Could Crypto-currency Disrupt Money?

JUNE 12, 2014 *By* Vikas Shah - Thought Strategy *in* FINANCE & ECONOMICS, MANAGEMENT & STRATEGY LEAVE A COMMENT

Money is a strange phenomenon. Our modern notion of it mean that (*in essence*) it is intrinsically useless apart from as a medium of exchange. Our government, regulators, law and communities agree that phenomena (*whether a physical banknote or an electronic ledger such as a bank account*) have certain value, in certain units and certain denominations.

From a cultural perspective however, things are not quite so clear. As society advances (*technologically and socially*) we find that many things which were thought of as *fiat (http://en.wikipedia.org/wiki/Fiat_money)* can change. Examples can be found all around us… In linguistics, it's not uncommon for words which (*previously*) existed as slang to be adopted and accepted into mainstream language. This is both a move of progression (*the expansion of culture*) and efficiency (*helping to communicate the zeitgeist more accurately*). Interestingly, with language- as with money- it is often only when the '*regulator*' (*for example, the dictionary producer*) agrees that a word is now accepted, that it is made so!

The Language of Money

Crypto-currency (http://en.wikipedia.org/wiki/Cryptocurrency) is an interesting phenomenon. It is a system of exchange which exists as *fiat* in nature, but which also has security. Traditional currency is secured by the notional protection of the central bank from where it is issued- whilst crypto-currency is secured by the integrity of the system itself. Subverting a traditional currency is made impossible due to the supranational power of the issuer, and subverting a crypto-currency is (*theoretically*) impossible due to the mathematics of breaking the encryption.

In recent years, novel entrants to the market such as BitCoin (https://bitcoin.org/) have moved crypto-currency from the fringes (*where they were akin to linguistic slang*) to the mainstream- where multi-billion dollar business are now accepting BTC's as legitimate payment for goods and services (http://www.fiercecable.com/press-releases/dish-accept-bitcoin).

So, could BitCoin disrupt money?

To learn more, I spoke to two world experts. Prof. Campbell Harvey (http://en.wikipedia.org/wiki/Campbell_Harvey) of Duke University's Fuqua School of Business (http://www.fuqua.duke.edu/) and Kate Craig-Wood (http://en.wikipedia.org/wiki/Kate_Craig-Wood) (*Founder of CipherMine (https://ciphertrade.com/), a virtual crypto-currency business quoted on the virtual stock exchange LTC Global (https://www.litecoinglobal.com/)*)

Q: What are the principles behind crypto-currency?

[Prof. Campbell Harvey] Crypto-currency is a means by which people can exchange property in a secure way without the use of a central institution like a bank or the Federal Reserve (http://www.federalreserve.gov/). The currency is digital and particular crypto-currencies like BitCoin go to extreme lengths so that you can only spend your digital currency once. Think of it this way. You can exactly make a copy of a picture or some music on the computer. It is a perfect counterfeit. You can do the same with a currency code. Hence, it is very important to keep track of the codes so that you only spend it once.

[Kate Craig-Wood] Crypto-currency is a type of digital currency. Unlike real money, they are decentralised and transactions are free; no bank in the middle taking their slice and nothing central to fail.

They are as real as real currency and can be used to purchase anything from Starbucks coffee (http://cointelegraph.com/news/111130/bitcoin_coffee_at_starbucks) through to Jaguar cars (http://www.bitcar.co/category/jaguar/), many well known brands are starting to accept BitCoin payments. In the US & UK crypto-currencies are viewed as commodities and there are several high value exchanges where you can exchange your coins for fiat currencies like the one you're using every day.

Let's not forget that currencies today are based on good will not gold reserves.

Q: What are the key forms of crypto-currency competing in the current market?

[Prof. Campbell Harvey] Digital currencies began in the 1980s. However, they only really became popular when BitCoin was introduced in 2009. BitCoin solved a key problem (*it prevented people from spending the digital currency twice*). Right now the market is very small. BitCoin is about $8.5 billion which is tiny compared to the amount of US dollars.

[Kate Craig-Wood]BitCoin, by far the largest crypto-currency market, is valued at USD $8.3 Billion. For comparison, the total size U.S. annual GDP is USD $17.234 Trillion. (source (http://cointelegraph.com/news/111703/what_are_cryptocurrencies))

However, there are now thousands of crypto currencies with Litecoin (http://en.wikipedia.org/wiki/Litecoin) the second most popular. The main difference is based on the scrypt algorithm (http://en.wikipedia.org/wiki/Scrypt) used to mine the coins. BitCoin uses the SHA-256 hashing algorithm (http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf), Litecoin, however, uses the scrypt algorithm, incorporating the SHA-256 algorithm, but its calculations are much more serialised than those of SHA-256 in BitCoin, making it far more secure.

It takes 2.5 minutes to generate a LiteCoin block, as opposed to BitCoin's 10 minutes. Aside from mining there is little to distinguish coins to the user.

Q: What has been the use of crypto-currency in the financial markets?

[Prof. Campbell Harvey] Many people speculate in BitCoin. It is approximately 8 times more volatile than the stock market. However, that is not the primary use of BitCoin. BitCoin is designed to efficiently and securely aid in transactions.

BitCoin is decentralized. There is no central clearing house. There is a central general ledger. People check the ledger to make sure you have the BitCoin to pay. After each transaction, the transactions go into a pool that will be eventually added to the general ledger. Anybody connected to the BitCoin network can check the ledger.

[Kate Craig-Wood] There is a new breed of ex-style trader who tend to be found at the BTC-e.com (http://btc-e.com/) toll box who are making waves and accumulating wealth via crypto coins.

Penny stock-style pump-and-dump schemes involving BitCoin, like the recent one organised by a trader known on Twitter as Fontas, have also started to attract more professional traders. In the US & UK crypto coins are now recognised which is a step closer to legalising the trading activities.

Excitingly, a new market has emerged where you can trade virtual company shares in exchange for crypto coins. The most famous BTC Trading Corp was closed down due to US pressure. Following its collapse a few of us are poised to launch CipherTade, the world's first fully regulated crypto-currency based on crowd-funding with after market. We started out thinking that we'd just be making a technical platform to replace LTC Global & co, but after becoming increasingly expert in relevant bits of regulatory frameworks, we concluded that the real opportunity is to become the world's first regulatory-compliant, cryptocoin-based crowdsourced startup funder with an aftermarket (*the order matching engine*). We are aiming to be a true pioneer bringing together the brilliant innovations of cryptosecurities (*cryptocoins' goodness, global Web access, API driven, complete transparency, etc*) with more traditional processes (*formal business management, due diligence processes [on users and issuers alike], policing of the after-market, corporate visibility, legal compliance, etc*).

Q: What are the risks and challenges associated with crypto-currency?

[Prof Campbell Harvey] The BitCoin general ledger is called the block chain (https://blockchain.info/). It is remarkably secure. To break into the chain, you would have to amass 25,000 of the world's fastest supercomputers. That seems completely infeasible. This is one of the big advantages of BitCoin – the ledger is practically unhackable. There are no technologies on the horizons that even come close, even including quantum computing.

Note that Mt. Gox (http://en.wikipedia.org/wiki/Mt._Gox) was a third party – a sort of bank. However, their security was lax (*and it was well known before the "theft"*). It was somewhat akin to a regular bank have their doors open, the vault open, no security, no employees, no cameras.

[Kate Craig-Wood]Inherently, crypto coins tend to be very secure thanks to their decentralised nature and publicly available block chain. Whilst they can be abused, it is now technically infeasible for BitCoin & LiteCoin. However the smaller emerging currencies are subject to 51% attacks.

The weak link in the security of your BitCoins tends to be where you store them – ie. on a laptop or phone that is lost or stolen.

Q: What are the alternative applications of crypto-currency?

[Prof. Campbell Harvey] The block chain or general ledger could be a secure repository of private information, property ownership, and conditional contracts. For example, consider buying a car. The dealership sells it to you and it goes into the block chain. You have a private code that identifies you as the owner. Only you can start the car with that code.

[Kate Craig-Wood] There are potentially other applications of crypto coins – due to the data that is stored in the block chain. Some believe it is possible to use coloured coins to make fully distinguishable security exchange. Such coloured BitCoins can be used for alternative currencies, commodity certificates, smart property, and other financial instruments such as stocks and bonds.

In my view, you would need to redesign some crypto currencies from the ground up. Most alt coins are merely code forks of BitCoins and don't generally include anything novel.

Q: What do you see as the future of crypto-currency?

[Prof. Campbell Harvey] BitCoin might not be the final model but it is definitely here to stay. Many have criticized BitCoin because it enables illegal transactions. I think the critique is lame. Did you know that 75% of the value of all U.S. cash is in $100 bills? Wonder why. Did you know the average wallet size (*cash/number of people*) is $4,000? Cash is the problem. Indeed, with BitCoin there is a record of every transaction every made. Criminals prefer cash.

[Kate Craig-Wood] Like types of credit card (*Visa, Mastercard etc*) there is room in the market for a handful of cryptocoins. I think that two things matter in determining which those will be:

1. Useful, functional differences to BitCoin.
2. First-mover advantage.
3. A community of users and developers supporting it.

Based on this, my top 4 cryptocoins which I think most likely to have a future are:

1) BitCoin (*BTC*). It has numerous flaws and is technically inferior to Litecoin and others, but history tells us that the most popular standard wins out – not necessarily the best. As a SHA256 coin, mining is now restricted to people with specialist hardware so it is becoming less of a hobbyist activity.
2) Litecoin (*LTC*). As above, Litecoin is the leading competitor to BitCoin. As well as being technically superior it also has a devoted community, loosely based around the Litecoin forum. It also

has a strong developer community and even its own association. Litecoin can also be cost-effectively mined with GPUs since scrypt is more memory-intensive than SHA256.

3) Anoncoin (http://www.anoncoin.net/) (*ANC*). Although cryptocoins are designed to be decentralised and thus somewhat anarchic, they can quite easily be traced. Since many of the users of cryptocoins want anonymity, a group of very clever guys created Anoncoin. Its main feature is that it can be routed through I2P, the Invisible Internet (https://geti2p.net/en/). Anoncoin is a scrypt-based coin like Litecoin.

4) Primecoin (http://primecoin.io/) (*XPM*). Primecoin differs mainly in the way it is mined. Mining Primecoins consists of finding ever-larger prime number chains (http://en.wikipedia.org/wiki/Cunningham_chain). In theory this work could be useful. SHA256 and scrypt coin mining is a complete waste of power and computation by comparison. Also, Primecoin can be effectively mined with CPU only.

Cryptocurrencies have the potential to challenge our financial systems as we known them today, a cycle of increased government taxation will incentivise people to turn to decentralised systems which are inherently harder to regulate and tax.

The Future

Change happens in waves. Innovations enter a culture, and are adopted with varying degrees of stickiness. In most cases, this creates [*often unexpected*] emergent phenomena which, over time, transform the way our world functions.

Technology has transformed commerce into something which is almost unrecognisable from the markets of even 50 years ago. High performance computing, connectivity and software innovation now mean that we now treat money as bits of information. Surely therefore it is only natural that bits of information should be treated as money?