ALTRY

AlpTurkCoin

Bitcoin has proven that a peer-to-peer electronic cash system can indeed process payment transactions without requiring trust or a central mint. However, for an entire electronic economy to be based on a fully decentralized, peer-to-peer solution, it must be able to: process transactions securely, quickly and efficiently, at thousands or more per hour, provide incentives for people to participate in securing the network scales globally with minimal resource footprint Provides an agile architecture that facilitates the addition of new core features and allows the creation and deployment of advanced applications, and can run on a wide variety of devices, including mobile devices. AlpTürkCoin meets all these requirements.

Introduction and Overview

AlpTurkCoin is a 100% proven crypto asset currency built from the ground up with open source Java. AlpTürkCoin's unique Proof-of-Stake algorithm does not depend on any implementation of the coin age concept used by other proof-of-stake cryptoassets and is resistant to so-called risky attacks. A total of 1 billion usable tokens have been distributed on the Genesis block. Curve25519 cryptography is used in conjunction with the more widely used SHA256 hash algorithms to provide a balance of security and required processing power. unlocked on network nodes On average, a block is created by accounts every 60 seconds. Since the entire token supply is already available, AlpTurkCoin is redistributed with the addition of transaction fees charged to an account when it successfully creates a block. This process is known as forging and is similar to the mining concept used by other cryptoassets. Transactions are considered secure after 10 block confirmations and AlpTurkCoin's current architecture and block size limit allows 367,200 transactions to be processed per day. AlpTürkCoin transactions are based on a set of basic transaction types that do not require any scripting or transaction input/output operations on the network nodes part . These transaction primitives allow basic support for:

asset exchange

nickname registration

encrypted messages

digital product store

entity system

voting system

step-by-step processes

account control

to mix up

account features

cloud data

Leveraging these primitive types of transactions, AlpTurkCoin core can be viewed as an agile, basic layer protocol on which unlimited units of services, applications and other assets can be built. This version of the white paper documents the features and algorithms implemented in AlpTürkCoin as of version 1.7.5. Future revisions will be made to reflect planned additional features and algorithm changes.

Core technologies

Proof of Collateral

In the traditional Proof of Work model used by most cryptoassets, network security is provided by peers doing business. They use their resources (computation/transaction time) to reconcile double-spend transactions and impose an extraordinary cost on those trying to reverse transactions. Tokens are awarded to peers in exchange for work, with a frequency and amount varying according to the operational asset meters of each crypto asset unit. This process is known as mining. The blocking frequency, which determines the current mining reward of each crypto-asset unit, is generally intended to remain constant. Consequently, the difficulty of the work required to earn a reward should increase as the network's working capacity increases.The stronger a Proof-of-Work network becomes, the less incentive there is for an individual spouse to support the network because its potential rewards are shared among more spouses. In their pursuit of profitability, miners continue to add resources in the form of proprietary hardware that requires significant capital investment and consistently high energy demands. As time progresses, the network becomes increasingly centralized as smaller peers (those who can do less) leave their resources or pool their resources. In the Proof of Stake model used by AlpTürkCoin, network security is a shareholder in the network.   managed by spouses. The incentives provided by this algorithm do not support centralization as the Proof of Work algorithms do, and the data shows that the AlpTurkCoin network has remained fairly decentralized since its inception: a large number of unique accounts contribute blocks to the network, and the top five accounts accounted for 42% of the total number of blocks.

AlpTürkCoin's Proof-of-Stake Model

AlpTurkCoin uses a system where each coin in an account can be thought of as a small mining rig. The more tokens held in the account, the greater the chance that account will earn the right to create blocks. The total reward received as a result of block creation is the sum of the transaction fees included in the block. AlpTürkCoin does not create any new tokens as a result of block creation. The redistribution of AlpTürkCoin occurs as a result of block producers charging transaction fees, so the term forging (in this context means creating a relationship or new conditions is used instead of mining).Subsequent blocks are created based on verifiable, unique and almost unpredictable information from the previous block. The blocks are linked by these links, creating a chain of blocks (and transactions) that can be traced back to the genesis block. Block creation time is targeted at 60 seconds. Blockchain's security is always a concern in Proof of Stake systems. The following basic principles apply to the AlpTürkCoin Proof of Stake algorithm:

A   cumulative difficulty value is stored as an assetmeter in each block, and each subsequent block derives its new difficulty from the previous block value. In case of uncertainty, the network reaches consensus by choosing the block or chain segment with the highest cumulative difficulty. This is discussed in more detail in section 3.4.1.

To prevent account holders from moving their stakes from one account to another as a way to manipulate their blocking probabilities, tokens must be stable within a 1,440-block account before contributing to the blocking process. Tokens that meet this criterion contribute to an account's   active balance , and this balance is used to determine miner probability.

To prevent an attacker from creating a new chain from the origin block to the end, peers allow chain reorganization of no more than 720 blocks behind the current block height. Any block submitted at a height lower than this threshold will be rejected.

Transactions are considered secure once they are encoded into a block 10 blocks behind the current block height, as the probability of any account taking control of the blockchain by creating its own blockchain is extremely low.

Contrast with Peercoin Proof of Stake

Peercoin uses a coin age asset meter as part of its mining probability algorithm . In this system, the longer your Peercoins stay stable in your account (up to 90 days maximum), the more power (asset age) is required to mint a block. The act of minting a block requires coin age value consumption, and the network determines the consensus by choosing the chain with the largest total consumed coin age. When Peercoin blocks become unclaimed, the consumed coin age is sent back to the originating account. As a result, the cost of attacking the Peercoin network is low, because attackers block until successful (grinding stake). they can continue to produce. Peercoin minimizes these and other risks by centrally issuing blockchain checkpoints several times a day to freeze the blockchain and lock down transactions. AlpTürkCoin does not use the coin age as part of its forging algorithm. An account's chances of mining a block depend solely on its active balance (which is a feature of each account), the time since the last block (shared by all miner accounts), and the underlying target value (which is shared by all). accounts).

tokens

The total AlpTurkCoin supply is 1 billion coins which can be divided into eight decimal places. All tokens were issued with the creation of the genesis block (the first block in the AlpTürkCoin blockchain) , leaving the genesis account with an initial negative balance of 1 billion AlpTürkCoin. The presence of anti-markers in the Genesis account has a few interesting side effects

The origination account cannot perform any transactions as its balance is negative and cannot pay the transaction fees. As a result, the genesis account's private password is free for anyone to use.

Any tokens sent to the Genesis account are effectively destroyed as the negative balance of the accounts will cancel them. In this way, several thousand AlpTurkCoin tokens were burned . The choice of word tokens is intentional as AlpTurkCoin is intended to be used as a base protocol that provides numerous other functions. The most basic function of AlpTürkCoin is a traditional asset system, but it is designed to do much more.

Network Nodes

A node in the AlpTürkCoin network is any device that provides transaction or block data to the network. Any device running the AlpTürkCoin software is considered a node. Nodes are sometimes called "Peers". Nodes can be divided into two types: special marked and regular. A privately marked node is a node tagged with an encrypted token derived from an account's private key, which can be decrypted to reveal a specific AlpTurkCoin account address and the balance associated with a node. The act of placing a distinctive feature on a node adds a level of accountability and trust, so nodes marked as private are more reliable than non-distinctive nodes in the network. The larger the balance of an account linked to a distinctive node, the more trust is given to that node. An attacker might want to stamp a node in order to gain credibility within the network and then use that trust for malicious purposes.Every node in the AlpTürkCoin network has the ability to process and broadcast both transactions and blocking information. Blocks are validated when received from other nodes, and in cases where block validation fails, nodes can be temporarily blacklisted to prevent invalid block data from spreading. Each node has a built-in DDOS (Distributed Denial of Service) defense mechanism that limits the number of network requests from any other node to 30 per second.

blocks

As with other cryptoassets, the ledger of AlpTurkCoin transactions is created and stored in a linked array of blocks known as the blockchain. This ledger provides a permanent record of the transactions that took place and also determines the order in which the transactions took place. A copy of the blockchain is stored at every node in the AlpTürkCoin network, and every unlocked account on a node (by providing the account private key) has the ability to create a block as long as there is at least one incoming transaction to the account. It has been confirmed 1440 times. Any account that meets these criteria is called an active account .At AlpTürkCoin, each block contains up to 255 transactions and all of them are preceded by a block header with descriptive asset meters. Each transaction in a block is represented by common transaction data, certain types of transactions also include transaction attachments, and certain transactions may contain one or more additional attachments. The maximum block size is 42 KB. All blocks contain the following assetmeters:

A block version, block height value, and block identifier

A block timestamp expressed in seconds since the starting block

The ID of the account that created the block and their public key

ID and hash of the previous block Number of transactions stored in the block

Total amount of AlpTurkCoin represented by transactions and fees in the block

Transaction data for all transactions included in the block, including transaction IDs

The hash of the block's payload length and the block's payload

Production signature of the block

One signature for the entire block

Base target value and cumulative difficulty for the block

Block Creation (Tattoo)

Three values are key in determining which account is eligible to create a block, which account has earned the right to create a block, and which block is taken as the authorized block in conflict situations: base target value , target value, and cumulative difficulty .

Core Target Value

To earn the right to create (create) a block, all active AlpTurkCoin accounts compete by attempting to generate a hash value lower than a certain base target value . This base target value varies from block to block and is derived from the previous block base target multiplied by the time needed to generate this block using a formula that provides an average block time of 60 seconds. The calculation is based on the following constants:

MAXRATIO = 67 – maximum rate at which the target is reduced when the block duration is greater than 60 seconds.

MINRATIO = 53 – the minimum rate at which the target is boosted when the block duration is less than 60 seconds.

GAMA = 0.64 and the following variables:

S – average block time for the last 3 blocks

TP – previous base target

Tb – calculated base target The base target is calculated as:

If $S > 60$ $\quad Tb = (Tp * \mathrm{Min}(S, MAXRATIO)) / 60$

Else $\quad Tb = Tp – Tp * GAMMA * (60 – \mathrm{Max}(S, MINRATIO)) / 60$

The logic behind this formula is explained here https://nxtforum.org/proof-of-stake-algorithm/basetarget-adjustment-algorithm and here https://nxtforum.org/nxt-improvement-proposals/fixing-the-blocktimes The goal is to incrementally adjust the target adjustments using the MIN and MAX ratio constants and increase the target so that using the GAMMA constant as the block time is limited from below to 0, the block times are reduced at a faster rate than lowering the target, but can be infinitely large.

target value

Each account calculates its own target value based on its current active stake. This value is: where: T is the new target value T b is the base target value S is the time elapsed since the last block in seconds B e is the effective balance of the account As can be seen from the formula, the target value grows with each second elapsed since the timestamp of the previous block. The maximum target value is 1.53722867 x 10 17 and the minimum target value is half of the previous block base target value. This target value and the base target value are the same for all accounts trying to get over a particular block. The only account-specific asset meter is the active balance asset meter.

Cumulative Difficulty

The cumulative difficulty value is derived from the base target value using the formula: where: D cb is the difficulty of the current block D pb is the difficulty of the previous block T b is the base target value for the current block

Tattoo Algorithm

Each block in the chain has a creation signature entitymeter. To participate in the block forging process, an active account digitally signs the production signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256. The first 8 bytes of the resulting hash are converted into a number called the account hit .The hit is compared to the current target value. If the calculated hit is lower than the target, the next block can be created. As stated in the target value formula, the target value increases with each passing second. Even if there are only a few active accounts in the network, one of them will eventually create a block because the target value will be too large. Therefore, you can calculate the time it takes for any account to generate a block by comparing the account hit value with the target value. The last point is important. Since any node can query the active balance for any active account, it is possible to iterate over all active accounts to determine individual hit values. This means that it is possible to predict with reasonable accuracy which account will win the next block forgery. A Since the balance shifting attack AlpTürkCoin share must be stable for 1440 blocks before contributing to the forging (via the effective balance value), it cannot be mounted by moving the stake to an account that will generate the next block. Interestingly, the new base target value for the next block cannot be reasonably predicted, so the almost deterministic process of determining who will generate the next block becomes increasingly stochastic as attempts are made to predict future blocks. This feature of the AlpTürkCoin tattoo algorithm helps lay the foundation for the development and implementation of the Transparent Tattoo algorithm. Since this algorithm has not been fully implemented yet and its effects on the AlpTürkCoin network are significant, it will be summarized in a separate article.For an in-depth analysis of the math and probabilities related to AlpTürkCoin block forging, refer to the mthcls document, AlpTürkCoin forging math, available at http://www.docdroid.net/e29h/forging0-5-2.pdf. .html When an active account wins the right to create a block, it combines up to 255 existing, unconfirmed transactions into a new block and populates the block with all required assetmeters. This block is then broadcast to the network as a candidate for the blockchain.The payload value, the generating account, and all signatures in each block can be verified by all network nodes receiving it. In a situation where multiple blocks are produced, nodes will select the block with the highest cumulative difficulty value as the authorized block. As block data is shared among peers, forks (unauthorized chain segments) are detected and disassembled by examining the cumulative difficulty values of chains stored in each fork.A node that receives a valid block representing a chain with a cumulative difficulty greater than its own chain will identify the highest common block between its chain and the chain represented by the new block, and then remove its own blocks from the chain to the common block. and undo any side effects of those blocks and then it builds its own chain based on the blocks received from other nodes.

balance rental

Because an account's ability to be a miner is based on the active balance asset meter, it is possible to forge power credits from one account to another without giving up control of the account-associated tokens. Using a lease Balance transaction, an account holder can temporarily reduce one account's effective balance to zero and add it to another account's effective balance. The targeted account forging power is increased for a certain number of blocks specified by the original account holder, after which the effective balance is returned to the original account.Leasing is recommended for large shareholders because the lessor account that leases its own miner power does not need to disclose its password to participate in generating new blocks. Only the tenant account needs to reveal its password and this account can generate a much smaller balance so the loss is minimal if their password is stolen. The finance lease balance does not affect the functionality of the lessor account, other than its ability to transact. Balance changes in the lessor account affect the miner power of the tenant account after block 1440.

Accounts

AlpTürkCoin implements a brain wallet as part of its design : all accounts are stored on the network with private keys for every possible account address directly derived from each account password using a combination of SHA256 and Curve25519 transactions . Each account is represented by a 64-bit number, which is an account address using a Reed-Solomon error correction notation that allows up to four errors to be detected in an account address , or to correct up to two errors.

is expressed as. . This eliminates the risk that a typo in the account address will result in loss of assets. Account addresses are always prefixed with an AlpTürkCoin prefix, which allows AlpTürkCoin account addresses to be easily recognized and differentiated from the address formats used by other blockchains. The Reed-Solomon coded account address associated with a secret password is generated as follows:

The secret password is mixed with SHA256 to derive the private key of the accounts .

The private key is encrypted with Curve25519 to derive the public key of the accounts .

The public key is hashed with SHA256 to derive the account ID .

The first 64 bits of the account ID are the visible account number .

Reed-Solomon encoding of the visible account number starting with ALPK- creates the account address .

The first time an account is accessed with a secret password, it is not secured with a public key. When the first outgoing transaction is made from an account, the 256-bit public key derived from the password is stored in the blockchain, which secures the account. The address space (2 256) for public keys is larger than the address space for account numbers (2 64), so there is no one-to-one mapping of passwords to account numbers, and conflicts are not possible. These collisions are detected and avoided as follows: When a specific password is used to access an account and it is secured with a 256-bit public key, no other public-private key pairs are allowed to access that account number.

Account Balance Features

There are several different balance types available for each AlpTurkCoin account. Each type serves a different purpose, and many of these values are checked as part of transaction validation and processing.

Effective balance , an account used primarily in forging accounts of an account. An account's active balance consists of all tokens fixed in that account for block 1440. Additionally, the Account Rental feature allows the active balance of one account to be temporarily assigned to another account. Account effective balance is calculated from the confirmed balance by reducing all balance additions in the last 1440 blocks .

The guaranteed balance of an account consists of all coins fixed in an account of 1440 blocks. Unlike the active balance, this balance cannot be transferred to another account.

Confirmed balance accounts for all transactions that had at least one confirmation of an account.

The unverified balance of an account is the one displayed to AlpTurkCoin customers. Represents the approved balance of an account, excluding tokens that are unconfirmed, included in sent transactions, or locked by certain types of transactions, such as CurrencyReserveIncrease and Shuffling transactions, or locked by progressive transactions that have not yet been executed or canceled.

The total amount of AlpTurkCoin that has been earned as a result of forged balance Calculator programs successfully forged blocks.

Approved and unconfirmed asset quantities and asset units are also tracked by each account presence.

Transactions

Transactions are the only way to change the status or balance of AlpTürkCoin accounts. Each transaction performs only one function and its record is permanently stored in the network after that transaction is included in a block.

Transaction fees

Transaction fees are the primary mechanism by which AlpTurkCoin is returned to the network. Each transaction requires a minimum fee. When an AlpTürkCoin account creates a block, all transaction fees included in this block are given to the miner account as a reward. Unlike other blockchains, minimum transaction fees are imposed by the blockchain, so transactions that do not specify a fee higher than the minimum fee for this type of transaction will not be accepted by nodes.

Transaction Confirmations

All AlpTurkCoin transactions are considered unconfirmed until they are included in a valid network block . Newly created blocks are distributed to the network by the node (and associated account) that created them, and a transaction included in a block is considered to have received a confirmation. As subsequent blocks are added to the existing blockchain, each additional block adds one more confirmation to the number of confirmations for a transaction. If a transaction is not included in a block before the deadline, it expires and is removed from the transaction pool.

Transaction Deadlines

Each transaction includes a deadline presencemeter set to a few minutes from the time the transaction is submitted to the network. The default deadline is 1440 minutes (24 hours). A transaction that has been broadcast to the network but has not yet been included in a block is called an unconfirmed transaction . If a transaction is not included in a block before the transaction deadline expires, the transaction is removed from the network. Transactions can be left unconfirmed until their deadline expires because they are permanently invalid or malformed, or because they do not meet certain temporary conditions, such as sufficient balance, or because blocks are filled with transactions that offer to pay higher transaction fees.

Transaction Types

Categorizing AlpTürkCoin transactions by types and subtypes allows for modular growth and development of the AlpTürkCoin protocol without creating dependencies on other core functions. As features are added to AlpTürkCoin core, new transaction types and sub-types can be added to support them. Multiple transaction types and associated subtypes are supported by AlpTürkCoin. Each type specifies a specific transaction and optional assetmeters, as well as the processing method. A complete list of all transaction types and subtypes is beyond the scope of this document.

Transaction Creation and Processing

The details of creating and processing an AlpTurkCoin transaction are as follows:

The sender specifies the assetmeters for the transaction. Transaction types vary and the desired type is specified when creating a transaction, but several entitymeters must be specified for all transactions:

private key for the sending account

the specified fee for the transaction

deadline for processing

optional referenced action

All values of transaction entries are checked. For example, mandatory assetmeters must be specified. Fees cannot be below the minimum fee for this type of transaction. The deadline for a transaction cannot be less than one minute in the future. If a referenced transaction is specified, then the current transaction cannot be processed until the referenced transaction is processed.

If no exception is thrown as a result of the entitymeter check:

The public key of the generating account is calculated using the secret password provided.

Account information is obtained for the originating account and transaction asset meters are also verified:

The balance of the sending account cannot be zero

The unconfirmed balance of the sending account must not be less than the transaction amount plus the transaction fee

If the sending account has sufficient balance for the transaction:

A new transaction is created with a type and subtype value set to match the type of operation performed. All specified assetmeters are included. A unique transaction ID is generated by the creation of the object

The transaction is signed using the private key of the sending account

The encrypted transaction data is embedded in a message that instructs the network peers to process the transaction.

Transaction is broadcast to all peers in the network

The server responds with a result code:

process id if process creation was successful

An error code and error message if any of the asset meter checks fail.

Encryption Basics

The key exchange at AlpTürkCoin is based on the Curve25519 algorithm, which generates a shared secret key using the fast, efficient, high-security elliptic curve Diffie-Hellman function. The algorithm was first demonstrated by Daniel J. Bernstein in 2006. AlpTürkCoin Java-based applications were reviewed by DoctorEvil in March 2014. Message signing at AlpTürkCoin is performed using the Digital Signature Algorithm (EC-KCDSA) based on the Elliptic Curve Korean Certificate specified by the KCDSA Task Force team in 1998 as part of IEEE P1363a. Both algorithms were chosen because of the balance of speed and security for a key size of only 32 bytes.

Encryption algorithm

When Alice sends Bob an encrypted plaintext:

Calculates a shared secret:

shared_secret = Curve25519 (Alice_private_key, Bob_public_key) Calculates N seeds:

seed n = SHA256 (seed n-1), where seed 0 = SHA256 (shared_secret)

Calculates N keys:

key n = SHA256(Inv(core n)), where Inv(X) is the inversion of all bits of X

Encrypts plain text:

ciphertext [n] = plain text [n] XOR key n

Bob decrypts the ciphertext upon receipt:

Calculates a shared secret:

shared_secret = Curve25519 (Bob_private_key, Alice_public_key)

Calculates N seeds (this is the same as Alices step):

seed n = SHA256 (seed n-1), where seed 0 = SHA256 (shared_secret)

Calculates N keys (this is the same as Alices step):

key n = SHA256(Inv(core n)), where Inv(X) is the inversion of all bits of X

Decrypts the ciphertext:

plaintext [n] = ciphertext [n] XOR key n

Note : If someone guesses some of the plaintext, it might decode some of the subsequent messages between Alice and Bob if they use the same key pairs. As a result, it is recommended to generate a new private/public key pair for each communication.

Core features

Advanced JavaScript client

A second generation, user-friendly client application, AlpTürkCoin is built into the core software distribution and can be accessed via a native web browser. The client provides full support for all core AlpTürkCoin features and is implemented in such a way that users' private keys are never exposed to the network. It also includes an advanced management interface and built-in javadoc documentation for AlpTurkCoin low-level Applications Programming Interface.

agile architecture

First-generation cryptoasset units were designed primarily as payment systems. AlpTurkCoin acknowledges that decentralized blockchains can enable a wide range of applications and services, but it is not prescriptive about what these services should be or how they should be built. By design, AlpTurkCoin removes unnecessary complexity at its core, leaving only the most successful components of its predecessors intact. As a result, AlpTurkCoin functions like a low-level, basic protocol: it defines the interfaces and transactions required to run a lightweight blockchain, a decentralized communication system, and a fast transaction processing framework, and allows higher-level components to build on these features. . .Transactions on AlpTürkCoin make simple adjustments to account balances instead of tracking sets of input or output credits. Additionally, the base software does not support any scripting language. AlpTurkCoin provides a set of basic, flexible transaction types that can be processed quickly and easily, creating a foundation that does not limit the ways in which these transaction types can be used and does not create a significant overhead for using them. This flexibility is further strengthened by AlpTürkCoin's low resource and energy requirements and highly readable, highly organized object-oriented source code.

Basic Payments

The most basic feature of any crypto asset unit is the ability to transfer tokens from one account to another. This is AlpTurkCoin's most basic transaction type and allows basic payment functionality.

Nickname System

AlpTürkCoin Alias System allows any text string to be permanently associated with a specific AlpTürkCoin account. Since its inception, a convention has been formalized for the format of these strings using JSON notation. As a result, an alias can currently be a human-friendly text alias for an account address or a Uniform Resource Identifier (URI). The ability to store any URI on the AlpTürkCoin blockchain enables the creation of any number of decentralized services based on small, persistent strings of text, such as a distributed Domain Name Server (DNS) system.

Arbitrary Messages

Random data strings up to 1000 bytes can be stored on the AlpTürkCoin blockchain using the Arbitrary Messages feature, and these strings can optionally be AES encrypted. These messages are intended to be removable when the size of the blockchain needs to be reduced in the future, however, they form a critical building block for a number of next-gen features.At a basic level, the system can be used to transmit human-readable messages between accounts, creating a decentralized chat system. However, advanced applications can use this feature to store structured data such as JSON objects, which can be used to trigger or facilitate services built on AlpTurkCoin. The most notable current application is AlpTürkCoin Multigateway (MGW), which is part of the AlpTürkCoin services layer, which uses the Arbitrary Messaging system to run an almost unreliable method of automatically converting Bitcoin, Litecoin and other crypto assets into AlpTürkCoin assets. on the concept of colored metallic assets that can be traded, bought and sold on a fully decentralized asset exchange).

Asset Exchange

A whole class of AlpTürkCoin transactions is used to implement a fully decentralized and automated asset exchange running on the AlpTürkCoin blockchain. Using the concept of colored coin assets, AlpTürkCoin assets can be issued and tracked in the AlpTürkCoin ecosystem, powered by transactions and transactions that allow asset transfer, bidding and order matching, and automatic order matching.

Since its inception, AlpTürkCoin Asset Exchange has been used for fundraising and development of advanced services such as IPO offerings, tip tokens and the Multigateway (MGW) system.Value added services can be created by combining the features of AlpTürkCoin Asset Exchange with other features such as Arbitrary Messaging System. Most importantly, another feature of the AlpTürkCoin Services layer is a system for automatic calculation and distribution of dividends based on the performance of existing AlpTürkCoin assets.

Digital Goods Store

AlpTürkCoin Digital Products store provides account holders the ability to list assets for sale in an open, decentralized marketplace. Goods can be purchased, downloaded, delivered, returned and transferred using a special class of transaction types that manage and secure store listings on the decentralized blockchain.

Device Portability

Due to its cross-platform, Java-based roots, Proof of Stake hashing, and ability to reduce the size of the future blockchain, AlpTurkCoin is highly suitable for use on small, low-power, low-resource devices. Android and iPhone applications are currently under development and AlpTürkCoin software has been ported to low-power ARM devices such as RaspberryPi and CubieTruck platforms. The ability to implement AlpTürkCoin on low-power, always-connected devices such as smartphones allows us to envision a scenario where most of the AlpTürkCoin network is supported on mobile devices. The low cost and resource consumption of these devices significantly reduces network costs compared to traditional Proof of Work cryptoassets.

concerns

Proof of Stake Attacks

In a no-hazard attack, miners try to build blocks on every fork they see because doing so costs them almost nothing, and ignoring any fork can mean losing the block rewards that would have been earned had that fork been. chain with the greatest cumulative difficulty. While this attack is theoretically possible, it is currently impractical. The AlpTurkCoin network does not survive long blockchain forks and the low block reward does not provide a strong profit incentive, moreover, sacrificing network security and trust for such small gains will make any victory hot.As part of the AlpTürkCoin development roadmap, a feature called Economic Clustering will further protect against such attacks by forcing transactions to contain hashes of previous blocks and grouping nodes into clusters that can detect and impose unusual behavior on the network. penalties (in the form of temporary loss of mining ability).

Date Attack

In a historical attack, someone buys a large number of tokens, sells them, and then tries to create a successful fork just before the tokens are sold or traded. If the attack fails, the attempt costs nothing because the tokens have already been sold or traded. If the attack is successful, the attacker gets their tokens back. Extreme forms of this attack involve obtaining private keys from ski accounts and using them to create a successful chain directly from the genesis block.At AlpTurkCoin, the basic history attack usually fails because the entire stake must be stable for 1440 blocks before it is used for forging, moreover, the active balance of the account that created each block is verified as part of the block verification. The extreme form of this attack usually fails because the AlpTurkCoin blockchain cannot be rearranged beyond the current block height by more than 720 blocks. This limits the time frame in which a bad actor can launch such an attack.

Distribution

Because blocks can only be created based on the current stake, at least some of the token supply must be available when a Proof of Stake network boots. As a result, AlpTurkCoin issued and distributed its entire token supply with the creation of the genesis block. The initial supply of AlpTurkCoin was distributed to 73 original stakeholders, many of whom were encouraged to further distribute their shares through the use of giveaways, contests and rewards. Eight months after its creation, AlpTurkCoin's largest single account contains 5% of AlpTurkCoin's total supply. In contrast, Satoshi Nakamoto is thought to hold almost 9% of the total supply of Bitcoin more than five years after these networks existed.AlpTurkCoin supporters will never be able to dispel the distribution concerns raised by the wider community. According to the profit levels achieved by early investors in IBM, Apple, Google, Facebook and Bitcoin, the amount of inequality found in the AlpTurkCoin blockchain is not out of line. When asked: How do you resolve the issue with fraud charges against the unfair distribution of AlpTürkCoin to 73 major stakeholders?, BCNext (creator of AlpTürkCoin) replied: This issue cannot be resolved. Even if we had a million stakeholders, [the other] seven billion people would call it unfair. A world with [sic] being cannot be perfect.

Transaction fees

As AlpTürkCoin value increases, so does the cost of minimum transaction fees, expressed in fiat. Plans are underway to lower the minimum fee scaled by transaction byte size to make microtransactions practical. This will be implemented after changes are made to the AlpTürkCoin internal database and this development will be planned for the 1.3.0 version of the AlpTürkCoin software.

Technical Report Timing

Most crypto-asset founders publish a whitepaper before the asset unit is booted. AlpTürkCoin's first official whitepaper was created almost eight months after the genesis block was created for the 1.2.2 version of the AlpTürkCoin software. The core development team was always of the view that AlpTürkCoin source code is its whitepaper: Since Java is human readable and full source is available, anyone can understand AlpTürkCoin mechanics by studying the source. This whitepaper can be seen as a translation of the core components of the Java source code into English and was created to make the design and function of AlpTurkCoin more accessible to people without programming skills.

Bitcoin Issues Addressed by AlpTürkCoin

AlpTurkCoin was created as a crypto-asset 2.0 response to Bitcoin. AlpTurkCoin adopts features that have proven to work well in Bitcoin and addresses aspects of concern. This appendix addresses issues related to the Bitcoin protocol and network that are alleviated by AlpTürkCoin technology.

Blockchain Size

The Bitcoin blockchain is a complete ordered collection of generated data blocks containing an electronic ledger for all Bitcoin transactions that have taken place since its launch in January 2009. Four years later, in January 2013, the size of the Bitcoin blockchain was about 4 gigabytes (GB). The amount of data required to store a two-hour movie on a DVD disc. Eighteen months later, in July 2014, the size of the Bitcoin blockchain had increased by almost five to 19 gigabytes (GB). The Bitcoin blockchain is showing exponential growth and to deal with it will require changes to the original Bitcoin protocol.

AlpTurkCoin Solutions

The block size of AlpTürkCoin is currently limited to 32 KB. Since its inception, almost 181,000 blocks have been produced and the blockchain takes up 390MB of space. In the future, AlpTurkCoin will implement a Blockchain Pruning feature (still under discussion) that will reduce the blockchain size by selectively removing information in persistent blocks and deleting other non-persistent data such as Arbitrary Messages.

Daily Transactions

In late 2013, the number of transactions processed on the Bitcoin network peaked at 70,000 per day, which equated to about 0.8 transactions per second (tps). The current Bitcoin standard block size of one megabyte, created every ten minutes (on average) by full node clients, limits the maximum capacity of the current Bitcoin network to about 7 tps. Compare that to the 10,000 tps processing capacity of the VISA network and you will see that Bitcoin cannot compete as it is today.Increasing public use of the Bitcoin system will cause Bitcoin to soon reach its daily transaction limit and stop further growth. To avoid this, Bitcoin software developers are working on the creation of thin clients that use simplified payment verification (SPV). To process more throughput in the same 10-minute average time, SPV thin clients do not perform a full security check on the larger blocks they process. Instead, they will examine multiple hash blockchains from competing miners and assume that the blockchain version created by the majority of miners is correct. In the words of Bitcoins Mike Hearn, Instead of verifying all the content, [SPV] simply trusts that most of the miners are honest…. As long as the majority is honest, [SPV] works … [However] , full node gives you better security. For example, if you run an online store, it makes sense to run a full node.

AlpTurkCoin Solutions

In its current state, the AlpTurkCoin network can process up to 367,200 transactions per day, more than nine times the current peaks of Bitcoin. The planned implementation of Transparent Tattoo will greatly increase this limit, allowing for near-instant processing.

Transaction Confirmation Time

Transaction confirmation times for Bitcoin ranged from 5 to 10 minutes for most of 2013. After the announcement in late 2013 that Chinese banks would not be allowed to process Bitcoins, the average Bitcoin transaction time rose significantly to 8 to 13 minutes, occasionally peaking at 19 minutes. Confirmation times have since reset to 8 to 10 minutes. However, since multiple verifications are required to complete a Bitcoin transaction (usually six confirmations are preferred), an hour can easily pass before the sale of Bitcoin-paid assets is complete.

AlpTurkCoin Solutions

It has been shown that the average block creation time for AlpTurkCoin has historically been around 80 seconds, putting the average transaction processing time to the same value. Transactions are considered secure after ten confirmations, meaning transactions are permanent in less than 14 minutes. Transparent Tattoo application will allow for almost instant procedures, further reducing this time.

Centralization Concerns

The increased difficulty and converged network hashrate for Bitcoin has created a high barrier to entry for newcomers and reduced returns on existing mining rigs. The block reward incentive used by Bitcoin has resulted in the creation of large, single-owner installations of private mining hardware, as well as a reliance on a small number of large mining pools. This has resulted in a centralization effect where large amounts of mining power are concentrated in the control of a decreasing number of people. Not only does this create the kind of power structure that Bitcoin was designed to circumvent, it also offers the real probability that a single mining operation or pool could collect 51% of the network's total mining power and launch a 51% attack. . There are also attacks that require as little as 25% of the total network hashing power.In early January 2014, GHash.io began voluntarily reducing its own mining power as it approached 51%. A few days later, the pool's mining power was reduced to 34% of the total network power, but the rate immediately started increasing again, reaching dangerous levels once again in June 2014.

AlpTurkCoin Solutions

Incentives provided by AlpTürkCoin Proof of Stake algorithm provide a low ROI of around 0.1%. Since no new coin is produced with every block, there is no additional mining reward that encourages efforts to consolidate block generation efforts. The data shows that the AlpTurkCoin network has remained fairly decentralized since its inception: a large (and increasing) number of unique accounts provide the network with blocks, and the top five accounts accounted for 35% of the total number of blocks.

Evidence of Work Resource Costs

Confirming transactions for existing Bitcoins and creating new Bitcoins to circulate requires enormous background computing power that must be constantly running. This computing power is provided by mining rigs operated by miners. Bitcoin miners compete among themselves to add the next block of transactions to the overall Bitcoin blockchain. This is done by aggregating all Bitcoin transactions that have occurred in the last ten minutes and trying to randomly encrypt them into a data block containing a certain number of consecutive zeros. Most test blocks created by a miner's hashing effort do not have this target number of zeros, so they make a small change and try again. One billion attempts to find this winning block are called gigahash.GH /sec. The first miner to produce the next pile of needle-in-a-chip, cryptographically correct Bitcoin block currently receives 25 newly minted Bitcoin rewards – approximately $15,750 at the time of this writing. This rivalry between miners repeats itself over and over every ten minutes, with its hefty prize. In early 2014, more than 3,500 bitcoins were produced daily, worth about US$2.2 million.With so many assets at stake, miners supported the fierce arms race in mining rig technology to increase their chances of winning. Initially, Bitcoins were mined using the central processing unit (CPU) of a typical desktop computer. Then, dedicated graphics processing unit (GPU) chips in high-end video cards were used to increase speeds. Field programmable gate array (FPGA) chips were then introduced, followed by application-specific integrated circuits (ASIC) chips dedicated to mining hardware. ASIC technology is best for Bitcoin miners, but the arms race continues as various generations of ASIC chips enter service. Current generation ASIC chips are 28nm units based on the size of their microscopic transistors in nanometers.The infrastructure of mining rigs currently available to support ongoing Bitcoin transactions is staggering. Bitcoin ASICs are like autistic experts. They can only do Bitcoin block calculation and nothing more, but they can do this single calculation at supercomputer speeds. In November 2013, Forbes magazine reported Global Bitcoin Computing Power Now 256X Faster than the Top 500 Supercomputers, Combined! He published an article entitled Statistics held on blockchain.info in mid-January 2014 showed that continued support of Bitcoin transactions requires a sustained hash rate of around 18 million GH/s. Over the course of a day, so much hash power generated 1.5 trillion test blocks created and rejected by Bitcoin miners looking for one of the magic 144 blocks to net $2.2 million.The power and cost involved in this wasteful background mining support of Bitcoin is huge. If all Bitcoin mining rigs had Monarch tiers as described above, they would represent a pool of 30,000 machines costing over US$63 million and consuming over 10 megawatts of sustained power when running on electricity. Invoices over US$3.5 million per day. The actual numbers are significantly higher for the current, less efficient pool of mining rigs that actually support Bitcoin today, and these numbers are currently moving up an exponential growth curve as Bitcoin is moving from one current transaction per second to the current maximum of seven transactions per second.

AlpTurkCoin Solutions

Analysis of the cost and energy efficiency of the AlpTurkCoin network shows that the entire AlpTurkCoin ecosystem can be maintained for around $60,000 per year, which is currently almost 2,200 times cheaper than the cost of running the Bitcoin network.

Evidence of Business Resource Costs for Owners of Mineral Assets

In addition to the huge electricity costs, there is a hidden fee for just holding Bitcoin. For each block found, the entity that created the block receives a salary. At the time of writing, this salary is 25 BTC, creating a 10% inflation in the total Bitcoin supply this year alone. For every 1000USD worth of Bitcoin someone owns, that person is paying 100USD per Bitcoin this year to pay miners to keep the network safe.