University of Wroclaw
Institute of Informatics

Igor Tryhub

"E-money. How it works? Benefits and threats."

Wroclaw 2015

Introduction and History

Modern money is credit by its economic nature. On the one hand, banknotes and coins issued by the central bank are its debt obligations in the form of guarantees to ensure the purchasing power of money and acceptability throughout the state. On the other hand, cashless funds raised by banks in deposits are obligations towards their depositors to return the money. Similarly, the electronic money is essentially a form of credit liabilities of their issuer. Electronic money in principle does not increase money supply, instead it increases the speed of their circulation, since they act as a means to support and accelerate commercial transactions.

Electronic money (e-money) is ambiguous and evolving term that is used in many meanings associated with use of computer networks and systems for transmission and storage of money. Electronic money define storage and transfer of both traditional currency and non-governmental private currencies. Handling electronic money can be carried out according to the rules set by or agreed with the government central banks and by their own rules of non-state payment systems.

In the EU, e-money mean monetary value as represented by a claim on the issuer which is:

- stored on an electronic device;
- issued on receipt of funds of an amount not less in value than the monetary value issued;
- accepted as means of payment by undertakings other than the issuer. [1]

The history of e-money began in 1983, when American inventor and computer scientist David Chaum introduced a research paper "Blind Signatures for Untraceable Payments" presenting the idea of digital cash.[2]

The main idea behind the blind signature algorithm was the following:

- A encrypts a document, and sends it to B.
- B, without seeing the contents of the document, signs it and returns back to A.
- A decrypts the document, keeping only the signature of B.

After execution of this protocol, B knows nothing about the message of A and cannot distinguish it among other envelopes he or she signed in the same manner.

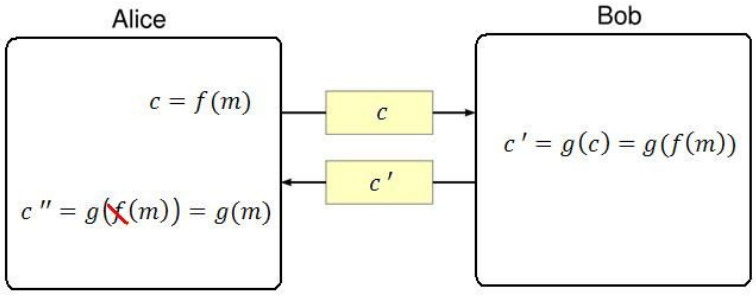

Image source: https://commons.wikimedia.org/wiki/File:BlindSignature.jpg

This scheme can be compared with an envelope, in which a document along with a copy sheet is placed. If you sign the envelope, the signature is printed on paper, and at the opening of an envelope document is already signed.

The purpose of a blind signature is to prevent the signer B to read the message of A, which he or she signed, and with the corresponding signature of A under the message. Therefore, later on the signed message cannot be associated with A anymore.

In 1997, Coca Cola offered buying from vending machines using mobile payments.[3] After that Paypal emerged in 1998. Other system such as e-gold followed suit, but faced issues because it was used by criminals and was raided by US Feds in 2005. In 2008, bitcoin was introduced, which marked the start of Digital currencies.[4]

Currently, electronic money is considered as a potential substitute of cash for micropayments. However, in quality electronic money can partially or completely displace cash payments. Artificial limiting of the amount that can be stored or transferred, caused by the uncertainty of regulators in the reliability and safety of such payment instruments. It is obvious that in the absence of negative examples these limits will be weakened or completely raised.

Classification

Usually, the circulation of electronic money takes place through computer networks, the Internet, payment cards, e-wallets and devices working with payment cards (ATMs, POS-terminals, payment kiosks). There are other payment instruments: bracelets, key rings, blocks of mobile phones and other devices equipped with a special payment chip.

There should also be distinction between the electronic fiat and non-fiat money. Electronic fiat money are necessarily denominated in one of the existing state, and are a variety of payment means at the payment system of the state. For example, many systems—such as PayPal, eCash, WebMoney, Bitcoin will sell their own electronic currency directly to the end user, while others such as Western Union, PayPal, Google Wallet would use USD, EUR or other existing currencies.

Nowadays, traditional centralized e-money systems which concentrate the whole power and control of the money circulation are steadily being replaced by decentralized systems such as cryptocurrencies. The latter ones are offering a community-based system with no authority overseeing and irreversibility of transactions. The most popular cryptocurrency systems today include: Bitcoin, Monero, Litecoin, Dogecoin.

A soft electronic currency is one that allows for reversal of payments, for example in case of fraud or disputes. Reversible payment methods generally have a "clearing time" of 72 hours or more. Examples are PayPal and credit card. Transactions with these currencies highly resemble transactions with bank cards.

A hard electronic currency is one that does not have services to dispute or reverse charges. In other words, it is akin to cash in that it only supports non-reversible transactions. Reversing transactions, even in case of a legitimate error, unauthorized use, or failure of a vendor to supply goods is difficult, if not impossible. Examples are Western Union, KlickEx and Bitcoin. Therefore, the security of the users' funds highly depends on their level of computer literacy and precautions. A hard currency can be softened by using a trusted third party or an escrow service. [5]

Benefits, Disadvantages, Threats

Electronic payment systems can simplify transactions between buyer and seller. In addition, they contribute to the development of e-commerce, as they allow a transaction almost instantly. Electronic money is particularly useful and convenient when implementing mass payments of small amounts. For example, payments in transport, theaters, clubs, public utilities, payment of various fines and so on. The process of payment by electronic money is carried out quickly, there are no queues, no need to give change, money is instantly transferred from the payer to the recipient. For these reasons, it is more correct to compare e-money with cash. On the contrary, cashless bank payments assume a necessarily personified money handling.

Increased use of electronic payment systems is inevitable, as they feature very important and undeniable advantages such as:

- availability - any user can open own free electronic account;
- easy to use - opening and using an electronic account does not require any special expertise;
- mobility - regardless of their location, the user can perform any financial transactions at his/her account;
- excellent divisibility - there is no need to give change;
- high portability - the money value is not associated with overall dimensions and weight, as in the case of cash;
- low cost of emission - no need to mint coins and print notes, use metals, paper, paint etc.;
- easier than in the case of cash to organize physical security of electronic money;
- the impact of the human factor is reduced;
- no need to count, package, transport, and organize special storage for e-money;
- electronic money do not lose their quality over time;
- security provided by cryptographic and electronic media - protected from theft, forgery, and changes in the nominal value.

However, as practically every new technology, e-money is still undergoing series of probations and adapts to the security and legal requirements posed by its users and regulatory institutions. At present, there are following weaknesses and challenges encountered by e-money:

- lack of trust of many users towards electronic money;
- lack of established legal regulation: many states have not yet decided how to treat electronic money;
- despite the excellent portability, electronic money instruments require special storage and handling;

- as in the case of cash, at the moment of physical destruction of the media of electronic money it becomes impossible to restore their monetary value;
- cryptographic protection, which protects the system of electronic money may not have a long history of successful operation;
- theoretically, interested parties can try to track the personal information of taxpayers and circulation of e-money outside the banking system;
- possible theft of electronic money, through innovative methods, using the lack of maturity of the protection technologies. However, it is worth noting that the security of electronic payments improves over time and significantly increases difficulty to gain access to someone else's bank or electronic account by fraudsters;
- substantial part of the electronic money is used for money laundering, terrorism financing and tax evasion purposes. Therefore, most state regulators, as well as public and private payment systems, are trying in different ways to encourage the personalization of electronic money and operations with them. For example, electronic money-based networks payment systems limit the size of e-wallet for the anonymous user, but allow increasing the limits for personalized users. For e-money based on cards they limit the maximum amount of the purse and introduce personalized replenishment mechanisms.

Cryptocurrencies

In theory, electronic money should provide as easy a method of transferring value without revealing identity as untracked banknotes, especially wire transfers involving anonymity-protecting numbered bank accounts. In practice, however, the record-keeping capabilities of Internet service providers and other network resource maintainers tend to frustrate that intuition. While some cryptocurrencies under recent development have aimed to provide for more possibility of transaction anonymity for various reasons, the degree to which they succeed—and, in consequence, the degree to which they offer benefits for money laundering efforts—is controversial. [6]

Nowadays, there are hundreds of types of cryptocurrencies. Most of them differ insignificantly from each other. However, there are some prominent cryptocurrency worth mentioning. Each of the following pioneer decentralized payment systems in their own way:

- Bitcoin, a peer-to-peer electronic monetary system based on cryptography invented in 2008 by a person or a group of people calling themselves Satoshi Nakamoto. It was one of the first cryptocurrencies using an open-source software and remains to be the one with the biggest market capitalization.
- Litecoin, the second-largest true cryptocurrency by market capitalization,[7] originally based on the Bitcoin protocol, intended to improve upon its alleged inefficiencies:
    - the Litecoin network aims to process a block every 2.5 minutes, rather than Bitcoin's 10 minutes, which its developers claim allows for faster transaction confirmation.[8] A drawback is a higher probability of orphaned blocks. Advantages can include greater resistance to a double spending attack over the same period as Bitcoin.
    - Litecoin uses scrypt in its proof-of-work algorithm, a sequential memory-hard function requiring asymptotically more memory than an algorithm which is not memory-hard.[9]
    - the Litecoin network will produce 84 million Litecoins, or four times as many currency units as will be issued by the Bitcoin network.
- Dogecoin, a Litecoin-derived system meant by its author to reach broader demographics. Compared with other cryptocurrencies, Dogecoin has a fast initial coin production schedule: 100 billion coins have been in circulation by mid 2015 with an additional 5.256 billion coins every year thereafter. This represents an inflation rate of 5.256% (in 2015), that will forever decrease though (e.g. in 2025 yearly inflation rate will be 3.4%, in 2035 2.5%). While there are few mainstream commercial applications, the currency has gained traction as an Internet tipping system, in which social media users grant Dogecoin tips to other users for providing interesting or noteworthy content.[10]

- Monero, focused on privacy, decentralization and scalability. Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and possesses significant algorithmic differences relating to block chain obfuscation.[11]

Let us now discuss the main features of cryptocurrencies in more details, taking Bitcoin system as an example.

One of the most important concepts inherent to cryptocurrencies is a digital signature. Digital signature is realized by using two different but connecting keys - a private key to create a signature and a private key the other can use to check it. In order to spend money, a payer needs to prove that he or she is the true owner of the public key (which can be newly generated unlimited number of times for anonymity purposes) form where the money was sent. It is done by generating a digital signature form a transaction message and his/her private key. Therefore, a digital signature is different every time and cannot be reused by someone else for a different transaction. Other nodes in the network, on the other hand, can utilize different functions to verify that the signature corresponds with the payer's public key.

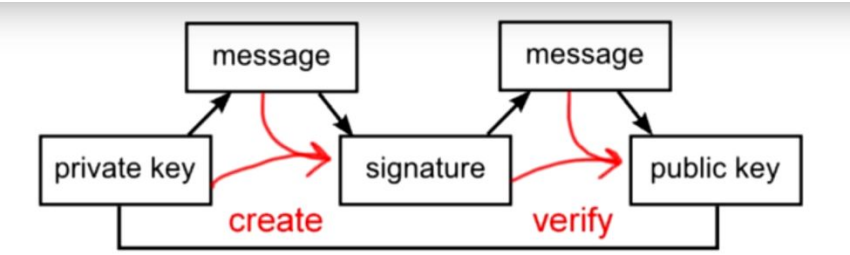

Image source: https://www.youtube.com/watch?v=Lx9zgZCMqXE

Another particularity of Bitcoin is usage of transaction chain instead of ledger of expanses. Every time a user tries to spend money from the account, the system looks back into history following the sources of the user's revenues and expenditures in order to verify they are enough to cover the current request. All the transaction history from the inception of Bitcoin is stored and duplicated at every user's device and is constantly updated by sophisticated algorithm to avoid the conflict of versions.

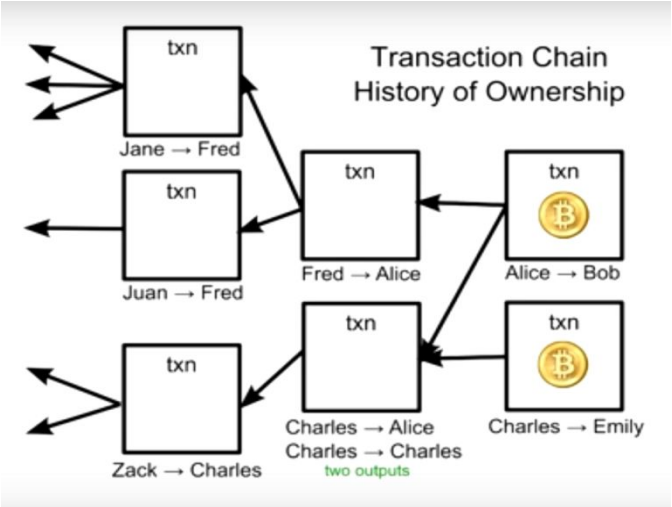

Image source: https://www.youtube.com/watch?v=Lx9zgZCMqXE

Sometimes, however, attackers possessing substantial computational power are trying to exploit this mechanism by double-spending attacks. In very rare cases, it is impossible to avert conflict of versions near to the end of the chain. Which is why it is recommended to wait several blocks before considering received money final.

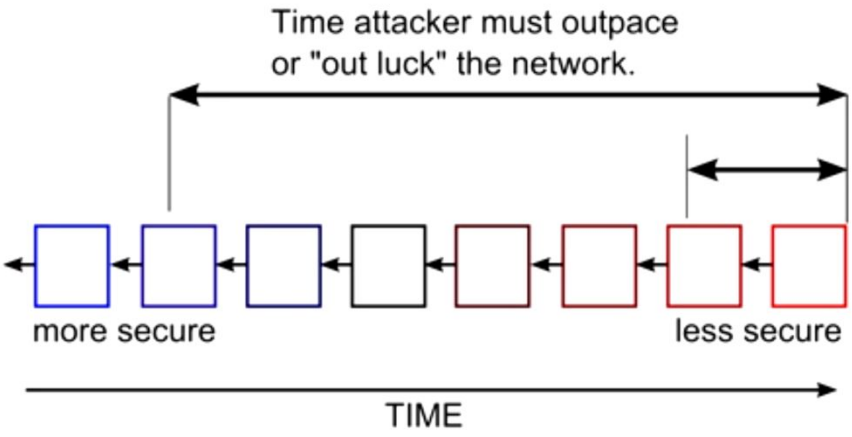

Image source: https://www.youtube.com/watch?v=Lx9zgZCMqXE

In order the Bitcoin system functions securely and sustains itself, there is a constant need in computational power. The particularity in such a high safety of Bitcoin transactions is usage of complicated hashing algorithms that are highly unlikely to be overcomputed by someone whose

computational power is substantially less than the one of the whole Bitcoin community. Therefore, the system rewards the honest users (called solo miners) or a group of people (pool miners) for solving "blocks" with extra coins. Blocks are solved in 10 minutes on average. Every 2 weeks all the Bitcoin software recalibrates the difficulty of the math problems to target 10 minutes. One of the challenges for such a system in the future might be usage of substantial amount of electricity.

To mine Bitcoins, miners must find an input that includes a list of all of the most recent transactions that need to be verified, and whose hash is smaller than some specified value. (This value is adjusted periodically to change the difficulty.) Once a miner finds such a value, he/she broadcasts it. The set of transactions that he/she included are now verified, and that set becomes the next block in the Bitcoin block chain. The miner then receives his reward for contributing his computational power to operate the Bitcoin protocol.

Since the only way to find such a value and earn the reward is by brute force search, faster and faster hardware has been developed to compute the SHA256 hash function quickly. The hash rate is the number of times this function can be computed per second. Some machines can now compute trillions of these hashes every second. [12]

It is worth noting that every 4 years a block reward is cut in half, so eventually no more coins will be released in about 2140, about 21mln in total will be created. Right now, miners would include transactions with no fees into blocks, because main incentive is the block reward, but in the future transactions will likely be processed in the order of fees attached.

Bibliography

1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML
2. http://blog.koehntopp.de/uploads/Chaum.BlindSigForPayment.1982.PDF
3. http://www.nearfieldcommunication.org/payment-systems.html
4. https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630
5. http://everything.explained.today/Electronic_money/
6. https://en.wikipedia.org/wiki/Money_laundering#Electronic_money
7. http://coinmarketcap.com/
8. http://arstechnica.com/business/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/
9. http://www.tarsnap.com/scrypt/scrypt.pdf
10. http://www.abc.net.au/pm/content/2013/s3931812.htm
11. https://news.ycombinator.com/item?id=7766161
12. https://www.quora.com/What-does-Bitcoin-hash-rate-mean