A study of digital currency cryptography for business marketing and finance security

Tai-hoon Kim

Abstract

A medium of exchange is an intermediary used in trade or business to avoid the inconveniences of a pure barter system. While many things could be used as a medium of exchange in an economy, fiat money including currency bills and coins is the most common and generally accepted as a unit of account which is deemed to represent a standard and store of value. In engaging in e-commerce, people may opt to send money through money remittance agents or through banks for a fee.

The Age of the Internet has finally brought upon us a new phenomenon known as digital currency cryptography. No intermediaries. No service charges. No legal fees. No delays. With ease, people of any country can be able to send, receive and store value on their digital wallets.

Keywords: Digital Currency, Cryptography, Currency, Business marketing, Business Security

1. Introduction

A digital currency is new class of virtual currencies with high degree of decentralization. It is a peer-to-peer using the process called cryptography, wherein ordinary information is converted into a secret code or unintelligible text in order to secure transactions, increase supply and prevent fraud[1][2]. The idea of using cryptography to make digital currencies aims to control the creation and transfer of money without relying on financial institutions and it is considered as an attempt to replace monetary transactions with a digital medium of exchange using peer-to-peer networking[3][4].

Digital currency has several important features. First thing is that it is decentralized. It is not being controlled by central authority or banking institutions. Being decentralized means that it is resistant to shutdown attempts, that if one part of system is offline, other transactions can still keep on going. Another thing is that it’s easy to set-up. Creating an online account is fast and does not file much legal documentary requirements. A bank account is not even necessary. Signing-up with such ease, gives an opportunity to all netizens to be able to engage in such activity. Digital wallet software which can be accessed through desktop computer or mobile phones may be utilized to check your account balance and make some transactions. Transactions, being
held online, give an opportunity for e-commerce participants to send digital currency cryptography fast in their respective online wallets or accounts in whatever country they are with minimal or no additional fees at all. Making business online can also give the buyer or seller the option to disclose their identities or not. Digital currency adopts the process of anonymization.

There are many types of digital currency cryptography. Common types include, Bitcoins, Ripple, Altcoins, Litecoins, Ethereum, Dash, Dogecoin, Stellar, Peercoin, Bitshares, NXT, etc. As of date, some types of digital currency cryptography having good reputation and large market capitalization are being used and accepted as payment for goods and services offered by legitimate merchants and e-commerce sites[3-6].

2. Brief Digital Currency Cryptography History

In the year 1982, David Chaum proposed a cryptographic untraceable payment system[7]. After six years, in the year 1998, a description of "b-money"—an anonymous, distributed electronic cash system was published by Wei Dai[8][9]. B-money was a purely personal project, it was more conceptual than practical. After a short period of time in the same year, Nick Szabo then created the "Bit Gold". In Szabo’s bit gold scheme, a participant must dedicate computer power in solving cryptographic equations assigned by the system[9]. Bit Gold was an electronic currency system which required users to complete a function with solutions being cryptographically put together and published. The solved equations will be sent to the Bit Gold community and the work will be credited to the person who solved it. The solution will then become a part of their computation, thus creating a chain of new property. Majority of the party must agree to accept new solutions in order to start on the next equation.

The first decentralized digital currency cryptography was introduced by a pseudonymous author Satoshi Nakamoto in 2009 with his article entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”[4][9]. Bitcoin, being the first type of decentralized digital currency cryptography introduced in online market, made a worldwide impact. It used a cryptographic hash function, as its scheme[1]. After this, many other digital currency cryptography have been created, with some having distinct features. Other types of digital currency cryptography which had low market capitalization have died and some survived until the present.

3. Cryptocurrency Transaction Processes

In digital cryptography, the original text known as "plaintext" is turned into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is then decrypted at the receiving end and turned back into plaintext[3]. This is the basic process done by the computers during the transaction processes in the digital currency cryptography system.
So how can someone obtain digital currency cryptography? In the present market, there are three primary ways. Buying them, accepting them as payment and mining new ones. Users may store their digital currency cryptography in their digital wallets including online wallets and mobile wallets.

3.1 Buying digital currency cryptography

The first way of obtaining digital currency cryptography is through buying it. One can be able to purchase digital currency cryptography by paying cash. There are online stores where you can buy through your credit or debit cards. Bitcoin, being the top digital currency cryptography, has partnered with machine manufacturing entities to produce bitcoin ATM. [Figure 1] shows two different models of Bitcoin ATM[10][11]. With the use of mobile phones, cash can be easily convertible into Bitcoins.

![Figure 1] Digital Currency Cryptography ATM

3.2 Accepting Cryptocurrencies as Payment

The second way of obtaining digital currency cryptography is through accepting them as payment for goods sold and services rendered[12][13]. People or business entities use bitcoins in e-commerce, in order to gain more coins[14]. Some of them advertise their products through websites and expand their payment channels by accepting digital currency cryptography payments. A few stores even post that they are accepting bitcoins as payment for the goods that they sell. To ensure profitability, merchants post that they accept bitcoins as payment but actually, it made partnership with business intermediaries. Intermediaries that accept the bitcoins, convert them into cash, and delivers the cash to the merchant.

3.3 Mining Cryptocurrencies
The third way to obtain cryptocurrencies is by mining them[15]. Simply stated Mining is the process of adding transaction records into the cryptocurrency’s public ledger of past transactions commonly known as the block chain[13]. Mining cryptocurrencies is not that easy because it was intentionally designed to be resource-intensive and difficult. It takes time and money to mine. Common investment and expenses required in this activity would be the hardware software used the electricity to run the computers and rent of office space if you don’t have one.

In the mining ecosystem, users have used various types of hardware to mine these blocks. Early digital currency cryptography used Central Processing Unit (CPU) Mining. After a while, Graphics Processing Unit (GPU) mining[16][17] a more efficient way was introduced. Other mining techniques such as Field-Programmable Gate Arrays (FPGA) mining[17], Application-Specific Integrated Circuit (ASIC) mining[17][18] was also integrated in other digital currency cryptography systems.

Mining digital currency cryptography has a limit. As for the Bitcoin digital currency cryptography, it only has a maximum limit of about 21 million bitcoins[19]. This will just be the amount that will circulate in the bitcoin system.

[Figure 2] shows a simplified diagram of how digital currency cryptography transactions work in a decentralized peer-to-peer network. One possible scenario in this figure is that Miners use past transactions and solve a mathematical function to produce a digital currency cryptography this will then be put on the digital currency cryptography exchange. A person may then obtain a digital currency cryptography by buying on the exchange. His digital wallet balance will then increase while the balance of the exchange will decrease. This person can also use this to buy goods on a store, after buying his balance decreases while the balance of the business man’s digital wallet increases.
4. Top 10 Cryptocurrencies

This part discusses things regarding the top 10 Cryptocurrencies based on their Market Capitalization (from greatest to least) as of December 5, 2015[13]. Ranking may vary in future dates.

[Figure 3] shows the logo image of a Bitcoin (BTC). It is the first implementation of the digital currency cryptography concept. It is open-source and it is publicly designed, nobody owns or controls Bitcoin and every account holder can take part of it. Through many of its unique properties, this type of digital currency allows exciting uses that could not be covered by any previous payment system[14]. Currently, it holds the largest market capitalization amounting to $5.5 Billion[13].

[Figure 3] Bitcoin (BTC)

[Figure 4] shows the logo image of the digital currency cryptography called Ripple (XRP). It is also an open payment network within which that currency is transferred. Ripple is a distributed, open-source payments system that is still in beta. The systems goal is to enable people to break free of the of financial networks ie, credit cards, banks PayPal and other institutions that restrict access with fees, charges for currency exchanges and processing delays[15].

[Figure 4] Ripple (XRP)

[Figure 5] shows the logo image of the digital currency cryptography called Litecoin (LTC). Litecoin is also
A study of digital currency cryptography for business marketing and finance security

a peer-to-peer digital currency cryptography based on the Bitcoin protocol. It differs from Bitcoin in the sense that it can be efficiently mined with consumer-grade hardware. This one provides faster transaction confirmations and uses a memory-hard, scrypt-based mining proof-of-work algorithm to target the regular computers and GPUs most people already have. Litecoin aims to provide a mining algorithm that could run at the same time, on the same hardware used to mine bitcoins[16].

[Figure 5] Litecoin (LTC)

[Figure 6] shows the logo image of the digital currency cryptography called Ethereum (ETH). This digital currency cryptography is a decentralized platform that runs smart contracts- applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. It was crowdfunded during August 2014 by its fans all around the world. It is developed by ETHDEV with contributions from great minds across the globe[17].

[Figure 6] Ethereum (ETH)

[Figure 7] shows the logo image of the digital currency cryptography called DASH. It’s name is derived from Digital Cash. This is a privacy-centric digital currency cryptography with instant transactions. It is also based on the Bitcoin system, but it has a two tier network that improves it. Like bitcoins, Dash anonymization
technology makes it impossible to trace the one who made the block chain. It is a great improvement in the system for it processes the anonymity through a mixing protocol utilizing an innovative decentralized network of servers called Masternodes. Thus there is no need for a trusted third party that could compromise the integrity of the system. All the confirmation work is done by the miners[18].

[Figure 7] DASH

[Figure 8] shows the logo image of the digital currency cryptography called Dogecoin (DOGE). It’s system is the same with other common digital currency cryptography. Aside from the dog mascot on it’s logo, Dogecoin sets itself apart from other digital currencies with an amazing, vibrant community made up of friendly folks. If you are a creator and you’ll find your fans can financially empower you, for the first time, you can directly receive cash from them rather than valueless likes or retweets[19].

[Figure 8] Dogecoin (DOGE)

[Figure 9] shows the logo image of the digital currency cryptography called Stellar (XLM). The Stellar Development Foundation is a nonprofit organization which builds a common financial platform, designed to be open and accessible to everyone[20].
A study of digital currency cryptography for business marketing and finance security

[Figure 9] Stellar (XLM)

[Figure 10] shows the logo image of the digital currency cryptography called Peercoin (PPC). Peercoin was inspired by , and it shares much of the and technical implementation of bitcoin. The Peercoin source code is distributed under the / software license[21][22].

[Figure 10] Peercoin (PPC)

[Figure 11] shows the logo image of the digital currency cryptography called BitShares (BTS). The platform itself is run and maintained by the BitShares community – an open consortium of individuals and organizations committed in providing universal access to the power of smart contracts[23].

[Figure 11] BitShares (BTS)
[Figure 12] shows the logo image of the digital currency cryptography called NXT. It was launched by anonymous software developer BCNext. NXT uses in order to reach consensus for transactions - as such there is a static money supply and, unlike, no mining. This digital currency cryptography was specifically conceived as a flexible platform around which to build applications and financial services. It has an integrated Asset Exchange which are comparable to, messaging system for its users and an online marketplace. Users also have the opportunity to create new currencies within the system. The last major release of NXT enabled capabilities and a plugin-system for the client[24][25].

![NXT logo](image_url)

### 4. Discussion

This part of the paper discusses things regarding the advantages and disadvantages of using Digital Currency Cryptography.

#### 4.1 Advantages of Using Crypto Currencies

##### 4.1.1 Simplicity

Despite the complex cryptographic technology, cryptocurrency providers designed digital wallets which are simple and easily accessible for the people and business entities. Signing up does not require much details and it does not require bank accounts to be linked in the user’s account. Sending money is as simple as sending an e-mail.

##### 4.1.2 Security

Its complex cryptographic technology - the blockchain system is the reason why it is secured making things impractical for hacking attempts.

Digital currency cryptography cannot be used for double payment. If a cryptocoins has already been sent to
another person, there is no way of getting it back except if the receiver would send it back to the sender. The ledger of past transactions known as the serves to transactions to the rest of the network as having taken place. The nodes in the process use the block chain in order to distinguish or verify legitimate transactions from attempts of the user to re-spend coins in other transactions. There is always a proof of work that can be verified by other users of the system.

4.1.3 Anonymity

Every person has an inalienable right to privacy. That includes financial privacy as well as privacy from surveillance of other people. digital currency cryptography may provide that financial privacy while eliminating the potential for identification fraud and theft of personal information. Since it adopts the process of anonymization, no one can be able to know your personal details except when opt to reveal it or unless you buy digital currency cryptography for cash using your cards, but after that, everything is in stealth mode.

4.1.4 Lower or No Transaction Fees

Opening an account is Free of fees. Currently there are either no fees, or very minimal fees when using digital currency cryptography for payments of goods or services acquired. In other transactions where the seller is linked with an intermediary digital currency cryptography-to-fiat money converter, they might include fees in order to process the transactions faster. Still it’s much cheaper compared to transacting with banks.

4.2 Disadvantages of Using Crypto Currencies

In order to properly store and use digital currency cryptography, one must have a certain degree of technical understanding of the system. This is one of the most challenging part of the digital currency cryptography society. The more you understand the safer your account will be.

Most of the top digital currency cryptography has volatility because of the fact that the amount of coins is limited in amount while the demand for it increases. Economic researchers expect that the volatility will decrease as time passes by. As of date, digital currency cryptography prices are bouncing up. However it might soon be unstable. Some small digital currency cryptography which have low market capitalization tend to go down and die.

Since digital currency cryptography are just newly introduced, it is still considered on its experimental stage. Although some merchants accept payment through digital currency cryptography, it is not yet widely accepted. Some people do not even know about these things. digital currency cryptography are still at its infancy stage. It is still subject to change. A digital currency cryptography having limited number, might not be enough to cater the growing demand of many countries and it still need some growth to do before it reaches its full
potential. Its future is not yet secured.

5. Conclusion

The emergence of digital currency cryptography is one of the innovative ideas to help improve business transactions. It has many advantages as well as disadvantages. There may be many people who are with this peer-to-peer system and there are many people who are against it. Since this technology is still young, digital currency cryptography at present still have many points that must be improved.

References


A study of digital currency cryptography for business marketing and finance security


