Virtual currencies and their potential role in cyber crime
Kevin Law

Technical Report
RHUL–ISG–2016–9
5 April 2016

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom
Virtual currencies and their potential role in cyber crime

Supervisor: John Austen BA MSc FBCS NEBSS

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:
# Table of Contents

List of figures and tables ........................................................................................................ 3

List of abbreviations and acronyms ..................................................................................... 4

1. Executive Summary ........................................................................................................ 5

2. Introduction .................................................................................................................. 6
   a. Nomenclature ........................................................................................................... 6

3. The law and virtual currencies ...................................................................................... 7
   a. Money ....................................................................................................................... 7
      i. Commodity money ............................................................................................... 7
      ii. Representative money ....................................................................................... 7
      iii. Fiat money ......................................................................................................... 7
      iv. Store of Value .................................................................................................... 7
   b. UK Legislation .......................................................................................................... 8
      i. Theft Act (1968) .................................................................................................. 8
      ii. Computer Misuse Act (1990) ............................................................................ 8
      iii. Terrorism Act (2000) ....................................................................................... 9
   c. UK Regulation ......................................................................................................... 10
      i. The Money Laundering Regulations (2007) ......................................................... 10

4. Operation of a “typical” virtual currency ...................................................................... 11
   a. Cryptographic Principles and Primitives ................................................................ 11
      i. Hash Functions .................................................................................................... 11
      ii. Hash Pointers ...................................................................................................... 11
      iii. Digital Signatures ............................................................................................. 13
   b. Bitcoin Limitations .................................................................................................. 14
   c. Units and Transactions ........................................................................................... 14
   d. Blockchain .............................................................................................................. 15
   e. Decentralised Consensus ......................................................................................... 16
   f. Distributed consensus ............................................................................................. 16
   g. Consensus without identity .................................................................................... 17
   h. Incentives ................................................................................................................ 18
   i. Proof of work .......................................................................................................... 19
   j. Blockchain forking .................................................................................................. 22
   k. Bitcoin in Use ......................................................................................................... 24
   l. Key storage .............................................................................................................. 24
   m. Hot Storage ............................................................................................................. 26
   n. Cold Storage ........................................................................................................... 26
   o. Key splitting ........................................................................................................... 27
   p. Altcoins ................................................................................................................... 28

5. Exploiting virtual currencies for criminal purposes ....................................................... 30
   a. General notes ......................................................................................................... 30
   b. Jurisdictional variances ......................................................................................... 30
   c. Anonymity and Pseudonymity .............................................................................. 30
   d. Theft ...................................................................................................................... 31
   e. Money Laundering .................................................................................................. 32
      i. Consolidation ....................................................................................................... 32
      ii. Layering ............................................................................................................. 33
iii. Repatriation and Integration .................................................................................. 33

f. Laundering with Bitcoin ......................................................................................... 34
g. Funding Terrorism .................................................................................................. 36
h. Illegal movement of funds ....................................................................................... 36
i. Extortion and Confidence Tricks ........................................................................... 36
j. Online marketplaces ............................................................................................... 37
k. Tumbling, Mixing and Splitting .............................................................................. 37
l. Dissociative Activity ................................................................................................. 39
   i. Places .................................................................................................................. 39
   ii. Hardware ............................................................................................................ 39
   iii. Identities .......................................................................................................... 39
   iv. Anonymity services ......................................................................................... 39
m. Crimes against Bitcoin ........................................................................................ 39
   i. Malware ............................................................................................................. 39
   ii. Dishonest exchanges / online wallets ............................................................... 40
   iii. Exchange hacking ............................................................................................ 40
   iv. Double spending .............................................................................................. 40
   v. Change the address ......................................................................................... 41
   vi. Early block attack ......................................................................................... 41
   vii. 51% attacks .................................................................................................... 41
n. Silk Road ................................................................................................................ 42

6. Possible mitigations to reduce the negative impacts of virtual currencies .......... 44
   a. Single controlling entity .................................................................................... 44
   b. Regulation .......................................................................................................... 44

7. Conclusion ............................................................................................................... 46

8. Bibliography .......................................................................................................... 47

List of figures and tables.
Figure 1 - Hashed pointer linked list .......................................................................... 11
Figure 2 - Merkle tree ................................................................................................ 12
Figure 3 - Merkle tree validation ............................................................................... 13
Figure 4 - Blockchain and transactions .................................................................... 15
Figure 5 - Mining difficulty over time ....................................................................... 20
Figure 6 - Blockchain fork ........................................................................................ 22
Figure 7 - Virtuous circle ........................................................................................... 23
Figure 8 - Public key to Bitcoin address .................................................................... 25
Figure 9 - Bitcoin address and QR code ................................................................... 26
Figure 10 - Coinjoin separate transactions ............................................................... 28
Figure 11 - Coinjoin transaction ............................................................................... 29
Figure 12 - Wikileaks donation page ......................................................................... 31
Figure 13 - Transaction tumbling .............................................................................. 38
Figure 14 - Tumbling example .................................................................................. 38
Figure 15 - Silk Road payment scheme .................................................................... 43
List of abbreviations and acronyms.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>United States Dollar</td>
</tr>
<tr>
<td>£</td>
<td>Pound sterling</td>
</tr>
<tr>
<td>altcoin</td>
<td>Alternative virtual currency system derived from Bitcoin</td>
</tr>
<tr>
<td>ARA</td>
<td>Asset Recovery Agency</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application specific integrated circuit</td>
</tr>
<tr>
<td>B</td>
<td>Billion</td>
</tr>
<tr>
<td>BTC</td>
<td>Bitcoin (when expressed as a currency)</td>
</tr>
<tr>
<td>CMA</td>
<td>Computer Misuse Act</td>
</tr>
<tr>
<td>ELC</td>
<td>English Common Law</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>Ghz</td>
<td>One billion cycles per second</td>
</tr>
<tr>
<td>H(*)</td>
<td>A cryptographic hash pointer to an entity</td>
</tr>
<tr>
<td>H(x)</td>
<td>The cryptographic hash of value x</td>
</tr>
<tr>
<td>ISIL</td>
<td>Islamic State in Iraq and the Levant</td>
</tr>
<tr>
<td>M</td>
<td>Million</td>
</tr>
<tr>
<td>Mhz</td>
<td>One million cycles per second</td>
</tr>
<tr>
<td>NCA</td>
<td>National Crime Agency</td>
</tr>
<tr>
<td>Nonce</td>
<td>Number used once</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First protocol</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-peer</td>
</tr>
<tr>
<td>QBD</td>
<td>Queens Bench Division</td>
</tr>
<tr>
<td>QR</td>
<td>Quick response</td>
</tr>
<tr>
<td>R</td>
<td>Regina</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>SOCA</td>
<td>Serious Organised Crime Agency</td>
</tr>
<tr>
<td>Thz</td>
<td>One trillion cycles per second</td>
</tr>
<tr>
<td>Tor</td>
<td>The Onion Router</td>
</tr>
<tr>
<td>VAT</td>
<td>Value Added Tax</td>
</tr>
</tbody>
</table>
1. Executive Summary.
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 reason 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. They may be considered geeks, libertarians, rebels, anarchists or revolutionaries 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 outwith of the control of those they distrust will be seen as having great utility.

For the ordinary citizen the additional utility provided by virtual currencies is limited and there is little one can do with a virtual currency that you cannot do with cash or a debit or credit card. In fact it could be said that virtual currencies are of less utility because unlike the cash in your pocket in order to use a virtual currency it is necessary to convert some real currency into the virtual currency in order to use it to buy the thing you want and then for there to be a wait period whilst the transaction is verified and before the value is transferred. If you are buying a coffee and a sandwich the retailer may be happy to take the risk with a small virtual currency transaction, if you are buying a supercar, a mansion or a train ticket perhaps the risk will be seen as too great. For the businessperson the acquisition of virtual currencies can be a profitable enterprise. Early adopters enjoyed large gains from “mining” currencies however these gains have dwindled over time for two particular reasons. The development of custom mining rigs using application-specific integrated circuits (ASIC) have increased the ease and speed of the “proof of work” activity however this has been countered by the virtual currency systems which throttle the mining of “coins” according to the amount of processing applied to the system as a whole. This has had the effect of raising the cost of entry for prospective “miners” and caused the establishment of large collaborative groups that share the proceeds of mining. The cost of entry together with recent drops in the prices of virtual currencies has made “mining” to be a less profitable exercise. I’ll delve deeper into the process of “coin” creation, proof of work and transaction processing in greater depth in section 4 when I discuss the operation of a typical virtual currency. More and more business are providing mechanisms to purchase using virtual currencies although I suspect that for the time being at least it is more to do with creating a newsworthy story to promote their business than it is because they are loosing custom because they don’t offer the service. As we will see later virtual currencies are inherently unstable and very quickly become a string of valueless numbers if there is no way to convert them to a traditional currency.

For the criminal or the citizen with criminal intent virtual currencies offer a unique opportunity to use money in a pseudo-anonymous way to undertake illegal activity and I’ll discuss the current legal landscape in section 3 before going on to discuss how that might be used when considering the potential for illegal activity in section 5.

Finally in section 6 I will discuss how the negative effects of virtual currencies may be mitigated and the potential impacts resulting from those interventions.
2. Introduction.
One of the challenges in any project of significant size or which is researched over an extended period is that during the course of the research and documenting there can be major changes in the environment. The world of virtual currencies over the last 24 months has been an area of significant public interest. Virtual Currencies have seen an increased interest from both the public as users but also from government and financial authorities over the last year. It is highly likely that by the time is project is submitted or is assessed that there may have been a major change in the landscape. That change might be as a result of the collapse of one of the major currencies or of a currency exchange. There is a similar risk that national or international regulation will have an impact upon usage, utility or legality of these currencies. Having said that, it is likely that whatever the legal and regulatory landscape whilst virtual currencies exist their usage within the criminal community will continue for as long as they provide a mechanism to make, launder or cash out crime.

a. Nomenclature.
Wherever possible within this project I will use the term virtual currency or digital currency to describe a non-traditional currency the terms are to all intents and purposes interchangeable and I will use them as such. The terms “currency”, “money”, “coin” etc. in relation to digital or virtual money can easily be disputed and I’ll make no judgement about their appropriateness, they are common reference terms and I will use them as such. Within section 3 below I will briefly describe the different types of money and monetary development but only to provide a context for the legislative aspects which I will then go on to discuss. Where I am describing the function of a particular virtual currency such as in section 4 below I will refer to it by its common name. In doing so it must be noted that whilst criminals may be using virtual currencies I will make no judgement about the complicity of those providing services which support those currencies and there is no inference or implication of complicity in any 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. This section does not intend to be an exhaustive and detailed documentary of those discussions or the associated issues; neither is it intended to form a detailed legal opinion. My intention here is to discuss 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. It should however be noted that at the time of writing there have been no significant UK cases which have included digital or virtual currencies as a primary factor and therefore case law necessary to make a definite assertion has yet to be defined.

a. Money

In preparation for a discussion of the legislation it is worthwhile briefly documenting the various accepted definitions of money.

i. Commodity money.

The use of commodity money dates back many centuries and has tended to be the first step that developing communities take in order to replace a bartering system. Commodity money is made from something that has an inherent value within the community. In many instances it has been a precious or semi-precious metal or stone although economies have been based upon commodities as diverse as rice, stone arrow heads, shells, decorated belts and according to a article by Justin Scheck (1), in the US prison system by cans or packets of mackerel fillets.

ii. Representative money.

Representative money as it name suggests is a representation of the value of a particular quantity of a commodity. The actual value of the coin or banknote is less than the quantity of the commodity that it represents. Many people will be familiar with the Gold standard where a unit of currency corresponds to particular quantity of gold.

iii. Fiat money.

Fiat money can be considered a type of representative money however the important nuance is that it derives it’s value from legal or government regulation and it is those processes that define and maintain it’s value.

iv. Store of Value.

A store of value is an asset which has an inherent value but which is separate to the currency in use in the particular locale, sometimes this occurs to mitigate government instabilities, high inflation or currency devaluation. A store of value has taken a number of forms over time and geographic area, property, drugs, stocks and shares have all been used in this way and it is probable that virtual currencies will fall into this category. It has been widely reported albeit largely unsubstantiated that during the Greek monetary crisis and the subsequent “bailout” discussions in July 2015 that Bitcoin was used as a store of value and.

A spike in transactions was certainly seen during the weekend leading up to the referendum and in the few days thereafter 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 is currently a matter of speculation.
b. UK Legislation

i. Theft Act (1968)
The Theft Act (2) defines "a person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it". The act goes on to define "dishonestly", "appropriates", "property", "belonging to another" and "permanently depriving" however the only of these which is germane to this paper is property.

At section 4(1) property is defined thus "'Property' includes money and all other property, real or personal, including things in action and other intangible property." At the time of writing the definition of money undoubtedly was notes and coins of a particular currency however this could extend to digital money however it does depends upon the definition of money which the courts chose to take. As briefly referred to above Oxford v Moss (1979) related to the case of a student of engineering at Liverpool University who in June 1976 stole an exam paper. The student had no intention of depriving the university of the exam paper, his intent was to borrow it in order to obtain the information it contained and then replace it without being detected. The stipendiary magistrate decided that theft had not occurred as the student hadn't permanently deprived the owner of any property tangible or intangible. The prosecutors appealed the finding, which was heard in the Divisional Court QBD (3) by three distinguished Judges who agreed with the stipendiary magistrate and dismissed the appeal. In the recorded finding Mr Justice Smith gave the opinion that there is no property in information, which his two fellow judges concurred with. Hence it would appear that it is not possible to steal information and as a piece of digital currency is simply a piece of information contained in a computer file it cannot be stolen. If the key had been printed on a piece of paper then if the person stole the piece of paper and did not return it they would be guilty of theft but the chances of a prosecution for the theft of a piece of paper ever coming to court feels highly unlikely.

Section 21 of the Theft Act also contains the offence of blackmail. Blackmail is committed when a person makes an unwarranted demand with menaces 21(1) (2) section 21(2) goes on to say that “the nature of the act or omission is immaterial”. The wording of the legislation implies the outcome of the blackmail does not matter therefore a demand for a virtual currency with menace could constitute a blackmail offence.

ii. Computer Misuse Act (1990)
The Computer Misuse Act (4) arose from a recommendation of Lord Justice Brandon of Oakbrook who was considering an appeal to the House of Lords in the case of Regina v Gold and Schifreen. Stephen Gold and Robert Schifreen had been prosecuted under section one of the Forgery and Counterfeiting Act (5) after they had obtained an engineer’s username and password for British Telecom’s Prestel system after observing him login. They had used the login and password to access the system and to gain access to the message boxes of a number of users most notably The Duke of Edinburgh. The pair where charged with creating a false instrument which had been “made” when they logged into the system using credentials that were not theirs but which the system had accepted as genuine (6). Whilst the initial prosecution was successful upon appeal to Criminal Division of the Court of Appeal and The House of Lords the prosecution was overturned and the Justice Brandon
observed the “The Procrustean\(^1\) attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury”. This ruling led to a review of English Common Law (ELC) that confirmed the belief that there was no statute under which the offence of “hacking” could be successfully prosecuted and this led to the Computer Misuse Act.

The computer Misuse Act sets of a number of offences;

Section 1 – Unauthorised access to computer material
Section 2 – Unauthorised access with intent to commit or facilitate commission of further offences
Section 3 – Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Three further offences were added in 2006 by the Police and Justice Act;

Section 3.A – Making, supplying or obtaining articles for use in offence under section 1 or 3.

One of the important aspects of the act is that it (only) requires “one significant link with domestic jurisdiction”, so an offence committed in the UK against a computer system in a foreign land is equally prone to prosecution as an offence committed in the UK against a UK system, an offence committed against a UK company on a system hosted overseas by a perpetrator who is not a British Citizen or a British Citizen committing an offence overseas against an overseas company on a system not within the UK.

iii. Terrorism Act (2000)
At section 18 of the act (7) the offence of money laundering in relation to terrorism is defined. The act simply refers to “money” and draws no distinction between cash, cheques, and electronic or virtual funds. The act makes it an offence to retain or conceal terrorist property (money and other property) by hiding, transferring or removing or in any other way being concerned with retention or concealment. One might argue that whilst not within the strict definitions of the act converting cash into virtual currency would be a form of concealment or transfer however this would need to be tested in a court of law.

The Proceeds of Crime Act (8) was enacted primarily to allow for the recovery of money and assets that had been gained as a direct result of criminal behaviour. Asset recover orders were then given to a new agency instituted by the act the Assets Recovery Agency (ARA). ARA were responsible for pursuing and liquidating the property and returning the money to the Government. The ARA was abolished as a result of the Serious Crime Act (9)(2007) and became part of the Serious Organised Crime Agency (SOCA) in 2008, which in 2013 was reformed into the National Crime Agency (NCA). In evidence given to the Home Affairs Select Committee in 2015 the Director-General NCA Keith Bristow QPM explained that it had been difficult for NCA to recover the assets which had been ordered by the courts and that although they were progressing a number of large asset recovery orders a number of those orders had been handed down with quantities that were unrealistic or for assets which where no longer reachable.

\(^1\) In reference to Greek mythology where Procrustes would fit his houseguests to their bed by either stretching them on the rack or by chopping off some or all of their legs.
Money laundering is defined in section 340 (11) and is defined as follows;

“(a) constitutes an offence under section 327 [concealing], 328 [arranging] or 329 [acquiring],
(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),
(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or
(d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.”

In addition to money laundering the act also covers all other forms of property which have been financed by the proceeds of crime, until such time as this has been tested in the courts it will be impossible to predict whether the definition of property includes virtual currency or whether the precedent set in Oxford v Moss in regard to information not being intangible property will remain.

c. UK Regulation
i. The Money Laundering Regulations (2007)

As the name suggests these regulations (10) refer to the laundering of money and apply to a number of business sectors not just banking. There is a direct correlation between the provisions described in the EU Directive 2005/60/EC (11), which was later amended by 2009/110/EC (12) and those provision enacted within the UK legislation in the money laundering regulations. The act puts an onus upon individuals and businesses engaged in credit and financial businesses, accountants, estate agencies, auctioneers, casinos, money service businesses (cheque cashing and international transfers) and high value dealers (a catchall for individual or apparently linked transactions amounting to €15,000). The act specifically refers to cash, defining it;

“‘cash’ means notes, coins or travellers’ cheques in any currency”

The act does not include any specific provisions in relation to the usage of digital or virtual currencies although it does talk about “representation of monetary value”. In particular the definition of “money service business” might lead one to conclude that operating a digital currency could well fall within the purview of the legislation. It defines a money service business as;

“‘money service business’ means an undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or cashes cheques which are made payable to customers;”

The regulations requires that users of the above services must be able to adequately identify themselves using either authoritative documentation or information received from “a reliable and independent source”. It is the responsibility of the person or business providing the service to undertake that due diligence at the same time it also the responsibility of service provider to identify suspect transactions or groups of transactions and report them to the NCA.
4. Operation of a “typical" 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 by any means however it solved a number of seemingly immutable problems that had held back the popular adoption of virtual currencies. The foundations for Bitcoin where laid when Satoshi Nakamoto described a pattern for a peer-to-peer(P2P) electronic cash system in 2009 (13). Nakamoto’s paper acknowledged the ground breaking work undertaken by David Chaum firstly in describing a blind signature scheme (14), relying upon a central authority that could sign transactions without knowing the users key and latterly with Amos Fiat and Moni Naor in their work on untraceable electronic cash (15). In doing so he described a system with an entirely public ledger, or blockchain as it became known, a solution to the distributed consensus problems that had previously necessitated management by a central authority and a solution to the double spending problem. Since Nakamoto’s paper numerous altcoins have emerged which either replicate the Bitcoin system or seek to build on the Bitcoin model to either improve or evolve it. As the Bitcoin model has become the de-facto implementation and the one to garner significantly larger usage I will use it as the example within this section. Having done so I will extend the description using the lesser popular systems designed to add anonymity to the Bitcoin model.

a. Cryptographic Principles and Primitives

Before starting to delve into the detail of Bitcoin it is worthwhile alighting for a moment upon the cryptographic primitives upon which it is built. It is not my intention to explain in detail the function of these primitives but would direct the interested reader to the book written by Prof Keith Martin (16), which supports the Introduction to Cryptography and Security Mechanisms module at Royal Holloway’s Information Security Group.

i. Hash Functions

A hash function is designed to take an arbitrarily long input and reduce it to a fixed length output. From a practical perspective it should be a mathematical function that is easy to calculate but imposible to undo without an exhaustive attack. From a security perspective there are three important functions that a hash function should discharge. Firstly a hash should be pre-image resistant meaning that if you have the hash of a value which I’ll refer to from now on as H(x) it should be very difficult to derive the value (x) without progressively checking every value of x. Secondly a hash value should be second pre-image resistant meaning that knowing x and H(x) it is very difficult to find y where H(y) is the same as H(x). Thirdly it is collision resistant meaning that it is difficult to find an H(y) which is the same as H(x).

ii. Hash Pointers

Building on the principle of the cryptographic hash it is possible to use this to build a list the contents of which cannot be modified. If you consider a typical linked list structure where every entity links back to the previous entity it would be very easy to include in an entity not just a pointer to the previous entity but also a hash of that entity, a hash pointer (referred to hereafter as H(*)). In doing so you create a tamper evident list as it would be impossible to modify an entity without recalculating the hash contained in all the subsequent entities.

Figure 1 - Hashed pointer linked list
The down side of the H(*) linked list is that in order to validate the previous block it is necessary to calculate the hash of every entity which precedes it so the time to validate grows lineally as the linked list grows. This might be acceptable in a simple application but in the context of a virtual currency block chain it might become a drain on the resources of consumers, especially in cases where the computing platform they are using may have limited capabilities, such as a smart-phone. There is a second issue as there is only one node on the list to which you can add data, if you are doing any proof of work hashing or the data blocks are significantly big and therefore take time to hash you risk having transactions backing up whilst the block is hashed and linked. If a virtual currency transactions were implemented in this way as the hashing delay increases so would the time to validate a transaction (the equivalent of clearing a cheque in the traditional banking system) hence some mechanism is required to regulate the wait time. Until the block was complete any transactions it contained couldn’t be re-spent without the risk of double spending.

A development on the H(*) linked list is a binary tree with hash pointers also known as a merkle tree in Figure 2 - Merkle tree. Merkle in (17) describes how you can incorporate a H(*) into a binary tree structure which provides a tamper evident structure where each node includes a H(*) to next node down the tree nodes thereby provide a tamper evident list. The merkle tree has several advantages over the linked list, it provides a system where multiple nodes can all be verified with a single hash. It also reduces the tree validation effort because unlike a linked list where every hash in the list needs to be verified right back to the first entity in the list it is only necessary to calculate the hash of each parent not every entity in the structure.
iii. Digital Signatures

Digital Signatures provide an important service within most digital currencies because they deliver a mechanism to assure the authenticity of information. In order to do so a digital signature needs meet several requirements.

- Only the person whose signature appears on the data should be able to sign it.
- You shouldn’t be able to remove the signature from one data item and apply it to another data item without it being detectable.
- You shouldn’t be able to sign something and then later on effectively deny that signature so the scheme should provide non-repudiation.

In order to provide this service most digital signature schemes use a form of public key encryption however it is wrong to think of this as simply encryption and decryption as the problem is more complex. In order for a digital signature scheme to be effective you need to be sure that the item bearing the signature is the item which has been signed and that the signature hasn’t been removed from a legitimately signed item and re-applied, to manage this risk most schemes will take a hash of an item and include it in the signature. You must be convinced that the item has been signed with a valid signing key so the person accepting the item as signed should also be assured that the item has been signed by the identity they think it has been signed by and check the digital certificate(s) used to sign the transaction then each and every certificate in the hierarchy up to a trusted root authority. Bitcoin uses Elliptic Curve digital signatures so also requires a good source of randomness not only in key generation but also in the signing process.
When considering a digital signature within a virtual currency context it is fair to think of a verified signature as an identity, taking that one step further if you want a new or multiple identities all you need to do is to generate a new signing / verification key pair, I will explore this in greater detail in section 5 below.

b. Bitcoin Limitations
It should be noted that at the present time both the hash functions and digital signature primitives in Bitcoin are fixed, they could be changed in software as described below but might well lead to a hard fork in the blockchain. Bitcoin currently uses two hash functions (RIPEMD160 and SHA256) and only one digital signature function (Elliptic Curve DSA over curve Sec P256). If the currency is to have longevity there are bound to be further cryptanalysis attacks upon the hash and signature functions and at some point they or the ever increasing processing power available will lead to these functions being seen as less secure at which point every node and client will have to switch in a synchronised way. Updating the hash or signature algorithms is a very big problem when you think about the distributed consensus with which Bitcoin operates. If a decision was made to introduce a new signature algorithm you would immediately be dependant upon all the software developers who had ever created a node or client to update their software, worse still for those miners who have invested heavily in custom hardware they will now have to update their hardware too. Inevitably there will be clients or nodes who have not updated and they will be in a position where some transactions will fail to validate because they are using a (new) signature scheme they are not aware of and miners may well find themselves in a position where blocks mined on nodes operating the new software fail to verify on nodes running the old software (relying upon the old primitives) and they will be rejected. This software update problem manifested itself in a small way early on 4\textsuperscript{th} July 2015 as has been widely reported in the technical press and formally reported on bitcoin.org (18). For a period of time a number of miners had been indicating that they were going to adhere to BIP66 (19) and enforce strict DER signatures. This problem arose from the way in which OpenSSL accepted various deviations from the DER standard but did not do so in a bug for bug compatible way between versions. The decision was taken to make signature parsing no longer reliant upon OpenSSL when 95% of the last 1000 blocks mined had been created with strict DER signatures. The entire network started to enforcing the strictness on the 4\textsuperscript{th} July 2015 unfortunately a number of miners did not have compliant software and built blocks which did not conform, unfortunately a number of nodes and clients where also not fully validating the signatures within blocks which caused them to build upon blocks which did not validate. This has increased the possibility of double spending value and it has also caused bitcoin.org to recommend that rather than the usual 6 transactions required to validate a payment (approximately an hour of elapsed time) that until all the nodes have upgraded to compliant versions of the software and all wallets have upgraded their software that 36 confirmations would be more appropriate (approximately 6 hours) to assure a payment.

c. Units and Transactions
When thinking about virtual currencies it is easiest to explain transactions as if it were a cash transaction however there are several important differences. Unlike a traditional currency when you buy Bitcoin there is no restriction upon the face value of the denomination you purchase. Unlike a traditional currency where notes or coins are restricted to the values manufactured under the authority of the central bank who controls that currency (£5, £10, £20 and £50 notes in the UK) when you buy Bitcoin the value of your virtual note is exactly the value...
you have purchased regardless of whether that is 0.0001BTC or if it is 10,000BTC or greater. The second difference is that however unlike transferring a specific amount from a bank account to a recipient a transaction operates in a manner more aligned to paying by cash with the exception that unlike a cash transaction in a shop where the purchaser gives a larger denomination note to the vendor who then provide the purchaser with the resultant change in Bitcoin the purchaser crafts two transactions to break up the larger denomination. One of those transactions transfers value to vendor and one that transfers value (the change) back to purchaser. The total value of the two transactions must be equal to or less than the total value of the coin being spent. It is important to note that the specification allows that the sum of the two transactions can be less than the value of the originating transaction and in that case the residue is transferred to the node that constructs the adopted block, this is covered in 4.h below.

d. Blockchain
The blockchain can be thought of as the central ledger for a virtual currency with the difference that instead of that ledger being held by a central authority it is instead stored in multiple places across the network, conventionally referred to as “full nodes”. The blockchain is an entirely public record of every transaction ever undertaken within the currency, arranged as a linked list of blocks with the transactions they contain in a merkle tree seen in Figure 4 - Blockchain and transactions. New Bitcoins are generated by the proof of work hashing puzzle that takes place during the block building process, see 4.i below. The configuration of the blockchain mitigates one of the most significant risks in any virtual currency, double-spending. Unlike a conventional currency that relies upon a unique physical token such as a banknote or coin a piece of virtual currency is just a collection of 0s and 1s which resides in a file on a computer or in a mobile application, making a copy of a “coin” is a trivial exercise, unlike the proposition of copying paper currency which is designed specifically to resist this threat. By arranging groups of transactions into blocks with associated hashes and linking blocks together by using hash pointers you can ensure that once validated transactions cannot be added or modified without it becoming obvious because the hash pointers would fail to validate when checked.

![Blockchain and transactions](image)

**Figure 4 - Blockchain and transactions**
In order for a transaction to be considered valid and therefore to be added to the blockchain it needs to satisfy four conditions;

- The transaction is signed by all the people who are spending virtual currency.
- The coins have not been double-spent.
- The coins being consumed were legitimately created.
- The value emerging from the transaction is equal to the value going in.

The Blockchain as it is currently configured isn't really scalable because every block is stored on every node the chain will become longer and longer as new blocks are added every ten minutes and as an entirely linear linked list it could become unmanageable over time. A potential solution is to periodically undertake a hard fork by removing the history and validating all unspent value and re-linking that to a new genesis block. It is likely that this could lead to a similar problem experienced during the BIP66 update referenced in 4.b above.

e. Decentralised Consensus
One of the espoused strengths of virtual currencies is that there is no central authority exercising control over it. When a payment is made the transaction is broadcast to all the nodes on the network and will be propagated as quickly as the P2P network allows. It will be signed by Alice when she makes a payment and be sent to Bob’s Bitcoin address (a derivation of his public key). Alice’s payment will contain a hash pointer to the transaction that gave rise to the value she is now attempting to spend. If Bob wishes to know when he has received a payment he either needs to be running a node and monitor transactions or he needs to have a digital wallet hosted by someone who is running a full node. Bob doesn’t need to have a wallet or run a node, the value in the transaction will be his as soon as the transaction is verified and will remain on the blockchain until such time as he chooses to check and then spend that virtual value. At any time every node in the network will have a sequence of blocks of transactions upon which consensus has already been reached as well as a pool of outstanding transactions. The outstanding transactions may or may not be identical simply because within a P2P network there will be delays and errors. The next block in the blockchain will contain a number of transactions and anything left over or missing should be included in the next block.

Bitcoin doesn’t work exactly as described in the preceding paragraph due largely to the latency in the P2P network and the fact that there is no concept of network time. Bitcoin does however introduce the concept of incentives discussed in greater detail in 4.h below. The convention is that it takes approximately 1 hour (or more precisely six new blocks) before consensus is said to have been achieved whatever happens value will only be spent once. During the course of the hour and beyond the probability that a transaction has been included in the blockchain increases exponentially however convention within the system is to consider six verifications as consensus unless there are extenuating circumstances such as those mentioned above.

f. Distributed consensus
This is traditionally driven by the reliability of distributed systems, in corporate provided environments with thousands of severs such as social network you want every server to contain all of the comments or likes and for every comment or like to be on every (or none) of the servers.
In a distributed system all of the valid nodes will have an input validation process to ensure only valid transactions are included. It is important to consider only valid nodes, in a distributed system there may be faulty nodes or nodes whose primary function is malicious. In order to achieve consensus all of the valid nodes need to complete the consensus process and each of the nodes should agree on the final value agree. The final value cannot be arbitrary but must be one of the values initially proposed by one of the valid nodes however Bitcoin makes no distinctions between nodes and relies upon proof of work to guarantee (or encourage) honesty.

Each transaction will be signed by Alice’s private key, will include Bob’s public key and will contain the hash of the transaction that gave rise to the value Alice is spending. It is entirely possible for each transaction to be considered in isolation and for consensus to be achieved on a transaction basis however this is inefficient and Bitcoin collects transactions into blocks and achieves consensus on a block basis. Bitcoin does not have a concept of network or global time simply because it as a P2P network with everything happening over the Internet, which is an imperfect network. As a result it is not possible for every node on the network to agree a common ordering of transactions, even if a network time source could be universally agreed and maintained there is a possibility that a malicious node could subvert it.

Bitcoin solves the distributed consensus by offering incentives to act honestly, this only works because it is a virtual currency and therefore has “value” to create and reward with. Bitcoin also copes with the randomness of the imperfect and latent network with consensus happening over an extended period of approximately one hour, even at the end of that period you cannot be sure that the block or transaction you are interested in has made it into the consensus.

g. Consensus without identity
Bitcoin nodes have no identity; it might be helpful if they did as the protocols could use those identities to make decisions, to initiation processes in a deterministic way or to identify malicious nodes. However in a P2P system it is very difficult to reliably assert an identity without some form of central authority, which would defeat one of the main attractions of a decentralised pseudonymous virtual currency. In a P2P (P2P) network it is relatively easy to create a copy of a node if an attacker creates a large number of malicious nodes they could have a disproportionate impact upon the integrity of the P2P network. This was discussed by Doucerc (20) who acknowledged Brian Zill for offering the term Sybil attack to describe this based upon a case of disassociated identity disorder described by Schreiber (21). In order to deal with this problem Bitcoin creates a token for every node, if an attacker creates a number of Sybil nodes each of those nodes will have the same identity.

When it is time to create a new block a random node is selected by the proof of work hash puzzle and this node proposes the new block using the transactions it has observed. Other nodes will then either reject the proposed block by extending the blockchain from the same previous block or accept the block by extending the blockchain from the new block proposed by the randomly selected node. The proposed block will only be accepted if all the transactions in the proposed block are signed with valid signatures and all the transactions contain previously unspent value. As each and every block in the blockchain contains the hash of the block from which it is extending the chain this is used to signal acceptance or rejection of the proposed block. Even if the node selected to propose the next block is malicious they will be unable to propose a transaction that spends someone else’s value because when the other nodes seek to
validate the transaction the signature will fail to validate and the block rejected and the next
node will be randomly selected. There is an opportunity for a node to simply ignore
transactions that send value to or from a particular address but as the node proposing the
transactions for the block is randomly selected the transactions which had been maliciously
ignored will simply be included in the next block which has been proposed by the next randomly
selected node.
The only remaining valid attack is the double spending attack, if Alice is acting maliciously and
she is maintaining a full node she could spend some Bitcoin with a merchant Bob, this
transaction would be included in the next block of transactions when proposed by a randomly
selected node, if however Alice has been randomly selected to propose the next block she could
modify the transaction so that the value isn’t transferred to Bob address but is instead
transferred to a second address which Alice also owns. To the system both transactions will
appear to be spending value that has been transferred to Alice legitimately and the coin isn’t
previously in the chain so it is as far as other nodes verifying the transaction are concerned
unspent. If the block with Alice’s fraudulent transaction is selected by the next randomly
selected node as the block to extend then on the basis of the systems approach which always
extends the longest blockchain Alice’s double spend to herself becomes the verified transition.
The block that contains the transaction to Bob has become an orphaned block and Bob never
gets the value transferred to him. Of course if Bob has been sensible he will wait for the
transaction to appear in a verified block before he honours Alice’s purchase, that may be
acceptable practice if Alice has brought an £8000 watch from an online store, if she is buying
something over the counter it is likely to be less acceptable.

h. Incentives
With random node selection there is nothing to guarantee that a node will act honestly and
even if it did there would be no way of not using a dishonest node again because nodes don’t
have an identity. Therefore Bitcoin takes an opposite approach, instead of trying to identify and
penalise malicious nodes it instead rewards honest nodes and this is the only method by which
new Bitcoins are created. The creator of each block that gets adopted into the blockchain
receives a reward in Bitcoin. At the time of writing the reward was 25 BTC = $5391.36 (Source
BTC-E 05-06-2015 0906 BST 1BTC = $224.64). This reward halves every 210,000 blocks which at
the current rate of production is approximately every four years although this is dependant
upon the quantity of computing power applied across the network to the proof of work activity
and the way in which the protocol adapts to even out the computational power by making the
proof of work progressively more difficult leading to the creation of a new block every 10
minutes or so as referenced above. We are currently in the second period; initially the reward
was 50BTC for the first 210,000 blocks, subject to the caveats above it is expected the reward
will halve again at some point in 2017. At the point at which a node selects a set of transactions
to form the next block it intends to work upon in addition to the valid transactions it will include
an extra transaction of the reward amount payable to an address of the nodes choice. At first
look it appears that the node will receive the reward regardless of whether it creates a block
with only valid transactions or whether the block includes malicious transactions however this is
not the case. The block will only get included in the blockchain by consensus when other nodes
independently verify the transactions in the block, therefore if a malicious node attempts to
create a block with spurious transactions the distributed consensus provided by honest nodes
will cause the malicious block to be rejected and not get included in the blockchain and the
malicious node will never be able to spend any value derived from the reward transaction.
associated with the maliciously created block. This mechanism does mean that eventually the total supply of Bitcoin will be exhausted at some point in 2040 based upon current consumption.

If this were the only incentive mechanism over time as the incentives to build blocks honestly decreases it is likely that so would the amount of computing power honest nodes would apportion to this activity it would also mean that in 2040 there would be no incentive at all to build blocks. The currency would either cease to exist or the only way to extract value would be in dishonest activity, which would have a significant negative effect upon the currency. Bitcoin however includes a second incentive mechanism which is best visualised as a “tip” or transaction fee. Section 4.b above explains how transactions are constructed with a payment to a recipient and the “change” being transferred back to the originator and that these two transactions can be less than the total of the originating transaction. The unapportion value or residue is the incentive for the block creator to include a transaction in the next block they create, over time as the block creation incentive steadily decreases the importance of the “tip” will become more important, a transaction without a tip or with a smaller “tip” is likely to be deprioritised and may never be included in the blockchain.

i. Proof of work
In 4.g above the process of selecting a node to propose a candidate block was discussed, many before me have discussed difficulty of making random decisions within computer systems, suffice it to say that deriving pure randomness is impossible to prove and sources of poor randomness have been used to attack numerous systems and protocols over time and has been the downfall of many crypto systems. Nodes need to be selected based upon an attribute that no one can monopolise, in the Bitcoin system this is done with a proof of work system based upon computing power. To do this a miner will construct a merkle tree of containing the requisite number of transactions and then generate a block structure containing a number used once (nonce), a hash pointer to the previous block in the blockchain and a hash pointer to the top of the merkle tree containing the transactions. In a merkle tree the hash pointer to the top of the tree is dependant upon the hash pointer to each child node, and each child to it’s child hence the integrity of the entire tree is guaranteed by that first hash pointer. The nonce in the block is used as the mechanism so that the miner can change the block every time they hash it and therefore get a different outcome, one that satisfies the difficult requirement for block generation. It is possible for a miner with a given set of transactions to try every possible nonce and still not find a result that satisfies the difficulty requirement, hence there is a facility in the transaction that the miners create in order to pay themselves the reward for successfully mining the block to also include a nonce. This nonce will ripple up the merkle tree as parents create the hash pointers to their children and therefore alter the hash pointer to the top of the tree thereby modifying the data being hashed by the miner meaning the entire set of nonces can be tried again but with a different set of base data. As outlined in 4.a.i above there is a requirement for a hash function to be pre-image resistant i.e. knowing the H(x) it is impossible to discern x, it is this property which Bitcoin exploits by specifying that the resultant hash of a block starts with a certain number of zeros. If the hash function is secure the node has no option but to progressively try different nonces until it finds a combination of nonce, pointer to previous block and transaction set which produces a hash that meets the criteria. The only thing a node can do to influence the speed at which blocks are hashed is to apply more computing power to the problem. This proof of work process is often referred to as “mining”.
Every 2100 blocks (roughly two weeks) the mining nodes calculate the average time to solve the hash puzzle and by formulaic process tune the difficult by ± 7% so that a new blocks continued to be created approximately every 10 minutes. Over time the difficult has steadily risen as shown the data from blockchain.info (22) in Figure 5 - Mining difficulty over time. As further advances are made in mining technology, as mining groups invest in faster and more specialised hardware and as smaller group coalesce to form larger groups with greater distributed power it is likely the difficulty will steadily increase.

As a result of the difficulty and necessary investment to solve this hash puzzle only a few nodes choose to invest resources to compete to solve the puzzle. The probability a particular miner will solve the puzzle and propose the next block is directly related to the amount of processing power they apply to the task, if they contribute .00001 of the total available computing power the probability is that they will successfully solve the puzzle 1 in 10,000 blocks. This proof of work removes the need to select a random node, nodes will start hashing and one will “get lucky” and find a nonce which satisfies the requirement of the block they are hashing, their block will go forward for verification and they will be rewarded with the block incentive and the transaction “tips”. It must however be noted that this process is exponentially probabilistic there is a chance that a block might be created a few seconds after the last block was created if the combination of nonce, pointer and transactions satisfy the difficulty, similarly it may take much longer to create a block, hence the difficulty being readjusted taking an average over 2100 blocks. Due to the nature of the hash function once the puzzle is solved and a block is published it is trivial for other nodes to verify the proof of work has been completed because the nonce is published within the block so unlike the miner who has invested significant resource in mining the block and has probably tried $10^{20}$ nonces, to verify the block the hash function only has to be run once.

In order to solve the hash puzzle a number of approaches have been taken over the development of Bitcoin.
In the initial deployment the majority of mining took place on general-purpose desktop machines. These machines could complete approximately $2^{24}$ hashes per second $\approx 20$ Mhz. At the time the difficult was much lower (Figure 5 - Mining difficulty over time) meaning that blocks were created with the small mining community and lower power in accordance with the expected 10 minutes per block. At the current difficulty it would take approximately 180,000 years to find a new block however you might just be lucky and the first nonce you try could yield success.

After the initial deployment miners started to develop new approaches to mining, their first refinement was to use the graphics processor units (GPU) in high end graphics cards. These processors are designed with a high throughput, they contain bit manipulation processes that can assist in hashing and support a degree of parallelism. The majority of the GPUs could be overclocked and it was possible to install a number of graphics cards in a single PC. The down side was that whilst the processing power was greater, so was the power consumption and the cards required significant cooling. This approach provided a step up in speed of mining and it was possible to accomplish $2^{27}$ hashes per second $\approx 200$ Mhz. With 100 cards operating simultaneously it would take approximately 180 years to find a block at the current difficult.

The next major development was the use of Field Programmable Gate Arrays (FPGA) that provided hardware like performance but in a programmable environment. This was the first point at which mining didn’t have the overhead of a consumer operating system operating on general-purpose hardware. The FPGAs could be programmed to only undertake the processing necessary to hash the transactions, they had better cooling and better power consumption. They did require more specialist skills, they weren’t optimised for 32 bit operation and it was found over time that they were less reliable (perhaps because they were being run at, or close to maximum at all times) which meant they were a significant investment. FPGAs can accomplish $2^{30}$ hashes per second $\approx 1$ Ghz meaning a rig with 100 boards would take approximately 25 years to create a new block.

The current stat-of-the-art is Application Specific Integrated Circuits (ASIC). These are truly hardware based mining rigs, there is no programming involved, you buy them, plug them in and are ready to go. Due to the state of the market it is necessary to pay for the ACIs before they are manufactured, the production runs are small, you don’t know what you are buying and have no idea whether the mining rig you are investing in will operate better than the competition. The speed of mining rigs continues to rise, at the time of writing 1 Thz machines are the standard giving approximately $2^{40}$ hashes per second, even with this technology it can still take 14 months to find a hash so a miner either needs to be very lucky or make a large investment in a number of these machines running in parallel. Because the production runs are limited and they require the consumer to invest up-front mining rigs have a very limited life span and it is entirely possible that hardware is obsolete 3 – 6 months after delivery it is also a widely held belief that half the profits from new mining rigs are achieved in the first 6 weeks after which the chances of successfully hashing a block is linked more to luck than it is to the computing power. Although not within the scope of this project it should be noted that ASICs rigs tend to be composed of a large number of individual processors working in parallel and consume significant power and require very efficient cooling so your geographic location can have a large impact on the profitability of your mining rig.
The proof of work solution also mitigates the Sybil attack described in 4.g above because in order for a malicious node to offer a new block it needs to have sufficient computing power to be able to solve the hashing problem.

j. Blockchain forking

It is entirely possible for two new candidate blocks to appear on the blockchain at effectively the same time. Candidate blocks are propagated across the P2P network in the same way as transactions. The network has no concept of a central time and due to the latency which is bound to exist within a global network it is entirely possible that two nodes will complete the hashing puzzle close enough in time for them to be published and propagated across the network leading to the circumstance depicted in Figure 6 - Blockchain fork.

![Blockchain fork diagram]

In this figure at time $T_1$ two separate nodes offer two candidate blocks that are propagated by the P2P network. Across the network nodes verify that the transactions within the candidate block are valid and that the proof of work validates; assuming the candidate blocks verify correctly they will be linked to the blockchain held by that particular node and propagated. Eventually the two candidate blocks will have been propagated to every node and will be linked to the blockchain held on those nodes and a fork has occurred. Mining nodes will start to hash the next set based upon the first verifiable block they receive and select a set of transactions to form the next block. Some will have received block $n+4a$ first and will start hashing the next block linked to $4a$, others will have received $n+4b$ first and will use that block as the basis for their next block. At time $T_2$ the blockchain has forked and different nodes will start building upon one or other of the forks until they have solved the hash puzzle. At time $T_3$ block $n+5a$ has been published and links to block $n+4a$ simply because this is the block which the mining node responsible for $n+5a$ saw first. The node working on $n+5b$ will stop working on the hash puzzle because a block has been found. The convention in the blockchain is to always extend the longest fork so after time $T_3$ mining node will extend upon $n+5a$ as the end of the longest chain. Block $n+4b$ will no longer be considered part of the blockchain; the transactions from $n+4b$ should already figure in $n+4a$ or $n+5a$ as nodes creating blocks operate with the same pool of transaction which are added to as transactions occur and removes as they figure in new blocks. The only exception is the transaction giving rise to the proof of work payment to the to the node which created $n+4b$ if the miner tries to spend the value the transaction will fail to verify as it does not appear in the confirmed chain of blocks hence $n+4b$ will have no effect going forward and will to all intense and purposes have never existed.
An alternative to the proof of work is a proof of ownership or proof of stake where you only allow someone to construct a block if they can prove they own a certain mount of the currency, Bitcoin does not do this although it could because with an entirely and completely open ledger it would be possible for a block producer to periodically issue a transaction on the blockchain to transfer the required amount to themselves. The fact that the input amounts would be validated would guarantee that the block producer owned the required stake.

The security of Bitcoin relies upon a circular relationship confidence in the blockchain, the vitality of the mining system and the value of the currency, all are interconnected and interdependent.

For the currency to be healthy it needs to be worth something otherwise there is no incentive to mine blocks or verify transactions, in order for this to be true the blockchain needs to be considered healthy and trustworthy you need to be confident that no one person or group can overwhelm the blockchain by operating more than 50% of the nodes and influencing the consensus process, in order to do that you need you need a mining environment which encourages people to participate and it needs to be worthwhile which takes you back to the value of the currency. In the early days, when Bitcoin was first implemented by Nakamoto there was only one user, one node, one miner and no value. Over time confidence has grown, investment has been made and distributed consensus and perhaps even trust has been established, there are bound to be numerous digital currencies in the future but all of them will need to make that leap from a great idea to a fully operational and trusted environment otherwise they will wither for want of support, enthusiasm and investment. It is also fair to observe that whilst Bitcoin is the de facto standard at the moment if any of those three important properties are lost or significantly harmed the currency is likely to collapse.

Blocks are nothing more than a convenient and somewhat arbitrary collection of transactions so that the miner has something suitably big to work upon, it ensures the input to the hash function doesn’t need padding and it also serves to keep the blockchain shorter and therefore more manageable. Referring back to the primitives explained in section 4.a above it is constructed as a linked list of merkle trees.

As we have seen earlier there is no limit to the number of nodes and anyone can download the software and start their computer as a node. There is no topology nor is there any hierarchy all nodes are equal and its design owes a lot to the P2P file sharing networks of the late 1990’s. After you’ve downloaded the software the first thing you have to do is contact your first node, this is accomplished by contacting a seed node, these are either bundled with the software or accessed from online sources. Once you have selected your seed node the software will send a message to that node asking which nodes it knows about, with that information the new node then contacts all those nodes and asks the same question this is much the same as the way in...
which routing protocols such as RIP and OSPF disseminate routing information around networks and internetworks (23). Using this process a node will build up a list of peers it can communicate with and will select a number to regularly communicate with. By convention if a node is off the network for three hours the peers who use it will forget it and it will be replaced by another peer obtained in a similar way, using this process the network removes inactive modes, self heals and constantly evolves. When an individual creates a transaction they will send it to a node either with the wallet software or by creating an online payment, the receiving node will send it to all the peers it maintains a relationship with but only after it has validated the transaction by ensuign the digital signatures validate, that the coins come from a legitimate transaction and that the coins haven’t already been spent. The Bitcoin protocol is a stack based scripting language not similar to Forth and all actions on the protocol are scripts drawn from a small number of commands. All scripts need to finish successfully otherwise they are deemed invalid and ignored, therefore the process of verifying the signatures, checking for double spend and validating the coins are legitimate happens as part of the script which forms the transaction published to the P2P network. As a result nodes will also validate not only that the script completes successfully but also that it is a valid script conforming to a small number of candidate scripts. If any of the validation operations fail or the script is of a non standard nature it doesn’t get propagated. Once content a node will propagate the transaction to all of its peers, the receiving node will do the same and the transaction will be gradually flooded across the entire network. If a node sends a transaction to one of it’s peers and the peer already knows about the transaction it will respond to the propagating node to indicate it already knows and won’t propagate it any further, this stops transactions from propagating forever and the network becoming congested. In this way nodes build up the list of candidate transactions for their next block if they are mining.

k. Bitcoin in Use
To spend a Bitcoin you need to know the identity of the coin and the value, both of which can come from the blockchain and the users secret signing key. Most people choose to use some form of electronic system to manage their coin but other than the frailty of human memory there is no requirement. The important thing to manage effectively is the signing key, as long as this is affected you’ll be able to spend your Bitcoin and others won’t.

i. Key storage
The easiest way to manage you keys is to store them as a file on a local device a phone, laptop or desktop computer. Of course this is only as utilitarian as the device itself, if the smartphone or computer is lost you lose the value of those coins stored on that device, there is no central authority to provide a refund the coin is lost. Many smartphones synchronise or backup to local computers and most now include cloud based backup however very few people regularly backup their home computers, if your device has been stolen and if the thief knows and understands virtual currencies and can access the device it is highly likely they will have spent (or obscured your coin) before you as the legitimate user can purchase a new device, restore from backup and move the coin to a different address. In a similar vain the Bitcoin stored upon a smartphone or computer is only as secure as the device itself. If the device becomes infected with malware, if the device is hacked or if the cloud storage upon which it is backed up is insecure the value stored there is at risk. There have been numerous pieces of malware which when activated search for Bitcoin related files. For instance a trojan called cointealer was discovered in March 2014 (24) which searched for bitcoin.conf (the Bitcoin software
configuration file) and wallet.dat (the file containing the information from a users’ wallet) and when found sends them to a remote location. Whilst having some virtual currency stored locally and easily accessible has utility in much the same was as having some cash in your wallet or purse you wouldn’t normally walk around with all your money in cash in your wallet. For local storage most people choose to use wallet software to manage their coin. This software will normally manage a number of Bitcoin addresses allowing the user to receive coin to a number of addresses and when a payment is made the wallet software will construct a transaction with one or many inputs which equal or exceed the required value, plus tip and where necessary creates a transaction to return the unspent value. It is important to appreciate that whilst it is often said that a user’s Bitcoin address is their public key this isn’t the case there is a correlation and the one is derived from the other but they are not the same. In order to transform a public key into an address the steps in Figure 8 - Public key to Bitcoin address are completed and these are all part of the standard script library in Bitcoin. There is an option in terms of hashing however hash160 is identical in output to the nesting of RIPEMD160(SHA256(public key)).

A Bitcoin address is represented as a base58 encoded string or as a Quick Response (QR) code. base58 is used by many digital currencies as a way to represent a series of random looking letters in a way they reduces the opportunity for an address to be mistyped by removing characters the can be easily be transposed, it also provides error prevention and detection. By using a reduced set of characters consisting of numbers and upper and lowercase characters but with I (uppercase i), O (uppercase o), L (lowercase L) and zero removed the opportunity for characters to be accidentally transposed is reduced.

The character space therefore is:

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

The Bitcoin address also includes further error checking (25) in addition to the base58 reduced character set. Having calculated the hash160 and obtained the public key hash the resultant hash is then hashed twice more with SHA256 and the first four bytes of that output is appended to the public key hash. As a result the validity of the characters entered by a user when they are entering a Bitcoin address can be validated before a transaction has been propagated and
therefore the chances of creating a transaction than cannot be validated once submitted are reduced.

Figure 9 - Bitcoin address and QR code shows a valid Bitcoin address represented as both a QR code and a base58 encoded address, these are both acceptable representations of a valid Bitcoin address.

m. Hot Storage
When storing Bitcoin there are two distinct options often referred to as hot and cold storage. Hot storage is the application and/or device referred to above easily accessible, normally online and frequently an application on a smartphone. In addition there are numerous online wallets and exchanges that will store Bitcoin for you. In most cases these are similar to an online banking portal where you can login from a browser or access the portal from a smartphone or tablet. In most cases these sites will store you keys and manage them for you so you need to be able to trust the administrators and security professions advising the companies and be confident that they are building secure services and managing keys appropriately.

n. Cold Storage
Cold storage is more akin to the deposit or savings account you may have with a traditional banking institution, it isn’t necessarily available 24/7, you probably can’t access it when you are out and about but it is there should you wish to add or remove funds. In a more traditional information technology world this is your offline secure backup facility, buried beneath a mountain in a former government owned nuclear facility or in a fire safe in the basement of a different office. The beneficial outcome of hot and cold storage is that it forces a user to have at least two key pairs and as a result two Bitcoin addresses, one which they expose to the world and carry around with them and one which is kept in a safe place. It is worth remembering that in order for a transaction to exist the receiving entity doesn’t need to be online or even aware of the transaction once the transaction is created by the sender the coin is gone and can only be spent by the person who has the private key linked to the Bitcoin address the value has been sent to. So when thinking about cold storage all you are storing is the private key necessary to spend that value, to move something into cold storage all you need is the address linked to the private key. When you wish to move value into cold storage you just create a transaction of the relevant value where the output is the Bitcoin address of the cold stored public/private key. That is a reasonable approach if you are content to put all your currency in one place however for reasons of privacy it is more normal to use a different address for every receipt of value, a rather clunky approach would be to generate a large number of key pairs at establishment of the cold storage, transfer all of the public keys to your wallet application and then take the cold storage offline, this quickly becomes unmanageable if a human or machine has to store all of the addresses and then consume them in a systematic way, once and only. Fortunately the ECDSA digital signature primitive used in Bitcoin offers a more elegant solution by implementing hierarchical key generation to provide large numbers of unique but linked public/private key pairs. This is accomplished by creating on the cold side two pieces of information,
address generation information is exported from the cold storage and private key generation information that remains forever offline in cold storage. It is worth noting that neither the public nor private keys leave the cold side so there is no key leakage only the address generation information. With this address generation information it is possible to generate any number of Bitcoin addresses, all the user needs is the address generation information and then to be told to use a certain key or in the case of moving coin from hot to cold storage they simply use the next address in the series. The user wishing to transfer value then creates a transaction that transfers the value to the newly generated address and then publishes it to the node they are using. At this point (assuming the transaction validates) the value has been moved to cold storage even though the cold storage has no idea this has happened, as it is permanently offline. This is of course a one way process which moves value from the hot to the cold side, at the point at which you wish to move value from cold to hot it is necessary to create a transaction, signed with the users signing (private) key and then for it to be fed into the P2P network in the normal way.

Up to this point cold storage has been described in a rather abstract way simply specifying it as offline. It might be reasonable to visualise this as a computer that isn’t network connected but that isn’t the only option. If it were is it likely that you’d want that to also have some physical security as if it is lost or stolen you have lost access to your Bitcoin “life savings” so you’d probably want to put it in a safe and for continuity purposes have a back stored in a similarly secure location. In a similar way a laptop or even USB “thumb drive” or external hard disk. You could print the information onto paper and store that in a safe, as with the previous example your security is as strong and reliable as the strength of the safe and the safety of the place that safe is stored. You could encrypt the private key information or private key generation information with a strong and reliable crypto system and then store it online or on a device, of course you are then dependant upon the user choosing a strong passphrase and on the software used to encrypt the information being reliable and the cryptographic primitive being reliable and implemented correctly in software and you’d still want diverse backup and recovery options and last of all the user needs to remember the passphrase, if they write it down that then needs to be stored correctly, it very quickly this becomes a “Russian doll” of nested countermeasures. The final option is to use a tamper evident device that stores and signs the keys and doesn’t allow the key to be removed or altered without some form of knowledge. In practise if you have a large amount of Bitcoin which you wish to store then you’ll probably blend a number of methods to cold store your Bitcoins.

o. Key splitting
There is however another method one might adopt in order to manage keys securely and this is to split them into a number of pieces at it’s most basic you chop it in half and put it in two places however there are much more elegant ways to do this, for the purpose of this project I don’t intend to go into this in any great detail as it isn’t germane to this project suffice it to say that it is possible to split a key into a number of pieces and then to require a number of those pieces to recombine in order to sign a transaction. The method of undertaking this is based upon a large prime number, a random number and the modulo function for the purpose of this project it is simply enough to understand that keys can be split into a number of parts and then used based on a specific number of those parts which may be all of them but could conceivably be two of three or seven of nine. Two of three becomes an interesting opportunity if you think of an e-commerce application if Alice decided to buy something from Bob via an
online shop hosted by Charlie she could just transfer the funds to Bob and trust that he will deliver to her the item as described; however if Alice knows nothing about Bob she may be unwilling to do this. When the transaction is created on Charlie’s marketplace the system could create a transaction with a three way split key where two parts are needed. One goes to Alice, one goes to Bob and one remains with Charlie. When Bob ships the item he will wait for Alice to contribute her part of the key if she is happy with the transaction and Bob can transfer or spend the value. If however Alice is unhappy she can withhold her key at which point she could approach Charlie making a case that the product wasn’t as described or has never arrived; similarly Bob could approach Charlie making a case that he shipped the item and that it was as described. Charlie will arbitrate and decide if Alice needed a refund or Bob required payment. Charlie could effect this by giving either Alice or Bob his part of the key thus allowing them to spend or transfer the value. This is more secure than transferring the value to Charlie and trusting him not to disappear off with the pseudo anonymous value.

**p. Altcoins**

A great many alternative coin systems based upon the Bitcoin model have grown up over time, few have anything close to the very limited usage that Bitcoin has however some have taken a step further towards anonymity. One of these is Dash (formerly Darkcoin) in which every transaction rather than standing alone is partnered with another transaction of the same value, a technology referred to as Darksend. Darksend is based upon Coinjoin an idea postulated by Gregory Maxwell (26) in which he describes a system that seeks to obscure the transfer of value in a blockchain by partnering transactions although in the original idea there was no requirement for transactions to be of the same amounts see Figure 10 - Coinjoin separate transactions.

![Figure 10 - Coinjoin separate transactions](image)

The advantage of Coinjoin over tumbling or mixing services is that unlike the services described in 5.k below this system does not require you to trust someone to act in an honest way with your coin. Every transaction has at least two inputs and at least two outputs, each of the input users will sign the transaction and the value will be transferred to two outputs see Figure 11 - Coinjoin transaction. For anyone observing the blockchain it will be impossible to discern which input went to which output. A side channel does however exist if a particular address makes a
payment on a regular basis to the same output address, such as someone who buys a coffee and pastry on the way to work everyday, if their transactions was joined with another their usage trend would immediately point to the other input belonging to the other output.

Figure 11 - Coinjoin transaction
5. Exploiting virtual currencies for criminal purposes.
Within this section I will discuss the criminal opportunities that virtual currencies present both in connection with “traditional” crimes that they could facilitate but also in respect of the crimes they could themselves fall victim of.

a. General notes
It should be noted that as I have already expressed virtual currencies are without any value, they have nothing intrinsic or concrete backing them up. In a similar vain they also have no central authority, there is no guarantee of any value and nobody to intervene if the wallet you use is emptied by someone else, the exchange you use is dishonest or at worst if the currency collapses. In many respects it might not be unkind to describe a virtual currency as nothing more than a ponzi or pyramid scheme. In a ponzi scheme investors are paid their returns from the monies raised by selling more investment opportunities with a person at the centre managing the interactions with investors / victims and collecting the money from them. A pyramid scheme operates in a slightly different way, the instigator of the scheme will sell an opportunity to a number of people who agree to give a percentage of everything they make to the person who sells them the opportunity. They in turn will then sell a similar opportunity to a number of people, who in turn do the same. Every time an opportunity is sold the seller gives a percentage to the person whom they bought their opportunity from, they in turn give a percentage to the person they bought their share from all the way up the pyramid to the top. For the person at the top this can be potentially exceptionally lucrative however as the scheme depends upon constant exponential growth they are rarely a long-term scam and collapse quickly. Whilst Bitcoin does not fit easily into either of these definitions the similarities are sufficient to give rise to concerns about investing hard cash or resource (computing power and electricity) into something with value not underwritten in any way.

b. Jurisdictional variances
For some time it has been an accepted fact within some criminal circles that the legal jurisdiction can drive the choices made by some criminals. In (27) Glenny quotes “one of Sweden’s most successful ‘carders’ [a person who trades in stolen credit cards]” who would never deal in cards issued in America for fear of the legal response from that jurisdiction if he were caught, instead they much preferred cards issued in Europe or Canada due to the lower likelihood of being detected, pursued and prosecuted. The regulatory and legal landscape that develops in regard to digital currencies will undoubtedly inform the way in which the public and criminals choose to use, or abuse these currencies.

c. Anonymity and Pseudonymity
Anonymous is defined (28) as “of unknown name; of unknown or undeclared source or authorship; impersonal”. It is often said that digital currencies are anonymous, Bitcoin as the de-facto stand is touted in the popular press and on various websites, see Figure 12 - Wikileaks donation page (29) as such 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 however is a more apposite definition (28) “writing; written under a fictitious name”. Pseudonymity is an important element is in the execution of a number of crimes, a bank robber doesn’t walk into a high street bank with a sawn-off shotgun with the intention of making an illegal withdrawal without concealing his identity and in the digital crimes I will describe in the section the criminal needs to conceal his identity in a similar way. The criminal who is using a virtual currency for a crime must also make efforts to conceal that element of the crime from the observer whether they be casual or authoritarian.

In order to effectively use Bitcoin in the execution of a crime the criminal must disassociate themselves from the coin itself and hence themselves 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 if you look at Figure 12 - Wikileaks donation page above that is clearly being encouraged, I am not suggesting within this project that the operation of Wikileaks is criminal that judgment is for others to make. 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 in a holdall.

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 mitigations, which I summarise at the end of this section after I have considered a number of crimes that one could perpetrate with a digital currency.

d. Theft

As referenced above in section 3.b above whether or not a criminal could be prosecuted for stealing Bitcoins or any other digital currency is a matter of some debate, indeed it is highly probable that they couldn’t given the outcome of Oxford v Moss (3) however it is certain that if someone attempted to steal digital currency from a mobile device or by accessing an online wallet which did not belong to them then they would be committing a CMA Section 1 offence. In order to steal Bitcoin they would need to use the private key in order to create a transaction that transferred the value to a Bitcoin address that they owned. There is no other way to steal the currency, the cryptographic scheme in Bitcoin has not been broken and therefore the only valid attacks are to obtain the private or for the attacker to convince the owner to transfer the...
value to them either through a confidence trick, social engineering or with threats of violence. In many respects digital currencies are safer than cash from theft because unlike a wallet full of cash that is almost entirely anonymous, in use a Bitcoin transaction can always be traced through the blockchain and whilst this can be obfuscated by tumbling and mixing, see 5.k below the value is still there. One might argue that the serial number on a traditional note is exactly the same as a Bitcoin address; it is unique and can be observed by anyone however the utility is completely different. Very few people will know the serial number(s) of the note(s) in their wallet or purse and even if they did they would be of very little utility because there is no possibility of disseminating that information to everywhere that note might be spent let alone getting every retail establishment to check the serial number of every note they accept. If someone does manage to obtain your private key and transfer the value to themselves they still need to be able to either spend it or convert it to cash both of which hold significant risk as we will see later on.

e. Money Laundering
For the purposes of this section I will use the illegal drug trade as a source of example however it should be noted that as Robinson (30) observes there are many reasons why money is laundered, large corporations do it to bribe officials in return for lucrative contracts, individuals do it to hide money during divorces and Governments have been known to do it either to ensure against political instability like Ferdinand and Imelda Marcos did or to finance convenient wars as the Reagan administration did in the mid-1980s when they sold arms to the Iranian government and re-directed the funds to the anti-Sandinista Nicaraguan rebels. Conservative estimates suggest that between $100B and $300B are circulating the globe at any point as a result of the illegal drug trade, the majority of which is in the process of being laundered. The drug trade also demonstrates the worst-case scenario of money laundering with very large quantities of small denomination currency needing to be combined and legitimised.

The desired outcomes from a money laundering operation are four-fold.

• Hide the true source and ownership of the money as it has been obtained through illegal means.
• Change the composition of the illegal money, there is little point in starting the process with a large quantity of small denomination sterling notes only to finish the process with a similar number of similar denomination notes; one pile of £5 notes looks to all intents and purposes identical to another and is equally difficult to explain.
• Obscure the trail the money takes, it should be sufficiently complex as to conceal where it came from and where it went, ideally at the end of the process the money should either appear to have come from a legitimate source or be usefully located where nobody cares where the money came from.
• Control should be maintained over the funds throughout the process; whilst there will be an expectation that the laundry process will cost money and less clean money will emerge, it will certainly be expected that it should take place in a controlled way.

i. Consolidation.
The first part of the laundry process is consolidation. A drug dealer is faced with the daily task of putting all of his money in one place. This is likely to be less of an issue for the street dealer who is selling “fixes” to consumers as they are likely to be using their gains to either purchase more product, to finance their own addiction or to live their lives. In his book (31)
Bartlett observes that studies (32) show that the average street dealer in the UK makes £15K to £20K per annum, which is unlikely to require laundering, indeed the study goes on to observe that in more than half the cases the “profit” is used to fund the dealers own drug habit. For the suppliers and distributors large volumes of small denomination notes quickly become very difficult to manage. Robinson refers in (30) to a time in the mid 1990s when Pablo Escobar the renowned Columbian cocaine cartel boss had to write of $40M which had rotted away in a California basement simply because he couldn’t launder money as quickly as he was generating it.

In order to consolidate funds you could;

- Feed the money into a banking system without causing suspicion, for a successful dealer or distributor that can mean placing millions of notes into the banking system which by any estimation is time consuming and near impossible without an army of “smurfs” paying small amounts into a diverse number of accounts. Even if this is happily effected the eventual consolidation and transfer will eventually exceed the limits in financial institutions and gather attention.
- Feed the money through successful cash heavy businesses using those businesses to change the currency up into larger denominations and using the business to legitimise the money by paying tax upon it. Casinos, restaurant chains and taxi businesses have been successfully used to legitimise large quantities of cash.
- Move it somewhere where large quantities of cash will not attract attention or if it does no one cares.

Exporting the cash after changing it up came into sharp focus in the UK in May 2010 when after a widely reported statement made by SOCA Deputy Director Ian Cruxton the selling of €500 note ceased as “There is no doubt that the main U.K. demand for the 500 euro note comes from serious organized criminals”. At that time £1M of £20 notes weighed approximately 50Kg as opposed to only 2.2Kg for the same quantity of €500 notes.

ii. Layering.
Layering is the process by which a laundryman attempts to disassociate cash from an illicit source by using as many bank accounts, companies and countries as possible. With each movement of funds it should be increasingly difficult to trace the money back to its source.

iii. Repatriation and Integration.
The final step in the process is where the funds are brought back into circulation as legitimate money, subject to tax and available for the criminal to freely use.

There are a myriad ways of achieving consolidation, layering, repatriation and integration the trick is to find one which will cope with the amount of cash the criminal regularly needs to legitimise and which won’t lead to a lengthy prison sentence. If a criminal had a relatively small amount to launder, £100,000 perhaps he might decide to change it into large denomination currency and head towards Eastern Europe with it. There he could purchase a large amount of antiques or collectables at the same time obtaining receipts showing deflated prices for the items. Using an overseas company as a front bring them back to the UK, paying tax and import duty as required and then sell them, via another front company or using local auction houses where you send people to overpay on your behalf for even

---

2 The term used to describe individuals who pay small quantities of money in multiple accounts in order to avoid detection.
more dirty cash; it should be noted that auction houses are required to report single or seemingly linked transactions exceeding €15,000. By doing so the criminal has legitimised their original £100,000 plus whatever they could sell the imported items for. Whilst this works for small amounts of cash turning this into a repeatable, long-term business would require a huge investment in time and effort with potentially little return.

f. Laundering with Bitcoin
Having considered the money-laundering problem from a traditional cash based perspective it is worth considering the benefits and dis-benefits that a virtual currency might bring to the problem. If you already have a large quantity of cash and want to convert it to Bitcoin in order to move it then there are very few options open to you. Although there are many UK presented coin exchanges 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. None of these are particularly a problem but if you are going to do this and remain beneath the law enforcement radar then why go to the effort of buying Bitcoin especially when most online sellers limit your initial transactions to about £100 and even after a 15 transactions impose similar limits to those seen in the traditional banking sector. If you can provide all of these confirmations, have the money in a UK bank account in small enough quantities to avoid being noticed 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 to be registered at the moment, the maximum transaction is £1,500. The problem is that there are so few ATMs at present if you have large quantities of money to change up you could easily spent 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 into Bitcoin 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 were people assemble to exchange Bitcoin for cash and vice-versa, sometimes referred to as a meet up. These are often frequented by virtual currency “evangelists” and their response to someone buying coin for illicit purposes might not be good. It is also unlikely that there would be sufficient Bitcoin available at a meet-up to satisfy the needs of an intermediate dealer. If you however were willing to pay over the odds it might create a market of it’s own and could be the first step to selling product in exchange for Bitcoin.

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. As we have seen above it is customary to get six confirmations before a transaction is considered “safe” this normally takes about an hour although at the time of writing due to the BIP66 problem mentioned above the current recommendation is to wait for 36 confirmations, about 6 hours. You might take it on trust for small amounts, the impact is lower and if you were a criminal you could easily resort to a more violent response to defaulters. The Silk Road used this particular business model for online sales, which I will cover in section 5.n below.
Assuming you have managed effectively to convert cash into Bitcoin it now exists everywhere as we have already discussed. The P2P nature of the network means that it is as soon as a transaction is published it immediately (or very close to immediately) is available everywhere, or at least wherever you can effectively use it either to purchase something or to exchange it for cash. You can transfer the value from place to place, you can combine and split value but it is visible to anyone who wishes to follow the trail in the blockchain. Mixing or tumbling services do exist, see section 5.k below and some alternative coins include this as a default service but there are a number of techniques which academic researchers are starting to develop to search the blockchain for transactions indicative of inappropriate behaviour but that is out with the scope of this project.

Finally the money launderer needs to legitimise the funds and bring them back into circulation and again the problem here is no different to the traditional money-laundering problem. You need to find a commodity you can buy with your illicit currency and sell on making it appear legitimate. There are lots of ways, especially in a cash heavy business to feed in quantities of illicit cash, in a virtual currency based scheme you do have the advantage of the value being identity agnostic so it would be possible for a few people to look like hundreds of consumers. Ideally you would want a business that didn’t require raw materials or something physical because you’d need to buy, store and then ship it to your fake customers. An online music or movie business might be an option as you could buy the rights to sell the product paying a royalty for ever sale. At this point you’d have legitimate virtual currency but you’d still have the problem of cashing it out and the options to change Bitcoin to cash are broadly the same as converting cash to Bitcoin. You can use an online exchange that will match sellers with buyers; you could set yourself up as a small-scale seller in an online market place. Using meet-ups to sell Bitcoin from a business perspective doesn’t really work as you’ll end up with a pile of cash that will need to be linked back into the business and this will always look unusual, you’ve effectively swapped one large suspicious pile of cash for another large suspicious pile of cash.

In the traditional money-laundering world one the most successful ways to dissociate tainted money is using shell banks. The world abounds with locations where buying a seemingly established bank with zero assets and a registered office is a remarkably simple matter. Funds can be transferred in and out and every time this happens it becomes more and more difficult to trace them back to their source. In just the same way as nobody would ever consider it suspicious that a bank had large amounts of cash withdrawals, loans, defaulters and international transfers if one extends the thought process to the logical conclusion in this connected world what could be less suspicious than a virtual currency exchange receiving large quantities of cash in exchange for virtual currencies. Consolidating those small payments into a large balance and then reselling that virtual currency. Perhaps one of the best ways to launder virtual currency would be to set up a legitimate coin exchange. If you can make the leap to receiving your illicit payments in virtual currency directly into something which looks like a coin exchange you have solved the cash problem. It is highly likely that at some point the world of regulation will catch up with virtual currencies as has been seen in New York recently at which point coin exchanges would either have to move or start to identify their customers effectively and undertake the due diligence necessary to mitigate money-laundering.
As a final though in relation to money laundering one possible option would be to start a Bitcoin mining business. You could buy a large quantity high specification Bitcoin mining servers, house them someone cool with cheap electricity and mine Bitcoin. Although you might have to explain how you had purchased your first few servers after a while you could just claim to be lucky, no one would ever need to know how many servers you really had working in parallel you could just claim to be lucky, much like people once did when laundering money through casinos. You would still however have the problem of converting the Bitcoins into traditional currency although it would seem to be legitimate.

g. Funding Terrorism
The opportunity for committing an offense in relation to The Terrorism Act see 3.b.iii above is simple. Anyone who attempts to raise funds or to move funds to support an act of terrorism is committing an offence; with a digital currency this is no different to collecting cash by passing a hat around a bar or place of worship. Digital currencies do offer the unique ability of moving themselves across borders without any assistance, as soon as a transaction is published to the blockchain it immediately starts to be promulgated across the P2P network to every node. At this point the value is everywhere and can be accessed by anyone with the private key regardless of where they are. This obviously adds significant utility in the context of collecting money for terrorists as it removes the need to travel carrying quantities of cash and negates the risk of being stopped at a border crossing and having to explain where the money came from and where it is going. To date there have been very few recorded instances where virtual currencies have been used in support of terrorism however the National Terrorist Financing Risk Assessment (33) acknowledges virtual currencies from the perspective of money laundering. In June 2015 a teenager from the United States pled guilty to “conspiring to provide material support” (34) after posting instructions on social media on how to use encryption and Bitcoin in support of Islamic State in Iraq and the Levant (ISIL). There is also a case in progress in the UK which has been widely reported (35) R v MOHAMMED AMMER ALI of a Liverpool man who it is alleged attempted to buy ricin from Silk Road, see 5.n below using Bitcoin, at the time of writing the case is still being heard.

h. Illegal movement of funds
In addition to the concerns relating to the support of terrorism and general money laundering many states legislate to limit the amount of currency entering of leaving their country. This can be for economic stability and taxation reasons as well as more general concerns about money laundering. Bitcoin offers a very clear advantage in this regard in that as soon as a transaction is published the P2P network picks it up and it can be used anywhere the private key happens to be, indeed when considering the global internet geographic location is a moot point and with Bitcoin there can be no way of stopping funds from appearing in your country. The only way to do so would be to stop every business in your country from accepting digital currency, stop anyone from operating a node on the digital currency network, block all P2P traffic which promulgated transactions or allowed them to be verified and stop the use of any tunnelling or encryption to conceal such transfers, in short a near impossible task.

i. Extortion and Confidence Tricks
Virtual currencies do provide some utility for extortion, blackmail or confidence tricks. They can provide insulation between the payoff and the criminal. Unlike the TV image many have of the
clandestine exchange on a park bench a blackmailer can see the value being transferred to their Bitcoin address as soon as it happens and knows that within a predetermined period of time it is verified, of course the value can be tracked easily through the blockchain and the criminal would need to take some action to disguise that or to make the cash-out process safer. Bitcoin has been used in several online attacks; most notably Cryptolocker. Cryptolocker appeared on the Internet in September 2013 (36) the trojan spreads by email and by machines that were already infected and operating as part of a botnet. When activated it encrypted files with a variety of extensions (documents, pictures etc.) on the hard disk and on connected network shares using a strong form of public key encryption. The individual who had been infected is given the opportunity of purchasing the key necessary to decrypt the files, different variants exist asking for payment in a number of ways one of which was Bitcoin. Prices varied but 1 or 2 Bitcoins ($700 or $1400 at the exchange rate at the time). Users who did not pay did not get their files back. There have been numerous reported incidents where online business have been hacked and held to ransom for Bitcoin, in July 2015 it was widely reported (37) that the online streaming media site Plex had been hacked and a message posted on their online forum offering demanding 9.5 Bitcoins ($2,400) in exchange for the data. Whether or not this is a legitimate claim or an opportunist attempt is unknown but it is clear that Bitcoin is being used for criminal purposes.

j. Online marketplaces
Bitcoin represents a significant risk in relation to online market places as its pseudonymity when married with other technologies can de-risk the purchasing of illegal or illicit items or services, it should however be noted that whatever an individual buys online in an anonymous or pseudonymous way still has to be delivered to a physical place through systems which, especially across borders examine every piece of post for illegal material. A short description of one of the most well known marketplaces Silk Road is included at section 5.n below.

k. Tumbling, Mixing and Splitting
Tumbling and mixing both refer to the way in which illicit Bitcoin value can be mixed with legitimate transactions to obscure the ultimate end point of output from illegal activity. There is no limit to the number of individual identities that a user can maintain. It is perfectly feasible to have multiple identities and to change them as frequently as you wish however you must remember that as the blockchain records every transaction in order to move the value from one identity to another a transaction is required which will be recorded forever on the blockchain. Tumbling services take input from a number of transactions, they take a fee and then they output the value to a number of different (and fresh) Bitcoin addresses.

In Figure 13 - Transaction tumbling I illustrate a scenario where five inputs are combined and then split into 19 output transactions. This needs to be done in such a way as an observer couldn’t re-combine the transactions easily, there needs to be some pseudo-randomness in the way the transactions are split, the commission that is paid and the number of output transactions. Although a simplistic example you can see how it would be difficult for an observer to decide from which input one of the outputs were derived.
Having tumbled a transaction it is critical to ensure that the value does not coalesce elsewhere, having gone to the trouble, and paid the fee for mixing the transactions it would be foolish if the criminal then moved the value around a couple of more times only to re-combine the transactions at the same cash out point or by spending the value at the same online store. It should also be noted that if the mixing service is taking a pseudo-random fee of between perhaps 2%-4% if you mix your coin a number of time the randomness of the fee will be flattened out until the fee is 3%.

An alternative approach is to insist that all the inputs must be of the same value, as long as some of the inputs come from legitimate sources then it would be impossible to tell which transactions contained the illegitimate value. If however 3 of 5 inputs where illicit output then on the other side an observer could still state that 3 of 5 of the inputs arose from illegal activity. It would be very easy to argue that anyone who used the services of a tumbler or mixer is doing so for nefarious reasons and ought to be suspected of some wrongdoing. It was often said when the UK Government was planning to introduce Identity Cards during the Labour
Government (2005 – 2009) that there could be no reason to object and that anyone with nothing to hide had nothing to fear. Nevertheless there was a huge community who objected on libertarian grounds and the scheme was eventually cancelled by the incoming Conservative / Liberal Democrat Coalition in 2009. There is however a second facet to a tumbling service which might prove useful to law enforcement, if an agency were so minded they could easily set up a tumbling service and would immediately have an insight into where payments were coming from and where they were going. If an individual was hoping to conceal their activity with the tumbling service using a service operated by law enforcement would attract more not less attention.

I. Dissociative Activity

In addition to using Bitcoin to pseudonymise activity there are several other actions the criminal would also need to take in order to break the link between themselves and the illegal activity they were seeking to undertake.

i. Places

They would probably want to make sure that they did not access the Internet from their home whilst undertaking the activity. Indeed they would probably want a number of access points to the Internet and use a variety of cafés, restaurants, hotels and transport hubs to undertake the activity.

ii. Hardware

They would seek to change the smartphones they used or in the case of laptop computers to change the MAC address frequently in order to disassociate activity.

iii. Identities

They would need to ensure that they maintained entirely separate identities, names, email addresses and logins. Failure to do so would easily lead to activity being linked. In a like manner there is little point in maintaining numerous Bitcoin addresses if they all lead back to the same smartphone based wallet or the same online exchange account.

iv. Anonymity services

When online it would be sensible for the criminal to use some form of proxy service to move online traffic to a far off place, ideally where they didn’t cooperate with international law enforcement. They might use encryption or a browser like Tor to obscure their activity, see 5.n below.

The challenge of maintaining all of these separate elements and not allowing them to come together is not insignificant and the slightest slip, accidentally emailing from the wrong email address, logging into the an online forum with the wrong credentials or paying a bill with the wrong Bitcoin address would all provide an advantage to investigators.

m. Crimes against Bitcoin

i. Malware

There are a number of malware variants that target Bitcoin. Inforstealer.Coinbit (38) is just one of these which searches the directories on users computers for the files normally associated with Bitcoin systems, primarily bitcoin.conf which is the file which contains
the details of the Bitcoin client on the machine and wallet.dat which contains the public / private key pairs for the Bitcoin addresses in use by the client. Loosing the private key associated with a Bitcoin address would mean an attacker would be able to search the blockchain for all unspent value paid to a particular address and the sign a transaction that transferred the funds to the attackers address. A number of pieces of malware monitor the clipboard for a variety of pieces of information in particular Bitcoin addresses and username and passwords to online exchanges and wallets. There have also been numerous reports of malware which uses the infected users computer to mine for Bitcoin, Trojan.Badminer (39) being just one example that can adapt it’s approach to mine using the normal PC processor or the graphics processor. How successful these pieces of malware are is unknown but clearly criminals are endeavouring to exploit Bitcoin for illegal purposes.

ii. Dishonest exchanges / online wallets.
In much the same way as your local high street bank doesn’t keep a shelf in it’s vault with your name on it where it stores all of your money, adding and removing funds as you deposit or withdraw the majority of online exchanges and wallets are not doing the same. They are simply recording the value you have purchased from them and then sending it out when you ask them to. It is entirely feasible that the amount of Bitcoin that they have at any point may not match the amount of coin that resides in user’s accounts. An exchange could periodically prove their holding by publishing a transaction that transferred their entire holding to themselves, but few do. If an exchange is holding all the coin belonging to their clients in a single wallet a dishonest employee could easily transfer some (or all) of the holding to themselves. If the dishonest exchange continued to show your balance as the amount you expected to have stored you would be none the wiser. Indeed the exchange could continue to operate with whatever residue it had left until such time as too much value was spent by their customers and they could no long “rob Peter to pay Paul”.

iii. Exchange hacking.
Bearing in mind the circumstances described in 5.m.ii above where an exchange keeps all of the coin belonging to it’s clients in a single hot wallet this is a very attractive target for hackers. In January 2015 bitstamp were hacked loosing 19,000BTC (approximately $5.1M), later leaked documents which appeared to have come from a forensic investigator alleged that a number of key individuals within the organisation had been subjected to a series of phishing attacks and when one of these was successful the resultant malware installed on the companies servers allowed the attacker to obtain the wallet.dat file for one of the hot wallets operated by bitstamp and the passphrase needed to transfer funds.

iv. Double spending.
As we have seen it isn’t possible for an attacker to spend another persons Bitcoin unless they have the private key needed to sign the transaction. Without a valid signature no honest node would include the transaction in their next block. If a dishonest node mined a block with a double spent in it this would also be detected when nodes verified the block. It is possible that a dishonest user could attempt to transfer value to two different people and inject the transactions into the P2P network simultaneously but geographically distant in the hope that they would be accepted by different nodes as being unspent value. When the next block was mined however only one of the transactions would be included and the other would be left in the pool. When the node then checked to see if the value was
unspent they would see the previous transaction in the most recent block and discard the double spend attempt. Even if a fork occurred as in Figure 6 - Blockchain fork and both of the double spend attempts were included one in each of the candidate blocks eventually the blockchain would settle upon which of the nodes was to form the longest chain and the other double spend attempt would fail. Once again this reinforces the need for people taking payment in Bitcoin to ensure they have the requisite number of confirmations before they consider the value transferred and the transaction safe.

v. Change the address.
A very simple attack would be to find an outlet that took Bitcoin payments in exchange for small value transactions and didn’t wait for confirmation. An attacker could easily print a different QR code that represented their Bitcoin address and stick it over the QR code used by the outlet. Every transaction would be paid to the attackers Bitcoin address until the outlet noticed and stopped taking Bitcoin payments or worked out what had happened. In a like manner if an attacker could change the Bitcoin address used on a website or online store this would have the same effect.

vi. Early block attack.
The early block attack could occur if a miner solved the hash puzzle very quickly but instead of publishing that block immediately they held it and used it as the basis for the next block. Whilst the difficulty of solving the hash puzzle is adjusted it is always possible that a node could solve the problem with the first value they tried. If having found the first block quickly you would allow the other miners to waste time and resource mining their own blocks and use the time to build a second block upon your earlier find. The chances are you would find your second block at around the same time or very soon after the other miners found their first block. As soon as you find your second block you can publish it and you immediately have the longest chain and the other blocks would be ignored. A brave miner who had significant mining resource might chose to hold back a number of blocks but of course they should be mindful that in the same way as they were lucky in finding the first block quickly they may also find a set of transactions that they struggle to solve the hash puzzle for and their time advantage could diminish until they lost the value of the first block and the subsequent blocks as the longest chain surpassed their early advantage. With the reward for creating a block at 25 BTC (roughly $5000) loosing the reward from a series of blocks quickly becomes very expensive.

vii. 51% attacks.
Ever since Bitcoin started to gain interest there has been concern and speculation about a single miner or mining collective having 51% of the available computing power within the network. This had occurred for very short periods over the history of Bitcoin however on the 16 June 2014 GHash were reported as having a greater that 50% share of the hashing power within the network for a period exceeding 12 hours. It is worthwhile looking at what an attacker can do if they have a significant quantity of power.

- Similar to the early block attack they could mine privately for an extended period and construct a very long chain of transactions that they could deploy in one go.
- Allied to the early block attack they could double spend keeping the transactions they wanted to confirm in their blockchain and allowing others to confirm the double spends until such time as the recipient accepted the payment had verified
and the transaction completed by providing the goods or service. When the 51% attacker deployed their longer chain the double spends in the other chain would be negated.

- They could ignore transactions from a particular address or service provider but the remaining transactions would just remain in the transaction pool and be added to the blockchain the next time a non-51% block was mined.
- The 51% attacker might try to change the incentive scheme and instead of paying themselves 25 BTC for each block they created they could pay themselves 50 BTC but legitimate nodes would just ignore the illegal block.
- The 51% attack might decide to retire from mining and allow the hashing difficult to steadily decrease over time to keep the 1 block every 10 minutes rate and then they re-join mining and take advantage of the slower hash rate to mine a large quantity of blocks very quickly but the advantage of this over being consistently one of the quickest miners is probably minimal if not negative.
- Lastly a 51% attacker could just decide to destabilise the currency by repeatedly creating double spends, repeatedly forcing forks and attempting to change the reward system. It would be pointless as they wouldn’t be able to make any profit and their investment in mining hardware wouldn’t deliver anything as the currency would collapse and return to be valueless.

Despite the many predictions that a 51% hasher could bring down the currency this hasn’t happened, perhaps because they are making too much money acting as an honest node.

n. Silk Road
On the 2 October 2013 the Silk Road a dark web site was seized by the FBI after Ross William Ulbricht, the alleged founder and owner was arrested in a San Francisco Library. The Silk Road was a market place for illegal and illicit items that had been operating on the dark web for up to five years. Bartlett (31) describes the Dark Net and the services and products available there in significant detail in his book and it is not my intentions to reproduce that detail here. The dark web or deep web are a series of websites not indexed by mainstream search engines, in order to use the dark web a user will normally use a browser designed to anonymise activity such as Tor (The Onion Router). Tor (40) uses a series of interconnected tunnels to connect a user to an endpoint, doing so renders it impossible for internet service providers or law enforcement to observe the websites a user is visiting, it also prevents websites from ascertaining the IP address of the person visiting them. Tor also provides a mechanism to host hidden services that are just like mainstream websites but are not searchable by normal search engines, not traceable and accessible only using Tor. The Silk Road was one of the most successful online market places hosted as a hidden service. Although now infamous as an online marketplace for drugs it offered all manner of illegal products such as weapons and armaments, contract killers, erotica of all types, pirated goods, forged and counterfeit items and medicine. Operating in a way similar to many online marketplaces it offered space for individuals to sell their products. There was a rating system for sellers and buyers. Of particular note for this project is that all purchases were made with Bitcoin. Instead of using a split key all the value was transferred to the operator of Silk Road who when the transaction had successfully completed would then transfer the Bitcoin, less a fee to the seller. Figure 15 - Silk Road payment scheme (41) contains a graphic used by the prosecution team during the trial of Ross Ulbricht that details the payment process.
According to a report produced by the United Nations (42) the dismantling of the “Silk Road” uncovered that the site had handled approximately $1.2B from the two to five years of operation all of which were Bitcoin transactions. When the FBI seized Silk Road in May 2013 Bitcoins to the value of $28M were seized from the administrators (42).
6. Possible mitigations to reduce the negative impacts of virtual currencies.

a. Single controlling entity.
A single controlling entity isn’t a viable option for a currency such as Bitcoin that has already been established upon the basis of consensus and distributed decision-making. The attraction of these type of currencies is that they aren’t controlled by anyone so attempting to exert some control from a central point is unlikely to be effective.

b. Regulation.
A number of governments either have or are considering introducing legislation or licencing for digital currencies however it is important to draw a distinction between those who are legislating to ensure the safety of consumers and to reduce the potential harm done by digital currencies and those who are simply seeing it as an opportunity to raise tax revenue. Unfortunately the majority fall into the latter category. Bolivia, Iceland, Vietnam, Kyrgyzstan and Ecuador all forbid the use of virtual currencies predominantly in order to exert control over capital entering or leaving the respective countries although in Vietnam it has also been linked to criminal activities. Within the United States the Internal Revenue Service (their tax office) have categorised virtual currencies as property and demand tax paid accordingly. In Wyoming and North Carolina they are seeking to treat digital currencies under their Money Transmitters Act in order to regulate usage and will require businesses to obtain a licence before operating a virtual currency business. The European Union has made no decision upon the legality or regulation of digital currencies. In Finland, Spain and Belgium they are VAT exempt and in Germany and Bulgaria the use of digital currencies has been brought within the purview of existing tax legislation.

The United Kingdom Government undertook a call for information in November 2014 (43), which sought the views from interested parties on the benefits of digital currencies as well as the risks associated with them and the impacts upon monetary stability. During the course of the call for information the Bank of England also issued a discussion piece (44) where amongst other things they explored the opportunities a central bank provided digital currency might offer. HM Treasury published the response to the call for information in March 2015 (45) that included the following next steps;

“1.5 - The government intends to apply anti-money laundering regulation to digital currency exchanges in the UK, to support innovation and prevent criminal use. The government will formally consult on the proposed regulatory approach early in the next Parliament.

1.6 - As part of this consultation on the proposed regulatory approach, the government will look at how to ensure that law enforcement bodies have effective skills, tools and legislation to identify and prosecute criminal activity relating to digital currencies, including the ability to seize and confiscate digital currency funds where transactions are for criminal purposes.

1.7 - The government will work with BSI (British Standards Institution) and the digital currency industry to develop voluntary standards for consumer protection.

1.8 - The government is launching a new research initiative which will bring together the Research Councils, Alan Turing Institute and Digital Catapult with industry in order to
address the research opportunities and challenges for digital currency technology, and will increase research funding in this area by £10 million to support this.”

Clearly there is more to be done in the area of digital currency regulation and whilst the next steps outlined by the UK Government might provide a legal framework to prosecute some of the offences set out above it will not provide an international framework to tackle online crime using digital currencies and may just drive currencies to the areas where online regulation is less rigorous.
7. Conclusion
As we have seen in the earlier sections of this project 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 unclear and certainly it will be interesting tracking the trend in such crime. The review of Internet Crime 2013 produced by the FBI Internet Crime Complaint Center [sic] (IC3) reported no specific virtual currency related activity even though it reported on CryptoLocker Ransomware (46). By the publication of the IC3 Annual Report for 2014(47) digital currencies where involved in just 392 of the total complaints which amounts to less than 0.24% of reports, the majority of these report related to victims not receiving the mining equipment they had ordered, people sending their mining equipment to participate in mining pools only to be scammed by operators and lastly people having their online wallets emptied.

From a money laundering perspective although useful for moving value across borders, converting cash to currency and vice-versa is so difficult at present that it doesn't appear to be a feasible solution. Focussing legislation and regulation

Future take-up of virtual currencies is bound to drive their usability for legitimate consumers as well as for the criminal. To date the most Bitcoin transactions in a single day took place in July 2015 when there were 214,487 (48) Bitcoin transactions world wide, compared to 51M (49) per day for Mastercard alone; this is a tiny share of the world financial market and until usage increases accessibility of services and vendors willing to accept Bitcoin will not increase, neither will the ability to covert cash to Bitcoin and vice versa and this will have a limiting factor upon the criminal who wishes to use virtual currencies for illegal or illicit purposes.

Although the opportunities exist for cyber crime based upon or utilising digital currencies at the moment there appear to be little evidence that it is being taken up. This might be that there is a reluctance to use this unproven technology but that is unlikely. It may be that reporting and detection is running at a much lower level than the actual amount of crime being perpetrated or perhaps it is because the currencies are being used for criminal purposes, à la Silk Road, making it difficult to report crimes. It may also be that law enforcement organisations are less attuned to digital currencies than they are to conventional money especially in the investigations of small-scale / small value crime which are rarely assigned to a specialist task forces that benefit from a wider pool of expert advice. This might well be the case as it was observed by the Home Affairs Select Committee in 2014 that there was a low awareness of online and digital crime in rank and file police officers.

The evolving regulatory landscape will also have an impact upon the use and policing of digital currencies as will the development of altcoin systems that seek to deliberately conceal or obscure the usage of their customers. In a like manner there is detailed research emerging that seeks to offer new ways to analyse transactions and attempts to untangle and highlight inappropriate usage.

Digital currencies will continue to offer utility to criminals whilst they exist in their unregulated form. It remains to be seen if the currencies will collapse before their utility, legitimate and illegitimate are regulated to such an extent that they wither and die of natural disinterest.
8. Bibliography


