BITCOIN – ORIGIN, TRANSACTIONS AND POLICY RECOMMENDATIONS

Nguyen Van Duc *

Abstract: *Blockchain has been revolutionizing the world in the 4.0 technology era. Cryptocurrency in general and Bitcoin in particular is an example of blockchain technology. Bitcoin has been circulating in the market for more than a decade yet not too many people in Vietnam have fully understood the origin of this cryptocurrency, how it works and how best to manage it. This article discusses these issues.*

Keywords: *Bitcoin, Cryptocurrency, virtual currency.*

1. What is Bitcoin?

Bitcoin is a Cryptocurrency, invented in 2008 by an unknown person or a group of people using the name Satoshi Nakamoto, detailed in a white paper "Bitcoin: A Peer-to-Peer Electronic Cash System", published in 2009.

Bitcoin uses SHA-256 (a secure hash algorithm, one of a number of cryptographic hash functions) based proof of work, peer to peer payment without the need for intermediaries. Some countries have allowed commercial transactions using Bitcoin.

Bitcoin functions more as a payment system than a currency. However as a Cryptocurrency, the value of Bitcoin is based on supply and demand and it can be divided into smaller units, named in homage to bitcoin's creator, a satoshi is the smallest amount within Bitcoin representing 0.00000001 bitcoins, one hundred millionth of a bitcoin. A millibitcoin equals 0.001 bitcoins; one thousandth of a bitcoin or 100,000 satoshis.

Table 1. **Basic information about Bitcoin released in August 2019**

1	Name	Bitcoin
2	Ticker Symbol	BTC
3	Creator	Satoshi Nakamoto (original author)
4	Initial release	03 January 2009
5	Time stamping scheme	Proof of Work
6	Hash function	SHA - 256
7	Block time	10 minutes
8	Block reward	12.5BTC/block
9	Halving	4 year/time
10	Next halving	May 2020
11	Circulating supply	17.850.600 (August 2019)
12	Supply limit	21.000.000 BTC
13	Website	http:/bitcoin.org/
14	Block browser	https://www.blockchain.com/explorer
15	Source code	https://github.com/bitcoin/
16	White Paper	https://bitcoin.org/bitcoin.pdf

.....(Source: Bitcoin Vietnam News).....

* Deputy Head, Faculty of Banking,
Hanoi University of Business and Technology

Bitcoin is a cryptocurrency. It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.

2. Pros and Cons of Bitcoin

a) Bitcoin pros

- Highly secure currency. Traditional currencies can be faked, but for Bitcoin it is difficult as the currency is in the form of pre-programmed software based on Proof of Work system.

- *No limit of transaction*. Traditional financial transactions are done through a system of intermediaries. For example, sending any amount of money to a person, the sender would need approval signature from the intermediary, or sending 5,000 USD via PayPal, there are conditions applied and a fee is charged to send the money. Almost no fee is paid when doing transaction using Bitcoin, and it can be from anyone to anyone, using the internet, at anytime.

- *Low transaction fee*. This is a fact. Because every Bitcoin transaction is peer to peer using internet connection, nobody is there is collect the fees on any transfer or purchase/exchange of Bitcoin. Fee, if any, is the processing fee of trading floor.

- *Personal information is protected*. Bitcoin is pseudonymous, meaning that funds are not tied to real-world entities but rather Bitcoin addresses.

- *Potential for ecommerce*. Bitcoin transaction is pseudonymous and irreversible, meaning seller can feel more secure against fake orders.

b) Bitcoin cons

- *Slow transaction confirmation*. Due to security, each Bitcoin is confirmed via many steps and some transactions take 6 steps and 10 minutes to complete.

- *Limited user community*. Despite availability of information about Bitcoin, there are not many users in Vietnam.

- *Difficult to use compared to traditional*. Because nearly all Bitcoin transactions are done through the Internet, those without internet skills will need time to learn and master the use of Bitcoin in transaction.

- *Money laundering and hacker*. Bitcoin is pseudonymous and Bitcoin exchange is under no governmental control, it can be used in illegal transactions and money laundering. It can be stolen as it is stored as digital wallets at trading floor and can be compromised by hackers.

- *Lack of legal framework*. Because of Bitcoin's decentralized nature and its trading on online exchanges located in many countries, regulation of Bitcoin has been difficult. Misinformation relating to Bitcoin is still rampant, making it difficult for the public to understand Bitcoin's nature and other crypto currencies.

3. Bitcoin transaction

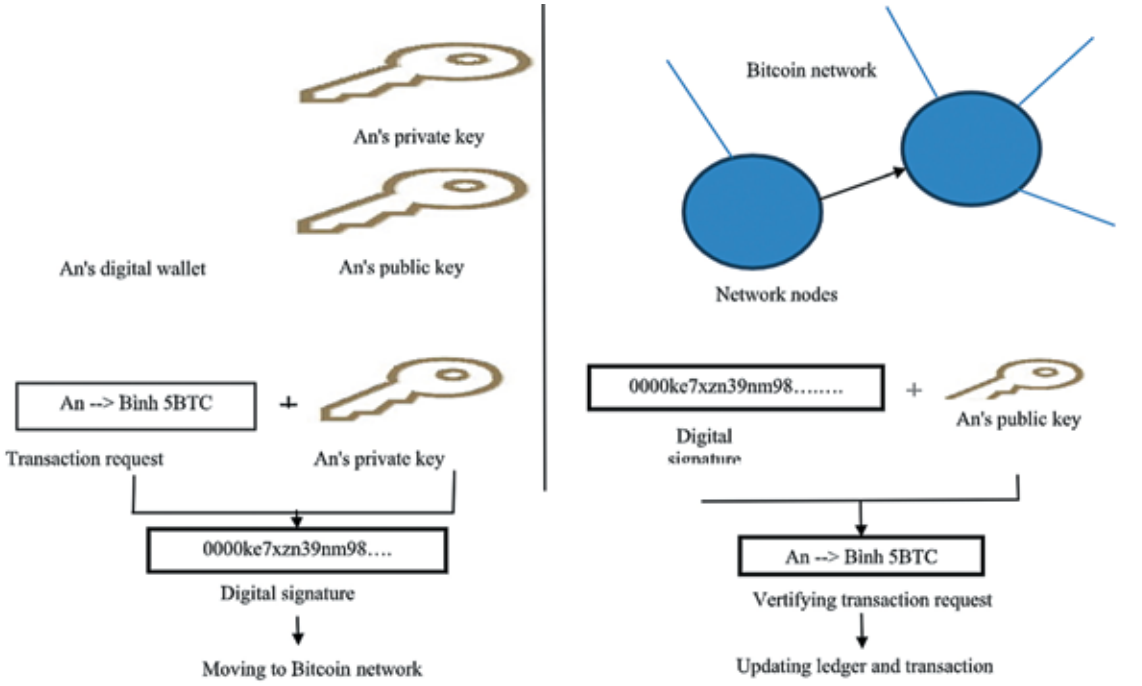
3.1. Bitcoin transaction steps

When payer A wants to transfer 01 Bitcoin to receiver B, it is required to confirm payer A owns at least 01 Bitcoin. In the blockchain network, there is no single record showing how much Bitcoin payer A is having. In order to find out how many bitcoins payer A has owned, it is required to calculate all previous transactions done by payer A to find out how many bitcoins payer A (when downloading the first Bitcoin software, a complete copy of the records of transactions from payer A will be included and it might take 24 hours to download.

When a record of transaction is downloaded, it is easy to find down how many bitcoins payer A owns at the moment).

After confirming payer A has sufficient Bitcoin for the transaction, the next step is to initiate the transaction. The transaction message includes the address of the sender and the receiver, the amount of Bitcoin and the digital signature of the sender. The message is broadcasted publicly; any transaction nodes in the blockchain can accept and execute the transaction.

In order to perform a transaction on a blockchain, payer A needs a digital wallet. This is a software allowing payer A to store and exchange Bitcoin payer A owns. Since only payer A can spend his own Bitcoin, the digital wallet is protected using a special cryptography, with a pair of public and private key. When the message is encrypted, the only person that can read the message is the person with the pair of public and private key. When payer A wants to send the bitcoin to receiver B, payer A will need to send an encrypted message using his own digital wallet and can only uses his own bitcoins, since he is the only person who knows the private key to open the digital wallet. Each transaction node in the blockchain can be verified if it is actually coming from payer A by using the decryption using the public key owns by payer A.



When encrypting a transaction request by payer A using his private key, he is creating a digital signature that can be verified by computer on the blockchain network to identify the owner and validity of the transaction. Digital signature is a chain of encrypted text as a result of combination of payer A's transaction request and his private key. If payer A changes one text in the transaction request, the signature is changed accordingly. That means no potential attacker can change the request of payer A or change the amount of bitcoins he is sending out..

3.2. Management of Bitcoin transactions

In order to manage the amount of Bitcoin each person owns in his account and record these transactions, we need a ledger. The bitcoin blockchain is a public ledger that records bitcoin transactions.

Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. To achieve independent verification of the chain of ownership each network node stores its own copy of the blockchain. To know the balance of the digital wallet, it is required to confirm and verify all transactions on the blockchain related to the digital wallet.

Account of owner	Bitcoin
Nguyen Van A ---> Dang Thi B	2
Dang Thi B ---> Dao Ngoc E	5
…	…

The verification of "balance" is done via calculation record of history of transactions. For example to send 01 Bitcoin to receiver B, sender A has to create a transaction request including links to history of records of previous transactions with total balance of 01 Bitcoin. These links are considered inputs, and "transactions nodes" in the network will verify if the total amount of currency in those transactions is equal or exceeding 01 Bitcoin or not? All is done automatically inside the digital wallet of sender A and can be verified by nodes on Bitcoin network about the activities of sender A in transaction of 01 Bitcoin to the digital wallet of receiver B using public key of receiver B.

The question is how the system can trust the legitimacy of input and its validity? In fact the nodes check all history of records related to the digital wallet of sender A. To simplify and speed up verification, nodes will retain a copy of unspent Bitcoin. This verification method avoids duplicating transactions. Owning bitcoin means having transactions recorded in the ledger linked to the address of the digital wallet that was not used for transaction input before.

All source code for transaction of Bitcoin is open source. Anyone with connected computer can perform transaction. If there is an error of the source code to broadcast transaction message, the bitcoin connected to that transaction is lost forever. Remember the network is decentralized, there is no customer service or technical support that can restore lost transaction or if password of the digital wallet is lost/forgotten. This means if you are interested in transaction on bitcoin network, please take care of the private key or password to your digital wallet.

Anyone can access Bitcoin network anonymously (via TOR or VPN) and send or receive transactions with their public key. However if a person uses the same public key many times, the transactions can be grouped to an owner.

The Bitcoin allows creation of any digital wallet. Each digital wallet has a pair of unique private and public keys. This allows receiving payment in different wallets without having to link them together. It is impossible to know the keys of the owners of different wallets, unless all bitcoins were sent to the same wallet.

Total number of address provided by Bitcoin network is 2^{160}, or equal to 1461 50637330902918203684832716283019655932542976 addresses. This enormous number can protect the network from attacks, yet allowing each owner to have

different wallets without having the same private key for two wallets.

Bitcoin network classify transactions into blocks. Each block has a certain number of transactions and linked to previous block. As time goes, the block will be longer and connected to the previous block as blockchain.

3.3. Bitcoin mining

To transfer Bitcoin, sender will have to send it from his digital wallet. So where does the Bitcoin on the network come from? To reward the complex work of transaction nodes in the blockchain system, the Bitcoin network rewards those taking part in solving mathematical problems in each block. Running blockchain software of Bitcoin in order to receive bitcoin is called mining. Bitcoin mining is the solving of mathematical problems and come up with a 64-digit hexadecimal number, called a "hash," then a block of bitcoin including information of transactions will take care of the rest. Miners will then be rewarded an amount of bitcoin from the network for their work. This reward is the main incentive for miners to invest in computers to operate the nodes, which in turn provide calculation power to the network and maintain stability of the blockchain. By August 2019, there is 17.850.600 Bitcoin mined from the total supply of 21 million. Mining bitcoin has become more difficult and by 2140, it is estimated that 21 million bitcoins will be completely mined. The block reward is halved every four years, leading to fiercer mining competition.

4. Regulations of bitcoins in the world

Management of Bitcoin and crypto currencies differ from country to country, ranging in the following:

First, ***accepting Bitcoin as a form of payment***. Japan is the first country accepting Bitcoin. Japan's Financial Services Agency (FSA) officially recognized bitcoin as a legal tender in Japan on April 1, 2017. There are about 10,000 Japanese businesses accepting bitcoin payment, including its largest cheap airlines. Japan also taxes Cryptocurrency exchange operators.

Belarus has legalized and decleared that transactions, sell, buy, creation of token and mined cryptocurrencies are tax-free until year of 2023.

Cambodia has been trying to legalize and manage transactions of cryptocurrencies as a tool for promoting the economic growth in the era of technology 4.0

Second, ***regulatory warning of risks for users and investors of bitcoin***. Developed countries like the UK, Canada, Norway, Sweden, and Finland… do not ban exchange and trading of crypto currencies and bitcoin income from those transactions are subject to taxation. These countries also warned of the risks of crypto currencies exchange and the state will not protect users/investors in case of risks.

Third, ***forbid the use of Bitcoin in banking and financial sector***. Countries like China, Nigeria… China does not recognize cryptocurrencies as legal tender and the banking system is not accepting crypto currencies or providing relevant services. The practice of raising funds through initial coin offerings (ICOs) is completely banned in China. On September 4, 2017, seven Chinese central government regulators—the People's Bank of China (PBOC), the Cyberspace Administration of China (CAC), the Ministry of Industry and

Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the China Banking Regulatory Commission (CBRC), the China Securities Regulatory Commission (CSRC), and the China Insurance Regulatory Commission (CIRC)-jointly issued the Announcement on Preventing Financial Risks from Initial Coin Offerings (ICO Rules) for purposes of investor protection and financial risk prevention.

Fourth, ***does not recognize and ban Bitcoin transactions***. Countries such as Bangladesh, Bolivia, Ecuador, Kyrgyzstan, Viet Nam, Iceland, do not recognize Bitcoin as a currency and consider all transactions and payment of Bitcoin as illegal. Those countries ban all individuals and institutions from transactions, exchange, buy and sell, use and invest in bitcoin and other crypto currencies in their territories.

5. Policy recommendations for vietnamese government

In the era of technology 4.0, the introduction of crypto currencies in general and Bitcoin in particular is an inevitable trend, an objective requirement of the digital economy. The failure to recognize and ban Bitcoin trading, exchange, purchase and investment activities will partly limit Vietnam's integration into the digital economy, which is becoming a typical trend in the world. In order to manage and promote the positive values of crypto currencies, in my opinion, the Government needs to study and implement some of the following policies:

Firstly, it is necessary to unify and assign the task of managing transactions, trading, exchanging, investing activities, etc. of crypto currencies to a state management agency (the State Bank) like some countries have been implementing (Korea, the UK, Singapore, ...).

Secondly, building a synchronous legal corridor to manage transactions, trading, exchanging and investing crypto currencies like some countries have done (Japan, Korea, Russia, USA,).

Thirdly, adopt tax policies consistent with the policy of managing crypto currencies. The choice of taxes on Cryptocurrency transactions partly reflects the views and attitudes of governments in crypto currencies management. When the government accepts and views the Cryptocurrency in general, and Bitcoin in particular, as a currency, as a legal tender, it is necessary to apply a tax policy in the direction of not levying VAT on transactions or exchange of traditional currencies and crypto currencies. However, the income or profit gained from trading activities, investing crypto currencies will be subject to PIT or CIT according to the laws./.

Reference:

1. Decision 1255/QD-TTg, dated August 21, 2017, on approving the scheme of completion of the legal framework on management of virtual assets, digital currencies and virtual currencies.

2. Herald (2014). "Korean – American caught buying illegal drugs with Bitcoin". The Korea Herald. Herald Corporation.17 March 2014. Retrieved 20 April 2018.

3. *Bitcoin, crypto-monnaies et blockchain: mirage ou miracle?* Alternatives Economiques, 18/11/2017.

4. McKenna, F. (2017). *Here's how the U.S. and the world regulate Bitcoin and other cryptocurrencies*. Market watch, 28 December 2017.

5. http:/bitcoin.org/, https://www.binance.com; https://remitano.com; https://bittrex.com

TIỀN THUẬT TOÁN (BITCOIN) – NGUỒN GỐC, NGUYÊN LÝ HOẠT ĐỘNG VÀ CÁC KHUYẾN NGHỊ CHÍNH SÁCH

Nguyễn Văn Đức *

Tóm tắt: Công nghệ blockchain đã và đang tạo ra một cuộc cách mạng thật sự trong kỷ nguyên công nghệ 4.0. Theo đó, đồng tiền thuật toán nói chung, và đồng Bitcoin nói riêng, là một ứng dụng điển hình của công nghệ blockchain. Bitcoin đã xuất hiện trên thị trường hơn 10 năm. Tuy nhiên, đến nay ở Việt Nam vẫn chưa có nhiều người hiểu chính xác, khoa học về nguồn gốc, nguyên lý hoạt động, cũng như chính sách quản lý Bitcoin. Đây là những nội dung chính được đề cập trong bài viết này.

Keywords: Bitcoin, tiền thuật toán, tiền ảo.

Ngày nhận bài: 19/08/2019

* Phó Chủ nhiệm khoa Ngân hàng,
Trường Đại học Kinh doanh và Công nghệ Hà Nội.