CRYPTO A.M. Our series on AI, Blockchain, Cryptoassets and Tokenisation

E: CryptoInsider@cityam.com @CityAm_Crypto In association with GFIA GIBRALTAR FUNDS & INVESTMENTS ASSOCIATION

PARTNER CONTENT

CITY A.M.'S CRYPTO INSIDER

JAMES BOWATER

Perhaps the most important part of Blockchain is the creation of trust through the transparency and immutability of records entered on the ledger. So it wasn't lost on me that the most common theme flavouring discussions I had this week revolved around the importance of creating the right conditions for institutions to be able to invest into cryptoassets as well as crypto funds. The usual topic of a clear regulatory framework was pervasive, however, one thing that stood out was the importance of custodial solutions and the need for those solutions to be rock solid and safe from being hacked.

One method is an escrow system designed to eliminate counterparty risk on OTC (over the counter) trades and would be key to building the trust and efficiency needed for the large transactions that institutions will want to make. Separately a custody solution is needed to ensure that for institutions, there is a regulated custodial solution available to allow them to easily and safely take positions on digital currencies and easily move those positions when needed. All a normal part of the capital markets infrastructure available for other asset classes that is now very much needed for digital assets.

Several companies I have been speaking to are racing to build such an ecosystem, for example I met up with Ahmed Ismail and Christopher Flinos the co Founders of HAYVN who are currently going through their licence application from the rigorous Abu Dhabi Global Markets Financial Services Regulator. Having worked together at Merrill Lynch their aim is to provide a compliant and insured proprietary custodian double escrow solution to securely store independently auditable and verifiable digital assets on behalf of financial institutions using institutional grade transparency, security, compliance and best execution practices.

Ancillary to laying the groundwork for institutional adoption, it was interesting to note that the EU held a workshop last week in Brussels, where a dozen volunteer lawyers and technologists came together to begin the definition of the stock certificate as a digital token for the 21st century. They got to work on issues like ownership, rights, loss and recovery, tradability, and more. "This was a great workshop," said David Siegel, CEO of the London-based Pillar Project, who put the team together. "We made a lot of progress, got to know each other, agreed on a name for our group, and will continue to work over the next few months to produce a standard everyone can use. This will help provide liquidity and a path to transform capital markets." The goal is that even the largest stock exchanges (NYSE, LSE, etc) will be able to use this token standard to replace existing "digital shares."

BITCOIN'S ANONYMITY: CLEVER OR CRIMINAL?

Designed by Phill Snelling, Bowater Media

Professor Kevin Curran believes that the growing phenomenon of email scams where attackers claim they stole your password and hacked your webcam while you were visiting naughty websites is enabled in large part due to the difficulty in associating a Bitcoin address with any other address in the Bitcoin network. This is a key feature that enables its users to remain anonymous. The separation of virtual currency accounts from real-world identities, along with the ability for an individual to create an arbitrary number of accounts enables the development of novel, complex layering transaction patterns. Thus, any Bitcoin user can create a number of addresses and operate anonymously.

Unfortunately, according to Curran, this characteristic of Bitcoin has also given rise to ransomware criminals. "Ransomware is enabled by digital currencies, along with denial of service attacks, since the use of Bitcoin and other cryptocurrencies allows hackers to get paid and remain untraceable, which was not possible prior to cryptocurrencies. Thus, it comes as no surprise that ransomware is one of the main threat to cryptocurrencies at the moment."

Moreover, Curran explains, we are starting to see virtual currencies forming the modus operandi of trading in a number of illicit goods. Additionally, it can facilitate the payment of services that may be regulated or criminalised in certain countries for example, online gambling. "The existence of these currencies is ideal for criminals wishing to hide their tracks and we should examine the implications for society when such a powerful anonymous virtual currency exists." Of course, given the correct resources, specific bitcoin transactions can be traced but if criminals use the proper 'mixing' techniques to launder their bitcoin, they will be untraceable.

Concerning the long-term future of Bitcoin, Curran believes we simply cannot foresee what lies ahead for this phenomenon. "Virtual currencies are here to stay, however, law enforcement and regulatory forces are – for the foreseeable future – facing a crisis in their investigations into virtual currency transactions. Furthermore, major problems such as the amount of energy now being used to mine coins may force national governments to step in. Of course, banning it would have to be a globally agreed solution, as Bitcoins cannot be easily traced to a geographical location. Bitcoin can be made truly anonymous with the use of the correct 'mixing' techniques."

A long-term pitfall is the verification of the blockchain, Curran points out. "In Bitcoin, for instance, the incentive to validate the blockchain lies in the mining process where miners compete to mine new coins. However, since that will end after 21 million are mined, it is hoped that the financial gains will then lie in the transaction fees but incentivising other blockchains may be a larger problem." Another issue is the governance of Bitcoin and other decentralised blockchains. "They usually have a governance group of lead developers to implement the agreed changes but there is nothing to stop a core of the blockchain from 'forking' off to a competing blockchain."

A major problem of blockchain currencies is the storage and safekeeping of the 'coins'. Curran points out that unlike traditional banking mechanisms, blockchain currencies can be stolen and moved to a thieves account with no means of recovery. "This is a real and ever-present danger with using cryptocurrencies and there have been ever-increasing incidents of coins being stolen." He echoes the European Banking Authority and others who have warned that Bitcoin users are not protected by refund rights or chargebacks and the use of Bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and media.

For banks, of course, they need to know who the transacting parties are. Curran highlights that the anonymity makes using Bitcoin or other cryptocurrencies impossible for now and believes that public confidence is the main stumbling block. "If there is money to be made in the future, watch them suddenly change this modus operandi! What affects confidence mostly is the theft of Bitcoins, failure of Bitcoin exchanges and the mad varying Bitcoin currency fluctuations. Once those become less worrying, public confidence will grow and real traction will take place. Underneath it all will be the blockchain, verifying transactions in a decentralised manner like we have never seen before."

In terms of what's needed next, Curran concludes that the skills required to 'follow the money' have exploded in the last year. "We are likely to need dramatically more computer security incident response teams, real-time collection of traffic data and search, seizure and expedited preservation of stored computer transactions. For now, the safest thing is to back up your data and try to simply become resistance to ransomware or denial of service attacks."

Curran is also passionate that "to combat the rise of cryptocurrency-enabled crime there needs to be more resources in the form of cyber defence in the UK. We need to upskill more people – from the public up to the IT people working in the industry – on how to do safe computing. In addition, we need more security and forensics experts in our police forces, as well as from a counter terrorist point of view. We must also spend more money in the IT space and reallocate money, which has traditionally been ring fenced for more traditional forms of defence. Modern warfare has changed and we are fighting less in the real world and more for our lives in the cyberspace. Those in charge need to recognise that."

> We should examine the implications for society when such a powerful anonymous virtual currency exists

Professor Kevin Curran, senior member of the IEEE and professor of cybersecurity at Ulster University, in conversation with James Bowater. Professor Curran is an award-winning cybersecurity expert who has made significant contributions to advancing the knowledge and understanding of computer networking and systems, and has served as an advisor to the British Computer Society in regard to the computer industry standards. o the computer industry standards.

GIBRALTER FUNDS & INVESTMENTS ASSOCIATION

Throughout 2018 the Government of Gibraltar and the Gibraltar Financial Services Commission (GFSC) have continued to work on making Gibraltar a centre of excellence for DLT and crypto businesses. As a logical consequence, Gibraltar has also seen the emergence of crypto funds. Fund promoters are attracted to the synergies that exist between the already mature DLT ecosystem that has been developed in Gibraltar and its firmly established funds regime.

Given the regulatory risks that exist with crypto funds (as with any new asset class), GFIA has recommended that all crypto funds, dealing with third party money, be regulated by the GFSC as Experienced Investor Funds (EIFs). EIFs require two local authorised EIF directors, an approved fund administrator and a local auditor. The fund will also require a bank account, crypto wallet(s) and an offering memorandum to the requirements of the EIF regulations.

Crypto funds need clear policies and processes on dealing with issues surrounding safekeeping, security, transmission and valuation of crypto assets. Crypto funds will also need to consider how to undertake AML checks on investors subscribing in crypto Such questions were highlighted by the GFSC in their statement dated 17 October 2018 on Funds Investing in Digital Assets.

EIFs do not require pre-approval from the GFSC before launching. EIFs are launched based on a Gibraltar legal opinion provided that the required documentation is submitted to the GFSC within 10 days. This means that there is no regulatory downtime when considering speed to market.

For further information on the Gibraltar crypto funds regime, please contact Valentina La Gatta of GFIA at info@gfia.gi.

TOKEN INTELLIGENCE
TokenIntelligence.io

A Call for National Public Infrastructure

As we look back over the roller-coaster ride that was the last year high points include the dawning of BitCoin in America (and so the world's) consciousness: Tips were exchanged over Thanksgiving dinners across that nation... "You've not got BitCoin yet?.. I just got some. Its going up like nothing I've ever seen... but young Billy bought a bunch couple years ago... Look at him now!". Followed by a S-storm of black propaganda from the likes of Jamie Dimon that hangs in the air to this day and continues to influence the debate among the uninformed.

By this Thanksgiving we've had the IMF's Christine Legarde calling for central banks to adopt the technology while the speculators gains were wiped away as we pass through the watersplash.

Perhaps most disappointing of all we've had the Task-Force's troika' disappointing response, its long awaited report, all but ignoring the huge opportunities presented to UK PLC in favour of navel gazing and risk assessment at a time when Britain needs to be thinking post Brexit, regardless of impact and the outcome, about its place in the world and in relation to the rest of Europe. Leadership or...

A little over six years ago I wrote an article counter-intuitively calling, for the first time, for the creation of an 'Innovation Unit' within the financial regulator (August 2012 in Real Business to be precise).

It took two years and a lot of hard slog for us to make the case to BIS, the Treasury and in Parliament. Along the way triggering the Blackett review and Sir Mark Walport's work resulting in establishment of our now world renowned regulatory innovation unit, sand boxes and – by no means least, Chancellor George Osborne instructing the FCA, in public, at the launch of Innovate Finance, that from henceforth regulation must support innovation.

Somewhere along the way we've seen the flowering of Fintech, with London as its world capital. For now. But let there be no complacency – there are plenty of contenders around the world aching to take that place at a time when agility and intelligence outpace mere heft. Which is why, depite all the bluster the USA, who're trailing miserably behind, are seeking to turn back the clock.

Over the year we've seen a growing consensus that we stand on the cusp of the next revolution. So at a time when the future is being formed for generations to come we find that government and regulator are not just flat-footed but so far behind the curve as to be an impediment. The cryptoassets Taskforce report will be politely received but it's a blueprint for obscurity and business as usual.

We've also seen the formation of the British Blockchain Industry Association (BBIA), a dedicated industry body with a vision for a better future, which I am honoured to serve as chair.

So today I'm again calling on government and regulators, especially the troika, to engage with the industry. Not just those hoping to burnish business-as-usual with closed DLT but also and especially those who understand the true potential of open Blockchain technology to create secure public infrastructure – that can serve us all, and propel us to a better future, leading the world.

I'm calling on government to commission a new report not narrowly on the seeming threat of 'Cryptoassets' but on the potential of creating national public infrastructure that could propel us forward in so many different areas: Health and the NHS, Logistic, Energy, Local government, Law and more.

Many commentators have pondered the role of government going forward. Well, perhaps, here it is.. if the will can be found, to look, learn and become what the world now needs and demands: Agile.

Email Barry.James@TokenIntelligence.io questions or listen to the latest at ICOrad.io

Crypto A.M. shines its Spotlight on CryptoCompare

Charles Hayter, CEO of CryptoCompare

CryptoCompare is the global cryptocurrency market data provider, offering retail and institutional investors real-time, high-quality and reliable market and pricing data on 5,600+ coins and 260,000+ currency pairs, bridging the gap between the crypto asset and traditional financial markets.

Today sees the launch of their new API service in response to customer demand for more complex and highly scalable cryptocurrency data solutions.

The existing free API service enables individuals and organisations to retrieve cryptocurrency market and pricing data with a high degree of granularity, offering real time and historical data for all coins and exchanges with full market coverage, at the lowest latency possible. By way of example, CryptoCompare's data is viewed between 20 and 180 million times per hour, peaking during times of higher market volatility.

The new commercial API service will be available in 3 different tiers, tailored to the cryptocurrency data needs of the institutional and retail investors as well as third parties, partners and developers. The commercial service will offer more flexibility such as extended historical data; customisable API endpoint solutions and call limits; dedicated support and service level agreements; and the ability to save/cache data locally for internal business purposes.

Finally, the tiered plans include commercial redistribution rights, enabling third parties greater flexibility in using CryptoCompare's data for their crypto investment products or market data needs.

The new commercial API service is now live on the CryptoCompare website and has been rolled out to CryptoCompare's universe of customers. CryptoCompare's global infrastructure allows for high availability and performance, ensuring the fastest data delivery for both free and commercial API services.

> CryptoCompare's data is viewed between 20 and 180 million times per hour

Charles Hayter, CEO and Founder of CryptoCompare, said: "There is a clear appetite in the industry to capitalise on digital asset trading due to their frictionless global nature. At the heart of this trend is accurate, reliable and real-time data. We continually invest in our technology and APIs to ensure our infrastructure remains robust and both the retail and institutional investor can access data as needed to execute trades on their investment portfolios. We adhere to rigorous standards to safeguard data integrity, normalising global data sources to ensure consistency and confidence in the market."

CryptoCompare has recently partnered with Nasdaq and VanEck's subsidiary MVIS (MV Index Solutions) to provide data for a series of digital asset futures contracts. In August 2018 CryptoCompare partnered with Thomson Reuters to provide order book and trade data for 50 cryptocurrencies to Thomson Reuters' Eikon platform.

For more information, please visit our website www.cryptocompare.com or follow us on Twitter @CryptoCompare.

CRYPTO COMPARE

THE ERA OF SECURITY TOKENS

Jonathan De Carteret, CEO INDX Capital

A year ago, the enforcement team at the SEC would have assembled around a large table to discuss how to deal with the booming ICO market. Crypto currency start-ups had overtaken Venture Capital in fund-raising and had caught everyone off-guard.

Observers around that table would have heard stories of multi-million dollar scammers, rampant and unrealistic claims and teenagers with nothing more than a flimsy whitepaper buying brand new Lamborghinis. The "Wild West of Crypto" was turning into the O.K. Corral and in desperate need of a sheriff.

Key players around that table identified the areas that required their attention.

1. Funds that raise investment using fake regulatory credentials.

2. Security offerings that were masquerading as ICO utilities.

3. Unregulated exchanges that were listing securities.

This challenged everything the SEC had worked so hard to preserve. Heads would have to roll.

A year on we now witness the end-game of that first phase of enforcement.

One of the first on the chopping block was Crypto Asset Management, which claimed to be "one of the first regulated crypto asset funds in the United States". They weren't what they claimed and were duly hit with a cease and desist order and slapped with a hefty fine. More recently the SEC made an example of two ICOs, Airfox and Paragon Coin, which were issuing securities through ICOs and failing to comply with existing statutes and rules. Finally, the founder of EtherDelta, a decentralised exchange, was charged over operating an unregistered exchange.

That was three out of three. Be warned, the SEC made it clear, we are watching and will act.