Understanding Cryptocurrencies and potential for XXXXX

By: Miriam Hussain

I. Understanding Cryptocurrency

A cryptocurrency is a complex and innovative digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. Cryptocurrencies can be classified as digital currencies, alternative currencies and/or virtual currencies. Cryptocurrencies use decentralized control as opposed to centralized electronic money and central banking systems. The decentralized control of each cryptocurrency works through a **blockchain**. Bitcoin, created in 2009, was the first decentralized cryptocurrency. Since then, over 1,800 cryptocurrencies have been created.

Cryptocurrencies emerged as a side product of another invention i.e. the Peer-to-Peer digital cash system in late 2008. The attempts at building a digital cash system without a central entity such as a Peer-to-Peer network gave birth to the cryptocurrency -- the missing piece to realize digital cash. To realize digital cash a payment network with accounts, balances, and transaction is needed. Usually, this is done through a central server that keeps records on balances. In a decentralized network this server does not exist, so every single entity of the network must work to avoid double or overspending of accounts. This solicits for all peers in the network to have a full list with all transactions, to check if future transactions are valid or if there are perhaps any overspend attempts. For end to end security and traceability, peers of the network need to be in absolute consensus about every single transaction.

Cryptocurrencies alike physical currencies are therefore just limited entries in a database that no one can change without fulfilling specific conditions. As opposed to a centralised server or ledger, they consist of a network of peers for transactional checks and authentication. Every peer has a record of the complete history of all transactions and thus of the balance of every account. A transaction is a file signed by an initiator‘s private key. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer using basic p2p-technology. The transaction becomes known by the whole network almost immediately, but only gets confirmed after a specific amount of time. Confirmation is a critical concept in cryptocurrencies. As long as a transaction is unconfirmed, it is pending and can be forged. When a transaction is confirmed, it is no longer forgeable, it can‘t be reversed and becomes part of an immutable record of historical transactions or the “blockchain”.

Blockchain, is therefore a digital shared record of transactions maintained by a network of computers on the internet without the need of a centralized authority. It has become a key technology in both the public and private sectors, given its ability to record and keep track of assets or transactions with no need for middlemen.

Only ***Miners*** can confirm transactions. They take transactions, stamp them as legit and spread them in the network. For this job, the miners get rewarded with a token of the cryptocurrency. The miner‘s activity is arguably the single most important part of the cryptocurrency system. Principally anybody can be a miner, however to prevent abuse such as through creation of thousands of peers and spreading forged transactions, miners need to invest/use their computers to qualify for this task, i.e. through locating/finding a ***hash*** or a product of a cryptographic function that connects the new block with its predecessor. This is called the ***Proof-of-Work***.

A hash is the basis of the cryptologic algorithm that miners compete to solve. After finding the solution, a miner can build a block and add it to the blockchain. As an incentive, he has the right to add a so-called coinbase transaction that gives him a specific number of cryptocurrency tokens (such as Bitcoins). Since the difficulty of the algorithm increases the amount of computer power the miners’ invest, there is only a specific amount of cryptocurrency token that can be created in a given amount of time and is part of the consensus no peer in the network can break.

Understanding Cryptocurrencies and potential for XXXXX

By: Miriam Hussain

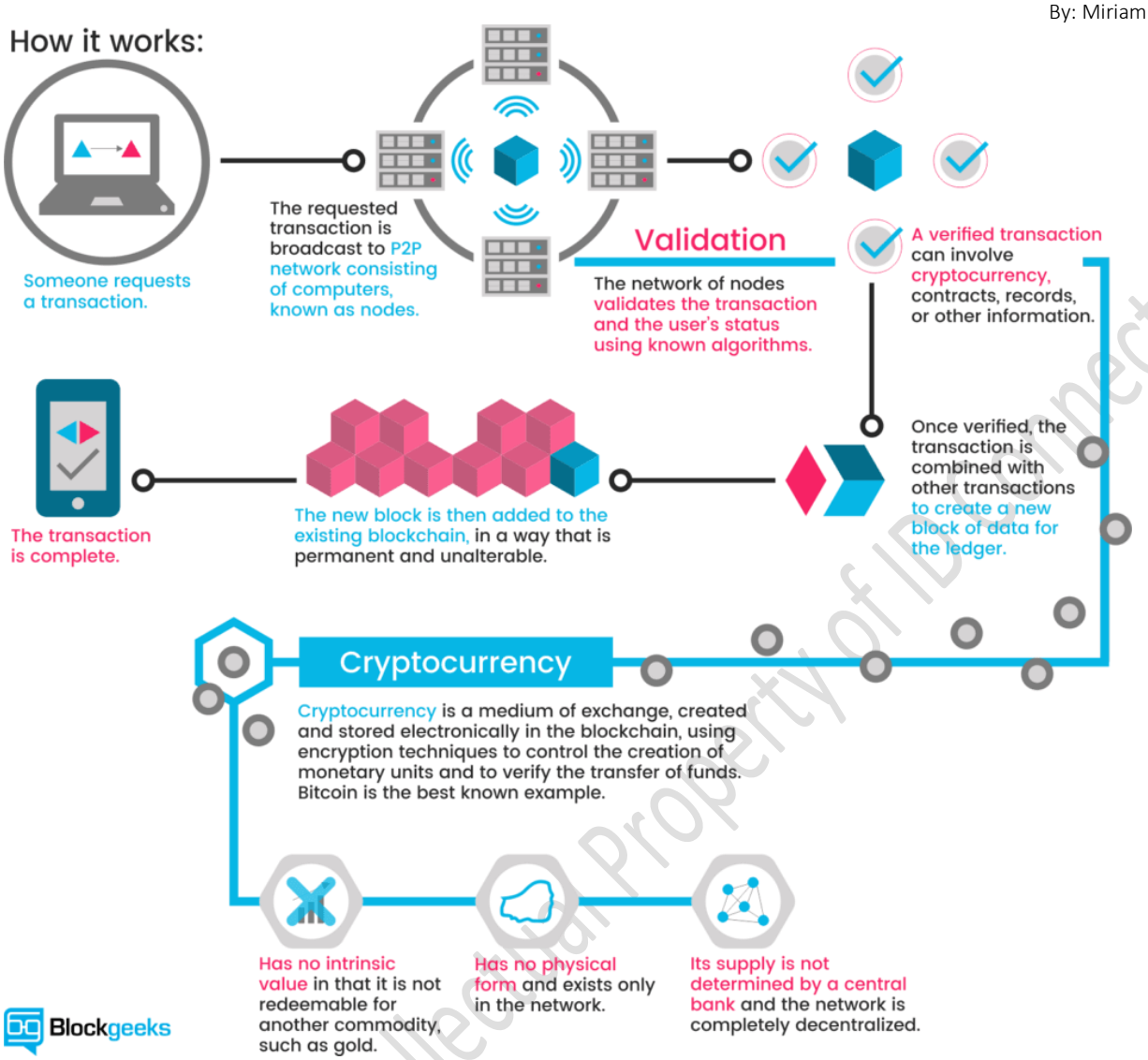

Figure 1: The Process

II. Existing Mechanisms and Peer Review

Blockchain digital identity to deliver international aid to Syrian refugees -- In 2015, AID:Tech teamed up with the Irish Red Cross and Lebanese humanitarian experts to implement the world's first aid delivery project using Blockchain technology. The objectives were to field test the AID:Tech platform focusing on Syrian war refugees living in camps and in the city of Tripoli in North Lebanon. The humanitarian objectives were to ensure refugees received aid in a transparent manner while preserving their dignity and humanity.

Blockchain and eye scan payments for refugees -- Thousands of Syrian refugees in Jordan's Azraq camp pay for their food by a scan of their eyes. Purchases are then recorded on a computing platform based on blockchain. Iris recognition devices at the checkouts of the camp's supermarket authenticate customers' identities and deduct what they spend from sums they receive as aid from the World Food Program (WFP). The U.N. agency launched the futuristic system in May as a one-month pilot involving 10,000 of Azraq's more than 50,000 inhabitants in a bid to explore blockchain's potential to cut costs and bottlenecks.

The UN Blockchain Club -- The innovation units at UNOPS, UNDP and U.N. Women started an informal grouping to exchange information about their blockchain work. The club has now grown to include around 10 members, including UNICEF and XXXXX.

UNICEF's Crypto Fundraising– UNICEF Australia just launched the HopePage that uses subscribers/users computers' processing powers to mine the cryptocurrency "Monero". Any earned or mined coin is then automatically donated

to UNICEF Australia as opposed to being paid to the miner. HopePage is a transparent, opt-in mechanism that borrows a computers' processing power and allows subscribers/users the ability to choose levels of power to be donated. It's entirely user-initiated, with participation totally at the discretion of users/subscribers.

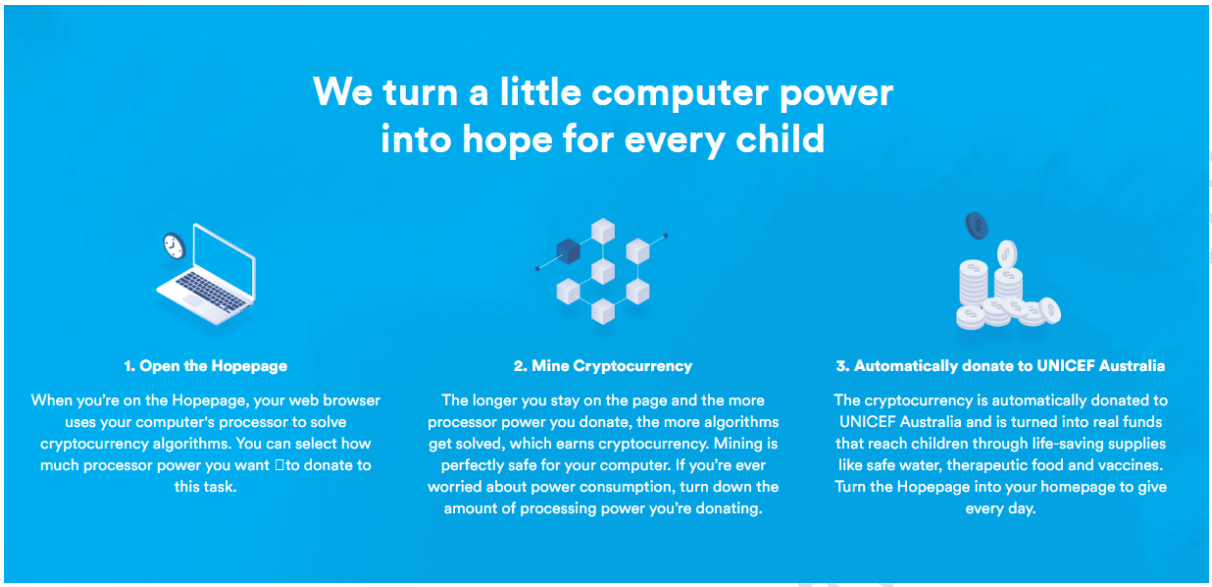

Figure 2: UNICEF Model

Previously UNICEF used mining for the cryptocurrency Ethereum to raise funds through its **Game Chaingers** project for children in Syria by targeting computer gamers. The project was noted to carry limited appeal and fell considerably short of its targets, since it required users to download mining software.

III. Potential for XXXXX

A comprehensive assessment of potential for XXXXX must be carried out in collaboration with respective stakeholders including XXXXX-Innovation (member of the UN blockchain club), XXXXX- Digital Identity (involved in implementation of blockchain initiatives in Lebanon and Jordan) as well as PSP-IG and Digital Engagement teams, who have a clear stake involved, owing to the nature of the business. Further this must be led by an external consultant with relevant expertise given the complexity of the subject matter.

Notably potential for XXXXX in financial terms may mean following a similar "mining" model to that of UNICEF, in which case respective initiative/campaign must be led by IG and/or Digital Engagement teams, simpler mining methodologies agreed and an exchange agent identified from the outset. Alternatively cryptocurrency donations for eventual exchange with cash[1] may also be accepted. However in this case, the wider acceptance/exchange of only the most popular cryptocurrencies with a wider dealership such as Bitcoins, Monero or Ethereum must be duly considered.

IV. General Risks

For a complete risk assessment please defer to Due Diligence findings. However vis-à-vis potential and despite full traceability, a few risks related to cryptocurrencies transactions susceptibility to "hacks" or "forgeability" remain, at least until they are mined and linked/entered on to the blockchain.

Further as cryptocurrencies are centred on the principle of decentralisation, they proactively work to take away transactional controls and hence risk management from a central authority, placing it in the hands of individuals. Whilst essentially anyone can be a peer or a miner, in absence of necessary background checks this could pose some reputational/brand integrity risks by association. In general, cryptocurrencies and particularly the most popular ones

[1] Coinbase, Gemini, CEX.IO, Kraken, Bitstamp and GDAX trade cryptoassets for cash. However, most dealers only trade a few biggest cryptocurrencies for cash. Further options are generally considered very limited when it comes to countries where cryptocurrencies can be used.

including Bitcoin, Monero and Ethereum are also prone to misappropriation, since owing to their virtual nature they could be used to fund clandestine activities[2], money laundering[3] and/or for tax evasion etc.

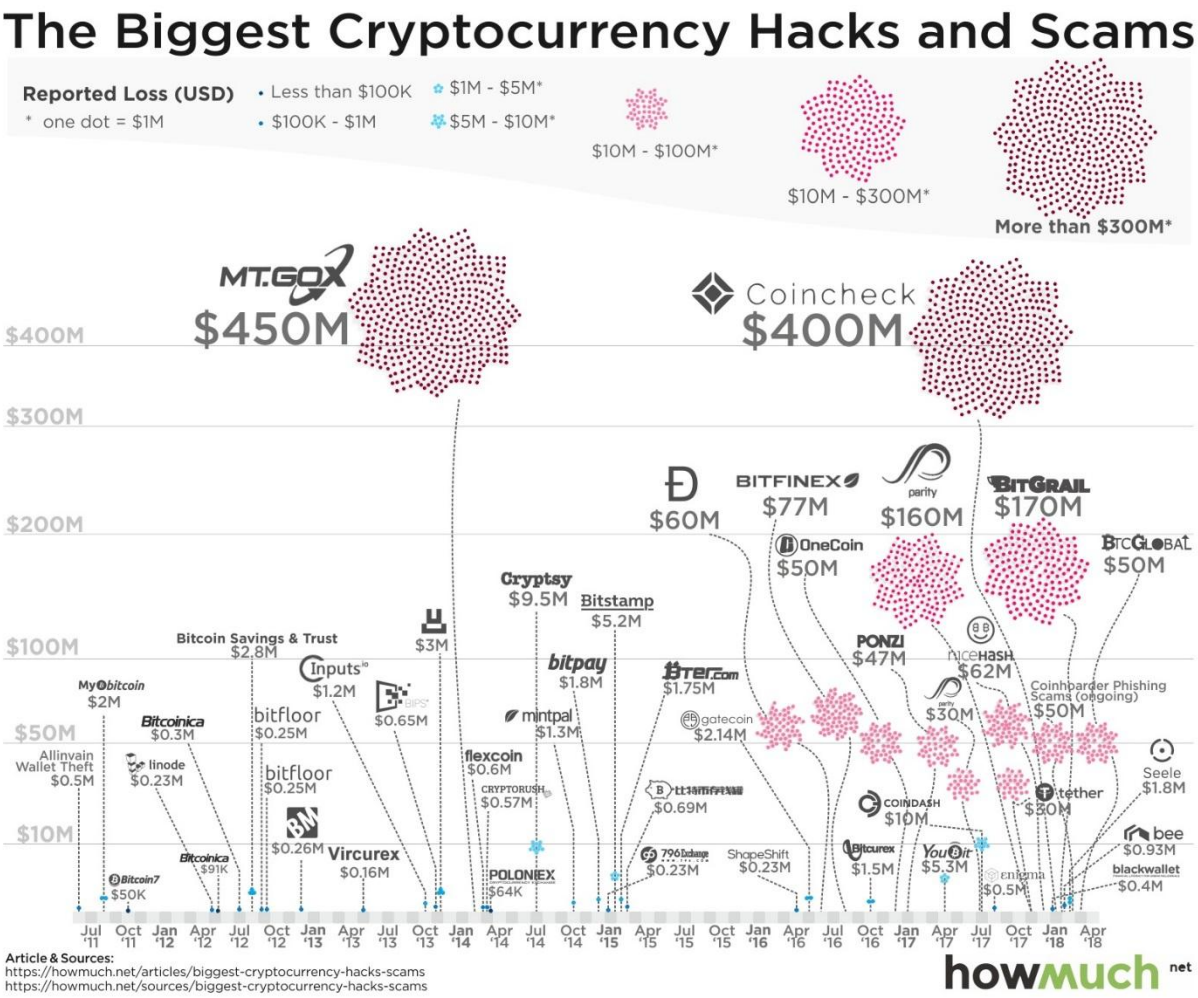

Figure 3: Hacks timeline of some leading Cryptocurrencies

[2] According to a Europol report in 2017, a significant proportion of cybercrime is carried out by financially motivated criminals who are increasingly using cryptocurrencies for trading in criminal markets or for extorting funds from their victims.

[3] Europol, estimates that criminals in Europe generate $140 billion in illicit proceeds annually, of which about 3 or 4 percent - $4 billion to $6 billion - is being laundered via cryptocurrencies.