Introducing - A New Crypto for Black Hat Hackers Only

Retrieved Friday 28th of July 2017 06:37:15 PM

All tools have destructive potential. Some would use blockchain technology to destroy the blood diamond trade. Others would harness it to create blood diamonds of their own.

Blood diamonds are mined in areas of conflict, to finance further conflict, often by slaves. To own one, is to own a fragment of condensed human suffering.

The UN attempted to stamp out the flow of blood diamonds from Sierra Leone and the Congo by adopting the “Kimberley Process” in 2003. But this process is a bureaucracy, and those with the skills can defraud the system. Rough diamonds raked from the earth by children working 48-hour shifts in brutal conditions still find their way on to the fingers of blushing brides to be.

A company called Everledger recently revealed its ambitions to evaporate the blood diamond trade with transparency. Its aim is to record the provenance of every diamond that is mined and track its progress from the earth to the store where it is sold, on a publicly available ledger, or blockchain. Every time a diamond changes hands, the transaction is recorded on to the ledger, so that the history of every diamond can be traced by anyone back to its source. It’s digitised more than a million diamonds now, and has its eyes set on incorporating fine art, classic cars and even ivory on to its blockchain. Freshly poached elephant tusks will be hard to sell as antiques if they’ve no history of ownership.

The transparency provided by public blockchains has the potential to destroy these illicit trades by making the history of the objects available to anyone.

But as the blockchain gazes into blood diamonds, the blood diamonds gaze back.

New Turkmenistan

One of the primary criticisms levelled at bitcoin is the colossal amount of energy it consumes. The bitcoin network uses more than 14 terawatt hours of electricity per year, equivalent to the nation of Turkmenistan. The energy required by the network to process a *single bitcoin transaction* could power five American homes for a *day*. And what does the bitcoin network achieve with all the energy it consumes? Nothing but the security of bitcoin itself.

Many bitcoiners argue that an auto-secured currency is a bargain at twice the cost, but others disagree. Such a vast network of computing power, working tirelessly – could it not be used more productively? A vast electronic brain of networked devices, working around the clock – why not use them to solve major problems facing the world, or even answer questions beyond the capacity of the human mind?

The idea that cryptocurrencies should be mined or minted in the pursuit of something greater than their own security has led to some interesting “altcoins” (any digital currency that isn’t bitcoin is classed as an altcoin, revealing the extent of bitcoin’s dominance). Primecoin for example, is a cryptocurrency mined by finding new chains of prime numbers. Computers in the network compete with one another to find rare primes and are rewarded with Primecoin. While some hunt for rare primes “for the glory”, the primes can be used for computational hardware development and aid in the study of number theory (although some hunt for primes). Although rather niche, it’s a great example of a cryptocurrency being actually productive, and achieving something other than its own security. I expect more cryptocurrencies like this will appear over time, with greater productive value.

What makes the concept of a cryptocurrency fascinating is the moral side to the story. If you can incentivise a global, decentralised network to achieve a task, why must these tasks be ethical? Why not give them a malicious task to complete? Why not offer them the carrot of currency only after they’ve destroyed your enemies?

And these are the fields where digital blood diamonds are mined. Welcome to DDoSCoin, where a currency is created by proving that you’ve broken the law.

Zombie hordes

DDoS stands for “distributed denial of service”. A DDoS occurs when a website receives so much internet traffic that it crashes, causing service to be denied to those wanting to browse it.

It is the internet equivalent of a horde of men trying to enter a camping tent all at once – the weight and stress causes the tent to collapse, and takes time to set up again. The internet traffic, or horde, can be quite innocent in intent – when mainstream news features a small website in a story, that website often crashes when everyone tries to see what the fuss is all about. As the website is small, it cannot support many users at once.

The bigger the tent, the more people it can hold – government websites are like big tops at a circus, and can only be collapsed by large hordes. Websites like Google are even bigger, great cavernous structures, accustomed to massive amounts of online traffic – Genghis Khan calibre hordes are required to take these down.

While a DDoS can occur unintentionally, they are more often deliberate, conducted by a tiny number of individuals, who have enslaved a network of computers to do their bidding.

These networks are known as botnets: everyday computers infected with software that links them together and allows a “botnet master” to control them. To perform a DDoS, the botnet master orders them to flood a certain website with traffic until it shuts down. To continue the metaphor, it is like a horde of suggestible zombies being ordered to charge at a specific tent their master dislikes.

Anything with access to the internet can become part of a botnet. In fact, the very device you are reading this on may be a member, moonlighting as a zombie without your knowledge or permission – few would be able to tell.

The advent of “smart” devices has created botnets that are increasingly large and bizarre. In October last year a botnet named Mirai (Japanese for “the future”) made up of 380,000 zombie devices, stormed massive tents like Twitter, Netflix and Airbnb, causing them all to crash under the strain.

What made the Mirai horde fascinating was that the zombie devices within in its ranks were not just everyday computers. It was made up of toasters, kettles, televisions, cameras and baby monitors; “smart” devices connected to the internet for ease of use. As they were connected to the internet, they could be infected with malicious software and become zombie devices, suggestible and ready to charge at a moment’s notice should the botmaster desire. The owners didn’t notice of course – a new mum checking on her child with a zombie baby monitor would have no idea that at that very moment the baby monitor was causing Twitter to crash.

Crypto from the Congo

Bitcoin operates using a “proof-of-work” protocol – miners are incentivised to prove to the network that they have verified bitcoin transactions, and are rewarded with bitcoin.

DDoSCoin also operates on a proof-of-work protocol, but not only must miners verify transactions; they also *must prove to the network that they have participated in a DDoS attack*.

Those with a grudge against a certain website, submit “bounty posters” to the miners, setting out how hard they want a website to be hit, and how much they are willing to pay for this to occur. Of the eligible candidates, the network reach consensus over which websites they fancy attacking and which they don’t, compiling a “victim list”. After submitting proof to the network that the victim has been hit with as much strength as described on the bounty poster, the miner receives the fruit of their criminal labour: DDoSCoin. This can be spent adding or removing a website from the victim list, or exchanged for other digital currencies.

DDoS attacks are illegal – DDosCoin’s very creation would be a crime. Mined from suffering, and used to finance more of it, owning DDoSCoin would be the digital equivalent of owning a blood diamond.

DDoSCoin has not actually been released into the “wild” as it were. It was created by a professor and a PhD student at the University of Michigan in the US, who wanted to explore the idea of a malicious proof-of-work protocol. They didn’t set up a DDoSCoin network, only prove it was possible to create one.

Innovation like this is fascinating and for better or worse, it is only the beginning for blockchain technology – the future is grey.

Until next time,

Boaz Shoshan

Boaz Shoshan

PS My colleague Sam Volkering has written a book detailing how he expects this digital currency market to explode, and how to take advantage of it. If you’re interested, click here.

PPS What do you think the future holds for these technologies? Will blockchain innovation be good for humanity overall? Let me know: boaz@southbankresearch.com.