Appendix 3.06.5 Cryptocurrencies and Fraud

Is GIGO the only blockchain threat?

No. These are some of the possible threats.[1] Blockchains are ultra-secure, but as with all technology, the criminal is one step ahead. For example:

Frauds and Blockchains

51% attack

The 51% attack is when a single miner node, which happens to have exceptionally more computational resources than the rest of the network nodes, dominates the verification and approval of transactions and controls the content of a blockchain. If it possesses more than half of the network's processing power, the dominant node can outpace all other nodes, manipulate the blockchain, insert fraudulent transactions, double-spend funds, or even steal asset from others.

Identity theft

Although blockchains can preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is acquired or stolen, no third party can recover it, unless there is some central permissions agency which stores duplicates. Consequently, all the assets this person owns in the blockchain will vanish, and it will be nearly impossible to identify the thief. The consequences may be more devastating than identity theft in the offline world, where third-party institutions (e.g. credit card companies) or central authorities safeguard transactions, control risks, detect suspicious activities, or help find culprits.

System hacking

Although it is difficult to hack and alter records stored in a blockchain, not so the programming codes and systems that implement its technology. MtGox, once the largest Tokyo-based Bitcoin exchange, was hacked in March 2014, and Bitcoins worth $700 million were stolen. Poorly-maintained and outdated codes allowed malefactors to double-spend. A more recent incident afflicted a Decentralized Autonomous Organisation that holds large quantities of Ethereum, the second cryptocurrency after Bitcoins (as per 2018). The hacker exploited a software vulnerability and stole $50 million worth of Ethereum.

Coindash (a cryptocurrency) ICO (initial coin offering)

This start-up raised $7m before a hacker changed the address to which money should be sent, causing subscriptions and donations to go to an unknown address. This actually happened twice.

Other issues to watch for

Regular users of the dark web and using cryptocurrencies have found a range of criminal, or fraudulent activities.[2] Many of these affected the cryptocurrency Ethereum losses – payments lost were made in ether. Ethers are second only to Bitcoins. These include:

[1] https://jfin-swufe.springeropen.com/track/pdf/10.1186/s40854-016-0046-5
[2] https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/

- Parity wallet breach – affected ethers. Bug in wallet allowed $60m in ethers to be stolen.
- The blockchain start-up Enigma saw its website, mailing lists and an administrator account compromised when fraudsters launched a fake token pre-sale, defrauding investors of more than 1,500 ethers.
- Parity wallet freeze – a bug suddenly occurred freezing $275m in ethers.
- Tether token hack – Tether is a cryptocurrency, someone hacked into their virtual treasury and stole $31m.
- Bitcoin gold scam – this involved a Bitcoin fork – a split to overcome the limitations of Bitcoin. (This is quite common with cryptocurrencies). Users found their wallets drained after processes involved in the split. Around $3m in a variety of cryptocurrencies was lost.
- NiceHash (a cryptocurrency mining market place) allowed an employee's computer to be compromised and stole 4,700 Bitcoins (around $50m at the time).

Bitcoin problems – a note

There is a problem with Bitcoins – that no one administers them and no-one can agree how they might be expanded.[3] To maintain the system, data processing providers (and this can be anyone) earn Bitcoins but this is steadily reducing in the amount earned. There is also a limit of seven transactions per second on the current available Bitcoin mining system, as of 2017[4] This may change. So new crypto-currencies, such as Ethereum, Ripple, and about 1,000 others are growing in volume.[5] Our guess is that the anonymity function won't survive on the most popular currencies going forwards. It may be an option, but legal constraints, implemented by governments, will mean that within Western and some Asian countries, anonymity won't be allowed, or if allowed it will be under stringent conditions.

We can't verify this, but we heard that PwC had actually produced a set of financial statements using Bitcoins in Hong Kong. The big issue is you have to take management's word for where the currency came from or was paid to. There is no other way with the anonymous Bitcoins. For systems outside the Bitcoin, recording that information is all important. But we can reference an article which claims PwC will accept payment by Bitcoins in Hong Kong.[6]

[3] *The Economist (31 October 2015).* The great chain of being sure about things
[4] *The Economist (20 May 2017)*
[5] Op cit.
[6] http://www.scmp.com/business/companies/article/2122349/accounting-big-four-pwc-accepts-bitcoin-payment-hong-kong