IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Generation of digital currency and application development (Digibucks)

Nikita Jadhav
nikijadhavs17@gmail.com
Sinhgad Academy of Engineering, Pune, Maharashtra

Dhanashree Biradar
dhanashreebiradar7@gmail.com
Sinhgad Academy of Engineering, Pune, Maharashtra

Akshay Olekar
akshay.olekar777@gmail.com
Sinhgad Academy of Engineering, Pune, Maharashtra

Saima Ansari
saimaansari50@gmail.com
Sinhgad Academy of Engineering, Pune, Maharashtra

ABSTRACT

Cryptocurrency has emerged as the most successful cryptographic currency in history. Cryptocurrency grew to comprise billions of dollars of economic value despite the only cursory analysis of the system's design. Since then the increasing literature has identified hidden-but-important properties of the system, discovered attacks, forth put promising alternatives, and singled out difficult future challenges. Meantime a large and vibrant open-source community has proposed and deployed numerous alterations and extensions. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. We provide a platform for using our cryptocurrency (digipack) for the users. We then provide different facilities like transferring and receiving digipack, viewing price charts, foreign transactions. The main aim is to provide more security to cryptocurrencies and reducing the update interval time. These modifications will attract more users and interest them in using this digital currency more frequently.

***Keywords**: Cryptocurrency, DigiBucks, Digital currency, Data mining, the SHA-256 hash algorithm*

1. INTRODUCTION

Cryptocurrency is a digital currency introduced as bitcoin in 2009. It pursues the ideas set out in a white paper by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. Cryptocurrency offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies. Today's market cap for all cryptocurrency (abbreviated BTC or, less frequently, XBT) in circulation exceeds $7 billion.

There are no physical cryptocurrencies, only balances kept on a public ledger in the cloud that along with all Cryptocurrency transactions is verified by a massive amount of computing power. Cryptocurrencies are not issued or backed by any banks or governments, nor are individual cryptocurrencies valuable as a commodity.

In recent years, interest in cryptocurrencies has increased. Cryptocurrencies are a compartment of digital currencies, which may have either have centralized institutions or are based on a decentralized network. DigiBucks (currency) users depend on the DigiBucks protocol to receive and send payments over the internet. Participants who want to switch over DigiBucks connect to a peer-to-peer network (transaction network), the DigiBucks network established on the basis of the DigiBucks protocol. Cryptocurrency technology as we know today has grown vastly due to its security, scalability as well as being a self-governing cryptocurrency that does not rely upon conversion and inflation of international borders. All in all, DigiBucks is a decentralized stage where no one association or state is accountable for its power and circulation. This very characteristic makes it so vastly used in large business, but the question arises, how secure is cryptocurrency? We want to inspect if DigiBucks wallets have the capability and easiness to be used on a normal day to day environment their security threats along with DigiBucks transactions in the light of secure block chains.

There is no physical proof of the DigiBucks. It is displayed only as balance in the account of the user of the DigiBucks profile. The balance is maintained keeping all the accounting intellect such as the ledger or the balance sheet. At the time of the transaction, a kind of verification is done as to undertake that the transaction of the money has been done without any kind of problem or mishandling.

The plan of DigiBucks is that the currency is termed as digital (Digi) and money is termed as bucks. The idea behind the creation of DigiBucks is the simple transfer of the money without paying a big sum of transaction fees. The traditional online payment charges some amount of transaction amount that is to be paid to the bank or other financial organization connected to the transaction.

DigiBucks is a digital currency. One popular component of DigiBucks is blockchain. Blockchain enables companies to carry out business without the intervention of a third party. In order to be successfully validated mining must occur – that is a cryptographic trouble must be computational. This results in a transaction. In the case that there is a suitable amount of DigiBucks credit, then the miner (member of blockchain network) can agree to the DigiBucks.

DigiBucks is also analyzed from a network viewpoint by looking into the network topology mechanisms and propagation methods are introduced for the secure updating and harmonization of transactions using network nodes and testing of how they interrelate with neighboring nodes to ensure that transactions are being successfully verified. Furthermore, the study is done within blockchain forks to remediate the process of blocks that clash with each slowing down transaction times. Often times, blockchain forks are hard to detect and for this reason, it is hard to mitigate this process. The possibilities of finding the fork block in a huge network of nodes are implemented through the use of timestamp techniques.

To make a transaction, a user broadcasts that an exchange of DigiBucks is preferred and all the computers on the entire network update their versions of files concerned. Transactions are a very public debiting and crediting of various accounts with complicated mathematical processes and functions protecting against fraud. DigiBucks are earned through a process called “ mining” . Instead of the traditional method of back-office bankers performing the transactional paperwork, checks, and updating ledgers the computers on the network of the DigiBucks society are “ paid” in the DigiBucks to perform these back-office functions (such as the blockchain security function mentioned earlier) on a collectively maintained public transaction log. This self-perpetuating system needs an ever growing level of computation to contest the ever-increasing complexity of mathematical problems which DigiBucks is based on.

There are many advantages of DigiBucks compared to the fiat currencies. Firstly, there is no central authority needed for the transaction or securitization of DigiBucks as the network of DigiBucks miners and users is based on the “ peer-to-peer” basis mentioned before. In this setup, every node connected to the network has right of entry to information about all the transactions that are being performed using the currency. However, this information contains only public keys, which in their substance are usable only for the transaction itself. This means that the physical payer or payee (a person) concerned in any of the transactions cannot be identified unless they decide to do so by publishing their private key of the transaction.

This also means that the cryptocurrency network cannot be brought down simply by shutting down some main server or by a hacker attack. Even if all the nodes would be shut down except for one, the functionality of the currency would not be compromised and could be restored.

The advantage is the impossibility of unexpected increase in the supply of DigiBucks in the market. As previously mentioned, DigiBucks are created by executing the transactions by finding a solution for a block connection problem. At every single point in time, the current amount of DigiBucks in circulation is predetermined.

This decentralized currency indicates that it is not run by government authorities or a state. Being managed by the network which has no power over the currency is the main reason why cryptocurrencies have increasingly risen up. It is also private, anonymous, fast and cheap.

DigiBucks clearly satisfies this definition as its aim is to function as money. It functions as a currency in any situation consisting of any single holding DigiBuck in his virtual wallet, companies accepting DigiBucks, the decentralized peer to peer network of nodes and the DigiBucks exchanges. The same value in real currency is mentioned as well as for any other currency on any foreign exchange. The exchanges for DigiBucks are opened 24 hours a day and the ticks are being made roughly every second.

Currently, the main users of the cryptocurrencies are technologically interested geeks who want to use the newest innovations, anarchists who have mislaid trust in the governments and the banking systems, and tentative risk-seekers looking for a new gamble.

Average block time: Average block time for cryptocurrency in current systems is 10 minutes. In our proposed system this average block time will be halved to 5 minutes or even less.

Security: For security SHA-256 algorithm will be used. SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. A one-way hash can be generated from any piece of data, but the data cannot be generated from the hash.

Algorithm 1: Mining Process

```
nonce ← 0
while nonce < 232 do
    threshold ← ((216 −1) 208)/D(t)
    digest ← SHA-256(SHA-256(header))
    if digest < threshold then
        return nonce
    else
        nonce ← nonce + 1
    end if
end while
```

Algorithm 2 presents a basic description of SHA-256. For details on message padding, initial hash values H(0), and constants Kj, see [12].

- The message M is divided into N 512-bit blocks M(0),M(1),...,M(N−1). Each of these blocks is further subdivided into 16 32-bit words M(i) 0 ,M(i) 1 ,...,M(i) 15 .
- The intermediate hash value H(i) is composed of 8 32bit words H(i) 0 ,H(i) 1 ,...,H(i) 7 .
- $Ch(x,y,z) \equiv (x \wedge y) \oplus (\neg x \wedge z)$
- $Maj(x,y,z) \equiv (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$
- $\Sigma0(x) \equiv x \gg 2 \oplus x \gg 13 \oplus x \gg 22$
- $\Sigma1(x) \equiv x \gg 6 \oplus x \gg 11 \oplus x \gg 25$
- $\sigma0(x) \equiv x \gg 7 \oplus x \gg 18 \oplus x \ 3$
- $\sigma1(x) \equiv x \gg 17 \oplus x \gg 19 \oplus x\ 10$

Algorithm 2: SHA-256

```
function SHA-256(M)
    for i from 0 to N −1 do
        for j from 0 to 15 do
        $W_j = M^{(i)}_j$
    end for
    for j from 16 to 63 do
        $W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$
    end for
    for j from 0 to 63 do
        $t_0 \leftarrow h + \Sigma_1(e) + Ch(e,f,g) + K_j + W_j$
        $t_1 \leftarrow \Sigma_0(a) + Maj(a,b,c)$
        $h \leftarrow g;\ g \leftarrow f;\ f \leftarrow e;\ e \leftarrow d + t_1$
        $d \leftarrow c;\ c \leftarrow b;\ b \leftarrow a;\ a \leftarrow t_1 + t_2$
        $H^{(i)}_0 \leftarrow H^{(i-1)}_0 + a;\ H^{(i)}_1 \leftarrow H^{(i-1)}_1 + b$
        $H^{(i)}_2 \leftarrow H^{(i-1)}_2 + c;\ H^{(i)}_3 \leftarrow H^{(i-1)}_3 + d$
        $H^{(i)}_4 \leftarrow H^{(i-1)}_4 + e;\ H^{(i)}_5 \leftarrow H^{(i-1)}_5 + f$
        $H^{(i)}_6 \leftarrow H^{(i-1)}_6 + g;\ H^{(i)}_7 \leftarrow H^{(i-1)}_7 + h$
    end for
end for
return $H(N-1)$
end function
```

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

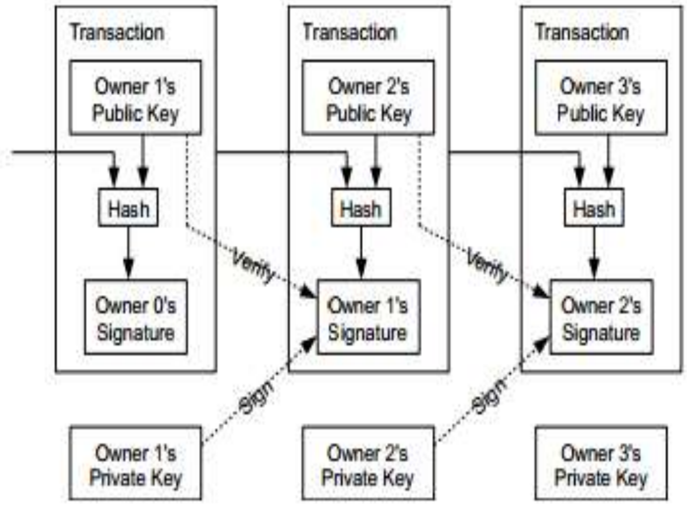

Fig. 1: Transactions

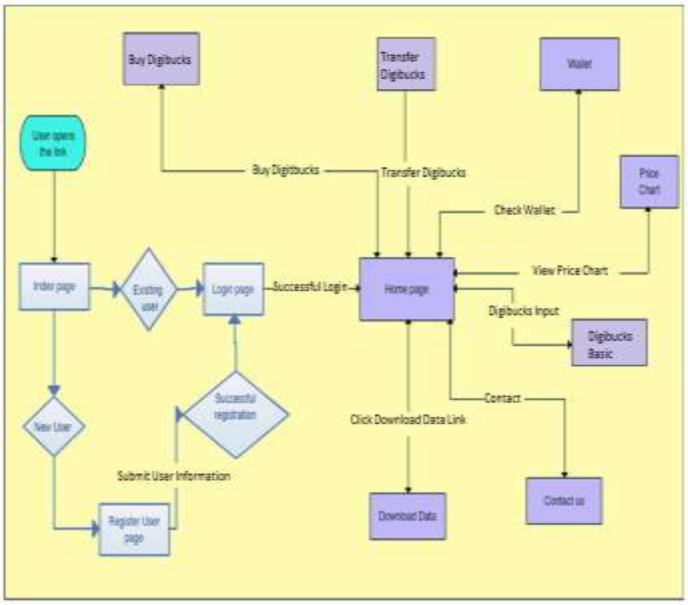

Fig. 2: Architecture

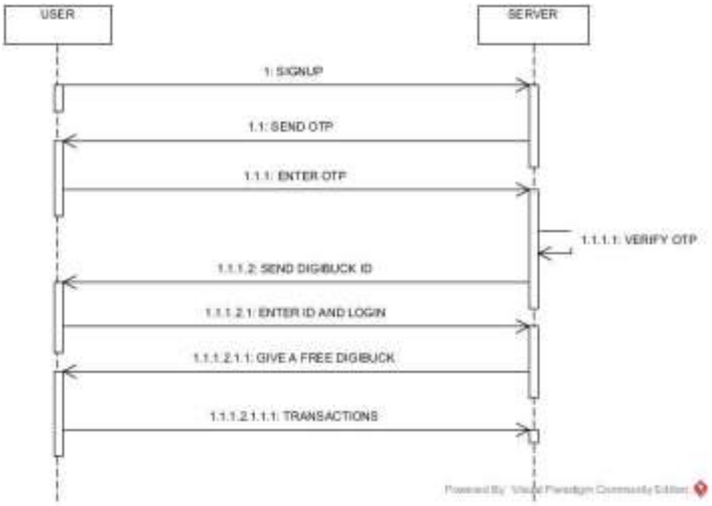
USER
SERVER
1: SIGNUP
1.1: SEND OTP
1.1.1: ENTER OTP
1.1.1.1: VERIFY OTP
1.1.1.2: SEND DIGIBUCK ID
1.1.1.2.1: ENTER ID AND LOGIN
1.1.1.2.1.1: GIVE A FREE DIGIBUCK
1.1.1.2.1.1.1: TRANSACTIONS
Powered By: Visual Paradigm Community Edition

Fig 3: Sign up

2. CONCLUSION

Cryptocurrencies such as Digibucks could play an important role in transforming financial services and other industries that many feels is ripe for disruption. Investment in this ecosystem of start-ups to date totals over $660 million, which is roughly on par with the level of early-stage investments in internet start-ups32. This strong showing of support from the risky capital community indicates the very significant economic potential seen for cryptocurrencies. However, there are no clear solutions on the horizon for some risks, such as the currency’s price volatility or technical vulnerabilities like a 51% attack. Individuals and institutions that are seeking to participate in this economy must take into consideration a wide range of risk factors that come with cryptocurrencies innovative but still maturing ecosystem.

3. ACKNOWLEDGMENT

The authors would like to thank the project guide Mr. A M Hattarge and the project coordinator Mr. Kiran Avhad.

4. REFERENCES

[1] SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2016

[2] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for Bitcoin with accountable mixes. In Financial Cryptography, 2014.

[3] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In Workshop on Bitcoin Research, 2014.

[4] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Financial Cryptography, 2013.

[5] Book:- Bitcoin and cryptocurrency technology: A comprehensive introduction

[6] W. Dai. b-money. www.weidai.com/bmoney.txt, 1998.

[7] G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno. Pinocchio Coin: building Zerocoin from a succinct pairing-based proof system.In PETShop, 2013.

[8] C. Decker and R. Wattenhofer. Information propagation in the bitcoin network. In IEEE P2P, 2013.

[9] A.K.R.DermodyandO.Slama.Counterpartyannouncement.https://bitcointalk.org/index.php?topic=395761.0, January 2014.

[10] J. A. D. Donet, C. Perez-Sola, and J. Herrera-Joancomartı. The ´Bitcoin P2P network. In Workshop on Bitcoin Research, Jan. 2014.

[11] List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses. bitcointalk.org, August 2014.

[12] S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to Better—How to Make Bitcoin a Better Currency. In Financial Cryptography, 2012.

[13] Bentov and R. Kumaresan. How to Use Bitcoin to Design Fair Protocols. In CRYPTO, 2014.

[14] I. Eyal and E. G. Sirer. The majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.

[15] S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, August 2012.

[16] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In WEIS, 2013.

[17] N. T. Courtois, M. Grajek, and R. Naik. Optimizing sha256 in bitcoin mining. In Cryptography and Security Systems, 2014.

BIOGRAPHY

Nikita Jadhav
BE Computer, Sinhgad Academy of Engineering

Dhanashree Biradar
BE Computer, Sinhgad Academy of Engineering

Akshay Olekar
BE Computer, Sinhgad Academy of Engineering

Saima Ansari
BE Computer, Sinhgad Academy of Engineering

Correspondence Author: A. M. Hattarge.