www.mplegal.im

M&P LEGAL

REVIEW

Bitcoin and the £230 million pizza - a brief history

back home forward

contact us

July 2023

Advocates, Solicitors & Attorneys
an incorporated legal practice

july 2023

Bitcoin and the £230 million pizza - a brief history

Advocate Lorcan O'Mahony of M&P Legal takes a look at the development of cryptocurrency and unravels some of the mystery and jargon that surround it.

There is no doubt that, since the publishing of a now infamous whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" on 31 October 2008, cryptocurrency has come to infect and often obsess the public conscience. However, whilst many of us have heard the various buzzwords on the topic, to many more the area remains a mystery. In this article, we hope to somewhat demystify some of the basic concepts and keywords around the topic.

Bitcoin

The godfather of cryptocurrency.

Whilst the publishing of the whitepaper was not the first time the idea of a decentralised cryptocurrency had been mooted, it is seen by many as the genesis of the theoretical becoming the practical, and of what we see today.

It is perhaps a little known fact outside of the crypto-sphere that the publisher of the whitepaper – Satoshi Nakamoto – does not, as far as we know, exist. It is understood that Satoshi is a pseudonym, hiding a person or persons who have rather successfully kept their identity a mystery in the years since 2008. Fittingly, the smallest unit of Bitcoin is named after him; a 'Satoshi' is equivalent to 0.00000001฿– or (as of the time of writing) ~£0.0002.

At its most basic, Bitcoin is best described by its own whitepaper – a "purely peer-to-peer version of electronic cash…[which allows] online payments to be sent directly from one party to another without going through a financial institution".

Traditionally, if I were to send money to a friend, I would have to instruct my bank to send a certain amount to their account. It is a transaction based on trust; both my friend and I have to trust our respective institutions that they have sufficient funds held to our order, and that they will transfer and hold those funds to the order of the recipient.

Bitcoin, and cryptocurrency transactions more generally, are transactions based on proof. To understand how that works, one needs to understand the basics of the blockchain.

Blockchain

In a very basic description, the blockchain is a shared database with a non-editable history. Think of it like a very large and very secure cloud-based excel spreadsheet, shared by its users.

The blockchain is 'decentralised', meaning that it is not stored in one location, but rather across a network of 'nodes'. A

Bitcoin and the £230 million pizza - a brief history

singular node is a computer which makes up part of the relevant blockchain network, and the blockchain is copied and retained on each of those nodes simultaneously. As of the date of this article, there are estimated to be well in excess of 10,000 full and reachable nodes operating in respect of Bitcoin alone.

This is equivalent to tens of thousands of people having a copy of that excel spreadsheet on each of their computers, updating in real time so that every person with a copy can see every change being made and which has ever been made.

Each entry on that spreadsheet is a new 'block' in the 'chain' – equivalent to a new line in the spreadsheet. However, that doesn't mean just anyone can make a new entry.

Every new entry to the blockchain has to be verified, by multiple nodes, by solving several layers of cryptographic puzzle (hence the 'crypto' part of cryptocurrency). That way, there is no way to make a fraudulent entry on the blockchain – any false or manipulated information will be discovered and the transaction will quickly fail, if it even manages to be input in the first place.

Once verified, the transaction will form part of the blockchain forever. Every transaction can be traced and verified, all the way back to the very first transaction on the blockchain.

For a bit of history – the very first real-world bitcoin transaction is widely accepted to have taken place on 22 May 2010, when Laszlo Hanyecz promised 10,000 Bitcoin to anyone who would buy him two pizzas. A forum user ordered the pizza for him (using cash), and upon receipt of the pizzas, he duly sent the fee. 22 May 2010 is celebrated annually as 'Bitcoin Pizza Day', although maybe not by Laszlo Hanyecz; as of the date of this article, those pizzas are currently worth ~£230,000,000.

Many of its strongest critics claim that cryptocurrency is only good for criminal activity and money laundering. In fact, the opposite is true – there are few more permanently traceable transactions than a transaction on the blockchain, as a result of the very technology it is built on. As a result, and as I was once told by a client, "only stupid criminals use Bitcoin".

Wallets and Private/Public Keys

In most cryptocurrencies, a '**private key**' is a secure code, similar to a password, which allows users to access their funds on the blockchain. It is an essential piece of every cryptographic puzzle which must be solved in order to effect any transaction.

Bitcoin private keys are 64 characters long, and are made up of letters and numbers.

Bitcoin and the £230 million pizza - a brief history

As a result, there are 2^256 possible combinations; in real numbers, that means you have a 1 in 115 quattuorvigintillion chance of guessing someone's private key on your first go.

Obviously, it is not so simple to remember a 64 character private key off the top of one's head, and so many users prefer to secure their private keys in a '**wallet**'.

A cryptocurrency wallet is not like a traditional wallet or bank account. Your balance of cryptocurrency is not held in your wallet – your balance is stored (and secured) on the blockchain itself. Instead, your wallet holds your private key, and uses that to sign and authorise any outgoing transaction. The wallet is secured normally, and can be accessed using a normal password, or more securely using methods such as two-factor authentification.

Conversely, a '**public key**' – as the name suggests – can be shared, and is the method by which users can receive cryptocurrency. The public key is paired to the corresponding private key, and points to the address at which cryptocurrency may be received without ever needing to disclose your private key. It is equivalent to the public key being your email address, which you make public in order to receive emails, and the private key being the password you use to access your private inbox and send messages.

It is roughly estimated that 20% of all bitcoin private keys have been lost – through various means, such as the loss or destruction of physical wallets, forgetting a wallet password, or by the wallet owner passing away without making provision for their wallet to be accessed after death.

That very brief tour through the cryptocurrency basics only touches upon the tip of the iceberg in terms of the possibilities and uses of cryptocurrency and the blockchain.

Presently, cryptocurrency exchanges on the Isle of Man are not required to hold a licence in order to operate (except in certain circumstances when issuing their own coin/token, in which case they may require a Class 2 (Investment Business) or Class 8(4) (issue of electric money) licence). Instead, exchanges are only required to register as a designated business – with the same level of oversight as estate agents, payroll agents and tax advisors – when engaging in 'convertible virtual currency' business.

Many in the industry would welcome and encourage a greater level of oversight. From a regulatory perspective, the Isle of Man is behind many jurisdictions all around the world, including the likes of Canada, Ireland and Lithuania (which require exchanges to be registered and regulated as Virtual Asset Service Providers), Dubai (which requires exchanges to be registered and regulated by the Virtual Assets Regulatory Authority,) and

Bitcoin and the £230 million pizza - a brief history

the United Kindgdom (with cryptocurrency now falling under the regulatory purview of the FCA).

With increased regulation would come increased comfort and trust – not only from consumers and potential investors but also governmental agencies and those with a burgeoning interest. It would also give cryptocurrency a better reputation in the wider public sphere than the slightly negative perception it currently has in certain sectors. An exchange operating in and from a robustly regulated jurisdiction would allow it to jump right into the heart of the market, affording its users a greater level of reliance than most.

It will be interesting to follow the application of the EU's MiCA regulatory framework – coming into force over the coming years – across Europe, and the effect it will have in jurisdictions across the world. Local exchanges will be keeping a close eye not only on whether the Isle of Man will follow suit, but whether similarly attractive alternative jurisdictions do the same.

If you want to know more, are interested in cryptocurrency and Isle of Man law, or have concerns about protecting your cryptocurrency during or after your lifetime, please get in touch.

Lorcan O'Mahony is a senior associate advocate at M&P Legal with experience of advising cryptocurrency companies in the Isle of Man. This article does not give legal advice; please always consult a specialist if advice is needed.

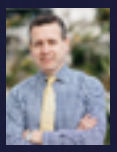
Please contact M&P Legal at law@mplegal.im or 01624 695800 if you have any enquiries.

M&P LEGAL REVIEW

back home forward
contact us

Profiles ..... Click on a profile to be taken to our web site for full details

John T Aycock
Managing Director
jta@mplegal.im



Damian P Molyneux
Director
dpm@mplegal.im

Amelia J Quinn
Senior Associate
ajq@mplegal.im

Michael J Mudge
Senior Associate
mjm@mplegal.im

David A Keates
Senior Associate
dak@mplegal.im

Lorcan O'Mahony
Senior Associate
lom@mplegal.im

Jamys E Quilliam
Associate
jeq@mplegal.im

Victoria H Kinrade
Associate
vhk@mplegal.im

Christopher J Murphy
Counsel and Consultant
cjm@mplegal.im

Carol A Young
Conveyancing Manager
cay@mplegal.im

Eve E Aycock
Trainee Advocate
eea@mplegal.im

Aiza H Khan
Trainee Advocate
ahk@mplegal.im