Many may still think of cryptocurrencies (effectively virtual currencies, largely unregulated and not sponsored or controlled by any national Governments) as the Wild West and a currency ecosystem largely inhabited by criminals and linked closely to the Dark web, money laundering and tax evasion. True – criminals do seem to enjoy the relative anonymity of conducting deals and purchasing illicit goods using Bitcoin, Ripple, Ether and several other popular cryptocurrencies. However, look a little closer and you will see a cryptocurrency industry expanding and increasingly used and accepted by a younger generation and steadily moving towards the mainstream.

An increasing number of retailers/companies have at various times already accepted cryptocurrencies or soon will do eg including Microsoft – for their online Xbox store, KFC Canada, Expedia – purchasing flights via cryptocurrency, Virgin Galactic. Starbucks and Norwegian Air are planning to start accepting Bitcoin in the near future. Note also Facebook’s plan with others to create a new cryptocurrency called Libra with lofty ambitions – billed as “A simple global currency and financial infrastructure that empowers billions of people. Reinvent money. Transform the global economy. So people everywhere can live better lives.” We can therefore expect the universe of companies willing to accept cryptocurrency to expand materially.

Cryptocurrencies are just one application built on the underlying technology of Blockchain – a type of distributed ledger technology (“DLT”) which is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers.

Its great selling point specifically in terms of Cryptocurrency is that DLT allows (i) anyone with a computer and an internet connection to participate (ii) the simplification (and some might say democratisation) of financial transactions that otherwise require the intermediation of a third party1 and (iii) a large degree of anonymity and security making use of cryptography. The mechanics of the cryptocurrency/DLT technology and how it sustains itself is fascinating but not the focus of this article2.

Once established, each cryptocurrency ecosystem is inhabited by several key participants being principally (i) users of the currency – people who buy cryptocurrency from another user or via a specialist platform using fiat money and buy goods and services with their cryptocurrency (ii) “miners” (who help maintain the workings of the Blockchain system by validating cryptocurrency transactions and who are paid to do so through newly created or “mined” cryptocurrency i.e. they are credited cryptocurrency in return for their efforts) (iii) cryptocurrency exchanges – who offer exchange services to users in return for a fee e.g. allowing users to sell or buy their cryptocurrency with fiat money (iv) trading platforms – which bring together users and allow them to trade their cryptocurrencies directly with each other and (v) wallet custodians - who provide users with e-wallets to safeguard their cryptocurrencies (specifically holding the private

---

1 Eg think your bank – which charges you a ridiculous margin to change your GBP£ into holiday Euros or your GB company to pay your Euro supplier-- cryptocurrencies can be used on a peer to peer basis to cut out financial institutions from many types of common currency transactions

2 Eg see Cryptocurrencies and Blockchain – Legal context and implications for financial crime, money laundering and tax evasion – Policy Department for Economic, Scientific and Quality of Life Polices - report July 2018 – for an excellent overview.
Cryptocurrencies moving mainstream

Cryptographic keys\(^3\) used to evidence ownership) and used for holding, storing and transferring cryptocurrency – similar in concept to your standard high street bank account.

**Regulation**

The regulators have been slow to oversee cryptocurrencies but this is changing and as regulation catches up, the shadier side of the use of cryptocurrencies will be increasingly pushed to the fringes or at least conducted more in regulation-lite international locations. Just two recent regulatory examples suffice to demonstrate very recent and material regulatory developments. First, 10 January 2020, saw the implementation of EU regulation over cryptocurrency exchanges and wallet custodians requiring them to register with their local regulator and demonstrate compliance with know-your-customer (KYC) and anti-money laundering (AML) procedures – just like other European financial institutions who have been regulated for many years.

While some crypto institutions have closed in response or chosen to relocate to lesser/non-regulated world locations (eg Panama) the longer term effect should be to bring cryptocurrency services into the mainstream (at least in Europe) increasing trust from the public in the use of cryptocurrencies and making their use more open and less susceptible to criminal use. In the UK, these cryptocurrency entities and their activities have been previously unregulated but will now need to register with the FCA and pay regulatory fees. The regulatory oversight and clarity this brings will also encourage mainstream financial institutions to get involved where they have previously shunned the industry in part for fear of the regulatory unknowns.

Second, earlier this week, the Indian Supreme Court overturned an April 2018 Indian Central Bank ban on banking access to cryptocurrency which had cut off access for crypto exchanges/platforms to India’s mainstream financial system and exchange into fiat currency – meaning that crypto exchanges/platforms had in 2018 either closed, left the country or restricted themselves to crypto-to-crypto trading only. Since this week’s Court decision, crypto exchanges have already announced the reinstatement of deposits and withdrawals via mainstream bank accounts and India’s cryptocurrency use (in a country of population circa 1.3B) is expected to grow exponentially as a consequence.

Regulatory development affecting cryptocurrencies continues in most developed countries and G20 Finance Ministers will be considering related reports later this year and we can expect further material regulatory developments in the next 12-24 months.

**Cryptocurrency and hacking**

With all new technologies come risks and cryptocurrencies are no different. As well as some exchanges and platforms sometimes unwittingly holding stolen funds in effectively anonymous accounts (eg nearly all ransomware ransom payments are made in Bitcoin), the exchanges/platforms and their customers themselves are increasingly subject to cyber-attack and theft. There have been several high value hacks over recent years including from Coincheck ($540m stolen in 2018), Mt Gox ($500m in 2014) and Bithumb (US$32m 2018)\(^4\). The anonymity issues and the difficulty in tracing the theft of cryptocurrencies (unlike thefts/frauds involving bank accounts – where monies can effectively be traced through bank accounts around the world, subject to the Court’s and the relevant jurisdiction’s assistance) makes the recovery of assets and conviction of the criminals difficult though not impossible.

Such hacks are often based on common cyber-attacks that ordinary companies and individuals face on a daily basis including phishing emails, malware etc directed at obtaining access to the private keys which prove ownership of any cryptocurrency. Most susceptible to hacking are the exchanges and platforms themselves and “hot wallets” used by users (ie e-wallets connected via a device to the internet eg via an App provided by the user’s crypto exchange). “Cold wallets” which store on devices

---

\(^3\) Effectively a secret number that allows bitcoins to be spent, evidences ownership and is only known by the cryptocurrency owner. It the key is lost or stolen, so the cryptocurrency is also lost to its rightful owner.

\(^4\) Reports suggest theft of crypto assets by hackers in 2019 worldwide totalled circa US$480m.
that are not connected to the internet are materially more secure.

Insurance

With these new financial services come new opportunities for insurers. While bank accounts are backed by Government schemes eg the FDIC in the USA and the FSCS in the UK, there is no central safety net for cryptocurrency account holders. While two years ago the market for crypto related insurance was very limited, the demand for insurance solutions to the risks of holding and using cryptocurrencies has recently been growing rapidly from both platforms/exchanges and individual users.

Insurance policies have been placed for some of the larger cryptocurrency custodians eg BitGo Inc. (which holds circa $2B in cryptocurrencies) reportedly has a $100m policy placed at Lloyd’s covering its offline cold storage wallets covering hacks, insider theft by employees and loss of the private keys evidencing ownership. Coincover also is said to have a $200m+ policy covering loss caused through security breach or hack, employee theft, or fraudulent transfer affecting its online handling services (it says it only keeps 2% of its crypto custodian assets online at any time). The policy does not cover loss through the account holder’s fault however – eg hacking of the individual user’s account or loss by the user of their private keys.

Lloyd’s Product Innovation Facility (PIF) was set up in June 2019 specifically to address these types of new technology opportunities. PIF is backed by a group of 24 Lloyd’s syndicates who have together committed over £100 million of underwriting capacity.

Only in the last few days, PIF and Lloyd’s syndicate Atrium in conjunction with Coincover has also launched a new insurance policy to protect cryptocurrency held in online wallets against theft or other malicious hacks with limits from as little as £1,000, to protect against losses arising from the theft of cryptocurrency held in online, hot wallets. To meet one of the crypto industry’s concerns, the insurance policy limit increases or decreases in line with the (often volatile) price changes of the insured cryptocurrency, meaning the insured will always be indemnified for the underlying value of their cryptocurrency at the time of any loss.

Commentary

The combination of increased regulation and the introduction of protective insurance products will likely accelerate the already increasing public interest and take-up of cryptocurrencies where potential customers have undoubtedly been deterred until recently by the risks and previously inadequate protection against theft and loss. With circa $300B of cryptocurrencies in circulation and only circa $1B of related insurance coverage currently said to be available, the ingredients are now in place for both a material expansion of the cryptocurrency ecosystem and the insurance sector supporting it.

Today cryptocurrencies of circa $300B are a small fraction of World Governments’ combined “narrow money” (i.e. notes and coins in circulation) of circa $40 Trillion and an even smaller fraction of broader measures of “money”, including bank accounts etc. Governments can never allow cryptocurrencies to materially challenge their incumbent currency systems (not unless those Governments exclusively own and control such cryptocurrencies). How far Governments will allow independent cryptocurrencies to flourish remains to be seen.

For further information please contact:

Stephen Reilly
Partner
+44 (0) 20 7469 0419
s.reilly@beale-law.com

Charlotte Gooch
Trainee Solicitor
+44 (0) 20 7469 0403
c.gooch@beale-law.com