ALLEN & OVERY

Virtual currencies

Mining the possibilities

2015

Virtual currencies: *Mining the possibilities*

There are two distinct narratives surrounding virtual currencies. One picks up on countercultural elements – an extreme free market environment beloved by anarchists and criminals. The other describes a technology as revolutionary as the TCP/IP protocol was to the internet, which has the potential to vastly change the financial services environment as well as any other industry which currently involves the use of a trusted third party to facilitate the transfer of value.

This difference in perception is significant – and it is worth examining the world of virtual currencies to understand how these two divergent views can both have some validity.

The Financial Action Task Force (FATF) provided some very helpful definitions in its 2014 paper on virtual currencies[1] and we use those as our framework in this paper.

[1] "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", June 2014, Financial Action Task Force http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf updated in 2015 with http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Defining virtual *Currency*

A virtual currency is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value, but does not have legal tender status in any jurisdiction. It is not issued or guaranteed by any government, and fulfils these functions only by agreement within the community of users of the virtual currency. It is distinct from fiat currency or "real currency", which is the physical money that makes up a country's legal tender, and distinct from e-money, which is a digital representation of fiat currency.

Open or closed?

Virtual currencies can be open (also known as convertible) or closed (non-convertible). Open virtual currency can be exchanged back and forth for real currency, while closed virtual currency can only be used in the environment for which it was designed. A good example of a closed currency is video game credits which can be used only within the chosen game.

Centralised or decentralised?

All closed currencies are by their nature centralised. A centralised currency has an administering authority which controls the system (issuing the currency, establishing rules for its use, recording transactions, etc). Decentralised virtual currencies, which are also known as cryptocurrencies, are distributed, code-based, mathematical, peer-to-peer currencies that have no central administrating authority. Cryptocurrency relies on public and private keys to transfer value. The integrity of a cryptocurrency ledger is ensured, not by a trusted third party, but by a network of mutually distrustful parties whose work protects the network in exchange for a fee or reward.

The most high profile cryptocurrency is Bitcoin.

What is *Bitcoin?*

Bitcoin was introduced to the world in October 2008 in a paper authored by a person or group using the pseudonym Satoshi Nakamoto.[2] (The true identity of Bitcoin's developer(s) has never been established.)

Nakamoto envisaged a transparent electronic means of transferring tokens of value without having to rely on third parties, such as banks. Rather than using a third party to manage the transaction, the necessary record-keeping is decentralised into a virtual ledger – which one might think of as a giant sequential (append only) spreadsheet of transactions. This ledger, known as the "blockchain", holds the transaction history of all bitcoins in circulation. Bitcoin miners collectively take responsibility for adding transactions to the ledger. Each miner collects pending transactions to form a "block" and then competes with other miners to add their block to the blockchain. To do this miners must solve a complex mathematical problem (by generating a "cryptographic hash" of, among other things, a list of the transactions included in the block and a hash of the previous block, which satisfies certain rules). Miners are rewarded (with bitcoins) for participating in the system and validating transactions.

From a user perspective, to make or receive payments you need Bitcoin wallet software to store the private key(s) used to access funds allocated to your public address and sign transactions.

What is a *Hash?*

A hash is a digital fingerprint of a digital file generated using a cryptographic hash function. Bitcoin uses a cryptographic hash function called SHA256. Applying SHA256 to a digital file – be it an email, a PDF or a Netflix movie – will produce a unique string of numbers and letters. If the digital file is changed in any way, however small the change, the resulting hash will be completely different.

For example see the next page:

[2] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf

Text	SHA256 hash
“Digital Currency.”	3cedd83703f89ae0c22286e0e906729ec2ebd5037638a47c42c4fd16bf627962
“Digital Currency”	88f69fd57cc1c8a73e7fd7650626935806654e224386c755009351b1d02ec377
“Digital currency”	33e20d64e63c47e9501ebad1e2be7be8e5b4577f82fd9a4d639a664847a4f0f0

An interesting property of SHA256 and similar hash functions is that whilst anyone can check the authenticity of a digital file (ie if given a copy of the digital file, they can use the same algorithm to generate the same hash, thus verifying its authenticity), it is impossible to extract the digital file from the hash alone.

The results in the table above can be verified here: http://www.xorbin.com/tools/sha256-hash-calculator.

Blockchain: *Key applications*

Success or failure of any new technology is determined by the size or impact of the problem that the new technology seeks to solve. Virtual currencies such as Bitcoin are attracting increasing interest. More broadly, the blockchain technology underpinning Bitcoin may offer solutions to any number of problems. We look at some key examples of these below.

Transfers of value

Particularly within the financial services industry, the blockchain is attracting a huge amount of interest because of its promise to deliver secure, verifiable transactions among entities online without the need for intermediaries. With no central register to pay for, blockchain promises frictionless transfers of value with much reduced costs. We are already seeing "real life" examples of blockchain technology in use. For example, in May 2015, Nasdaq, one of the world's largest suppliers of exchange, clearing house and depository services and technology, announced that it planned to use the blockchain to run its Private Market, with a view to incorporating blockchain technology into the other offerings that it provides to its clients.

Virtually all of the major banks are experimenting with and assessing blockchain technology for use in their own operations, with areas such as international money transfers, trade finance, syndicated lending and collateral management all seen as good contenders.

Micropayments

One can see particular application for blockchain technology in the area of micropayments, where the costs of making transfers of very small sums of money have previously made many potential micropayment models unfeasible. One influential start-up in this area has been Streamium, where a stream of small, off-chain payments is made to a broadcaster every second as a viewer watches a video, and all of those micropayments are then combined into one larger payment that is made via the blockchain.

Managing registers of assets

Honduras announced a pilot programme to create land titles based on blockchain technology in May 2015, and one can imagine similar applications in the future using distributed ledgers in areas such as software and hardware licences, and registrable intellectual property rights such as patents, copyright and trademarks and more. Musician Imogen Heap is working on a project called Mycelia which is based on the idea of a blockchain database to enable artists to distribute their music directly to fans. The core idea behind Mycelia is to use the blockchain to track (and associate revenues with) every copy of a recording that is made.

Similar applications might be used to prevent fraud. An interesting start up in this area is London-based Everledger. Everledger uses the blockchain to establish the provenance of diamonds (although the application could in time extend into any high value items whose provenance might otherwise be reliant on paper certificates and receipts). Everledger creates a digital record from 40 metadata points specific to each diamond that it records to create a tamper-proof "fingerprint".

Smart contracts

Smart contracts are computer programmes that can automatically execute the terms of a contract. The idea of a smart contract (effectively based on the "if...-then…" logic of programming) has been around since Nick Szabo proposed them in the 1990s, but Bitcoin and blockchain have given the idea new impetus, by directly linking the contract to the assets affected. In other words, a smart contract is a computer programme that can automatically effect a payment or asset transfer. Ethereum, Orisi, Hedgy, Symbiont and Eris are some of the companies working on projects in this area.

Looking further ahead, smart contracts may one day power an "internet of things", with objects able to negotiate and make or take payments. Imagine, for example, that you want to hire a car. A hire car could, through a series of smart contracts, take your payment to hold in escrow, check a central register to ensure that your driving licence is current, transfer a digital key to your mobile phone and give you access to the car for the selected period of time. Another example might be your home router negotiating and selling your excess broadband capacity to other users.

Autonomous agents

Further down the rabbit hole, cryptocurrencies can provide a platform for incorporated autonomous software agents to buy and sell services. An oft-cited example is a self-driving vehicle that owns itself, sells rides online and collects payments through virtual currency. It uses its virtual currency to obtain electricity, bandwidth, and maintenance.

Legal *issues*

The regulation of virtual currencies is nascent and, as one can appreciate from the range of ideas encompassed by the term "virtual currencies", not all virtual currencies will be treated in the same way by regulators.

Many regulators are wary, to say the least, of how to approach the regulation of virtual currencies. A recent opinion paper from the European Banking Authority[3] set out a comprehensive list of possible risks created by virtual currencies and identified a number of ways of mitigating these risks through regulation.

It then went on to acknowledge the difficulties of implementing such a framework due to both resource constraints and the global nature of the response required.

It concluded that:

"Until a comprehensive regulatory regime is developed, (if it is developed at all), only those risks can be mitigated that arise in the interaction between VC [virtual currency] schemes and the regulated financial services sector (but not those that arise from activities within or between VC schemes). This would include risks of money laundering and financial crime, the risks to conventional payment systems, and some risks to individual users. To that end, the EBA recommends that national supervisory authorities discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling VCs, thereby 'shielding' regulated financial services from VCs."

This fairly negative tone and "wait and see" approach does not offer innovators in the market much certainty over how their offerings may be impacted by regulators in the future. Generally, however, the mood music for virtual currencies, and particularly blockchain technology, is increasingly favourable – one example of growing acceptance in the broader market is that Goldman Sachs recently led a USD50 million investment round into Circle Internet Financial, a start-up that aims to use the blockchain to improve consumer payments.

Further evidence of the momentum behind distributed ledger technology was given recently in the news that a consortium of high profile banks is backing R3, a New York-based start up trying to build the first true "financial grade" distributed ledger.

The overall direction of travel for regulation in the Fintech space has been positive and thoughtful, with regulators keen to balance the protection of financial stability with a desire to enable and realise the benefits of innovation – so we view this market optimistically. However, below, we pick out some of the areas that we believe regulators may focus on, and that our clients should be mindful of.

[3] EBA Opinion on 'virtual currencies', July 2014, European Banking Authority https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

Who to regulate?

Decentralised networks by their very nature are not centrally owned, which could present problems to regulators in much the same ways that BitTorrent networks have presented problems to those concerned with the protection of certain intellectual property rights. The global nature of virtual currencies may present a further challenge. However, while the German financial regulator BaFin acknowledges the difficulties of regulating a distributed network, it also notes that Bitcoins are traded via internet platforms, such as exchanges, and that these activities generally do require authorisation by BaFin.

AML/CFT

Convertible virtual currencies are certainly in the sights of regulators due to concerns over money laundering (AML) and financing of terrorism (CFT). Where virtual currencies are characterised as having non face-to-face customer relationships, or as permitting anonymous funding, there may rightly be concerns about the sources of funds or the purposes to which funding is put. Further, the issue of who to regulate (identified above) is very much in play here. However, in the UK, for example, the Government published a "Call for Information" in November 2014 to gather evidence on the benefits and risks associated with virtual currencies. In summarising the evidence gathered in this process, the UK Government in March 2015 announced its intention to apply anti-money laundering regulation to digital currency exchanges in the UK (though further formal consultation is still planned).

Privacy

Transactions in a distributed ledger such as Bitcoin are anonymous (in so far as your name is not associated with the transaction) but not private, because every transaction is permanently visible on the ledger. This fact is behind the AML and CFT concerns outlined above. Conversely, there are concerns about how easy it is to de-anonymise transactions in the blockchain, with there being a sound argument that in many cases someone committed to discovering the identity behind a bitcoin transaction could do so. This privacy paradox (combined with the digital nature of virtual currencies and the inherent difficulty in securing private keys) may in future attract the attention of data protection supervisors.

Consumer rights

The interface between virtual currencies and consumer protection is an interesting one. Structures for payment guarantees and refunds form an integral part of consumer protection frameworks in many countries but are not consistent with, for example, the irreversible nature of Bitcoin transactions. Virtual currencies are also typically not caught by deposit protection schemes operated in many jurisdictions.

Outlook

Virtual currencies are attracting more interest from users, institutions, governments and regulators. Organisations are also beginning to explore and exploit the blockchain technology which underpins Bitcoin. There are plenty of challenges ahead and increased growth in use will undoubtedly lead to greater regulatory scrutiny and oversight. However, this in itself is likely to lead to increased trust in virtual currencies and we predict continued growth in adoption. The lower transaction costs and other efficiencies that virtual currencies offer certainly present a big prize for financial institutions and users alike.

Our *team*

For more information about virtual currencies or about Allen & Overy's Fintech group, please ask your usual Allen & Overy contact or the authors of this report:

Simon Toms
Partner – M&A

Tel +44 20 3088 4681
simon.toms@allenovery.com

Michael Zdrowski
Associate

Tel +44 20 3088 4034
michael.zdrowski@allenovery.com

Rose Hall
Head of Business Development,
Life Sciences and TMT

Tel +44 20 3088 3618
rose.hall@allenovery.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,000 people, including some 527 partners, working in 45 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (associated office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Toronto
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.

This document is for general guidance only and does not constitute definitive advice.