FUTURE OF VIRTUAL CURRENCY

Edith Mihaela DOBRESCU [49], PhD
Emilian M. DOBRESCU [50], PhD

Abstract

Virtual coins are deployments of the "crypto-coin" concept and operate by virtue of a distributed database, each transaction being validated via nodes connected without the need for a supervisor such as a central bank. Each participant has the opportunity to create new Bitcoin coins for the personal use of these coins, thus being rewarded for participating in the validation of other transactions in that virtual currency.

Bitcoin coins are not real money. It's like an online token that can be exchanged for goods and services in the places that accept it, just as someone gives someone a dollar because they bought something worth one dollar. But, unlike the dollar, which has series and number, Bitcoin - is an electronic record without registration number or other kind of mechanism that could be used to trace buyers or sellers.

Keywords: bitcoin, coin base, virtual currencies, XBT.

JEL classification: E4, E44, E52

Introduction - What is Bitcoin?

Bitcoin is a virtual currency built around a complicated cryptographic protocol and a global computer network that supervises and checks what coins have been spent by whom. Due to its anonymous character, bitcoin is a popular choice for illegal activities because it is extremely difficult to find out who uses Bitcoin.

Bitcoin appeared in 2009, being - after other authors - the creation of Satoshi Nakamoto, which can be both a name and a username. Bitcoin is "electronic cash, it's not real, it's just the bearer in our computers" (Andrei Andone, Romanian expert in bitcoin). Bitcoin it is a transfer between a real money seller and the bitcoin buyer, who can be the same person, with the help of a mediator, usually a trading platform (behind which is one or more specialists). To buy bitcoin, you can offer economic goods (commodities and services) or another currency - real, this time - in exchange, according to the parity of the day of the transaction. To sell bitcoin is similarly procedure.

Bitcoin is a so-called virtual currency, decentralized and secured by cryptography. All virtual bitcoin coins physically exist simultaneously on each user's computer (or the server used by him), but only bitcoin owners have access to them. Market capitalization, that is, the value of all current bitcoin coins at current quotation, is 15 billion dollars, investments in profile launches start-up have exceeded one billion dollars, and only the current consumption of the system is 170 MWh, similarly with the production of the current of medium-sized thermal power plant.

Bitcoin coins are not real money, they are obtained by completing missions (or equations) called "mining". In practice, users use their computers for the trading system, and in exchange for providing transaction processing power they are paid in bitcoin. Bitcoin can buy a range of goods and services from computer games, web services, jewelry, weapons or even cocaine, precisely because bitcoin does not have a registration number, so transactions are protected by anonymity.

Since 2014, the symbols used to represent Bitcoin are BTC, XBT. Small quantities of bitcoin used as alternative units are: millibitcoin (mBTC), microbitcoin (µBTC) and *satoshi* - called as a tribute to the creator bitcoin, a *satoshi* is the smallest amount of bitcoin, representing 0.000.000.01 bitcoins, 1/100.000 .000 of a bitcoin. A millibitcoin is equal to 0.001 bitcoins, which is a one thousands of bitcoin. A microbitcoin is equal to 0.000001 bitcoins, which is a millionth of bitcoin.

On October 7, 2014, the Bitcoin Foundation unveiled a plan to apply for a bitcoin ISO 4217 currency code, and referred to BTC and XBT as their preferred candidates.

[49] Institute for World Economy, Romanian Academy, Bucharest, Romania, e-mail:edithdobrescu@gmail.com
[50] Institute for National Economy, Romanian Academy, Bucharest, Romania, e-mail:dobrescu@acad.ro

Building on the unsuccessful success of bitcoin, in the years 2016-2017, other electronic coins appeared:

a)On December 27, 2016, *Ether* - the virtual currency required to operate the Ethereum network, which was then 7.22 dollar on the Poloniex stock exchange; over four months, on May 7, 2017, the value of an ether was 986.76 dollar. Vitalik Buterin invented Ethereum, the main competitor of the bitcoin network at just 19 years of age; has 23 years now and is a millionaire given the nearly 500,000 of his own, according to his own statements;

b)*Monero* – is another virtual currency, which was on May 22, 2017 worth 31 dollar, is very far from 1 bitcoin, worth about 2,000 dollar. If, in the case of Bitcoin, any transaction can be tracked through its virtual catalog, Monero is evolving in this respect, and transactions can be anonym despite their public nature. Monero is, therefore, the preferred currency for hackers and in illegal transactions that take place in the “dark area” of the Internet, the so-called Dark Web;

c)*Ripple* is the third virtual currency as a value on the cryptographic market and is a payment protocol, currency exchange and a real-time settlement system.

Who is Craig Wright?

Australian contractor Craig Wright publicly acknowledged the bitcoin inventor, writes BBC. Wright also provided technical evidence to support his assertion that he was the "parent" bitcoin. Members of the Bitcoin community and development team have confirmed that it is he who invented one of the most controversial coins in the world.

Craig Wright has revealed his identity to the BBC, The Economist and GQ. After meeting with the BBC, Wright signed digital messages using cryptographic elements developed in Bitcoin's first internships, linked to the virtual currency and the "mind" behind it.

Craig Steven Wright is an IT specialist. He completed the Padua College in Brisbane (Australia) in 1987. He was a computer science professor and researcher at Charles Stuart University, where he also completed a second doctorate. He has worked in IT for several companies, such as OzEmail, K-Mart and the Australian Securities Exchange. He thought architecture for Lasseter Online's first online casino.

Wright was the CEO of Hotwire Preemptive Intelligence Group, which was planning to launch Denariuz Bank, the world's first Bitcoin bank, but faced problems with Australian regulators and abandoned the project. Wright is also the parent of DeMorgan, and Panopticrypt Cyber Security Company.

In 2015, Newsweek announced that he had "discovered" the creator of the virtual bitcoin coin in the person of a 64-year-old Japanese-American who lived near Los Angeles. Then the magazine said he found the mysterious "Satoshi Nakamoto," the person whose name is related to the creation of the coin.

"The discovery" turned out to be a false track, and Dorian Nakamoto (named Satoshi baptism) came to sue Newsweek after saying that his life was all over his head. In December 2015, a new publication, Wired magazine, claims that Satoshi Nakamoto is a pseudonym used by a 44-year-old Australian cryptologist named Craig Steven Wright: "Wright either invented the bitcoin, whether it is a shining fern who strongly wants to believe he is the inventor, "writes Andry Greenberg and Gwen Branwen. The Wired Magazine quotes surface documents that it claims to reveal talks between Wright and his lawyers, saying: "I've done my best to hide that I've been running Bitcoin since 2009."

Wright's blog was deactivated shortly after the Wired article, and its Twitter account was completely deleted. According to online profiles that remain online, Wright leads DeMorgan, a Sydney-based company that analyzes "alternative currencies."

Surfing documents and the fact that Wright holds a huge volume of bitcoin come to support what Wired magazine writes.

How Bitcoin Virtual Machine Works

Imagine the bank's safe-deposit box. Enter yourself and you have the key only from your box, which you know the number. You can open it and download it. But the value boxes also have a slot, like mailboxes, where you can enter content into anyone else's box. But you do not have the keys and you do not know who the owner is unless he told you. Each user can keep a copy of the entire vault with all the value boxes. Thus, all users can be present in the vault with value boxes, alone and simultaneously at the same time. Everything is so certain that nobody has ever managed to forge a key, break a box, or stick his hand through the slot. Instead, be careful, if your key is stolen, or you entrust it to someone who does not need it, the robbery becomes trivially easy. Even anonymity is not fully guaranteed - disclosure of identity for a single transaction can help identify all operations made from the same box. Rigorously meaningful is the bitcoin description as a pseudonym coin.

Actual coins are "mined", which anyone can theoretically do. Each bitcoin is earned by solving a cryptographic problem that requires large processing resources. The time and resources required to solve are perfectly predictable, but they are getting longer with each bitcoin already produced. It is an industrial business like any other - it costs equipment, wages and (very much) current. Sales are virtually guaranteed, with the risk being the price at which they will happen. Most bitcoins are now produced in China, three to four very large farms; up to now about 15-16 million bitcoins have been produced. In the current trading system, the maximum possible number of bitcoins is 21 million and will be reached in a few years if the current bit rate quote continues.

Trading Levels

In the short term, bitcoin also appreciated 16% in a single day, trading close to dollar 300 per unit hours after San Francisco's Coinbase announcement, which introduced the bitcoin virtual currency to the US market. But the lack of confidence of those who participated in making bitcoin transactions brought back its quote.

In August 2016, 1 bitcoin was trading at a rate of 233 dollar to change for 730 dollar on December 2, 2016, and the bitcoin market was available for 9 billion dollar worth of transactions. Against the backdrop of geopolitical instability, bitcoin has steadily advanced in recent months in 2016, reaching a level of 1,131.15 dollar on Jan. 5, 2017, near the record high of 1,141.16 dollar according to the Coindesk platform. Throughout 2016, the currency advanced by 122%. China and India have been major buyers.

So at the beginning of 2017, Bitcoin recorded trading at dollar 1,163 on the Bitstamp European exchange from the end of 2013. Then, on January 10, 2017, 1 bitcoin changed to 773 dollar for May 1917 to reach the maximum trading threshold of 1,900 dollars for 1 bitcoin, and on May 22, 2017 it exceeded the threshold of 2,000 dollar for 1 bitcoin to reach dollar 3,000 for 1 bitcoin in June 2017!

Theoretically, the bitcoin system allows 12.5 coins to be added to the system every 10 minutes. When Bitcoin reaches the maximum quotes - shown above - its total bitcoin value in the system is at a maximum of over dollar 16 billion, roughly equivalent to an average company, part of the UK FTSE 100 stock index.

In 2016, bitcoin was the best performing currency, outpacing 125% of all censuses of coins issued by central banks. Bitcoin has likely been boosted in the last year by increased demand in China amid a 7% Yuan annual devaluation in 2016, the worst performance of the Chinese currency in more than 20 years. According to the data, most of the bitcoin transactions are made in China.

Advantages of Virtual Coins

Virtual coins are a means to transfer money globally quickly and anonymously and are not subject to any authority, making it attractive for those who want to escape capital controls. Bitcoin is also attractive for those worried about a cash crisis such as India. "The increasingly tough war against cash and capital controls make the bitcoin currency a viable alternative, though risky," says Paul

Gordon of the UK Digital Currency Association, and co-founder of Quantave, a company that tries to facilitate institutional investors' access to virtual currency exchanges.

Virtual coins can be used to sell or buy services, products, or other currency by downloading an application to your mobile phone or computer. Here's an example: "There is no central site, but windows sites to the bitcoin world. The coin is just on the phone or computer in your own wallet. For example, I offer 700 dollar and receive 1 bitcoin in my wallet. Download an application on your phone and create a private key and wallet in your device's memory, "said an experienced user in the bitcoin transactions field. „I think it is an interesting alternative asset, especially as a means of protecting you against demonetization or other geopolitical factors," said David Moskowitz, CEO of Attores, a platform that uses blockchain technology to execute contracts.

The bitcoin was generally characterized by high volatility, and in 2015 and 2016 it gained more stability. Bitcoin popularity as an alternative asset for refugees is rising among investors because the virtual currency is considered to be less influenced by government regulation and monetary policy changes.

Disadvantages of Virtual Coins

The maximum total market capitalization of all bitcoin coins in circulation is about 16 billion dollars. But, compared with all other assets, especially gold, shares, real estate, 16 billion means very little. Although generally characterized by high volatility, the virtual currency has gained more stability over the past two years. The meteoric rise of bitcoin in recent months may be partly due to an imbalance between supply and demand, which may be mitigating in the future. The bitcoin currency has therefore been extremely volatile in its history so far, with transactions often being disturbed by hacking scandals on various platforms.

The production and trading of bitcoin virtual currency transactions implies a very high consumption of electricity resulting from the cryptographic algorithm processing on which this coin is based. One of Bitcoin's first deployments works with a distributed database, each transaction being validated via the connected nodes without the need for a supervisor such as a central bank. Moreover, each participant has the opportunity to create new Bitcoin coins for their personal use, thus being rewarded for participating in the validation of other virtual currency transactions. The recipe used has a disadvantage: the production and intermediation of transactions in the Bitcoin coin implies a very high consumption of electricity resulting from the cryptographic algorithm processing on which this coin is based.

If, at first, the problem of energy consumption was rather theoretical, as more and more individuals and businesses joined the effort to generate as many bitches as possible, energy consumption rose: in the most pessimistic scenario envisaged by Sebastian Deetman, the computing systems used to process Bitcoin transactions could reach, by 2020, an electricity consumption of more than 14 GW, equivalent to a modern European country, such as Denmark.

Despite currency claims, Bitcoin cannot be used because of the huge volatility. Even sites claiming to "accept" payments with Bitcoin actually have prices denominated in dollars, euros or other real currency, and only accept Bitcoin as a method of transferring funds at the current quotation. Transfer to Bitcoin is by far the cheapest of all - down to 0.0001 bitcoin, that is below 5 cents per transaction. Money collects all of the "miners", because also confirming transactions is a service that requires computing resources. The biggest use of Bitcoin - in the area of illegal transactions (drugs, weapons, etc.) on sites like Silk Road - is, in fact, a major drawback for Bitcoin.

Blockchain - Technology for Virtual Coins

Blockchain is comparable to the world of finance with what it was twenty years ago for the world of information: a technology that allows fast, secure and decentralized transactions. Bitcoin was the first Blockchain application.

Blockchain in the Vision of Some Central Banks

The Bank of England is exploring the possibility of introducing a coin called RSCoin, on which it has complete control and eliminates the need for commercial banks - clients would settle their transactions directly with central banks.

China's Central Bank wants to move to a digital version to help internationalize the Yuan, but still allow it to preserve monetary sovereignty.

The Central Bank of Russia will allow banks to use the blockchain to operate transactions between them. And the Central Depositary in Moscow wants to start an electronic voting system by blockchain.

The Central Bank of Australia made a block bill transaction simulation with 10 of the world's largest banks in early 2016.

Canadian Bank of Canada tests blockchain technology for a money transmission system.

The Central Bank of the Netherlands, a member of the Eurozone, mentions in the 2016 report the possibility of creating a parallel national currency based on bitcoin, to which he found a new name: DNBCoin.

The European Central Bank is of the opinion that Distributed Ledger Technology (the generic name for blockchain) is "panacea or straw fire".

The US Federal Reserve is "optimistic" about the blockchain and believes it will lead to the deepest transformation of the financial system of the 1970s of the last century.

Blockchain in the Vision of Commercial Banks

The 42 large commercial banks of the world formed in 2016 the R3 consortium, development and blockchain research. Among them are Goldman Sachs, JP Morgan, Citi, and Bank of America, Société Générale UBS, Credit Suisse, RBS, BNP Paribas, HSBC, Barclays, Nomura, Deutsche Bank, Société Générale, Unicredit, and ING.

Vice President Sberbank, the largest bank in Russia, predicts the disappearance of banks in just 10 years as a result of blockchain technology.

Billon is a regulated blockchain payment system, backed by a number of large Polish banks and set at one-to-one parity with the Polish zloty.

Blockchain in the Eyes of Card Issuers

Visa believes the potential of technology is still underestimated. He hired developers to develop a scalable version of the blockchain.

MasterCard is cautious in approaching, but not from inertia but because it does not want to be "blindsided", meaning to ignore any further potential technology with even greater potential.

Blockchain Seen by Technology Companies

Microsoft offers "Blockchain as a service" on the Azure cloud computing platform.

Intel has already published an experimental code from its research into the application of blockchain technology to the so-called "Internet of things".

Amazon prepares to include blockchain in the giant machine of the AWS application suite, precisely to "disrupt financial services."

IBM builds a blockchain-based payment system to sell to banks.

Blockchain Electronic Settlement System

Blockchain is the technology that makes it possible to operate the Vault Vault described above - an algorithm that allows the encryption of public key transactions, access to them with private keys, and the public distribution of the entire resulting log. In traditional finance, an important transaction is settled through the escrow account: the money is held by a third party. However, the escrow account has substantial costs because it requires highly qualified human supervision, so it is only used for large transactions and important contracts. With the help of blockchain, the escrow function can be programmed into the payee itself, so the actual transfer is only made when the algorithm finds objective (but also observable online, which is an important limit at this time). In this case, the electronic money leaves bankers, accountants and lawyers in a single shot.

Blockchain technology provides an easy way for banks to make payments directly to each other. Equally well, Blockchain technology may be the factor that will neutralize the dominance of US administration in the global financial sector, and some analysts believe that this seems to happen as quickly.

On Aug. 24, 2016, four of the world's largest banks announced they will join in creating a new financial solution protocol built on Blockchain technology: Deutsche Bank in Germany, UBS in Switzerland, Santander in Spain and Bank of New York Mellon joined forces to launch a new coin called Coin Utility Settlement. Like Ripple, Setl, Monetas and other rival technologies, Utility Settlement Coin could end the US banking system's dependence on cross-border payments and transactions. Banks will be able to make payments to each other in a direct way without passing through US money.

The total costs of clearing and settlement of international financial transactions are estimated at 65-80 billion dollars a year, according to a report published in 2016 by Oliver Wyman, a global consultancy firm. This has enormous implications, especially for American banks. For example, the Federal Reserve has already warned that financial technology could pose stability risks for the US financial system.

The Trading Network

The Bitcoin network has a 30,000 times more power than the world's top 500 supercomputers, $ 200 million worth of equipment, and 100 million dollars in day-to-day transaction security, ZF said Andrei Andone, founder of StartHash: "To take control of the network, someone should practically invest $ 200 million in equipment and spend $ 1 million a day on energy consumed. Bitcoin spends each day to secure himself so the money is not faked or stolen. "

There is a public register that records the bitcoin virtual currency transactions. Transactions in the form of the payer X sends Y bitcoins to the payee Z are running on this network with easily accessible software applications. Network nodes can validate transactions, add them to their copy from the registry, and then send these additions to the registry of other nodes. The block chain is a distributed database to independently verify the property chain of each bit hole, and each network node stores its own copy of the block chain. Approximately six times per hour, a new group of accepted block transactions is created, added to the block chain and quickly published to all nodes. This allows the bitcoin network software to determine when a certain amount of bitcoin has been spent, this being necessary to prevent double expenses in a non-centrally supervised environment. Since a conventional register records real banknote transfers or promissory notes that exist besides it, the block chain is the only place where bitcoins can be said to be in the form of unspent transactions.

The property right associated with bitcoin money assumes that a user can spend bitcoins associated with a specific address. For this, a payer must digitally sign the transaction using the appropriate private key. Without knowing the private key, the transaction cannot be signed, and bitcounters cannot be spent. The network checks the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other proof of ownership; the coins thus become unusable and are actually lost. For example, in 2013, a user said he lost 7,500 bitcoins worth 7.5 million dollars when he dropped a hard drive containing his private key.

A transaction must have one or more entries. For the transaction to be valid, each entry must be an uncompleted output of an earlier transaction. Each entry must be digitally signed. Using multiple entries corresponds to the use of multiple currencies in a cash transaction. A transaction may also have multiple exits, thus allowing for more payments.

To send money to a bit-bit address, users can click on the links to the web pages; this is done with a bitcoin temporary URI scheme using a template recorded with IANA. Bitcoin customers, like Electrum and Armory, support bitcoin URIs. Mobile customers recognize bitcoin URIs in QR codes, so the user does not need to manually enter the bitcoin address and quantity. The QR code is generated by user input data based on the payment amount. The QR code is displayed on the screen of your mobile device and can be scanned by a second mobile device.

Bibliography

Bouri, E., Gupta, R., Lau, C. K. M., Roubaud, D., & Wang, S. (2017). Bitcoin and Global Financial Stress: A Copula-Based Approach to Dependence and Causality-in-Quantiles (No. 201750)

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016, March). Bitcoin-NG: A Scalable Blockchain Protocol. In NSDI, pp. 45-59

Karame, G. O., & Androulaki, E. (2016). Bitcoin and Blockchain Security. Artech House, pp 35 -39

Li, X., & Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems, 95, 49-60.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, pp 66-70

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin, pp 86 - 92

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.