Virtual currencies and their potential role in cyber crime[1]

Authors
Kevin Law, MSc (Royal Holloway, 2015)
John Austen, ISG, Royal Holloway BA MSc FBCS NEBSS

1. Abstract

Virtual currencies have been promoted by many as offering great utility for consumers but much has also been said in recent years about their use in terrorism and other criminal activities. This article provides a short introduction to the legal landscape within the UK, the opportunities for illegal activity undertaken or supported by virtual currencies and the current barriers to those illegal activities.

2. Introduction

The motivation for people to engage with virtual currencies is many and varied. In any community there will always be marginal groups who, for whatever reasons, do not trust the Government or administration in the areas in which they reside, or for whom the data collection and mining by large corporate entities causes significant distrust and nervousness and I make no judgement about their personal belief systems or their frames of reference. For these people an online payment system which is anonymous, or which feels anonymous and is outside the control of those they distrust will be seen as having great utility. For many ordinary citizen the additional utility provided by virtual currencies is at the moment fairly limited, there is little one can do with a virtual currency that one cannot do with cash or a debit or credit card. For the citizen with criminal intent virtual currencies offer a unique opportunity to use money in a pseudo-anonymous way to undertake illegal activity. I will discuss the current legal landscape before going on to discuss how virtual currencies might be used when considering the potential for illegal activity.

3. The Law and virtual currencies

Policing the Internet has been a matter of significant discussion in many forums ever since the first online crime was detected over forty years ago. My intention here is to summarise the law within the UK as it currently stands and how it might be brought to bear in dealing with crime related to digital currencies. Within the UK the legislative landscape changes slowly and updates to legislation are few and far between. Interpretation of the nuances of a piece of legislation happen in court presided over by a Judge and often challenged in the court of appeal at which point they are considered case law and provide the legal profession with amplification and direction for future cases. As yet there have been no major cases that have needed to address the nuances that relate to virtual currencies but these will undoubtedly happen over time.

Whether or not virtual currencies can be considered as money in their true form is debatable. In some jurisdictions it is treated as money, in others as property. However it should be noted that

[1] This article is to be published online by Computer Weekly as part of the 2016 Royal Holloway info security thesis series. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full MSc thesis is published on the ISG's website.

these definitions have largely arisen in order to apply some form of taxation on virtual currency purchases or ownership. Virtual currencies are best thought of as a store of value, an asset which has an inherent value but which is separate to the currency in use in the particular locale. It should however be noted that much like the frequently quoted tulip bubble of the 17th century the bubble can quickly burst and the store of value can lose some or all of its value overnight. It has been widely reported, albeit largely unsubstantiated, that during the Greek monetary crisis and the subsequent "bailout" discussions in July 2015, Bitcoin was used as a store of value. A spike in transactions was certainly seen during the weekend leading up to the referendum and in the few days afterwards but whether this was as a direct result of Greek citizens attempting to mitigate their concerns about the stability of the euro in their country remains a matter of speculation.

The legal definition of virtual currencies is an important one, some legislation and the case law that has derived from that legislation draws a distinction between money, property and information. For instance the Theft Act 1968 definition states "'Property' includes money and all other property, real or personal, including things in action and other intangible property." However case law in Oxford v Moss (1979) found that information could not be stolen. Therefore we might assume that as a piece of virtual currency is nothing more than information it cannot be stolen. However if the courts decide it to be money it could be stolen. The same act defined the offence of blackmail in which "the nature of the act or omission is immaterial" leading one to conclude that blackmail in exchange for virtual currency is an offence. The Computer Misuse Act (1990) is concerned with unauthorised access and impairment of systems so would apply to virtual currencies. It also only requires "one significant link with domestic jurisdiction", an important nuance when prosecuting online crime. The Terrorism Act (2000) refers to "money" and draws no distinction between cash, cheques, and electronic or virtual funds but also talks about retention, concealment, transferring and removing money or other property. The Proceeds of Crime Act (2002) talks about money, property and assets, an all-encompassing description that must include virtual currency. The picture is confused and resolving it will rely heavily upon how virtual currencies come to be defined within the legal system.

4. Important operational aspects of a typical / popular virtual currency

Over the last couple of years Bitcoin has emerged as the de-facto standard within the virtual digital currency arena. It wasn't the first digital currency but it solved a number of seemingly immutable problems that had held back the popular adoption of virtual currencies. For this reason I will use it to explain some of the important aspects of a virtual currency. More in-depth discussion can be found in the full project report available on the ISG website.

Bitcoin operates without any central authority. Neither is there a place to go if you lose access to your currency or it gets stolen from you. Bitcoin operates using an entirely public and distributed ledger, organised as a linked list of blocks of transactions with transactions arranged into a binary tree using hash pointers to link each node. The use of a hash pointer provides a mechanism by which any modification in the transaction list is immediately obvious as the hash at the top of the tree is dependent upon the two children and so on right to the bottom of the tree where the transactions reside. This also has the benefit of limiting the checking required when verifying transactions as it is only necessary to calculate the hash of the sibling and then the ancestors. Nodes on the network can be operated by anyone who wishes to download the software and apply resource to maintaining a copy of the ledger. Some nodes also choose to undertake the proof of work puzzle which forms transactions into blocks. When a person creates a transaction they publish it to a node on the network and the transaction is then replicated across the system. Transactions are verified by each node on receipt, to ensure that the value is legitimate, that it has not been spent before and that it has a valid digitally signature. If the verification fails it does not get replicated. Across the network there is no concept of identity, an individual can use an unlimited number of identities and these are represented by a base58 encoded string or a QR code. The identity is derived systematically from the public key that was created alongside the private key when the identity was "created". With the obvious exception of the genesis block new Bitcoins are created as a reward for the nodes that have processed transactions into blocks. In order to regulate the reward mechanisms for creating blocks, in addition to verifying the validity of transactions and forming a hash pointer binary tree, nodes must also solve a hashing puzzle. The difficulty of this puzzle is flexed over time based upon the computing power applied to solving the problem, and a new block is created roughly every 10 minutes.

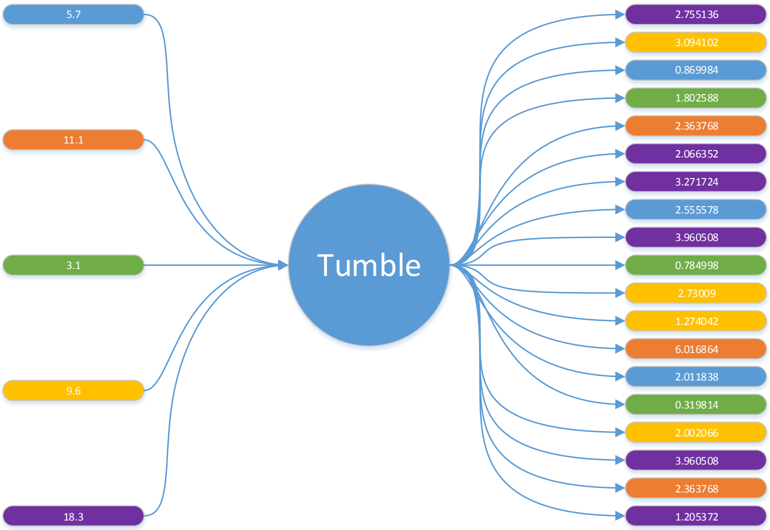
Bitcoin address and QR code

5. Anonymity and Pseudonymity

Anonymous is defined as "of unknown name; of unknown or undeclared source or authorship; impersonal". Bitcoin is touted in the popular press and by various online sources as anonymous but as we have seen above this cannot be the case. Every transaction is very publicly published and is clearly attributed to a declared source, the Bitcoin address. Pseudonymous is a more apposite term: "written under a fictitious name". Pseudonymity is an important element in the execution of a number of crimes, a bank robber doesn't walk into a high street bank with the intention of making an illegal withdrawal without concealing his identity. In digital crimes the criminal needs to conceal his identity in a similar way. The criminal must also make efforts to conceal that element of the crime from the observer.

In order to effectively use Bitcoin in the execution of a crime the criminal must disassociate themselves from the coin itself and hence from the crime. One of the key opportunities which digital currencies offer is the ease with which a perpetrator can operate numerous identities. However keeping these identities separate is not an easy undertaking. If you are operating an illegal business handling hundreds or thousands of small transactions every month it would be very easy to have every transfer made to a separate identity, it is as simple as generating a fresh address and some online business provide that as part of the standard payment package. However the use of multiple addresses just gives you the same problem that the criminal has in a cash business: a large number of small denomination transactions is not dissimilar to a large pile of £5 notes. Some currencies do operate a system in which they will join transactions together so that it isn't clear which recipient is receiving value from which sender. There are also coin "tumbling" services where value from a number of senders goes into a central pot, a variable fee is taken and the remaining value is split into a number of transactions.

One has to question why anyone would obscure transactions in this way if there were acting in a wholly appropriate way. Setting up a mixing and tumbling service with very low fee would be an excellent source of intelligence for a law enforcement organisation and would be at least self-funding if not profit making for the public purse. In order to maintain the pseudonymity perhaps even promoting it to anonymity the criminal needs to augment the open but disassociated nature of digital currencies with some additional mitigation such as concealing their IP address and the places where they connect to the internet.



Transaction tumbling

6. Crimes using virtual currencies

The crimes that might be assisted by virtual currencies are predominantly those associated with cash transactions or the movement of monetary value. These fall into broadly three categories;

- *Moving and mixing* – Whether it is money laundering, managing donations in support of terrorism or just moving value without falling foul of currency restrictions or taxation the desire to receive, move and convert to cash are the key attributes. Virtual currencies certainly facilitate the reception and movement of funds. A transaction is immediately replicated across the entire system irrespective of geographic location as soon as it is created and verified. The unspent value will be there in the blockchain until the recipient transfers the value elsewhere. In many respects the open transaction model means that unless the criminal employs a mixing or tumbling service all value can be traced back to its origin. If you know the starting point of an illegal transaction you can trace it through the system to the point it is cashed out or where a legal transaction has taken place. As we will see later on the ability to convert between cash and virtual currencies is the problematic aspect in achieving these crimes.
- *Extortion* - Virtual currencies have been used in a number of attempts to extort money either from people who have accidentally installed trojans or who are being threatened with distributed denial of service attacks or the release of stolen personal data. The transparency of the blockchain means that whilst the criminals could receive the value it could be traced to the cash out point where more traditional law enforcement intervention would be required.
- *Market places* - A great deal has been written in the popular press about online market places on the dark web, receiving value for drugs and other illegal materials using virtual currencies. In the early days value would be held by the online marketplace provider who would then transfer it to the vendor, less a fee once the transaction was complete. The advent of multi-sig, multi-output transactions means that marketplaces no longer need to hold large quantities of virtual currency. The transparency of the blockchain does mean that unless the marketplace and vendor takes steps to churn the recipient address on every transaction every payment will get linked to the marketplace or seller.

The difficulty of converting virtual currencies into cash is the severely limiting factor in the use of virtual currencies in the committing of crime and it is this factor alone that is stopping virtual currencies from becoming a major enabler in cyber-crime. Although there are many coin exchanges in the UK which will exchange sterling for Bitcoin the majority of them are run in accordance with the UK and EU regulations on money laundering. They insist that customers have a UK bank account or credit card, they expect customers to be able to provide and verify mobile telephone numbers, addresses and provide identification. If you can provide all of these confirmations and are content to work in sufficiently small quantities to avoid being noticed then perhaps it would be easier not to convert the money to Bitcoin.

A second option to convert cash to Bitcoin is to visit a Bitcoin ATM. At present there are only three operational ATMs within the M25 (approximately 1,100 sq. miles which includes central London) and less than 20 in total in the UK. Most ATMs do not require identification or registration at the moment but the maximum transaction is £1,500. If you have large quantities of money to change you could easily spend all day feeding cash into the ATM and apart from the obvious inconvenience it would quickly become very obvious what was going on. Alternatively you could use an army of smurfs to handle the cash for you at which point you could just as easily be putting the cash into a bank account and avoiding the transaction charges and commission.

The final option to change cash into Bitcoin is to go to one of the places where people assemble to exchange Bitcoin for cash and vice-versa, sometimes referred to as a “meet-up”. It is unlikely that there would be sufficient Bitcoin available at a meet-up to satisfy the needs of anything other than a casual criminal. An alternative would be to take your payments in Bitcoin and move the problem of converting cash to virtual currency to your purchasers. This does give rise to a different problem because Bitcoin transactions aren’t immediate. Having moved your currency into virtual currencies cashing out is equally difficult unless you can buy everything you need in Bitcoin which at the moment very few people have been able to achieve.

7. Crimes against Bitcoin

The greatest threat to virtual currencies is dishonest exchanges and wallet providers or attacks against legitimate exchanges and wallets. Many consumers purchase value from exchanges and store the value in a wallet linked to an exchange. If a criminal breaks into their systems and steals the private key(s) and transfers all the value the consumer has very little recourse.

An attacker could change the recipients address on a website or in a QR code in a retail environment but eventually the operator would notice that the value they thought they should be receiving wasn’t appearing and would change their address.

Another attack, the early block attack, relies upon a node getting very lucky and solving the hashing puzzle very quickly and instead of publishing that achievement they hold it back so that they can create a number of blocks and then force a fork with them taking the reward for a series of blocks.

Ever since virtual currencies have become popular there has been a concern that because systems rely upon distributed consensus if someone is able to control 51% of the available computing power within the network they also control the consensus. The entity with 51% would then have control over the entire system and could attack or poison the currency. The problem with this is that in order to reach the 51% position an attacker would have made a significant investment in computing power and it would be more sensible to keep the currency stable and continue to reap the rewards of being the first to solve the hashing puzzle the majority of the time.

8. Conclusion

As we have seen in the earlier sections of this abstract opportunities certainly exist for digital currencies to be exploited for the purposes of cyber-crime. The reasons why this has yet to happen on a large scale are likely to stem from the cash in and cash out difficulties. Focussing legislation and regulation in this area will consequently be a priority for the future. How much you can virtually know your virtual customer is a challenge as is the entirely non-geographical nature of virtual currencies. Many administrations have sought to licence or regulate exchanges and business accepting virtual currencies and whilst this will have an impact upon legitimate businesses within the geographic area it will do nothing to control the criminals who exist without a geographic anchor.

Biographies

Kevin Law is a 2015 MSc graduate in Information Security from Royal Holloway. He is responsible for all aspects of security within a major Government Department managing risks associated with all aspects of personal, procedural, physical and technical security. Prior to this he was IT Security Officer for a major Department of State and previous to that the security manager for a desktop service providing a variety of office and business functions to over 26,000 users.

John Austen (BA, MSc, FBCS, NEBSS) is a consultant lecturer in the Information Security Group at Royal Holloway University of London. He is a specialist in cyber-crime and investigation techniques, international law, and organisational security. After studying at the FBI National Academy in Quantico, Virginia he became the founder and Head of The Computer Crime Unit New Scotland Yard from 1984 - 1996, an operational specialist unit and the forerunner of the National Hi-Tec Crime Unit and the e-Crime Unit. He was the first Chairman of the Interpol Computer Crime Committee, from 1990 to 1996, which was responsible for the worldwide standardisation of Police procedure and international training in the area of cyber-crime investigation and digital forensics. He was the 2003/4 President of the U.K. Chapter of I.S.S.A. (Information Security Specialists Association).