Virtual currencies and their potential role in cyber crime

Kevin Law

Abstract:

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.