MEDIC COIN

Tabla de Contenido

FEATURES:

There are 199 coins in each PoS block. Masternode operators enjoy 159.2 coins or 80% of PoS block found. Staking allows you to enjoy 39.8 MEDIC coins or 20% of PoS block. To be a masternode operator you need 199999 MEDIC coins. A single wallet can do both staking and masternode at the same time. At the same time, you can have multiple masternodes in a single wallet.

There are 77 coins in each PoW block. The difficulty retargeting is every block. The last PoW block is 99,999. At that time Stanford University's Folding@Home kicks in to allow you to earn MEDIC coin through using your CPU/GPU to help scientists find the cure for Alheizmer's, diabetes, congenital diseases, etc.

MEDIC COIN SPECIFICATIONS:

Coin Name : Medic Coin

Coin Ticker : MEDIC

PoW Algorithm: Scrypt

Difficult Retargeting: Every 1 block

Maximum Block Size: 3MB

Max Supply: 500,000,000 MEDIC Coin

Block Time: 90 seconds

Stake age : 1 Hr

PoW Block Reward : 77 coins per block

Last PoW Block : 99,999 Block

PoS Block Reward: 199 Medic Coin (80% to Masternode Operators and 20% to Stakers)

Masternode Collateral: 199,999 Medic Coins

DARKSEND BASICS

DarkSend provides true financial privacy by obscuring the origins of your funds. All the Medic Coin in your wallet is made up of different “inputs” which you can think of as separate, discrete coins. DarkSend makes use of an innovative process to mix your inputs with the inputs of two other people, without your coins ever leaving your wallet. You keep full control of your money at all times.

The DarkSend process works like this:

DarkSend starts off by breaking your transaction inputs down into standard denominations. These denominations are 0.01 Medic Coin, 0.1 Medic Coin, 1 Medic Coin and 10 Medic Coin – kind of like the paper money that you use every day.

Your wallet then makes requests to specially configured software nodes on the network, called “masternodes”, These masternodes are then informed that you are interested in mixing a certain denomination. No identifiable information is sent to the masternodes, so they never know “who” you are.

When two other people send similar messages, indicating that they would like to also mix the same denomination, a mixing session is started. The masternode mixes up the inputs and instructs all three users’ wallets to pay the now-transformed input back to themselves. Your wallet pays that denomination directly to itself, but in a different address (called a change address).

In order to fully obscure your funds, your wallet needs to repeat this process a number of times with each denomination. Each time the process is completed, it is called a “round”. Each round of DarkSend makes it exponentially more difficult to determine where your funds originated from.

This mixing process all happens in the background without any intervention on your part. When you would like to make a transaction, your funds will already be anonymized. No additional waiting is required.

IMPORTANT: Your wallet only contains 1000 of these "change addresses." Every time a mixing event happens, one of your addresses is used up. Once enough of them are used, your wallet must create more addresses. However, it can only do this if you have enabled automatic backups. Consequently, users who have backups disabled will also have DarkSend disabled.

Code Review K.Atlas 2014

DarkSend TECHNICAL DETAILS (ADVANCED USERS)

DarkSend is a unique, decentralized mixer for creating an on-demand system of removing the history from coins on the network. This is mainly for fungibility, which is the attribute of money that allows any token to be exchanged with any other token, without having a difference in price in the form of a premium for tokens with less or no history. Without DarkSend, tokens with less history would become increasingly valuable as the network grows, because of their lack of association with prior transactions. Without fungibility, there is a risk that certain tokens could be "red listed" and lose some or all of their value if at any point in the past they had been found to be used in illegal or questionable activities. Nobody wants to hold money that was involved in illegal activity, yet after the activities take place, tokens re-enter the supply and pass to new users who had no connection with the prior illegal acts. We remove this issue with the implementation of DarkSend, which is included as part of the core protocol of the Medic Coin network.

DarkSend Status Codes

The system has various modes which enable servers to keep track of the current state of their mixing pool. These mixing pools are single use, allowing three people to use them at a time. Statuses are idle, queued, accepting_entries, finalizing_transaction, signing_transaction and transmitting transaction.

Users start off by connecting to a node, which is in the idle state. The masternode then moves the status to “queued” and sends a message to the network, telling other users that’s it’s currently available for mixing. Users can utilize multiple servers at a time to mix, what is called multi-session mixing. This greatly speeds up the mixing process at the cost of creating more addresses and therefore requiring more frequent wallet backups.

Privacy Through Ambiguity

Mixing is the process of joining multiple transactions together, from multiple users, where all unique information about the users is removed from the transaction. Users send tokens to themselves through the system, and at no time do these tokens ever leave the users’ wallet. masternode operators are therefore completely separate from the process of mixing. masternodes simply serve as a transit method for the storing and signing of transactions, allowing users a safe place to initiate the process in an anonymous way.

Privacy is achieved by using denominated amounts of 100, 10, 1 or .1. Each session initiated on a masternode only carries a single denomination, such as having 10x 100 Medic Coin inputs and 10x 100 Medic Coin outputs. Users then individually sign their inputs to the collective outputs, allowing the transaction to be valid once complete and broadcastable.

Fee Model Anonymity

In other implementations of mixing software, fees can be used to break the transactions apart and identify users on the networks. On the Medic Coin Network this is avoided by allowing masternodes a special type of message which allows them to broadcast fee-less transactions. We use this technology to decouple the fees from the transactions, so that for every 10 transactions using the DarkSend technology, there is only one fee transaction. This prevents a timing attack on the DarkSend implementation.

Phases of DarkSend

The process begins when a user denominates some funds to be used as a "cash account". They then simply tell a random masternode they would like to mix a specific denomination such as 100 Medic Coin. The masternode has no information about the transaction at this point, since the denomination carries no information about which inputs the user would ultimately like to mix. The masternode receives the request and issues a message to the network saying that it is ready to mix that denomination and that there is a user waiting.

At this point if other users are wishing to mix inputs of that denomination, they can connect to the masternode that is hosting the other user's transaction. When three users queue themselves on the same masternode, the next stage, "accepting_entries," is initiated.

In this stage, all users send their inputs and outputs to the masternode, where they are collected and put into memory until all users have identified the full list of inputs/outputs they would like to mix. Once this is complete, the process moves onto the next stage, "finalize." At this point, the masternode sends a message back to the users, showing the merged transaction they all jointly created. All inputs are from the user's wallet and all outputs are sent back directly to the user's wallet. The funds involved in this process never leave the user's wallet at any time, allowing the masternode to be completely segregated from users' funds. This is how the process of DarkSend remains trustless and secure, without risking user's funds or exposing masternodes to excessive legal risk. Once the finalized transaction is approved, the process moves onto the next phase, "signing."

Users sign only the inputs for which they have keys, and the funds are then released to all outputs simultaneously. It's worth noting that inputs and outputs are not directly tied to each other in this process, since inputs are in a separated list and only tied to each other. Outputs are also in a separated list, only tied to each other. This means, literally, that all users are paying all users in this process. The users are not only paying themselves, but everyone else. This means you can't say input #4 went to output #14 (e.g. you can't trace the input to the output, they are processed in concert).

When all inputs are signed to all outputs, the transaction suddenly becomes valid, and the masternode broadcasts using a special message called DSTX. The network keeps track of these messages, allowing masternodes to submit one DarkSend transaction every n hours without paying fees.

WHAT IS INSTANTSEND?

InstantSend is an advanced service that allows for near-instant transactions to take place. With this system, inputs can be locked to specific transactions and verified by consensus of the masternode network. Conflicting transactions and blocks are rejected. If a consensus cannot be reached by the masternode network, validation of the transaction will occur through standard block confirmation. InstantSend is able to solve the double-spending problem without the longer confirmation times of other cryptocurrencies such as Bitcoin.

FOLDING@HOME AND MEDIC COIN

Once the last block of PoW is done, Folding@Home kicks in to allow you to earn Medic Coin through CPU/GPU protein folding. Folding@Home software runs while you are doing other things. While you are busy with your everyday activities, your computer is working to help us find cures for diseases like cancer, ALS, Parkinson's, Huntington's, and many others.

MEDIC EMR

Blockchain Quick Review

Blockchain is fundamentally a new type of database technology that is optimized to tackle a unique set of challenges. Historically, databases have been used as central data repositories by organizations to support transaction processing and computation. However, databases are rarely shared between organizations due to a variety of technology and security concerns. Blockchain is a shared, distributed database of transactions among parties that is designed to increase http://atlant.io 10 transparency, security, and efficiency. Blockchain is a database (with copies of the database replicated across multiple locations or nodes) of transactions (between two or more parties) split into blocks (with each block containing details of the transaction such as the seller, the buyer, the price, the contract terms, and other relevant details) which are validated by the entire network via encryption by combining the common transaction details with the unique signatures of two or more parties. The transaction is valid if the result of the encoding is the same for all nodes and added to the chain of prior transactions (as long as the block is validated). If the block is invalid, a "consensus" of nodes will correct the result in the non-conforming node.

Blockchain Ledger Transactions Blockchain has the following advantages over a conventional centralized database:

Security: Blockchain relies on encryption to validate transactions by verifying the identities of parties involved in a transaction. This ensures that a "false" transaction cannot be added to the blockchain without the consent of the parties involved. A complex mathematical calculation known as a "hash" is performed each time a transaction is added to the blockchain, which depends on the transaction data, the identities of the parties involved in the transaction, and the result of previous transactions. The fact

that the current state of the blockchain depends on previous transactions ensures that a malicious actor cannot alter past transactions. This is because if previous transaction data is changed, it will impact the current value of the hash and not match other copies of the ledger.

Transparency: By its very nature, blockchain is a distributed database that is maintained and synchronized among multiple nodes – for example, by multiple counterparties who transact with each other frequently. In addition, transaction data must be consistent between parties in order to be added to the blockchain in the first place. This means that by design, multiple parties can access the same data (in some cases locally within their organizations) – thus significantly increasing the level of transparency relative to conventional systems that might depend on multiple "siloed" databases behind firewalls that are not visible outside a single organization.

Efficiency: Conceptually, maintaining multiple copies of a database with blockchain would not appear to be more efficient than a single, centralized database. However, in most real-world examples (including several of the case studies we examined in capital markets), multiple parties already maintain duplicate databases containing information about the same transactions. In many cases, the data pertaining to the same transaction is in conflict – resulting in the need for costly, time-consuming reconciliation procedures between organizations. Employing a distributed database system such as blockchain across organizations can substantially reduce the need for manual reconciliation, thus driving considerable savings. In addition, in some cases blockchain offers the potential for organizations to develop common or "mutual" capabilities that eliminate the need for duplication of the same effort across multiple organizations.

HIPAA Regulations and Compliance Guidelines

Before the discussion concerning its implementations, it is imperative to discuss issues regarding Health Insurance Portability and Accountability Act of 1996 (HIPAA). There are a couple of primary concern rules that include cloud computing guidelines, privacy, and security rule. The main aim of this paper is not to conduct a HIPAA law full investigation. Upon the moment of relevant application, issues that are pertinent to implementation discussion will be discussed explicitly.

Privacy Rule

According to the Medico EMR business model, it is imperative for the Privacy Rule requirement to be observed. This is due to the private health information transmission and storage. The privacy rule, in this case, refers to the health plans, health care clearinghouses among other healthcare organizations that transit their work using the electronic form. Another party that is affected by HIPAA compliance is the service providers that act on their behalf. When it comes to the second hand agents also known as the Business Associates (BA), adhering to Business Associate Contract (BAC) is crucial. For many years, HIPAA has placed a strict requirement to the above agreements.

From an initial investigation, there are points of merit that include the requirements of them that are authorized to use, the use of the de-identified information and the definition of the private information is defined. De-Identified health information has been defined as the health information that provides an identification of a person where no reasonable basis that ensures that the information can be used in individual identification. When it comes to De-identified data restrictions that use restrictions, below is the summary of the restrictions. For example, there are no restrictions when it comes to the use or disclosure of the de-identified health information. In this case, this information does not provide an individual identification or even provide a reasonable basis to identify an individual. A boundary that separates identifiable and de-identifiable data acts as a source of information that restricts individuals. This boundary is associated with 0.04% of the US population.

HEALTHCARE INFRASTRUCTURE CONUNDRUM

Nowadays, prescribers can use a system known as e-prescribing to transmit prescriptions electronically. According to IOM Report titled Future Directions for the National Healthcare Quality and Disparities Reports, the quality of care delivered can be improved and medication cost reduced if prescribers start adopting health IT as a tool. Medical errors that occur during prescription, description, administration and patient's care monitoring stages can be reduced through e-prescribing adoption.

According to various studies, medication errors can also be reduced through the elimination of the handwriting interpretation. Through this elimination, the communication time between office staff and pharmacies is also reduced. The move can also avoid the high costs of adverse drug events. In a year, adverse drug events come to approximately 380,000 and 450,000 in the US. This results in a cost of $3.5 billion in a year.

Among many aspects of e-prescribing, the clinical decision has a large number of computerized tools that are directed towards improving patient's care. The clinical decision support has computerized reminders, offers advice related to drug selection, dosage, allergies and interactions among many others. Once a prescription has been placed in the system, it follows the patient that ends up in handoff errors avoidance.

Open Source to Start the Movement

In the medical world, open source is comparable to a peer review. Through the software code, users are in a position to test, poke at, test drive and criticize the software since its public. Unlike other EMR's, users in this software can improve, customize it and learn to code. Through this source, physicians can also learn what many have considered as a black box that only magicians can open. Through open source, we (patients' and physicians) get enlightened about tools we use. I was in a position to train myself coding without attending a class through GitHub.

Lastly, open source is affordable with no license fee or entrance fee. In this case, anyone can join it. Through this community, issues of common interest between patients and physicians can be discussed. For them that think of starting an open source from scratch is a major issue, I got you covered. Despite many developed EHRs, this section focuses on Medic EMR. This EHR largely addresses the issue of privacy where patients can control their health information.

Medic EMR

Medic EMR is a branch of OpenEMR. We forked OpenEMR and provide support and integrate it with Medic Coin to create a Medic Coin ecosystem. Medic EMR, like OpenEMR, will be Meaningful Use 2 certified. Users will be able to hope from Medic EMR and OpenEMR flawlessly. Here are some rich features of the OpenEMR software that Medi EMR will benefit.

A feature-rich solution

Our vibrant community of volunteers and contributors have maintained critical OpenEMR features for over a decade. With over 30 supported languages, many customizations, and full data ownership.. On top of this, users in need of support can take advantage of our volunteer support network as well as over 30 vendors in over 10 countries.

Scheduling

Advanced scheduling allows clinics to create repeating events, automated-workflows triggered by check-in, and patient reminds.

e-Prescribing

Enter a prescription into an encounter and have it electronically sent to the patient's pharmacy.

Medical Billing

Export billing data in standardized, including X12.

CMS Reporting

Generate CMS Meaningful Use reports with just a few clicks

Lab Integration

Have lab orders automatically sent to a lab and integrate the results into a patient's chart automatically

Clinical Decision Rules

Navigate complex patient algorithms using the clinical decision rules engine to ensure the highest quality of care for patients.

Advanced Security

HIPAA-friendly, fine-grained access control objects, and industry-standard password hashing helps to protect your practice from intrusion

Multilingual Support

Available in over 30 languages, and customizable to add more.

Medic EMR is an open source EMR with blockchain features. With the integration of Medic Coin payment system, patients can pay doctors for their visits. Doctors can reward patients with Medic Coin for keeping their blood pressure and diabetes under control. Pharmaceutical companies can pay doctors in Medic Coin for data mining.

Medic Phone Telemedicine App

According to Grandview Research Inc,. the global telemedicine market is expected to reach USD 113.1 billion by 2025. Key drivers of the market include increasing incidences of chronic conditions and rising demand for self-care. Furthermore, enhancing application of internet, virtual medicine and rising demand for centralization of healthcare are expected to save on cost incurred, which is one of the critical success factors attributing for the growth of telemedicine market.

Virtual medicine is benefits by reducing the emergency room visits and hospitalization rate, thereby augmenting the market growth. The telemedicine market is segmented on the basis of products, and region. The service offers prime channel for various providers to communicate on the same platform and thus, centralize all the available data.

Medic Phone is integrated with Medic EMR to give patients a complete set of medical records. Medic Phone is part of the Medic Coin ecosystem. Through Medic Phone, doctors can accept Medic coin for online visits.

CONCLUSION

Medic Coin is paramount to the success of the world because it is unique and it is a force with potential to do good things and make life better. Owners of Medic Coin enjoy the profits of masternode at the same time knowing that they are contributing to a better society.