Payments
CARDS & MOBILE
Payments Industry Intelligence

24th Feb 2015

Can We Trust Crypto-Currencies?

It is a truth universally acknowledged, that a currency system seeking successful adoption must be in want of trust. Trust that a representation of value, such as a paper note, is backed by real value or a genuine obligation to repay; trust that those representations will be accepted by others as such; and trust that the representations of value are not counterfeit.

Early currencies were actual coins made of precious metals, which people trusted to have an intrinsic value that they could use to obtain goods or services. Today, most countries use fiat currencies which have no intrinsic value and are not tied to any physical value such as precious metals. Instead, fiat currencies are backed by government guarantee – entirely lacking in physicality and intrinsic value, fiat currency demands ultimate trust – *writes Mark Deem, Partner at Cooley LLP in London.*

The identity of those involved in a transaction (and the ability to verify such identity) is invariably a key component of this trust equation. In order for the fiat currency system to function, the currency issuer and each of the key players in a payment chain must be trustworthy to ensure that the currency is not counterfeit and that the currency will not be stolen before reaching its final destination.

But in the deliberately anonymous world of cryptocurrencies, where value is established by algorithms and verified by the electronic transfer of data, how can trust be established without proof of identity? In light of the widely reported vulnerability of e-wallets, can we ever truly establish the same trust in cryptocurrencies that we have in our own fiat ones today?

The answer perhaps lies in an appreciation that the trust deficit will only be met once there is sufficient confidence in the technology which underpins the currency and the key market players in cryptocurrency transactions are held to a high level of accountability. In fiat transactions today, “money” must pass through many hands before reaching its final destination. When you pay for your shopping with a credit

card, your personal details are collected by the shop, transmitted to their acquiring bank that then transmits your details again to your card issuing bank.

After initial approval, these details are transmitted along this chain once more before the funds are actually released. This chain demonstrates a number of potential points for a security breach. Despite this, society generally trusts in the system because the banks and payment processors are regulated and we can feel secure in knowing that the parties involved are required to enforce a high level of security. Even if a breach occurs, we know that the parties involved will be held accountable and trust that we as participants will have the opportunity for redress.

Cryptocurrencies, on the other hand, are entirely decentralised and value passes directly from payer to payee. Quite clearly, there are far fewer potential points for a security breach along the Bitcoin payment chain that solely consists of a payer and a payee. There has also never been a recognised security breach or defrauding of the actual Bitcoin ledger, known as the Blockchain, to date. The Blockchain is considered to be extremely secure as it publically records every transaction that is ever made.

For a system that seems to be so secure in its technology to be plagued with instances of hacking and fraud (most recently the hack of the popular Chinese Bitcoin exchange Bter), the real trust issue lies with the gatekeepers between cryptocurrencies and their traditional fiat relations.

Cryptocurrency-related businesses that act as interfaces with fiat currencies, such as exchanges and payment processors, are largely unregulated by any regulator worldwide. They have also been the generators of the largest reported hacks to date, causing widespread mistrust in the system and extreme volatility in cryptocurrency pricing. However, this mistrust stems from the lack of accountability of the cryptocurrency-related businesses that are able to operate without any required disclosure of identity or location.

To condemn cryptocurrencies as a whole based on the poor security of a few rogue market players would be tantamount to condemning a fiat currency because of a few bank thefts. If currency is stolen from a bank, its security is increased. Consequently, when a cryptocurrency exchange is compromised, it should follow that the solution should be increasing the security of exchanges. However, unless and until the loss falls on the exchange, there is no incentive on the exchange to change its behaviour.

Indeed, it is only when the behavioural and organisational standards are enforced by industry or national regulators that the collective conduct and security of the cryptocurrency industry will be elevated. When responsible conduct of participants is required, confidence in the market will follow. It is therefore in the best interests of most cryptocurrency-related businesses to support the push for regulation and instil trust in the wider currency platform.

It is only by learning how to play this trust game effectively that cryptocurrencies have any real shot at viability: if consumers feel able to trust in the industry that has thus far been plagued by hacks and security breaches, cryptocurrencies could even revolutionise the way we live.

It should therefore be a truth universally acknowledged that a cryptocurrency exchange in possession of fortunes, must be in want of good regulation.