**Forward - Age of Digital Currency**

Computer technologies are developed rapidly in 21st century and changing human’s life personally and socially. For instance, development of social networks change how people communicate with each other. On the other hand, the development of digital currency changes how people buying and selling goods.

Bitcoin is one of the most outstanding digital currencies in these few years. The rise of Bitcoin leads concerns. One of the hottest topics is what government should react to bitcoin. In this report, the background, advantages, disadvantages, social issues and governments’ attitude toward bitcoin will be discussed.

**Background of Bitcoin**

Some of the fundamental information of bitcoin will be covered in this section. For example, the historical background of bitcoin and the computer technologies being used in Bitcoin network.

**What is Bitcoin/bitcoin?**

Bitcoin is the first decentralized cryptocurrency in the world. A decentralized currency is a currency without a central organization to manage. A cryptocurrency is a digital currency that makes use of the principles of cryptography to secure the information.

Strictly speaking, ‘Bitcoin’ and ‘bitcoin’ describe different concepts. ‘Bitcoin’ represents the entire network and technology of the decentralized digital currency while ‘bitcoin’ is a common unit of currency with a short form called BTC.

**Who created Bitcoin?**

It is believed that Satoshi Nakamoto(中本聰) is the creator of Bitcoin. However, it is just a name in the Internet and no one knows the true identity behind. Dan Kaminsky, a security researcher, thinks that Satoshi Nakamoto is either a team of people of a genius.

In October 31, 2008, Satoshi Nakamoto published a white paper named <Bitcoin: A Peer-to-Peer Electronic Cash System> through a mailing list on [metzdowd.com](http://metzdowd.com). The paper describes what are the major problems of a currency such as the double spending problem and provide a decentralized solution named Bitcoin currency. The white paper covers different aspects in computer science and economics.

In November 9, 2008, Bitcoin project is hosted on [SourceForge.net](http://SourceForge.net). Two months later, on January 3, 2009, The First block of Bitcoin chain is created. This block is also called Block 0 and the genesis block. Bitcoin network is therefore officially launched.

**Computer Technologies**

Since bitcoin is a digital currency, it is impossible to be developed without make use of technologies in computer science. In this section, some of the important computer technologies will be introduced.

First of all, Internet is the basic requirement in order to develop a digital currency. Without the Internet, computers cannot connect to each other and form a giant network with great computational power and do transactions.

In Addition, bitcoin is a decentralized. In order to do so in the Internet, it has to make use of the peer-to-peer (P2P) technology. Bitcoin is a decentralized network and each node in this network acts as client as well as server. For example, each computer that runs the bitcoin mining program are responsible to create new bitcoin and verify transactions in Bitcoin network.

Last but not least, Bitcoin make use of different principles in cryptography in order to secure the content of transactions and make sure no counterfeit bitcoin can be produced. SHA-256 is the cryptographic hash function. It generates a 32-bit words which representing the original message. By verifying SHA-256, computers can identify if the message is real of fake. Besides SHA-256, public-key cryptography, a popular encryption and decryption technology on the Internet, is used to secure the information transmission from one node to another node in the Bitcoin network.

**Advantages of bitcoin**

In this section, the major advantages of bitcoin will be covered.

**Decentralization**

Most of the currencies in the world, including the physical and digital currencies, are centralized currencies. A centralized currency means that there is an authority to control the supply of money. Usually, the central bank of the country is responsible to do so. Furthermore, verification of transactions is done by banks. Transaction fee is charged in order to provide this service to the customers.

However, bitcoin is different. It is a decentralized currency. Creation of money is not controlled by a single organization but a transparent mathematical algorithm. Total number of bitcoins can be created is predictable and fixed. Moreover, Bitcoin is a P2P network and everyone who joins the network are involved to create bitcoins and verify transactions. As a result, transaction fee is lower then that in traditional banks or even no transaction fee is required in bitcoin transactions.

**Anonymity**

Many people have a big concern on privacy, especially in this digital age. Nowadays, we have to provide our personal information in order to create a bank account to do traditional money transactions via banking system. As a result, the true identity behind the transaction is traceable by banks or even the government.

The creator of bitcoin understands the privacy issue of traditional way of money transactions. Therefore, transactions using Bitcoin can be done anonymously. This does not mean that all the details of transaction will not be disclosed. In fact, transaction records of bitcoin are public and easy to be traced. For example, we can check bitcoin transaction and block generation records on website such as [blockexplorer.com](http://blockexplorer.com) and blockchain.info. Although the transaction records are public, we cannot know the true identity of the parties involved in the transaction if they created a new bitcoin wallet only for that transaction. In this way, Bitcoin network can safeguard user’s personal information.

**Trust**

Beside the privacy issue, traditional currency also have a problem of trust. People can only have a blind trust to the law of the country or particular country. Those currency may lose efficacy if the country is bankrupted. Bitcoin used a new trust model, trust-by-computation. In this model, no one actor is trusted, and no one needs to be trusted. There is no central authority or trusted third party in a distributed consensus network. Trust is ensured by requiring participants to demonstrate proof-of-work, by solving a computationally difficult problem

**Counterfeit banknotes**

Traditional currency is protected by security features but no one can sure the security features haven’t been broke. If those security features is perfectly broke by someone, there is no method to verify the banknotes is counterfeit or not. Bitcoin is protected by Bitcoin network. Every mined bitcoin has its own hash, the hash will submit to bitcoin network and verified by all node. And this give a way for us to back up our banknotes ourselves. A traditional banknotes cannot be backup, we can’t make a copy it, but we can backup bitcoin very easily as it is a digital currency.

**Bitcoin History**

Is bitcoin really so prefect? Bitcoin is invented by one people only. There must be something he haven’t consider at the very beginning.

**Technical issue**

### Frist major vulnerability

The first a major vulnerability in the Bitcoin protocol was spotted on 6 August 2010.Transactions weren't properly verified before they were included in the transaction log or "block chain". This allow hacker bypass Bitcoin's economic restrictions and create an indefinite number of bitcoins. This the vulnerability was exploited after 9 days and within hours the bug was fixed. In this case over 184 billion bitcoins were generated in a transaction, and sent to two addresses on the network. After the bug was fixed, the bitcoin network is forked to an update version of the Bitcoin protocol and those transaction is being removed.

### Over 50% Attack.

The 51% (or more accurately, >50%) attack is generally accepted as a method which allow an attacker to

1. Prevent some or all other miners from mining any valid blocks
2. Prevent some or all transactions from gaining any confirmations
3. Reverse transactions that he sends while he's in control
4. double-spend transactions

However, this it is all speculative – as it has never been done before.

Ghash.io, a bitcoin mining pool, which used the p2p technology to allow people to join there network for bitcoin mining. As a result, it grow up very quickly. In 2014, its own 40% of overall hashing power for bitcoin and it draw the attention from the bitcoin community. As a result, Ghash.io release a press statement said they will try to prevent reaching 51% of all hashing power, in order to maintain stability of the bitcoin network. The bitcoin community also think is there any way to prevent over 50% attack.

People are keep leaving Ghash.IO, Form January, 2014 to April, 2014, The hashrate of Ghash.io decrease from 43% to 29%.

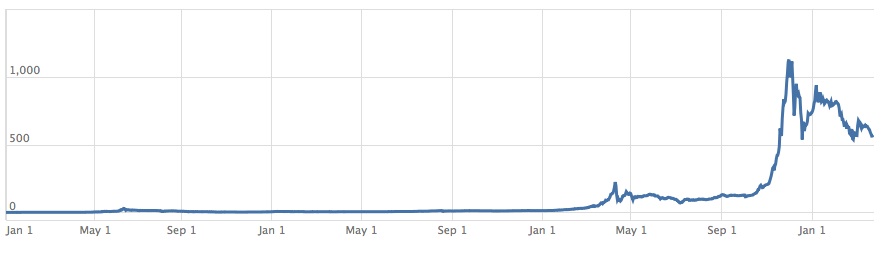
**Mt.Gox, Bitcoin’s $460M Disaster**

There are also some events that raise the concern of public or government. One such event is the shut down of Mt.Gox. Mt.Gox was a bitcoin exchange company lauched in July 2010 in Tokyo. It was one of the biggest Bitcoin exchange in the world. In 2013, Mt.Gox was processing 70% of all bitcoin transactions. However, a disaster happened and caused the shut down of Mt.Gox.

The incident began in February 2014. Mt.Gox reported that its computer system was hacked and eight hundred and fifty thousand bitcoins were missing. Among the missing bitcoins, one hundred thousand were belonged to Mt.Gox and the rest were belonged to its customers. That missing bitcoins represent 7% of the world's bitcoin supply and worth around $460 million US dollar at that time. After that, the company filed for bankruptcy protection in Tokyo and this offically marked the end of Mt.Gox, once the biggest bitcoin exchange in the world. However the CEO of Mt.Gox still has to face the lawsuit filed by his angry customers for his mismanagement of the company. The collapse of Mt.Gox had hurt people's confidence in digital currency. Many Mt.Gox investors have problems recovering their money. Although some of the missing bitcoins were discovered in March 2014, many people started to question bitcoin's reliability because these platforms are not regulated by the government and hence the interests of investors' cannot be protected.

**Rapid Increase of Bitcoin Price**

Another event that cause the concern of government is the rapid increase of the bitcoin price. The following graph shows the price of bitcoin from year 2011 to 2014. The different cycles of appreciation and depreciation shows that the the price of bitcoins has fluctuated rigorously.



Since the inception of bitcoin, the project only get attention from a small group of people who are interested in cryptography. However, in early 2011, public's interest in Bitcoin was growing. The value of one bitcoin quickly increased from around thirty cents to $32 US dollars before returning to $2 dollars. A small amount of organisations such as Wikileaks and Electronic Frontier Foundation also began to accept bitcoins for donations.

In 2012, BitPay made an annoucement that over one thousand merchants are accepting Bitcoin using its payment system. Bitcoin was also featured as the main subject in a CBS's TV drama. As the popularity increases, the bitcoin price began to climb and reach to a peak of US$266, before returning to around US$50. At the same time, 5.2 million of Bitcoins have been generated, which is 25 percent of the expected total.

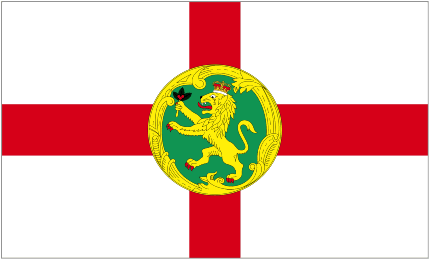
In 2013, large numbers of merchants and organisations have adopted Bitcoin. Chinese internet giant Baidu had allowed clients to pay with bitcoins for some of its services. On the other hand, the China-based bitcoin exchange BTC China replaced Mt.Gox to become the biggest bitcoin exchange in the world. On 19 November, the bitcoin price reached to US$1100 in China which the highest price ever since the inception of bitcoin and the popularity of bitcoin has caused the concern of the government in different countries.

**Governments’ Concerns**

In January 2014, the head of an influential Senate committee on virtual currencies asked his committee surveyed over 40 countries on their official stances on Bitcoin. The survey covered over 40 countries. As you can see, most countries are neutral to Bitcoin at this moment, they don’t officially ban the use of Bitcoin while warning the people about the dark side of it.

|  |  |  |
| --- | --- | --- |
| NEGATIVE | NEUTRAL | POSITIVE |
|  |  |  |

Here are the highlight of some countries’ stance towards Bitcoin:

Alderney is trying to take the lead and become the central hub for the bitcoin, by minting and issuing physical bitcoins and creating an international center with a bitcoin storage vault service that complies with anti-money laundering rules.

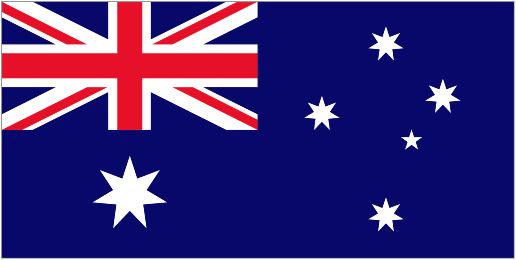
Brazil passed a law in October 2013 specifically for electronic currencies

Canada welcomed the first Bitcoin ATM last year.



Germany treats Bitcoin as foreign currency

  
Financial institutes claimed no need to be worry about Bitcoin. Law enforcement agency claimed that they won’t hunt down Bitcoin like a monster. This leaded to a rise in Bitcoin price from 200 to 1200 USD.

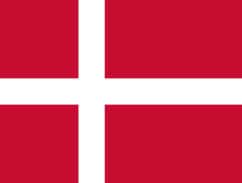
Australia was aware of an Australian Bitcoin bank being hacked in Oct 2013, resulting US$1 million lost.

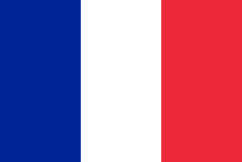
Estonia has no official stance, but warned that Bitcoin might be a Ponzi scheme.

Bitcoin is a potential payment method, but it’s different than ordinary currency. It is not regulated by the central bank so there are risks.



Spain government has a Bitcoin wallet.

Denmark’s Finanstilsynet (Financial Supervisory Authority) has issued a statement rejecting the bitcoin as a currency and stating that it will not regulate bitcoin use.

  
The central bank of France has criticized it as speculative and warned about its use for nefarious dealings.

  
Netherlands doesn’t see virtual currency as being an electronic money.

Russian law firm thinks that using it to buy things there could be illegal given that the Russian ruble is the exclusive means of payment in the Russian Federation per the law.

How Hong Kong Government reacts to Bitcoin?

There is nothing official at the moment, though John Tsang, the Financial Secretary talked about he’s view on Bitcoin on a blog. He said that bitcoin no physical or issuer support, does not guarantee the real economy can be converted into currency or commodity. However, existing laws forbid its use for fraud or money laundering. At this point, Hong Kong is neutral to bitcoin.

How China Government reacts to Bitcoin?

In Dec 2013, China declared that Bitcoin is not a currency and should not be circulated and used in the market as a currency. Financial institutes warned people to get away from Bitcoin. This was interpreted as China was going to ban Bitcoin. In fact, people are free to buy and sell Bitcoin, only financial institutes are prohibited from processing transactions using Bitcoin. That means you cannot pay off your credit card using Bitcoin. In this case, it is not being treated as a real currency in China and China is not in favor of Bitcoin.

How European Union reacts to Bitcoin?

European Union are one of the largest economies in the world, their attitude towards bitcoin have a serious impact to the development of bitcoin. After a week China banned Bitcoin transactions in financial institutes, the European Banking Authority said “Currently no specific protection exists in the EU that would protect consumers from financial losses if a platform that exchanges or holds virtual currencies fails or goes out of business”. Besides, European regulators said that the digital currency is vulnerable to hackers, might lose its value and any misuse could prompt law enforcement agencies to close Bitcoin exchange platforms and keep consumers from accessing their investment. It seems that EU also not welcoming Bitcoin too.

Should the government ban bitcoin?

At this moment, most countries that go against Bitcoin claim that there is no law or regulation can be applied on bitcoin right now. However, we don’t agree on this as the German government said, “Bitcoin can be treated as foreign currency and regulated by corresponding law”. Other criticisms are based on the uncertainties of bitcoin. Some countries like Turkey and Estonia warned that Bitcoin is suspicious, it looks similar to a Ponzi Scheme or Tulip mania in Holland. As a responsible government, they should find out the truth instead of making decision based on rumors or guesses.

Bitcoin is still young, we believe there will be many possibilities in the future. We are against “killing the baby in the cradle” by over-regulating Bitcoin. There are “good things” in the virtual currency, and likened the current situation to the early days of the Internet. However, if we ban Bitcoin simply because we don’t get familiar with it, because someone uses it to launder money, then we will never see the good side of it. Therefore, the government should not ban Bitcoin while keep an eye on the development of Bitcoin.