@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™