Ercan Buluş[1)]
Bülent Eker[2)]
Halil Nusret Buluş[1)]

1) Computer Engineering, Namık Kemal University, Tekirdağ/Turkey
ercanbulus@nku.edu.tr
nbulus@nku.edu.tr

2) Biosystems Enginnering, Namık Kemal University, Tekirdağ/Turkey
beker@nku.edu.tr

INVESTIGATION OF BITCOIN CRYPTO CURRENCY METHOD WAS DEVELOPED FOR SHOPPING OVER THE INTERNET

Abstract: *A crypto currency is a medium of exchange using cryptography to secure the transactions and to control the creation of new units. Crypto currencies are a subset of alternative currencies or specifically of digital currencies. Recently "Bitcoin" is used as crypto currency. Bitcoin was invented by Satoshi Nakamoto. It was implemented as open source code and released in January 2009. Bitcoin is often called the first crypto currency although prior proposals existed. No one controls it. However, bitcoin's most important characteristic, and the thing that makes it different to conventional money, is that it is decentralized. No single institution controls the bitcoin network. In this study we try to explain that, what is it?, is it legal?, how's it work?, is it has got enough security?*
Keywords: *crypto currency, bitcoin*

1. INTRODUCTION

Bitcoin is a crypto currencies [6]. Under Bitcoin protocol and independent P2P payment scheme, users may send any amount of bitcoins over internet to anywhere in the world near instantly with near zero costs. Today, more than 100.000 e-sale merchants or real-world shops including the well known Dell computers accept bitcoin as a means of payment.

Visa credit card network handles 6000 tps (transactions per second) in a busy day. However, Bitcoin network on average, hosts 2 tps. Bitcoin is not yet truly tested to its limits. To decide on whether Bitcoin is "a short-term cult with no future" or a "technological advance that can not be omited" in order to keep up with developed countries, Bitcoin and similar crypto-currencies should be evaluated in terms of sustainability and scalability for supporting many users. In this context, we will be searching for some answers, in terms of how user trends evolve via a quantitative analysis. On the other hand, as Bitcoin does not fit into definition of other digital assets, it has no lawful classification, and hence current laws for electronic money in general does not apply to Bitcoin. A decentralized cash-like currency such as Bitcoin demands its own regulations. As an example, exchange sites on internet should have different regulations than banks. For this reason, the current existing problems for exchange sites should be well investigated. In other words, although the proposed project does not involve any packages about politics or is not directly related to economics; it is expected to yield results that will prove useful for lawmakers.

Within the project bounderies, we will be focused heavily on Bitcoin, which witholds the 95% of crypto-currency market. However, the results are associated with other Bitcoin-like crypto-currencies, which in turn make use of the block chain structure of Bitcoin [5].

2. HISTORY OF BITCOIN

Bitcoin was invented by Satoshi Nakamoto, who published his invention on 31 October 2008 in a research paper called "Bitcoin: A Peer-to-Peer Electronic Cash system".It was implemented as open source code and released in January 2009.

One of the first supporters, adopters, contributor to bitcoin and receiver of the first bitcoin transaction was programmer Hal Finney. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto in the world's first bitcoin transaction.

Other early supporters were Wei Dai, creator of bitcoin predecessor b-money, and Nick Szabo, creator of bitcoin predecessor bit gold.

In 2010, an exploit in an early bitcoin client was found that allowed large numbers of bitcoins to be created.

Based on bitcoin's open source code, other cryptocurrencies started to emerge in 2011.In March 2013, a technical glitch caused a fork in the block chain, with one half of the network adding blocks to one version of the chain and the other half adding to another. For six hours two bitcoin networks operated at the same time, each with its own version of the transaction history. The core developers called for a temporary halt to transactions, sparking a sharp sell-off. Normal operation was restored when the majority of the network downgraded to version 0.7 of the bitcoin software.

In 2013 some mainstream websites began accepting bitcoins. WordPress had started in November 2012, followed by OKCupid in April 2013, Atomic Mall in November 2013, TigerDirect and Overstock.com in January 2014, Expedia in June 2014, Newegg and Dell in July 2014, and Microsoft in December 2014. Certain non-profit or advocacy groups such as the Electronic Frontier Foundation accept bitcoin donations. The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada [2].

3. HOW DOES IT WORK?

3.1. The basics for a new user

Once a new user have installed a Bitcoin wallet on her computer or mobile phone, it will generate her first Bitcoin address and he can create more whenever he need one. He can disclose her addresses to her friends so that they can pay he or vice versa. In fact, this is pretty similar to how email works, except that Bitcoin addresses should only be used once.

3.2. Bitcoin block chain

The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

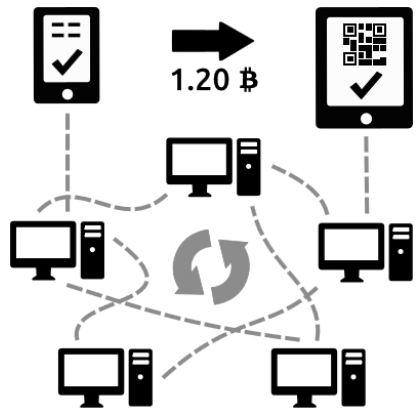

Figure 1 *- Bitcoin block chain*

3.3. Transactions-Private keys

A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called mining.

3.4. Processing-mining

Mining is a distributed consensus system that is used to confirm waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain.
This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends [4].

4. IS BITCOIN LEGAL?

People are increasingly using virtual money, like Bitcoin, that's not backed by any government. Many central banks have cautioned against it. But most authorities take a hands-off approach [3] [8].

5. CONCLUSION

Marc Andreessen, founder of Netscape, recently wrote the best piece. he wrote that " Further, there is no shortage of regulatory topics and issues that will have to be addressed, since almost no country's regulatory framework for banking and payments anticipated a technology like Bitcoin." [1]

On the flip side, Paul Krugman, Nobel Prize Winning economist seems to think it's the devil's spawn, ratcheting up the rhetoric in his recent piece titled, "Bitcoin Is Evil." No ambivalence there. [7]

We think that Use of crypto-currencies like bitcoin will increase in the future.

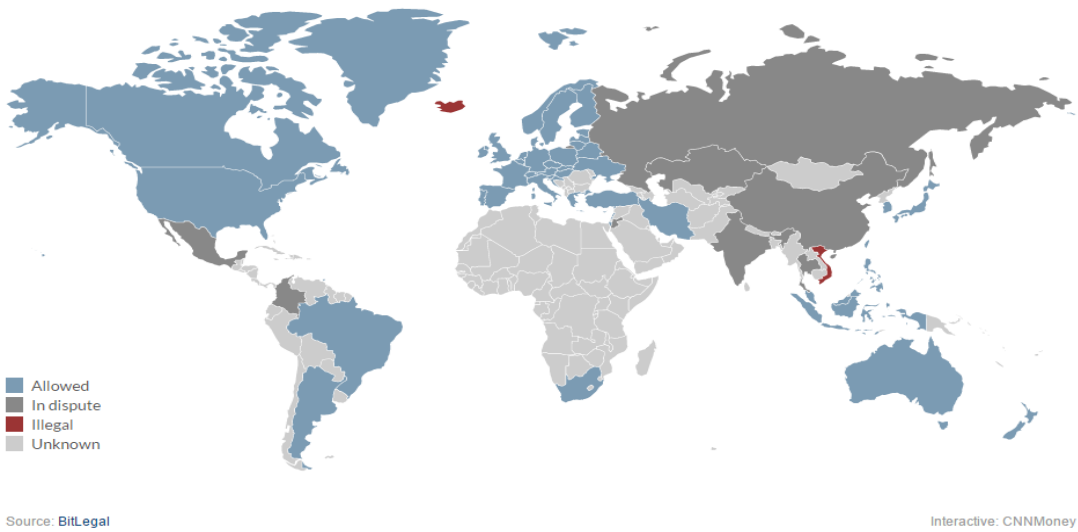

Figure 2 - *Bitcoin's Legality Around The World*

REFERENCES:

[1] Andreessen, M. (2014). Why Bitcoin Matters, The Newyork Times, Retrieved from: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/?_php=true&_type=blogs&smid=tw-share&_r=1
[2] Retrieved from: Bitcoin, http://en.wikipedia.org/wiki/Bitcoin
[3] Frequently Asked Questions, Retrieved from: https://bitcoin.org/en/faq
[4] How it works, Retrieved from: https://bitcoin.org/en/how-it-works
[5] Kaşkaloğlu, K. Near Zero Bitcoin Transaction Fees Cannot Last Forever. *The International Conference on Digital Security and Forensics* (DigitalSec2014)
[6] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System Retrieved from: http://bitcoin.org/bitcoin.pdf, 2008
[7] Rosenblum, P., Bitcoin: The Currency Of The Future? Forbes, Retrieved from: http://www.forbes.com/sites/paularosenblum/2014/01/27/bitcoin-the-currency-of-the-future/
[8] Where is Bitcoin legal?, Retrieved from: http://money.cnn.com/interactive/technology/where-is-bitcoin-legal/