Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3805-3811

Research Article

Alt -Coin: An Energy Coin to Empower the Future

[1]Sumitra Samal, [2]Kaveri Kar, [3]Taniya Jain

[1,2,3](Asst.Professor, Department of Computer Science and Engineering)
[1,2,3](Shri Shankaracharya Institute of Professional Management and Technology, Raipur)
[1]samal.sumitra07@gmail.com, [2]kaverikar03@gmail.com, [3]er.taniyajain@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

***Abstract*—**An authenticated peer-to-peer version of e-cash would allow online transactions to be sent directly from sender to receiver without going through any financial institution. Alt- Coin is a digital currency that unlike traditional currencies, do not rely on a centralized authority. Instead, Alt-Coin is based on a community of volunteers that collectively implement a replicated ledger and verify transactions. Digital signatures give us a part of the acknowledgement, but the main benefits are gone if a responsible third party is still needed to prevent multiple-spending. While transactions are conducted between people, bit coin can't give solid privacy guarantees: any transactions are being recorded in a decentralized public ledger, from which far more information can be abstracted. But Alt-Coin doesn't tackle some of these privacy issues by unlinking transactions from the payment's origin like zero coins do. It shows transaction destinations details and given amounts just like bit coin, and has the same functionality as of bit coin. In Block chain, people performing Forks could be ignored as they are indicative of unpredictability among the copies in the network. We then show what may be accomplished by pushing the modern-day protocol to its restriction with unilateral modifications to the customer's behavior. The network timestamps affair by hashing them into an in-progress chain of hash-based verification-of- work, forming a record that can't be changed without doing it again the verification-of-work. The longest chain not only shows as verification of the order of events being watched but proof that it came from the largest pool of CPU power. Many Alt-Coin has achieved only scant consumer transaction volume, with an average well below one daily transaction for the few merchants who accept it. Its volatility is significantly higher than the volatilizes of widely used currencies, imposing considerable short- term risk upon users. We then show what can be obtained by pushing the current rules to its limit with unilateral changes to customer behavior. We then display what can be completed with the aid of promoting the current protocol to its restriction with unilateral changes to the purchaser's behavior. In this paper, we will get a top-level view of ways alt-coin can be fork form bit coin.

Keywords: Alt-coin, Decentralized, Digital signature, Bit coin, Ledger

I. INTRODUCTION

A Block chain is essentially a database of records or public ledger of all digital occasions which have been accomplished and shared amongst collaborating parties [1]. Each settlement in public accounting is proved by Consensus of a better part of a contributor in the system. The digital currency bitcoin itself is highly controversial, but the underlying technology has worked flawlessly and found a wide range of applications in both financial and non-financial world. It contains a particular provable and unquestionable record of every single transaction ever made. Bitcoin is the decentralized, end-to-end e-currency, and it is the most famous example that uses this technology. Bitcoin [2] is one of the first e-currency to obtain universal assumption. The currency owes its rise in part to the fact that unlike traditional e-cash schemes, it needs none of the trusted parties. Instead of having a central bank, Bitcoin got to have ledger known as the Block chain to store transactions done between people. Because mutually-distrustful peers widely reproduce the Block chain, the knowledge it contains is public accessible While people may engage many identities to upgrade their privacy, an increasing body of research shows that anybody can do Bitcoin by using the info in the Block chain such as the emergence of the agreement graph as well as the value and dates of agreement. As a result, Bitcoin is unsuccessful to present even a fraction of the isolation provided by traditional payment systems. Bitcoin is that the most well-liked example that's as such tied to technology. It is additionally the foremost disputed one since it helps to change an international market of anonymous transactions with none governmental management. Hence, it's to influence a variety of regulative problems involving national governments and money establishments. To protect their privacy, users, therefore, would like an immediate, risk-free, and, most significantly, automatic guarantee that doesn't reveal their public transactions and account balances in open access. Their Anonymous transactions additionally guarantee that the market price of a coin is freelance of its

history, therefore ensuring legitimate users' coins stay fungible. Despite receiving in-depth public attention, theoretical understanding is restricted related towards the worth of Bitcoin, as expressed in their exchange rates against ancient currencies. Anonymous transactions additionally guarantee that the value of a coin is freelance of its history, therefore making certain legitimate users' coins stay fungible. According to our analysis, within the short term, the Bitcoin rates per unit adjusts to changes in economic fundamentals and market conditions. We tend to additionally determine a significant impact of mining technology and a decreasing significance of mining problem within the Bitcoin exchange worth determination.

There are several goals of this project; one of the principal aims is to facilitate transactions between willing people who would otherwise have no means that trust each other. The most honest of judgment, usually tough to seek out, comes naturally from a fair recursive interpreter. Transparency, or having the ability to visualize precisely however a state or experience passed through the group action log and rules or educational codes, never happens utterly in human-based systems since language is necessarily imprecise, information is commonly lacking, and acceptable recent prejudices were challenging to shake. overall, we want to layout a system for all users where unique people from exclusive parts of the society can do the transaction with absolute confidence and without worry approximately safety concerns. We want to propose a concept how of obtaining an altcoin fork with bitcoin as well, which is in trend in the market, that's later analyzed in the marketplace state of affairs similarly inside the paper.

II. ENERGY COIN A DECENTERALISED CURRENCY

Energy coin, which extends Alt -coin to provide strong anonymity guarantees. Like many e-cash protocols employs zero-knowledge proofs to prevent transaction graph analyses. In the past, some of the e-cash transactions do not need to conform through digital signatures to validate e-cash, nor does it require a central bank to prevent double-spending. Instead, authenticates coins by proving, in zero-knowledge, that they belong to a public list of valid coins (which can be maintained on the Block chain). Taken as an entire, are often viewed as a transaction-based state machine. We start with a genesis state and incrementally execute transactions into some final rule. It's this final state that we tend to settle for because of the canonical "version" of the coin. The state will embody such info as account balances, reputations, trust arrangements, knowledge about the altcoin. Transactions, therefore, represent a sound arc between state; the 'valid' half is essential—there exist way more invalid state changes than valid state changes. Invalidate changes would possibly, e.g., be things like reducing associate account balance while not associate equal and opposite increase elsewhere. The sound state transition is one that comes about through dealing. Transactions are collated into blocks and blocks are chained along implementing a hash, as a method of reference. Blocks operate as a journal or ledger, recording series of transactions in conjunction with the previous block and associate symbol for the final state (though blocks don't store the final state itself—that would be so much too big). Additionally, punctuate the dealing series with incentives for nodes to mine. This takes place as operate, adding price to a nominative account.

III. ENERGY COIN MINING TECHNOLOGY

The digital currency depends on its correctness and stability on a mixture of cryptography, distributed algorithms, and behavior. Tend to examine as accord game and confirm that it depends on separate accord regarding the foundations and regarding the game state. A significant side of Energy coin's style is that the mining mechanism, in which participants expend resources on determination process puzzles to gather rewards. This mechanism supposedly protects against bound technical issues like inconsistencies within the system's distributed log arrangement. Tend to additionally show however intended antagonist may be able to disrupt the system and "crash" the currency. Finally, we argue that would require the emergence of governance structures, contrary to the control read within the community that the coin is. Consensus regarding the foundations may be a human process. Participants should come back to a common understanding of what's allowed, so the foundations are encoded into the computer code that every participant uses. In Bitcoin, small teams and people can exert oversize power is implemented in energy coin as well. Consensus regarding state may be a technological drawback in distributed systems design. Every player will see a part of the state. Therefore the players got to get together, in massive numbers and across a probably unreliable network, to achieve a consistent understanding of the world state. The technological accord should be achieved despite the chance that some players can deviate from the printed rules. Within the distributed systems' literature, devious behavior ("Byzantine failures") will usually be tolerated if a comfortable majority of players square measure honest and cooperate. However, in Bitcoin, we tend to assume that players can behave according to their incentives expressly. Hence we expect miners of energy coin to act in the same manner. (Assuming cooperation despite the fact that incentives to the contrary would build the planning a lot of less complicated, though impractical.) Finally, the accord that Bitcoins square

measure valuable is that the same kind of agreement necessary for any enactment currency. Such price is commonly sculptured as a put concentration ina coordination game (because players would like one thing to use as a medium of exchange and a unit of account, they opt for a neighborhood currency as a result of it is available). Such associate analysis is critical; however, not comfortable to elucidate the Consensus that Bitcoins square measure valuable. A basic model enlightens anyway players choose whether or not and the path to mine. Imagine a replacement energy coin player, Minnie, World Health Organization desires to work out whether or not or not to become a manual labourer. Minnie has the choice to take position resources (say, equipment and electricity) in mining at a price of C bucks per second, and should decide whether to form the investment. Say that this investment can permit Minnie to make P = f(C) puzzle guesses (hashes) per second, a puzzle takes G guesses to solve in expectation, which with success resolution a puzzle (i.e., mining a block) offers a gift of Bitcoins with price V Finally, assume that every face a similar call (i.e. that no player has access to special technology or significant discounts that aren't accessible to different players. Then Minnie can earn P V /G expected bucks per second then could invest if. G= PV/C

IV. HOW TO MAKE YOUR OWN ALT-COIN

The guide is developed by compiling on Linux ubuntu 16.04 LTS. We must follow the steps mentioned below.

A. Obtain a working codebase and build it.

You can start by having a copy of litecoin v.17 in your own system. You can fork the project from the official litecoin repo **https://github.com/litecoin-project/litecoin.** Command to follow:

1) git clone https://github.com/litecoin-project/litecoin.git
2) cd litecoin

Compile sequence

1) ./autogen.sh
2) ./configure
3) make
4) make install # optional

Now you have a working litecoin project, and we can start editing.

B. Rename Litcoin to your own coin name

In our case, we will use the name Energycoin, and instead of LTC we will use ENC

1) find ./ -type f -readable –writable -exec sed -i "s/Litecoin/Energycoin/g" {} \;
2) find ./ -type f -readable –writable -exec sed –i "s/LiteCoin/Energycoin/g" {} \;
3) find ./ -type f -readable -writable -exec sed –i "s/LTC/ENC/g" {} \;
4) find ./ -type f -readable -writable -exec sed –i "s/litecoin/energycoin/g" {} \;
5) find ./ -type f -readable -writable -exec sed –i"s/litecoind/energycoind/g" {} \;

Recompile the source.

C. **Remote Procedure Calls**

Port numbers change In our case, we will use the name Energycoin, and instead of LTC we will use ENC

1) find ./ -type f -readable -writable -exec sed –i "s/Litecoin/Energycoin/g" {} \;
2) find ./ -type f -readable –writable -exec sed -i "s/LiteCoin/Energycoin/g" {} \;
3) find ./ -type f -readable –writable -exec sed –i "s/LTC/ENC/g" {} \;
4) find ./ -type f -readable –writable -exec sed –i "s/litecoin/energycoin/g" {} \;
5) find ./ -type f -readable –writable -exec sed –i "s/litecoind/energycoind/g" {} \;

Remote Procedure Calls: Remote Procedure Call (RPC) [3] is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. A procedure call is also sometimes known as a function call or a subroutine call.RPC uses the client-server model. The requesting program is a client, and the service providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned. However, the use of lightweight processes or threads that share the same address space allows multiple RPCs to be performed concurrently.

Litcoin uses 9332 as the default RPC port, and we look into the list of all know TCP UPD ports and select a unique

1) find ./ -type f -readable -writable -exec sed –i "s/9332/6332/g" {} \;

D . Change the starting letter of the public addresses of the Blockchain

Go src/chainparams.cpp
L:138:base58Prefixes[PUBKEY_ADDRESS]=std::vector
<unsignedchar>(1,48);
This effects the starting letter of your public address, here in litecoin 48 is used for letter L.
We check the list of prefix and change this accordingly https://en.bitcoin.it/wiki/List_of_address_prefixes [4]
We will use 33 to get E as the first letter in the public addresses Update the PUBKEY_ADDRESS base58 prefix to
in the source code at
src/chainparams.cpp
base58Prefixes[PUBKEY_ADDRESS]=std::vector<unsigned char>(1,33);
Also we set the below line to a unique value
base58Prefixes[SECRET_KEY]=std::vector<unsigned char>(1,35);
base58Prefixes[EXT_PUBLIC_KEY]=0xff, 0x88, 0xB2, 0x1E

E. Change pchMessageStart

In src/chainparams.cpp
Change these to unique values L:115:
pchMessageStart[0] = 0xfb;
pchMessageStart[1] = 0xc0;
pchMessageStart[2] = 0xb6;
pchMessageStart[3] = 0xdb

F. Change pchMessage Start

Goto src/consensus/consensus.h L:19: static const int COINBASE_MATURITY = 100; Coinbase transaction outputs can only be spent after this number of new blocks (network rule). The above line states that the newly generated coin can only be spent after 100 blocks are generated.

G . Change Change maximum supply

Goto src/amount.h, and change L:26 , L:26: static const CAmount MAX_MONEY = 84000000 *COIN; Here, 84000000 is the maximum coins possible in the network and COIN is a static const variable whose value is defined as 100000000. Note that 84000000 is not the total no. of coins in the chain; it is the maximum allowed coins in the chain. We can change this 84000000 according to our needs

H . Change pchMessage Start

L:84: consensus.nPowTargetTimespan = 3.5 * 24 * 60 * 60;
// 3.5 days
L:85: consensus.nPowTargetSpacing = 2.5 * 60;
Set according to the need

I. Premine and Block Rewards

Goto src/validation.cpp, L:1162 function: GetBlockSubsidy()
And update it as follows:

```
CAmount GetBlockSubsidy(int nHeight, const Consensus::Params consensusParams)
{
int halvings = nHeight / consensusParams.nSubsidyHalvingInterval;
if (halvings >= 64)
return 0;
CAmount nSubsidyBase;
if (nHeight == 1)
{ nSubsidyBase = 1000000000; }
else { nSubsidyBase = 5000; }
CAmount nSubsidy = nSubsidyBase * COIN;
nSubsidy »= halvings;
return nSubsidy;
}
```

Here, if(nHeight ==1) nSubsidyBase = 1000000000; gives the total premine which is generated on mining 1st block and nSubsidyBase = 5000; is the block reward for each ming each block

J . Remove seed nodes

Goto src/chainparams.cpp, L:132 and remove all
vSeeds.emplace_back(". ")

K.Create Genesis Block

To produce a genesis block **https://github.com/lhartikk/GenesisH0**

python genesis.py -a scrypt -z "NY Times 05/Oct/2011040184710fa689ad5023690c80f3a49c8f13f8d45b8c857fbcb c8bc4a8e4d3eb4b10f4d4604fa08dce601aaf0f470216fe1b51850b4acf21b179c45070ac7b03a9"-t1317972665–n2084524493

L. Remove checkpoint

In src/chainparams.cpp,

L:153,

Replace the checkpoint data with the genesis block, like below

checkpointData ={ { { 0, uint256S("0xadb40498108648a3e9033e306d93ff5712054386ed3e912985572da9b6529fee")}, }};

here , 0 is the 0th block that is genesis block and uint256S("0xadb40498108648a3e9033e306d93ff5712054386ed3e912985572da9b6529fee") is the transaction hash of it.

And also change the chainTxdata just below the checkpointData chainTxData = ChainTxData{ // Data as of block adb40498108648a3e9033e306d93ff5712054386ed3e912985572da9b6529fee (height 0). 1580814925, // * UNIX timestamp of last known number of transactions 0, // * total number of transactions between genesis and that timestamp

// (the tx=... number in the SetBestChain debug.log lines) 0

// * approximate number of transactions per second after that timestamp };

Some important commands

Replace energycoind with (yourcoin)d

energycoind -- deamon //To start the blockchain deamon

energycoind -- printtoconsole //Start blockchain and print on console

energycoin-cli getblockchaininfo //To get the Blockchain info when deamon is running

energycoin-cli generate 1 // To mine a new block, it may take time acc to the system

energycoin-cli generatetoaddress 1 "..." // mine 1 block to given address

energycoin-cli getpeerinfo // Get information on peer connected to the node

V. HOW TO INVEST AND GET BENEFITS

As we know, Alt-coin follows market patterns of bitcoin and variate accordingly so hereby we will get some info on bitcoin and its related topics. Just to get an overview of the scenario bitcoin has created. Bitcoin - Bitcoin is the first decentralized digital currency. All Bitcoin transactions are documented on a virtual ledger called the block chain, which is accessible for everyone to see. Bitcoin gives you complete control over your money, unlike other assets you own which are regulated by banks and governments [5,6]. As bitcoin gains more popularity, more and more places accept it as a payment method. Bitcoin Mining - Bitcoin mining is the process of updating the ledger of Bitcoin transactions known as the block chain. Mining is done by running extremely powerful computers (known as ASICs) that race against other miners in an attempt to guess a specific number. The first miner to guess the number gets to update the ledger of transactions and also receives a reward of newly minted Bitcoins. Bitcoin Wallet-A Bitcoin wallet is a device or program that stores your private keys and allows you to interact with the Bitcoin block chain (i.e. send and receive Bitcoins). Altcoin-Altcoins, or alts for short, are cryptocurrencies that are not Bitcoin. The word altcoin is an abbreviation of alternative coins. Litecoin, XRP, Ethereum or any other non- Bitcoin cryptocurrency all fall under the category of altcoins.

How to invest in altcoins-

1) Choose a trustworthy fiat-to-crypto exchange-At first. The user needs to register at a gatewayy service. Gatewayy or fiat-to-crypto platforms are exchange services where users can purchase cryptocurrencies with fiat. The most reputable and beginner-friendly fiat-to-crypto platforms are Coin base (exchange review), Binance (exchange re- view), and few others.
   The user should look for a service that suits their need and is not blocked in their jurisdiction and pay attention to the deposit and transfer fees. Multiple gateway coin exchanges offer fast credit/debit card transfer services, but they usually charge more than a standard transfer.
2) Register and Buy Bitcoin or Ethereum-After choosing the most suitable exchange, it is time to get there, register an account and purchase Bitcoins or Ether (or altcoins if they are listed there). As we know

Bitcoin, Ethereum and altcoin are Cryptocurrencies popular and widely accepted.

3) (Optional) Register On Altcoin Exchange-If the user can get the altcoins they want using a fiat-to-crypto exchange, most of the work is done. Typically, however, fiat-to-crypto exchanges don't have a wide variety of selection of altcoins, so there isn't really what you're looking for. That's why so-called altcoin (crypto-to-crypto) trading platform is widespread. Alt- coin or crypto-to-crypto platforms are platforms in cryptocurrency with no fiat pairs and deposit alternatives. Such markets usually succeed via offering the least common, new, and innovative ventures which arrive at such a low price but also in the longer term could dramatically improve the wealth of buyers. It's easy and quick to exchange them for cryptos. Before choosing an altcoin exchange, the user must pay attention to its reputation and security measures. Be careful with such past record of attacks or negative feedback on the websites. For the most part, crypto- to- crypto markets remain open, so act responsibly but never take chances where you cannot easily lose.
4) Shift Cryptocurrencies Via One Market to Another, to make a deposit once you have chosen an acceptable altcoin exchange. The user can do so by withdrawing their crypto assets (most likely BTC or ETH) from your gateway (fiat-to-crypto) exchange wallet to the altcoin (crypto-to-crypto) exchange wallet. The methods across all exchanges are easy and uniform. First, the user needs to find and copy the deposit address in the altcoin exchange. Ensure that wallet address is only for the investment that you would be depositing. For example, a user must never send Ether to a Bitcoin address. When you are transferring Bitcoin, make sure to send it over to a Wallet address for Bitcoin. This is a simple yet critical step! If you fail to do it right, you may lose your funds. Next, head to the gateway y exchange and navigate to the withdrawal section. Insert the wallet address of your altcoin exchange (check if it really is accurate) then click the withdraw wallet section. In some exchanges, you will need to confirm the withdrawal using your email. The coins should arrive within minutes or an hour at most, based on how fast and congested is the network.
5) Once the deposit reaches your crypto-to-crypto exchange wallet, the user can head to the market and trade your BTC or ETH for altcoins. Be mindful before buying low-key altcoins, as they carry greater threats; this has been proved over the time and widely known ventures. Little-known coins of unknown members of the team and also too promising to be true claims will turn out it was just complex fraud.

VI. FUTURE SCOPE

The slant back towards inside the first long stretches of 2022 is likewise the start of another bull-run, driven by a resuscitated certainty or comprehension inside the space. Late business improvements have reinforced expenses, as J.P. Morgan's positive advancement with the framework that it runs on the organization. The ascent of the furthermore presumably being halfway by expanding scope of coins getting into the market. Line with, it at present colossally numbers more than 5000. All elective things being same; this could scale back bitcoin strength this might be dealing with through at present that conviction has up inside the space overall. Has in addition been a region wide lift from, the best exchange inside the United States of America. It is making an arrangement for institutional financial backers by expanding its capacity to store advanced coins for their benefit outside the United States of America. Inside the language, arrangement giving has just gotten 2 significant exchange from driving firm Grant de-underwriter, subsequently is likewise drawing in extra institutional money into the world. The issue is additionally thirsting inactively expected drives from driving players like a couple of dispatch, that seem set for Gregorian schedule month 2022. This significant move up to the second-biggest organization supports a few undertakings during this space is anticipated to make a gigantic qualification to managing speeds among elective things. The tremendous inquiry is-whether Bitcoin can start to beat again because of the inquiry that is anticipated in might. It regularly happens that once in like clockwork the compensation to Bitcoin excavators is split, along these lines diminishes the quantity of most recent reachable Bitcoin to sell on the lookout. Have contended inside the verbally expressed correspondence that, the probabilities of Bitcoin substitution the world monetary set-up have without a doubt finished, at present a ton of nations and multinationals company like-Facebook square measure having the chance to dispatch of their own.

REFERENCES

1.]http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf
2. https://99bitcoins.com/bitcoin/
3. https://searchapparchitecture.techtarget.com/definition/Remote-Procedure-Call-RPC

4. https://en.bitcoin.it/wiki/List_of_address_prefixes
5. https://big-profit.website/business-news-in/7832249/index.html
6. https://99bitcoins.com/altcoin/