Restricting the Illegal Transactions in Cryptocurrencies

Utkarsh Wadhwa
Information Technolgy
Galgotias College of Engg. & Tech.
G. Noida, India

Vivek Tomar
Information Technology
Galgotias College of Engg. & Tech.
G. Noida, India

Jasmine Bedi Khurana
Information Technology
Galgotias College of Engg. & Tech.
G. Noida, India

ABSTRACT

The trend of digital currencies is catching fire these days, more and more people want to use digital currency. When we talk about digital currencies then how can we forget taking the name of Cryptocurrencies like Bitcoin. These currencies because of their P2P nature have won lot of hearts. You must have heard that "Every Rose has a thorn", similar type of thing is with Cryptocurrencies too. Because of the reason these currencies are P2P nature and there is no 3rd party who controls these cryptocurrencies, these are being used for illegal drugs – arms dealing and for purchasing weapons online which are used in the terror attacks. We have found out a solution in order to put an end to it and the solution is Freezing of Assets. In this the owner will have the liberty to freeze any account whichever seem fishy and the freezed accounts will have their money intact, just the difference will be that they won't be able to transfer the money.

Keywords

Bitcoins; Cryptocurrencies; Ethereum; Freezing assets; cryptographic algorithms

1. INTRODUCTION

Cryptocurrency [1] is made of two words Crypto + Currency. Crypto means that it uses Cryptography in order to secure the transaction and Currency we all know is the medium of exchange in the economy. We can define Cryptocurrency as a digital asset which works as the medium of exchange in a secure environment.

In the year 2009, first decentralized cryptocurrency which we all know today as bitcoin was discovered by a person named Satoshi Nakamoto [2] (identity still unknown). Bitcoin is a P2P network which does not require any 3rd party to control the currency that is the reason behind its decentralization. The transactions in the currency takes place over the blockchain, which is a distributed ledger. In every transaction, a mathematical problem is attached that is solved by the miners in the blockchain. These Miners have highly sophisticated computers made only for solving mathematical problems of cryptocurrencies.

The question is why these people try to solve these problems, this is because the person who solves this problem first will be rewarded one block of bitcoin which currently equals to 12.5 bitcoin [3]. Nowadays, due to increased complexity people get involved in mining pools (Large chunk of people combining their resources to solve the mathematical problems) and the block captured by one mining pool can be shared amongst its miners.

Basically, the main reason why these cryptocurrencies were discovered simply to make the economy more inclined towards people instead of the bankers. You will see that many people invest their money in commodities because they are more trustable than Dollar, Pound, Euro, etc.

2. LITERATURE SURVEY

In the past 2 years, cryptocurrencies have emerged a lot and many new innovations have been made in the proof of work but some of the significant one's are the addition of the central administrator and the central minter in the cryptocurrencies. This is a fact that every 4 years' blocks [4] of blockchain are halved. It is said that after 125 years, bitcoin will not exist. In this case, central minter would be able to circulate more amount if there is a requirement in the blockchain.

In London, a research was conducted by some scholars and in that they thought that although decentralization save us from the cruel national political system but it has a lot of computational cost involved and the problem of scalability is there. So, what they invented is a new cryptocurrency named RSCoin [5]. It has the control of the central banks along with the distributed set of authorities which helps in saving it from the double spending attack. This will ensure full transparency and partial centralization. RSCoin successfully removed wasteful hashing and is a scalable currency.

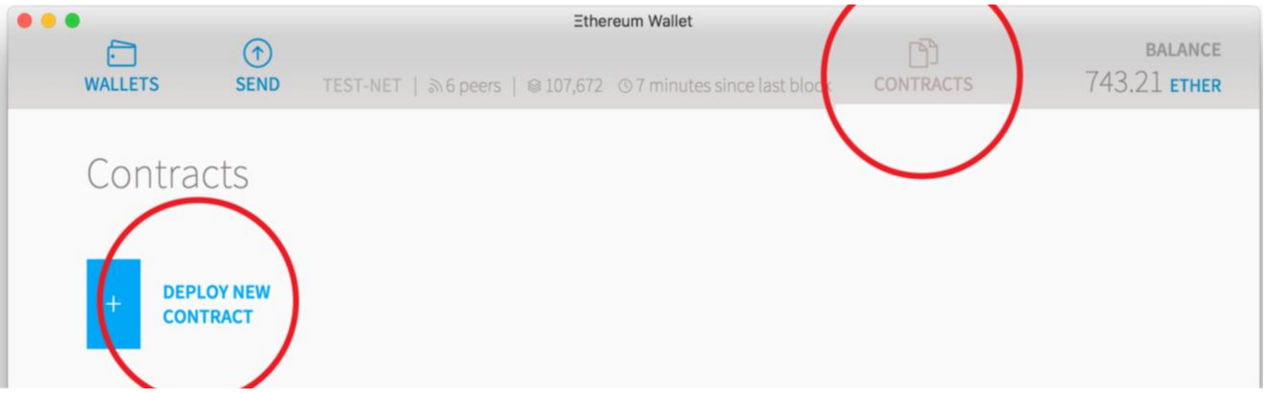
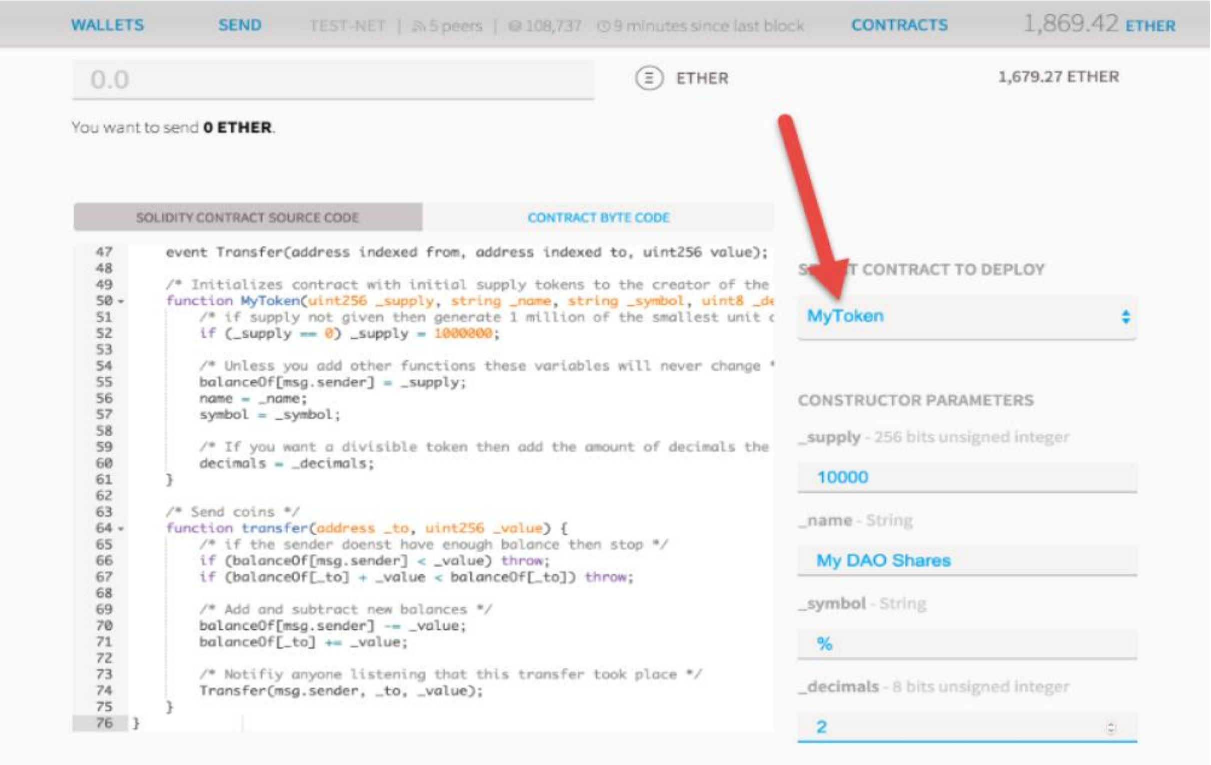


Figure 1 - Deploy New Contract


WALLETS
SEND
TEST-NET | 5 peers | 108,737 9 minutes since last block
CONTRACTS
1,869.42 ETHER
0.0
ETHER
1,679.27 ETHER
You want to send 0 ETHER.
SOLIDITY CONTRACT SOURCE CODE
CONTRACT BYTE CODE

```
    event Transfer(address indexed from, address indexed to, uint256 value);

    /* Initializes contract with initial supply tokens to the creator of the
    function MyToken(uint256 _supply, string _name, string _symbol, uint8 _de
        /* if supply not given then generate 1 million of the smallest unit c
        if (_supply == 0) _supply = 1000000;

        /* Unless you add other functions these variables will never change *
        balanceOf[msg.sender] = _supply;
        name = _name;
        symbol = _symbol;

        /* If you want a divisible token then add the amount of decimals the
        decimals = _decimals;
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        /* if the sender doenst have enough balance then stop */
        if (balanceOf[msg.sender] < _value) throw;
        if (balanceOf[_to] + _value < balanceOf[_to]) throw;

        /* Add and subtract new balances */
        balanceOf[msg.sender] -= _value;
        balanceOf[_to] += _value;

        /* Notifiy anyone listening that this transfer took place */
        Transfer(msg.sender, _to, _value);
    }
}
```

S T CONTRACT TO DEPLOY

MyToken

CONSTRUCTOR PARAMETERS

_supply - 256 bits unsigned integer

10000

_name - String

My DAO Shares

_symbol - String

%

_decimals - 8 bits unsigned integer

2

Figure 2 - Adding Code along with constructor parameters

3. THE CODE

Ethereum which is also known as the currency of the future because it is a more robust compared to Bitcoin. In doing all the practical part we have used Ethereum [6] wallet as our tool and we will be appending the freezing assets code in the code of Ethereum coin. The software which we are using has the capability of mining the testing ethers which could easily be consumed for all the tests.

In figure 1, where code of the Ethereum coin has been typed and as soon as we select the contract to deploy which in our case is "MyToken". This will further open up the space for many constructor parameters which you can fill based on your preferences.

4. IMPROVING THE CODE

We are adding the feature freezing of assets which will be a great help in putting an end to the terrorist purchasing arms and drugs with the help of this digital currency.

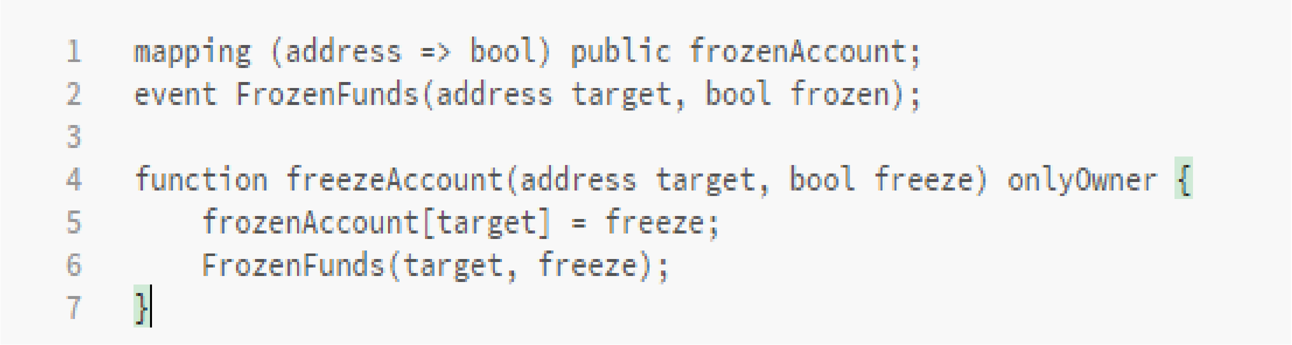
4.1 Freezing Of Assets

As we have discussed till now that it all depends on the use case that who can and cannot use the cryptocurrency. Suppose there is a scenario that there is some illegal purchase of arms is happening so noticing the use case the owner will freeze the assets of the person.

Freezing should not be confused with deleting the account because freezing will ensure that the balance or the currency in his account remain intact just the difference will be that the person won't be able to move his money from one place to another.

In figure 2, it can be clearly seen that there is a code which consist of variable and functions. This code can be added anywhere inside the contract. Only the single thing which should be taken care of it is mappings should be put with other mappings and the events should be with other events.

In figure 3, the code depicts that all accounts by default are unfrozen and when the time comes the owner may turn any account to be a frozen account.

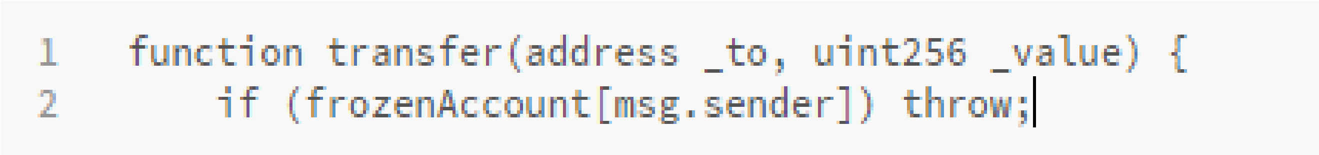


```
mapping (address => bool) public frozenAccount;
event FrozenFunds(address target, bool frozen);

function freezeAccount(address target, bool freeze) onlyOwner {
    frozenAccount[target] = freeze;
    FrozenFunds(target, freeze);
}
```

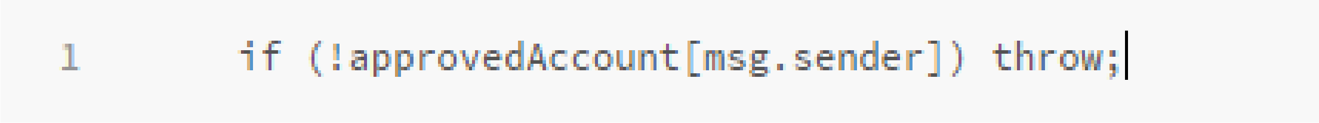
Figure 3 - Adding the basic code for mappings and events

Now we know that any account which is frozen still has all the funds safe and difference is that nothing can be transferred. If the owner feels that the use case is good, then the FreezedAccount could be changed to approvedAccount. One more thing is that you can change the last line to: -



```
function transfer(address _to, uint256 _value) {
    if (frozenAccount[msg.sender]) throw;
```

Figure 4 - Freezing Account



```
        if (!approvedAccount[msg.sender]) throw;
```

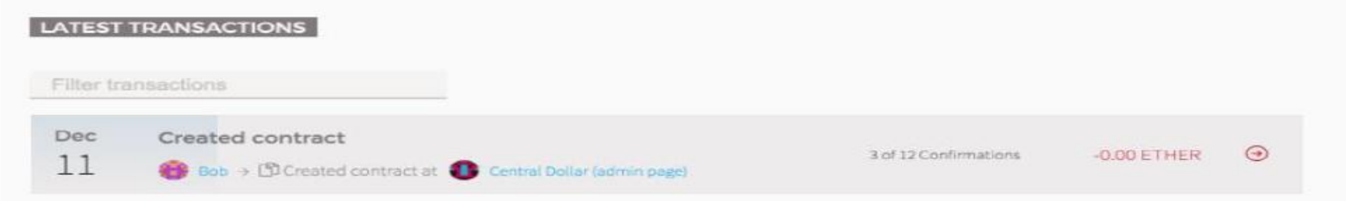
Figure 5 - Replacement of the last line

5. DEPLOYMENT OF CODE

Now we have created the token with a robust feature known as the Freezing Accounts.

Deployment plays a major role in this currency because of different nature of the currency. Now we have created the token with a robust feature known as Freezing Assets. The next step is to apply the parameters and design the contract. We already have the test ethers so the contract can be made and system will charge some of the ethers [7]. One thing you have to keep in mind and that is more is the charge, faster will be your transaction. Normally a contract will do 12 confirmations before a contract is made. More are the confirmations, more will be the chances of successful execution. Figure 5 shows the contract creation process.

In figure 6, it can be clearly seen that addition of owner is done. This is the owner who will be responsible for all the activities i.e. this owner will have the authority to freeze or approve any asset. The address of the owner needs to be added in the space provided.

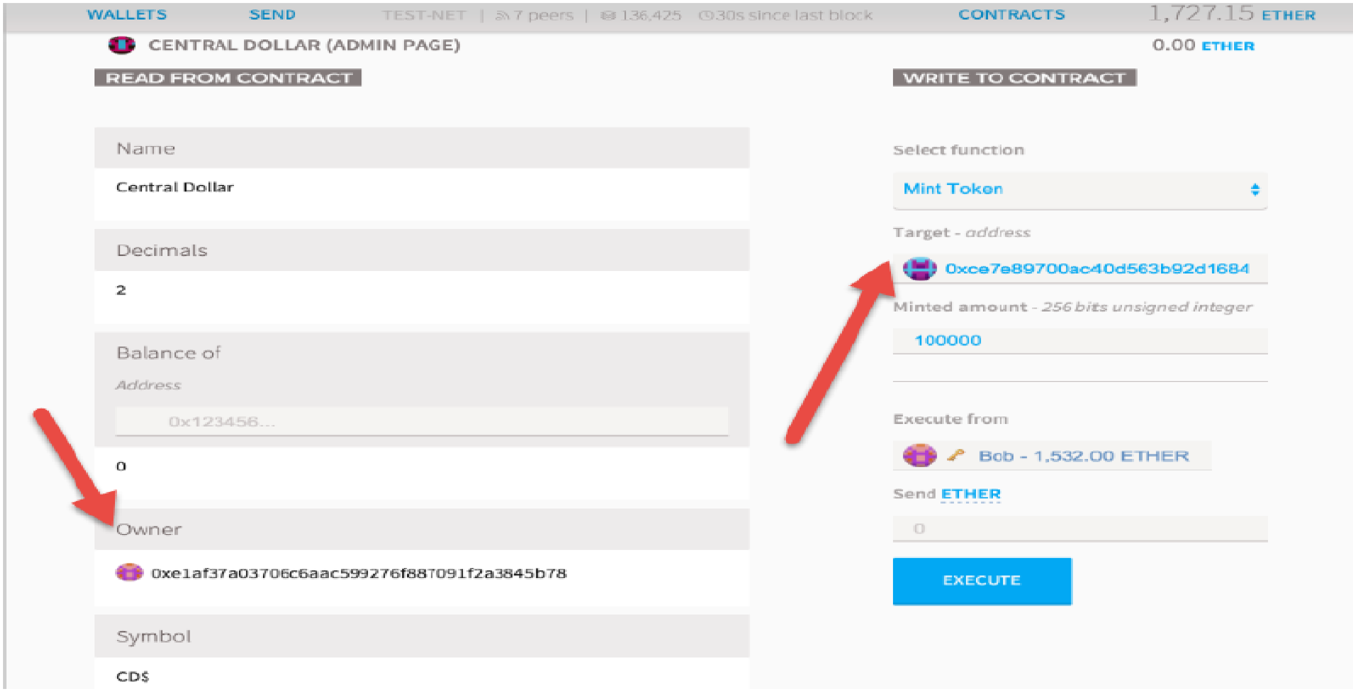


LATEST TRANSACTIONS

Filter transactions

Dec 11 — Created contract — Bob → Created contract at Central Dollar (admin page) — 3 of 12 Confirmations — -0.00 ETHER

Figure 6 - Contract Creation Process



CENTRAL DOLLAR (ADMIN PAGE) — 0.00 ETHER

READ FROM CONTRACT

Name: Central Dollar

Decimals: 2

Balance of — Address: 0x123456... — 0

Owner: 0xe1af37a03706c6aac599276f887091f2a3845b78

Symbol: CD$

WRITE TO CONTRACT

Select function: Mint Token

Target - *address*: 0xce7e89700ac40d563b92d1684

Minted amount - *256 bits unsigned integer*: 100000

Execute from: Bob - 1,532.00 ETHER

Send ETHER: 0

Figure 7 - Owner Addition

After this your token is ready to be used as a digital currency and can be sent to any of your friend. But before your friend receives the amount he needs to do the task done in figure 7. He needs to add the initiation address of the token and rest of the details will automatically be filled. Sometimes due to network problems details will not be added automatically so you have to manually enter the details. Once all details have been entered your friend would be able to see the currency in his account.

6. CONCLUSION

To assimilate, we can clearly say that with the Freezing account feature inside cryptocurrency will give extra power to it as the fishy accounts could Froze by the owner. This will not only help in curbing crime due to purchase of illegal arms and drugs but also help in adding a sense of centralization to the blockchain. The P2P nature of digital currency will be intact. By constructing a blockchain-based approach that makes relatively minimal alterations to the design of successful cryptocurrencies such as Bitcoin, we have demonstrated that this centralization can be achieved while still maintaining the transparency guarantees that have made (fully) decentralized cryptocurrencies so attractive. We have also proposed a new consensus mechanism based on 2PC and measured its performance, illustrating that centralization of some authority allows for a more scalable system to prevent double spending that completely avoids the wasteful hashing required in proof-of-work-based systems. Moreover, in this report we tried adding two new features which can be made common to both the coins that are central administrator and the central minter. Basically, these can mitigate the problem of illegal purchase of drugs and weapons online as the mafias would not be able to purchase anonymously as someone is always looking at the transactions.

In bitcoin, the problem is that its block are halved every 4 years so supply [8] is getting less and the demand is increasing so there should be a balance between the demand and supply. This creates the need of a central minter. This will be the person who will be able to regulate the supply of money in the network.

Future scope lies in developing these currencies in such a way that there will be efficient use of the network and the central administrators [9]. The key feature of these currencies was there anonymous feature and that should be intact.

7. REFERENCES

[1] Ethereum. Wikipedia Available at- https://en.wikipedia.org/wiki/EthereumS

[2] Nakamoto, - "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, bitcoin.org/bitcoin.pdf.

[3] L. Luu, J. Teutsch, R. Kulkarni, and P. Saxena, ―"Demystifying incentives in the consensus computer in proceedings of ACM CCS", 2015, to appear. http://www.coindesk.com/making-sense-bitcoins-halving/

[4] George Danezis - UCL Computer Science https://cointelegraph.com/news/www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf

[5] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies"

[6] Aldridge, Judith, a David Décary-Hétu. 2014. "Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation". SSRN Working Paper. https://www.toptal.com/bitcoin/blockchain-technology-powering-bitcoin

[7] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. Sok: "Research perspectives and challenges for bitcoin and cryptocurrencies". In 2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015, pages 104–121, 2015.

[8] F. Reid and M. Harrigan. "An Analysis of Anonymity in the Bitcoin System. In Security and Privacy in Social Networks", pages 197–223. Springer New York, 2013.

[9] M. Peck. "Bitcoin-Central is Now The World's First Bitcoin Bank"...Kind Of. IEEE Spectrum: Tech Talk, Dec. 2012. spectrum.ieee.org/techtalk/telecom/internet/bitcoincentral-is-now-theworlds-first-bitcoin-bankkind-of.