mytime

Technical Paper 1.0

English version
31 October 2017

mytc.io

Contents

Glossary

Deposited cryptocurrency is a cryptocurrency in the state of transitional ownership when counterparty A no longer owns it, and counterparty B is entitled to receive it but has not received it yet.

Service is a business interacting with users through applications.

Application is a software product providing services to customers and containing functionality for automation of data exchange and accrual of deposited cryptocurrency.

Proof-of-Time is an algorithm based on DPoS, where the deposited cryptocurrency significantly increases the voting weight.

Time confirmation principle is a validation of spent time by depositing cryptocurrency.

The Chronos protocol is the operation rules for two blockchains (Time and Money) based on the time confirmation principle using the Proof-of-Time consensus algorithm.

Time blockchain is a public register of validated time.

Money blockchain is a public register of financial transactions.

mytime is an open decentralized blockchain platform used for time validation, based on the Chronos protocol, the Money protocol, smart contracts, and services.

MYTC is a cryptocurrency, means of payment within the **mytime** platform.

MYTC emission is a dynamic minting of MYTC following new blocks production, depending on the amount of time confirmed, distributed among users proportionate to the votes for nodes, using the Proof-of-Time algorithm.

1. Introduction

mytime is a decentralized platform with a new blockchain architecture, in terms of social and economic aspects. The following factors determine the novelty of architecture:

- The essential platform function is to assign a value to users' time.
- Deposited cryptocurrency is a modification of an escrow transaction.
- The time confirmation principle and the Proof-of-Time algorithm allow transferring ownership rights to the cryptocurrency to another platform participants.
- MYTC emission depends on the Chronos internal state at any moment of time.
- Reputation is derived from the transactional activity of platform participants.
- Metadata in transactions, giving value to the cryptocurrency according to the operation rules defined by applications.

mytime will support smart contracts on the protocol level. Smart contacts will secure the complex logic of service-user interaction. The simplest example of such an interaction is splitting the reward using the deposited cryptocurrency between a service and a user.

While developing **mytime**, we rely upon the best project principles and practices: Cardano, Plasma, EOS, NEM, as well as various Graphene modifications.

mytime developers follow the business first principle. Our primary goal is to reduce costs related to business processes, and the mass attraction of users through integration with large B2C businesses.

The short-term metric of the **mytime** project is the rapid growth in the number of connected services and users.

The medium-term metric of the project is to increase the number of transactions between services and users.

The long-term key metric of **mytime** development is reducing transaction costs within the network while increasing transaction volumes. Following this metric will ensure protocol stability in case of a slowdown or disruption in the cryptocurrency market.

1.1. Business Challenges

The number of services that require a human's attention to operate is constantly growing.

However, our time is limited and will never be enough for every activity which genuinely interest us.

Services and users interact without any effective and measurable tools to assess time.

We propose turning time into a liquid value by providing a platform to monetize it by validating its value. User time is validated by the instant transfer of MYTC ownership rights from the service to the user.

Services are further incentivized to validate user time by MYTC emissions. The amount of MYTCs received by services increases with growing user reward amounts, audience, ratings and frequency of reward.

User time is validated by the Chronos protocol based on the Proof-of-Time algorithm, protecting from abusers and bad actors.

mytime ensures mutually beneficial interaction of users and services

Examples of how **mytime** can be used:

- Loyalty programs in which the company pays a user for time spent on a service, thereby motivating him/her to return.
- Selling user time to a third party in exchange for cryptocurrency.

- Compensation for time spent watching videos or playing computer games.
- A learning incentive system to propel users through online courses.
- Effective accounting for work hours.
- Per-minute royalties.

mytime represents value due to low transaction costs and the expression of business processes through the true value of time. All economic processes can be estimated and verified using time characteristics for interactions between objects. This allows for the mutual conversion of any contribution, costs, participation interest or other ways of interaction.

The protocol makes it possible to estimate each participant's contribution into related processes of creating added value in a global economic model.

1.2. Technological Challenges

The **mytime** platform operation involves a large audience and a huge number of transactions that contain arbitrary metadata. This creates the following challenges for the **mytime** team and community:

1. How to ensure the economic stability of the **mytime** system and motivate all its participants?
2. How to ensure the storage and integrity of information regarding time value and related metadata for dozens, hundreds of million users?
3. How to properly resolve the contradictions between services competing for the same time spent by a user?
4. How to prevent user data from being copied by a potential application (or a node), or a bad actor in the course of processing?
5. How to build an effective reputation system for users and applications?
6. How to secure the network consensus while installing critical updates to the **mytime** protocol?
7. How to protect the platform from potential attacks?

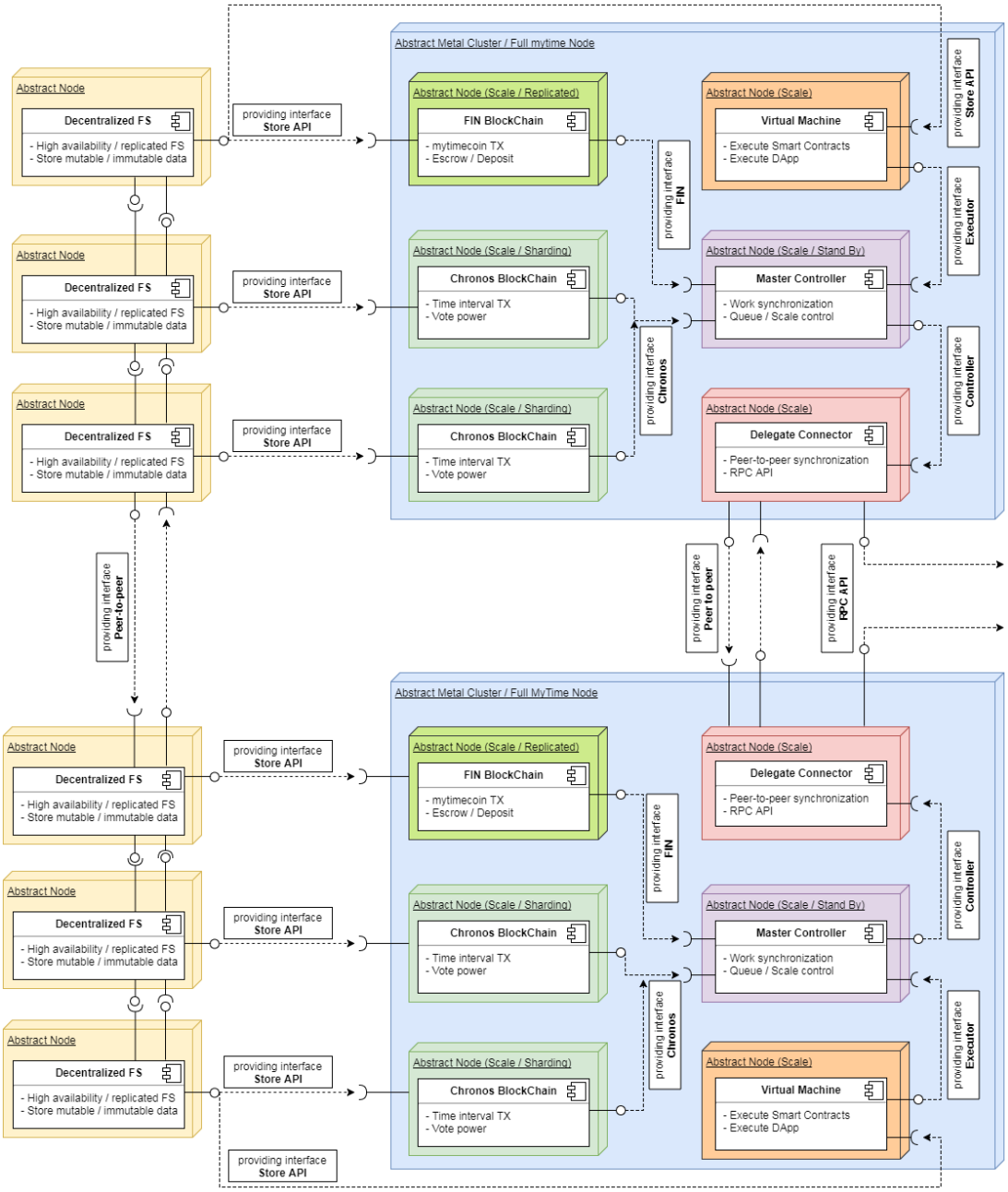
In this document, we describe the strategy for solving these technological challenges.

2. mytime Architecture

The **mytime** platform architecture consists of the following components:

1. Full mytime Node.
    - **A.** Connector.
        - **I.** Peer 2 Peer Public Interface.
        - **II.** RPC Public/Private Interface.
    - **C.** Master Controller.
    - **D.** Money BlockChain Controller.
    - **E.** Time BlockChain Controller.
    - **F.** Virtual Machine / Smart-Contract Executor.
2. Light mytime Node.
    - **A.** Connector.
        - **I.** Peer 2 Peer Public Interface.
        - **II.** RPC Public/Private Interface.
    - **C.** Light BlockChain Controller.
3. Decentralized File System.
4. Applications.
5. Public API.
6. Zero Application.
    - **A.** Wallet.
    - **B.** BlockChain Explorer.
    - **C.** Marketplace.

See the component diagram below:



2.1. Full Node

Full network nodes (delegates) is a central component of the entire **mytime** platform. This component ensures uninterrupted operation of block packaging and voting processes and also supports the network consensus.

Full nodes process the entire volume of transactions of parallel blockchains within the **mytime** platform, ensuring data integrity and consistency.

2.1.1. Connector

An internal component of the full node, provides a peer-to-peer public interface for data exchange with other network nodes. In addition to data exchange, the component provides the ability to connect to a node using RPC technology. It can be scaled horizontally to increase throughput.

2.1.2. Master Controller

An internal component of the full node, manages other components, generates the task queue and monitors their status. It can scale up other node components to improve their throughput if the resources are insufficient. The main function is to link components together. The component monitors the execution of distributed applications and smart contracts, creating isolated virtual environments and virtual machines for execution. The component has a state that can be stored in the external memory of the node (Redis / Memcached). Resilience is ensured by creating StandBy component replicas. In case of emergency, it automatically switches to a live instance of the component.

2.1.3. Money BlockChain Controller

An internal component of the full node, supports the operation of the blockchain handling financial transactions. The component verifies and monitors the state of blocks containing financial information. It can use a decentralized file system for storage. It can use external memory for storing transactions not yet included in the block (for example, escrow transactions). The component can be replicated to increase block packaging performance and verify the state of the blockchain.

2.1.4. Time BlockChain Controller

An internal component of the full node, ensures the operation of the Time blockchain. The component verifies and monitors the state of blocks containing time intervals. In the event of a critical application disconnection, it may force termination of the time record session. The component can use a decentralized file system for storage. The component can be scaled by user identifiers to improve the packaging performance of the blocks and verify the state of the blockchain.

2.1.5. Virtual Machine / Smart-Contract Executor

An internal component of the full node, provides a virtual environment for executing an arbitrary code, for example, for executing the smart contract code. A full node can contain different types of virtual machines, including an isolated execution environment for containerized applications.

2.2. Light Client

Light clients serve as the basis for interaction with the client applications blockchain, for example, wallets or applications that record users' time in automatic mode. This component is designed specifically to run in an environment with limited resources. The light client does not control the entire state of the blockchain, only what is directly related to the platform participant, for example, financial transaction chains related to a particular wallet, or time intervals referring to a particular application. The component can use a decentralized file system to store its state. Light clients cannot participate directly in the production of new blocks, but they can perform validation of certain chains.

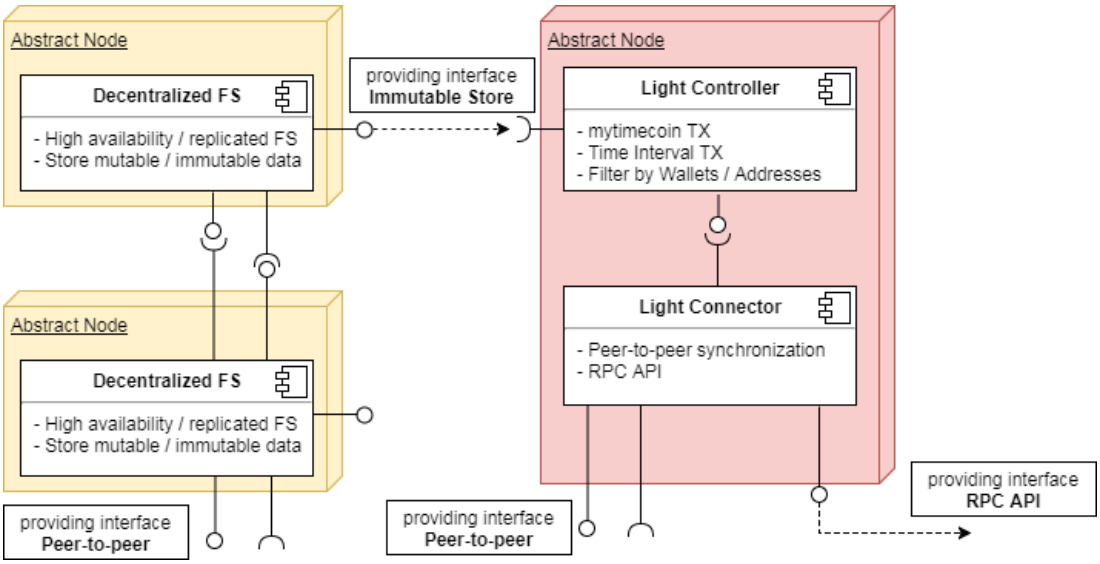
2.2.1 Connector

An internal component of the node, provides a peer-to-peer public interface for data exchange with other network nodes. In addition, the component provides the ability to connect to the node using RPC technology. The node

provides a limited ability to use the RPC interface, it is possible to control only the information related to the node (added to it earlier) through the interface.

2.2.2 Light BlockChain Controller

An internal component of the node, supports operations with parallel **mytime** blockchains. The component stores and checks only the information that relates directly to the node. All transactions that do not include an ID of the user connected to the node will be ignored.

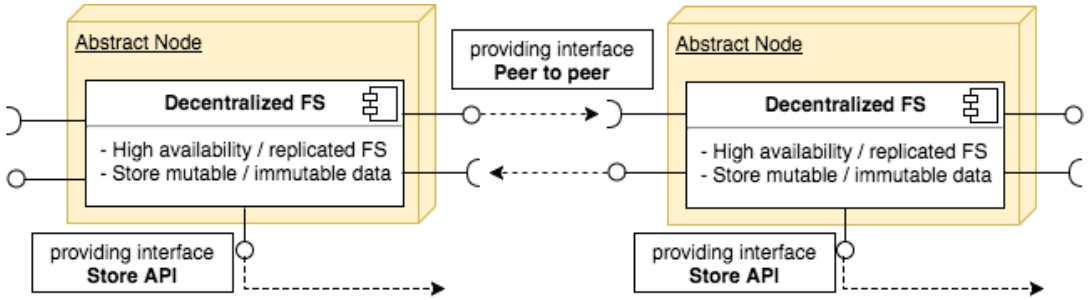


2.3. Decentralized File System

To store information about financial transactions and registered time, as well as the conditions under which such registration took place, the **mytime** platform will use a decentralized file system. Such a file system shall have adequate resilience and availability.

High resilience can be achieved through excessive replication of data and by maintaining the necessary minimum of replicas, as well as their constant verification. High availability can be provided by proper geo-positioning of the file system nodes. Furthermore, such file system shall be a trusted system.

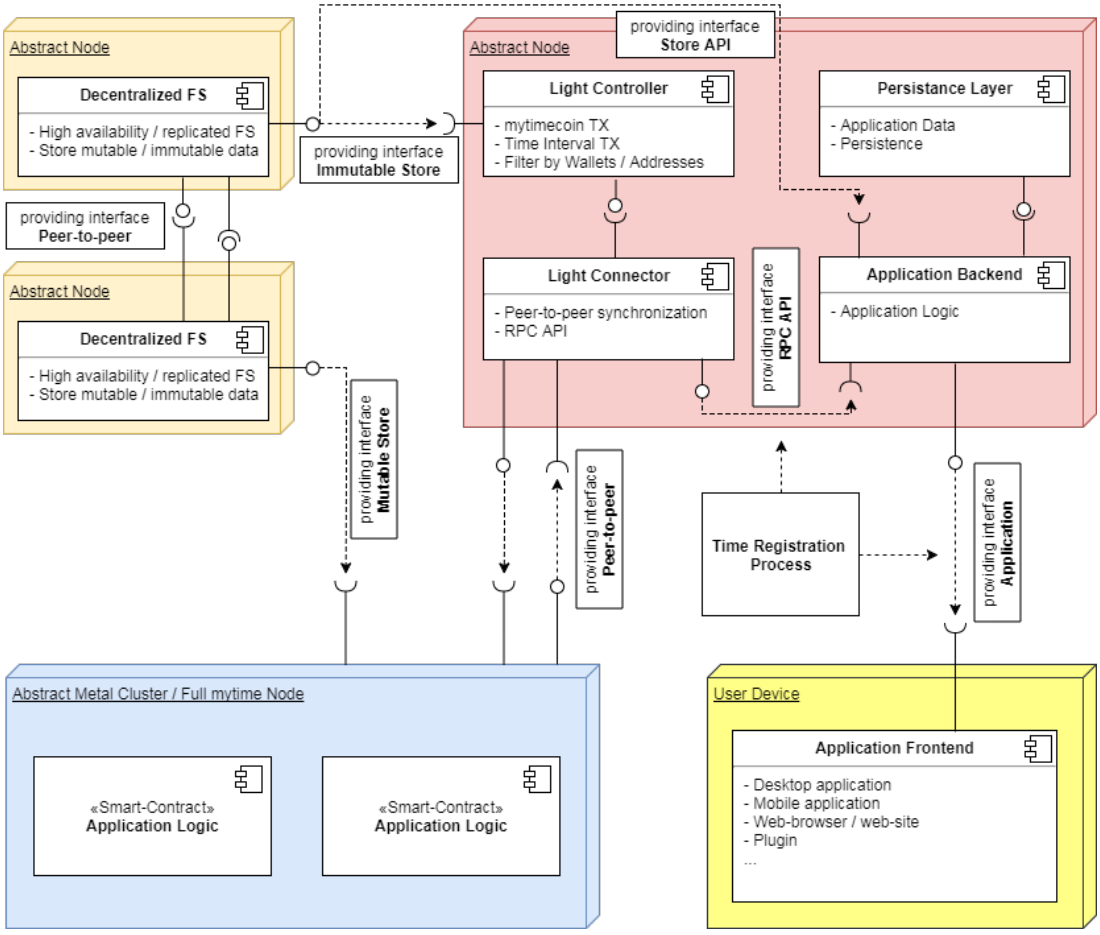
We consider using the existing similar file systems like Storj, FileCoin, Maidsafe, Siacoin, EOS, as well as developing our own version of the decentralized file system within the **mytime** platform based on IPFS.



2.4. Applications / Services

Applications and services within the **mytime** platform automatically record time and deposited cryptocurrency. Applications are motivated to disclose information about themselves in exchange for increased participation in emission and **mytime** platform regulation through improving their own reputation.

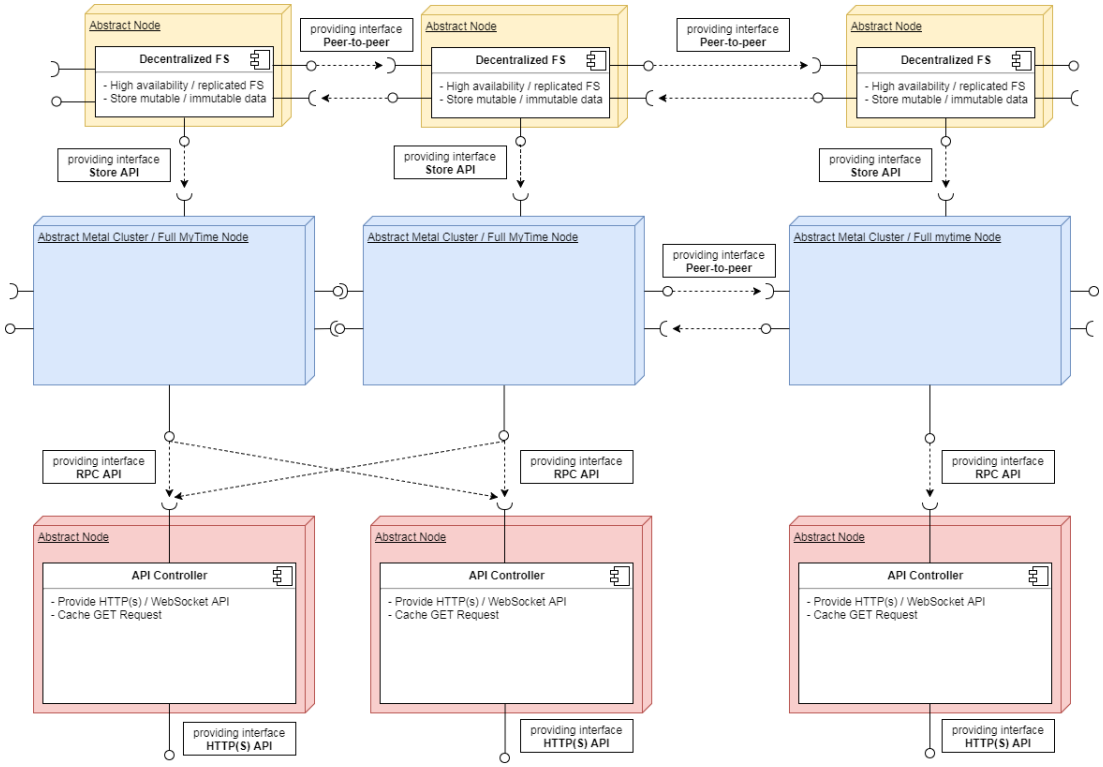
Becoming a platform member, an application gets its unique address. Any platform user can allow an application to record his/her time spent within the application. An application can be a software for a desktop computer, a mobile application for any platform, a website, a browser plugin, etc. A user can assess the application by rating it. To do so, a user shall send a special transaction to the network. An application can be linked to a set of smart contracts in order to implement special mechanics to reward a user for certain actions. To store its state and data, an application can use a decentralized file system.



2.5. Public API

For easy interaction with the **mytime** platform, a decentralized high-performance public API will be provided, allowing any operations with the Time and Money blockchains. The API solves the problem of fast network connection where own node cannot be launched or its launching is inexpedient, whether it is a full or a light node. The API will implement standard HTTP / HTTPS connection interfaces, WebHooks, and WebSockets.

Standard requests for reading data (such as GET) will not be limited in quantity and will be free of charge, other requests that require large computational resources and changing data states may be charged and limited in quantity.



3. Blockchain

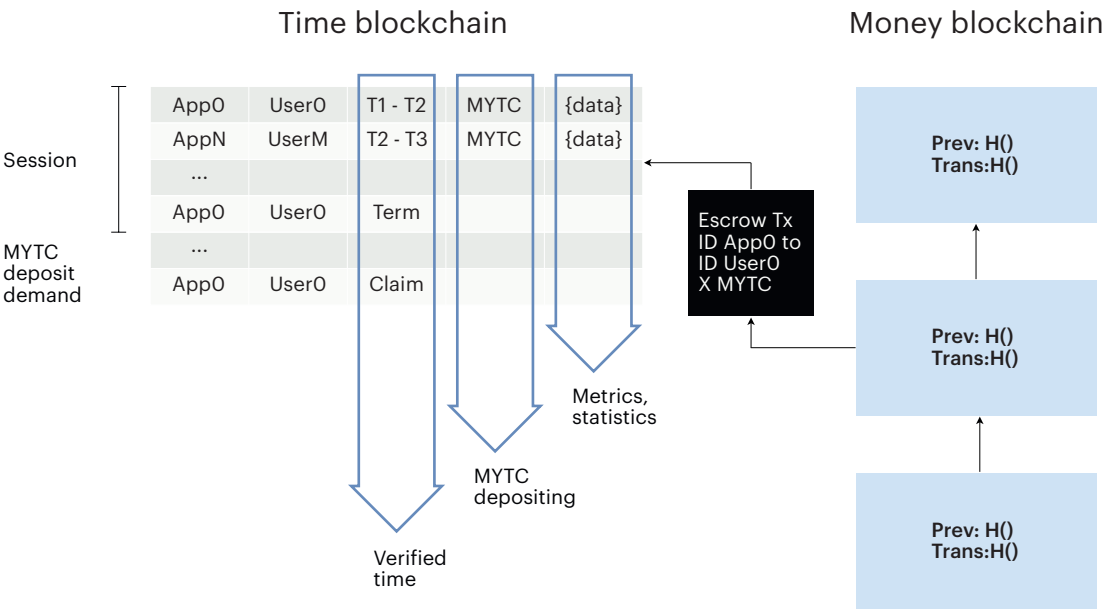
The **mytime** platform operates on two interconnected blockchains, Time and Money, performing complementary functions.

The Time blockchain records user sessions and helps applications or services deposit MYTC. The Money blockchain serves for financial transactions.

The Proof-of-Time algorithm supports the operation of reputational metrics and a voting system using the Delegated Proof-of-Stake consensus algorithm.

The figure below shows a schematic representation of the **mytime** blockchains. The node fulfils the following tasks as related to the Chronos protocol:

1. Records user interaction time and in parallel – deposited MYTC, keeping an arbitrary data set in the record.
2. Controls the session, i.e., registers the first deposit and records the end of session.
3. Detects intersecting sessions, performs algorithmic conflict resolution, unless otherwise regulated by the smart contract code.
4. Controls the amounts and signs the last escrow transaction of the financial application.

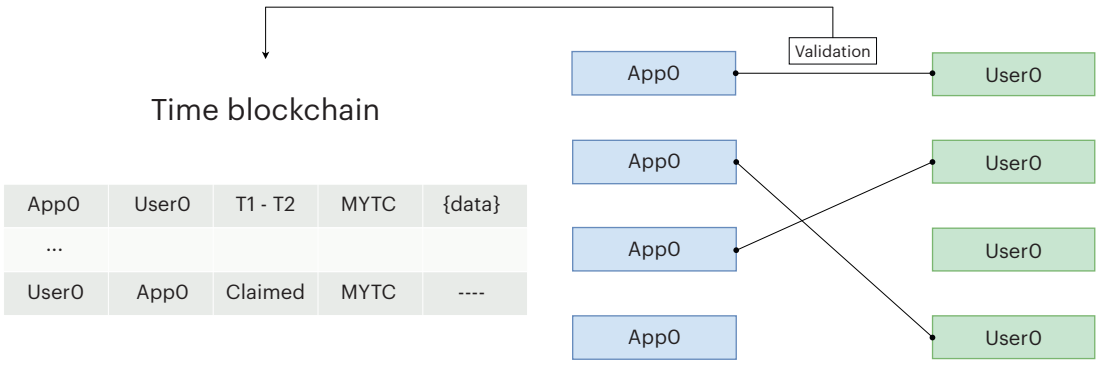


Chronos blockchain and MYTC Money blockchain interaction scheme

Blocks of both Time and Money blockchains are produced in one and the same node within the slowest blockchain. It is understood that the technical parameters of the whole system will be determined by the most loaded Time blockchain, whose parameters will be detailed in the course of further protocol development, identifying the economically feasible volumes of additional data in the time deposit record. Furthermore, it is possible to generate links in the data record block of the Time blockchain to ensure decentralized storage of various information relevant to the applications and services generating the record.

Let’s take a closer look at the Time and Money blockchains interaction mechanism, using the example of a user’s transaction, to demand the deposited MYTC in exchange for the confirmed time.

3.1. Getting the Deposited Cryptocurrency



User0 time validation in App0 in Chronos protocol

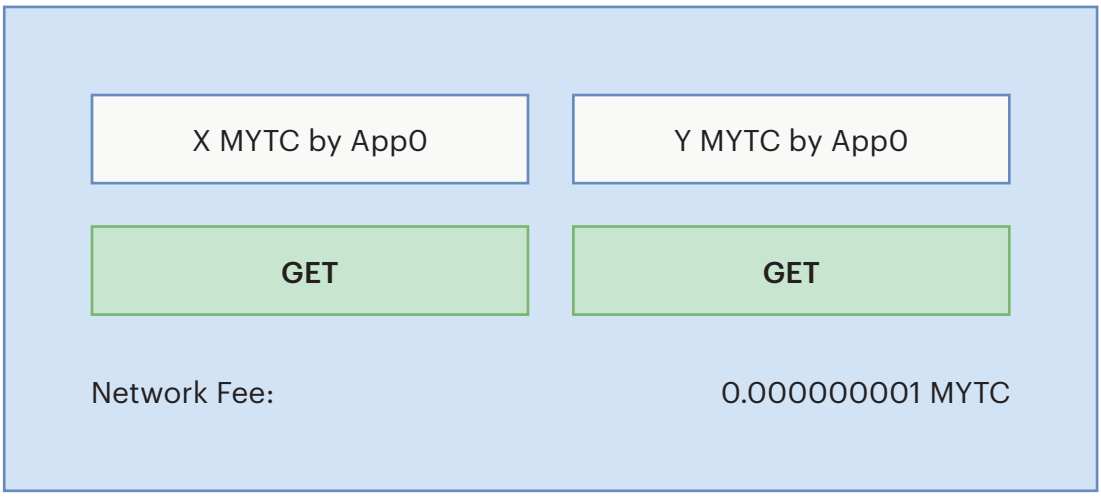
In the process of interaction between an application (service) and a user, user time is validated by the application, for instance, App0 (see the figure above). As a **mytime** platform participant, App0 deposits the MYTC cryptocurrency in the **mytime** system, creating a record in the Time blockchain as follows:

Application ID	User ID	T start	T end	MYTC Sum

The Time blockchain has a limited capacity. Therefore, it only stores records of applications depositing MYTC amounts exceeding the minimum threshold. The latter may vary from time to time.

Double spending related to cryptocurrency depositing is excluded via the Money escrow transaction, reflected in the network by App0 simultaneously with a record in the Time blockchain. The node checks the amount of time spent in the Time session, and together with the application generates a Money transaction of type M from N multi-signatures. After a user requests the funds from the client application, the node checks the closed sessions and signs the Money escrow transaction. Thus, the MYTC cryptocurrency is transferred from the application wallet to the user's wallet.

The **mytime** node accumulates time records and fixes the moment when a user requests MYTC transfer to his/her wallet. Below is a detailed description of the process.



Time payments displayed in the user's basic application

The amount of pending MYTC and the network fee are displayed in the user's basic application. This information is available via the **mytime** API and relies on the information stored in the public **mytime** blockchains and the current network load. User0 can receive funds by clicking the Get button. This event triggers the Proof-of-Time algorithm and MYTC are credited to a user.

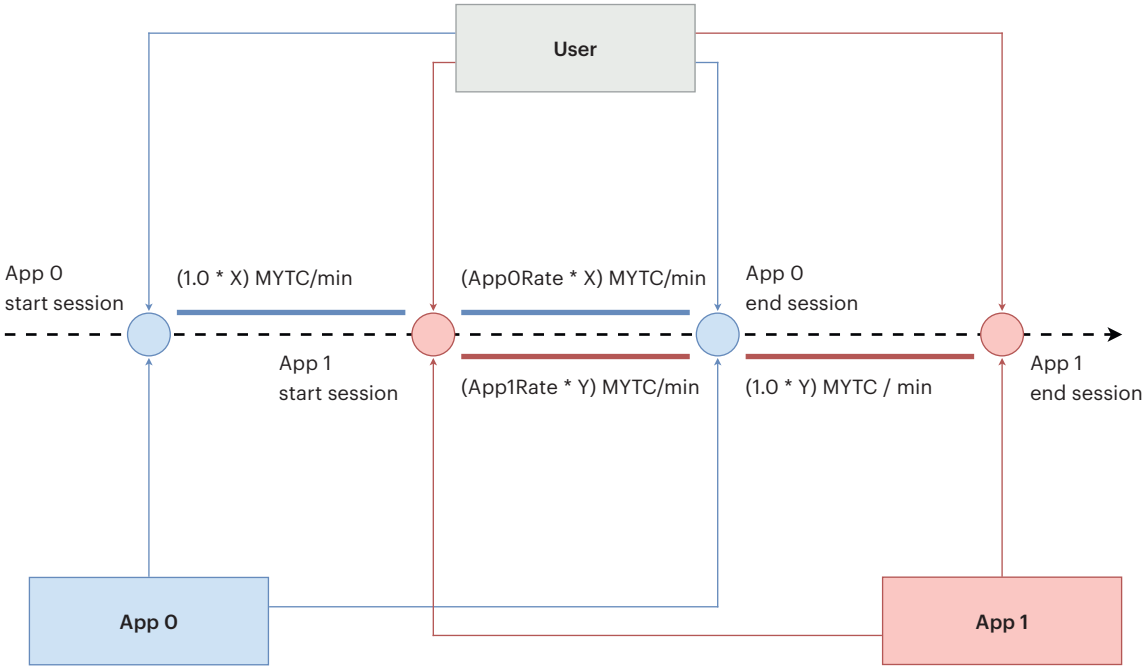
In the process of confirmation, the node verifies the compliance with the final escrow transaction in the network where the **mytime** application or service funds are locked and entries in the Chronos blockchains. If the **mytime** platform rules are met (a user receives a reward only for the time spent in one application), the **mytime** node signs the Money transaction, which is further entered into the Money blockchain, and the user receives the requested amount of cryptocurrency in exchange for invested time, net of the network fee.

3.2. Time Record Conflict Resolution

A service can register user time both on an exclusive basis and in combination with other services. In case there are several parallel time record sessions, the conflict is resolved based on the user's preferences. A user may specify which time record session (which application) has a higher priority for him/her. In case the priorities are set, a reduction factor is applied to the time value within the session.

If priorities for the time record session are not explicitly set by a user, the system selects a session most beneficial to a user. In this case, less beneficial sessions are ignored.

An application may set its own priorities and rules for exclusive registration. For example, an application may ignore concurrent sessions and pay a user the full cost of his/her time, or vice versa, requiring a user to exclusively spend time within its session only.



4. Proof-of-Time Consensus Algorithm

mytime will use the Proof-of-Time consensus algorithm, being a DPoS modification. The differences are mainly related to the calculation of voting weights and voting rewards.

DPoS (Delegated Proof-of-Stake) is a modified version of PoS (used in Peercoin, Blackcoin, NXT). The main difference is that blocks cannot be produced by all network participants, only by a small group of selected miners.

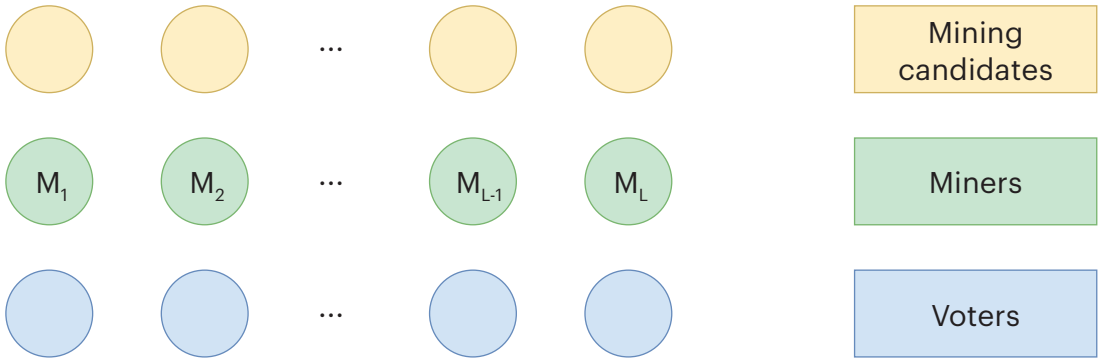
DPoS has more than once proven its efficiency - first applied in BitShares in 2014, today it is used in such projects as EOS, Lisk, Steem, Tezos. The total capitalization of these projects by October 2017 was more than 1 billion U.S. dollars. So far this is negligible compared to the total capitalization of PoW-based cryptocurrencies, but we believe that PoS/DPoS has a great future.

To join the network and become a delegate (producer) of blocks, it is enough to install the Full Node software for a computation node developed by the **mytime** team and have the minimum required wallet balance.

4.1. Network

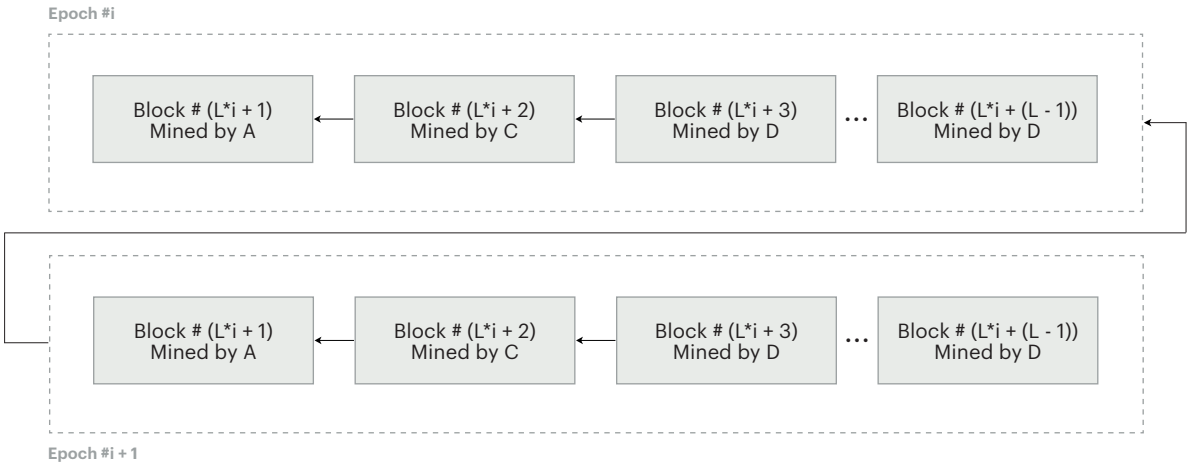
Let's take t_0 as a certain point of time. All addresses referenced in blockchain transactions till t_0 can be divided into three categories:

- Miners (getting fees for placing transactions in a block).
- Mining candidates (willing to mine, but having insufficient reputations).
- Voters (unwilling to mine, but voting for one or more candidates).



4.2. Epoch

To ensure adequate competition between candidates, network voting must take place on a continuous basis. Therefore, the term **epoch** has been introduced to denote a sequence of L blocks, each assigned to a specific address. If during the B_{time} (block time) a miner fails to create a block, the queue moves to the next miner. After the last block is produced miner reselection takes place as described below.



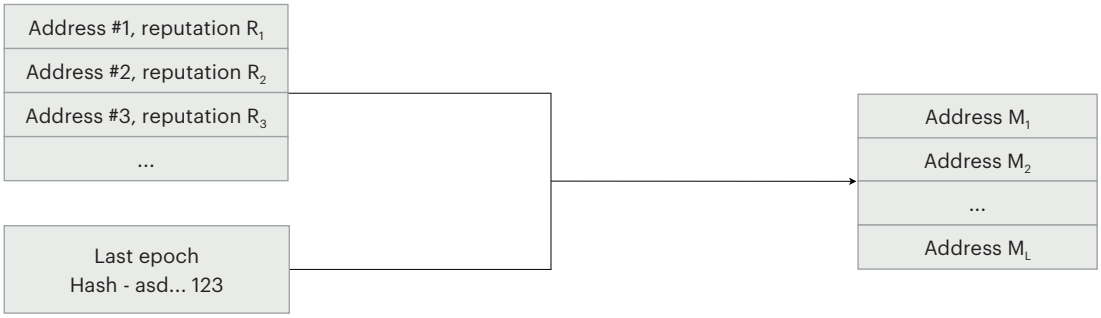
4.3. Miner Selection

At the end of each epoch L new miners need to be selected for activities in the next epoch. Each network address is guaranteed the right to run as a miner. The intention is documented in a special transaction, as implemented in Lisk. Subsequently, there is a non-zero probability that the address is listed as an epoch's miner.

To ensure network security the following challenges shall be addressed:

- Miners are selected in a pseudo-random way, thereby minimizing the chance for abusers to be regularly listed as miners.
- The chances of an address to become a miner should be proportional to its reputation. Otherwise, a dominant cluster of addresses may be created and manage the mining process.
- Miners who miss their queue shall be fined as it increases the time of transaction confirmation.

A pseudo-random factor will be generated using the hash of the last block, thereby ensuring a single result for the entire network.



4.4. Reward for Mining

Aside from the challenges described above, there is another vector of attack. Due to the cold start of the entire system, a list of L candidates will form quickly, and their reputation will be significantly higher than that of all other candidates. Because of this, they will find themselves on the list of an epoch's miners much more often than their ordinary competitors. This may lead to network centralization.

In BitShares, this problem is solved by excluding the address from the candidate list for some time ($t_{down\ time}$) in case an account was mining in an epoch. We chose a different way: to avoid such a situation, the reward for a block will be shared between the miner and those who voted for it. Thus, voters will be motivated to support candidates with a lower rating, which will intensify the competition of nodes for participation in the epoch.

4.5. Voting Weight of Deposited Cryptocurrency

The voting weight of a mining candidate depends on several parameters:

- R_{voter} — reputation of the voting address (it can be either a user or a and service).
- D_{voter} — amount of MYTC deposited by the voting address.
- R_{miner} — miner's reputation.
- S_{miner} —user success in the previous mining process.

The amount of MYTC deposited by the voting address has the biggest weight in the final formula.

S_{miner} means a user's up-time, that is, the ratio of created blocks to participations in the voting as a candidate.

4.6. Voting Address Composition

Services will be the overwhelming voting majority since the mechanics of services operation implies MYTC depositing, ensuring their highest voting weights.

We believe that services are best suited for the voters' role because their actions unlike those of an ordinary user will create the reputation and added value, thereby motivating services to behave as honestly as possible in relation to the platform and users.

5. User Reputation and Profile

The Chronos protocol in its basic form is subject to various attacks of intruders who, for example, create networks of bots and confirm their time. Even advanced machine learning technologies cannot suppress bots because bots use the same technologies. It is always possible to create a bot that is indistinguishable from a person in its service interaction patterns.

To effectively repel such attacks, we introduce the reputation concept in the protocol.

Definition 1. Users directly linked by transactions.

Users U_i and U_j are deemed directly linked by transactions if there is one or more transactions in the Time blockchain or Money blockchain involving both users.

Definition 2. Transaction graph.

Transaction graph is a weighted graph $G = (U, T)$, where:

$U = \{ U_0, U_1, \dots , U_n \}$ - a set of vertices representing all **mytime** users (wallets).

$T = \{ T_0, T_1, \dots , T_n \}$ - a set of edges connecting vertices, representing a direct link through transactions.

Each graph edge is assigned a weight W_{ij}, being a numerical expression of the transaction history between two users (wallets) U_i and U_j. The mathematical expression of weight W_{ij} is to be further investigated and implemented during platform balancing.

Definition 3. User transaction profile.

User transaction profile U_p is a subgraph $G^p = (U^p , T^p)$ of the transaction graph, where:

$U^p = \{ U_0, U_1, \dots , U_n \}$ - a set of vertices representing user U^p and users directly linked with U^p through transactions.

$T^p = \{ T_0, T_1, \dots , T_n \}$ - a set of edges connecting vertices, representing a direct link through transactions.

Definition 4. Transaction distance.

The transaction distance D_{ij} — shows the connection between **mytime** users U_i and U_j . Transaction distance depends on the shortest path between U_i and U_j in the transaction graph, as well as on the maximum cryptocurrency flow between the users. The exact mathematical expression for D_{ij} is under development.

Definition 5. User reputation.

The reputation of user U_p or the degree of trust the network has to the user, used to diversify the transaction profile, is calculated as:

$$R_p = \frac{1}{n\,(n-1)} \sum_{i \in U^p} \sum_{j \in U^p,\, j \neq i} R_i D_{ij}$$, where:

$U^p = \{ U_0, \dots , U_n \}$ - a set of vertices representing the users directly linked through transactions with user U_p

n — number of users directly linked through transactions with U_p

R_j — reputation of user U_i

D_{ij} — transaction distance between users U_i and U_i

The less connected the users directly linked to user U_p are, the higher is their own reputation, the more is U_p trusted as a real person.

The mathematical model of reputation is under development and can be changed in the future.

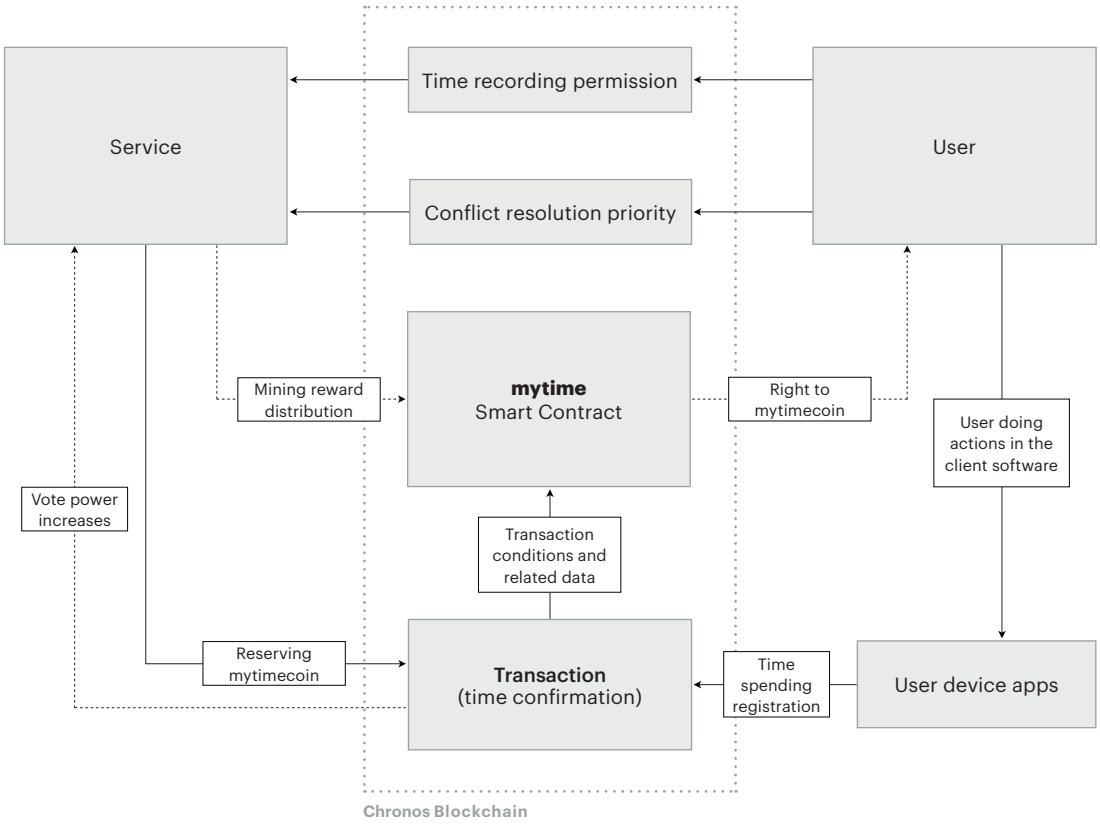
In addition to using reputation to protect the network from being abused by bots, the transaction profile can be used in look-a-like searching of users with similar transaction profiles.

6. Smart Contracts

The protocol will support smart contracts. Such contracts make it possible to implement more sophisticated time mechanics, as well as transparent mechanics to reward users for performing certain actions in applications. Any application can use an associated contract to ensure transparent transactions dealing with time.

Smart contracts allow implementing various options of economic relations based on the **mytime** protocols, in particular:

- Contracts for a user's future time.
- Transparent accounting of time and remuneration.
- MYTC distribution in communities and gaming clans.
- Receipt of MYTC for fulfilling certain conditions.
- Exchange of data between services without directly accessing that data.
- Targeted sponsorship — payment of studies.



7. MYTC Cryptocurrency

MYTC is a classic cryptocurrency, and fees are charged on all transactions. The fee amount depends on the current network load.

The competition for placing a transaction in a block determines the minimum cost of the time interval. The minimum cost is adjusted to the current load of the Time blockchain. No transaction can be executed if the amount of deposited cryptocurrency is less than the minimum threshold.

A user gets the cryptocurrency deposited in Chronos by calling a special function in his/her personal wallet. Calling this function generates a request for a transaction, recorded in the Time blockchain. The node, before placing this transaction in the block, and after checking the closed paid sessions, signs the escrow transaction in Money.

8. MYTC Emission

Every minute N MYTCs are emitted as a reward for block production and distributed among all those who have voted for the node. To participate in voting, one must have a minimum share of MYTC (the principle of DPoS).

The deposited cryptocurrency forms a deposited Stake, which substantially enhances the service vote for block producers. The Stake enhances the vote with due regard for the number and frequency of entries of deposited time accumulated on the service account, as well as service users' reputation.

The effect of the deposited Stake decreases with time. The most important are records with a minimum past period. Such mechanics make it profitable to regularly validate the time value of **mytime** users.

Nodes (delegates) dealing with the packing of blocks, check the uniqueness of the minute-user records and, in case a simultaneous record is made for the same minute, adjust the time value proportionate to the number of services interacting with users.

This ensures there are no collisions, when a user tries to get a reward from more than one service at the same time.

The final formulas for emission and effects of the deposited Stake on the vote power will be specified following the results of simulation modeling.

9. Platform Constitution

9.1. Purpose of the Constitution

It is evident from the development history of such popular blockchain protocols as Ethereum, Bitcoin or Zcash that any initial specification is not ideal and always changes in the course of use. To date, most controversial issues related to development of any platform are resolved by means of forks, implemented by a narrow group of people who have the biggest impact on the platform.

We believe that such approach a priori threatens the very idea of a distributed peer-to-peer network, which is why the **mytime** blockchain will be developed with an eye to Tesoz and EOS as far as self-regulation is concerned.

Our platform will provide users with certain basic rights:

- The right to express their opinion on matters concerning the current or future state of the network, or to maintain neutrality.
- The right to have a user's vote documented regardless of his/her actions.
- The right to at any time offer its own solution to the community.

By formalizing these rights and implementing them as part of the protocol we will position **mytime** as a truly decentralized platform where any proposals are made and implemented by users of the platform, rather than a narrow circle of developers and/or investors.

9.2. Constitution in Practice

Voting for adoption of a new protocol amendment will last for a predetermined number of blocks $N_{\text{voting length}}$. During the first two years of **mytime** operation the Chronos Foundation reserves the right to veto any change proposal.

To make a decision, more than 80% of active users should participate in voting. This bar is conditional for the time being, and will be specified in the course of modeling.

The main voting process is divided into 4 stages, each taking a quarter of $N_{\text{voting length}}$

1. Anyone may post his/her version of the protocol that they believe solves the problem.
2. The outvoting version of the protocol is put to a general vote, and one may vote for, against or abstain (the percentage of neutral votes will also be taken into account in the final decision).
3. If the quorum is reached and the required number of votes is collected, the protocol is implemented in testnet, or rejected if not.
4. If the protocol is successful in the testnet and passes another voting (by the same rules as the previous one), the new protocol will be implemented in the main network.

10. Platform Integration

Any independent developer may create its own application using **mytime** protocols, and to integrate them with other platform applications. A developer may launch its own service based on its application, or integrate with third-party services.

Various tools will be developed to make it easier for developers to create and launch new applications:

- API for interacting with **mytime** blockchains, DPoS voting, cryptography
- Software for running full and light nodes
- Wallets
- Smart contracts
- Access to the distributed data store
- API for access to exchanges
- Marketplace of business requests for new **mytime** services
- Test infrastructure
- Other services rising in demand as **mytime** develops.

10.1. Applications

An application integrated with the **mytime** platform means any software product using the API to interact with the Chronos protocol.

Examples of applications:

- A desktop application for any operating system.
- A mobile application for any operating system.
- A web-based application.

- A messenger bot for Slack or Telegram, etc.
- A plug-in for any system, for example, JIRA.
- A server software.
- Other apps.

Applications may be developed with any programming language.

10.2. Basic Applications

In addition to the protocol specification, the **mytime** team will develop the following basic applications:

- Reference implementation of software for nodes supporting the protocol.
- Basic user application.
- Messenger plugins to integrate social communities into **mytime**.

The basic user application serves two purposes:

- Reference implementation of the protocol.
- Mass user attraction to the **mytime** platform.

The basic user application will consist of the following components:

- A wallet.
- A miner client that guarantees a certain minimum income.
- **mytime** platform application marketplace.

The following applications developed by the **mytime** team will be immediately available on the application market:

- An application for social communities interaction and a community management plugin.
- A video viewing application.

The basic user application is developed on account of the following requirements:

- The application is designed for the mass user.
- Installed in one click and immediately adding value.
- User interaction is built on the game mechanics.

To attract more users, simultaneously with the basic application we are developing bots for popular instant messengers: Telegram and Slack.

11. Chronos Foundation

The development of the community will be handled by a separate structure — the Chronos Foundation.

We will grow and support the community around the platform to help sustain global distribution and high penetration of the MYTC cryptocurrency.

This support will include:

- Chronos protocol development and its basic implementation, all open-source.
- **mytime**-integration support.
- Development of the standardized solutions for accurate recording of user time.
- Investments in services that integrate with **mytime**.
- Arranging conferences and hack days.
- Encouraging developers of open-source products used in **mytime**.

12. Protection from Attacks

Attack	Problem	Solution
Attack on DPOS	Generation of applications and addresses to outvote in the mining node voting and get a reward	Economic, reputation mechanisms
Double spending	Application making a double payment to improve statistics/reputation, or as a result of errors or due to other reasons	Escrow mechanism
Secret chain attack (falsification of transaction history)	Getting the economic effect from double payment by substituting a false chain of blocks (smart contract or ordinary transactions)	DPoS
Attack of the majority on the reputation mechanism (analogous to the attack 50 + 1% on the hashrate)	Generation of several applications and miscellaneous addresses to attack the reputation balancing mechanism	Reputation algorithm properties
Sybill attack	With a small number of nodes, an attacker substitutes one of the nodes and falsifies the blockchain information in order to get benefits	Trusted nodes, economic punishment for attacking nodes
DoS	1. Spam transactions. Lower value transactions are more exposed to such attacks. 2. Peak network loads. 3. Other computationally intensive operations that may impact the functioning of network protocols and nodes	mytime economic properties
Cryptography hacking		Using ready-made NIST solutions for SHA-2 and SHA-3 encryption algorithms
Package analysis	Viewing mytime network traffic in an arbitrary case	Encryption
Wallet theft vulnerability		Developing a reference wallet with a maximum functionality: recovery seed, file encryption
Other software errors and security holes in the protocol, not yet detected	Problem in developing a fast-response mechanism	Updating protocols

13. mytime Economy

The long-term efficiency of projects involving blockchain technologies is largely determined by economic factors. If all participants are motivated to develop the platform and attract new system members, create applications and maintain its efficiency, etc. such a system will be functioning for a long time and continuously evolving. A project is unlikely to develop without such motivations. That is why, we place a strong focus on the **mytime** economy.

13.1. Deposited Cryptocurrency

Deposited cryptocurrency is an unconditional right of A to receive funds from B. The difference from escrow transactions is that depositing cryptocurrency is beneficial to A itself as it increases its vote power in DPoS and, consequently, the reward amount. Technically depositing is comprised of two transactions: one in the Time blockchain and the other in the Money blockchain as an escrow transaction.

Properties of deposited cryptocurrency:

- Serves as a reward to A.
- Not owned by A.
- Brings no reward to B (unless otherwise provided for in a smart contract between A and B).
- Owned by B.
- Confirms the cost of B's time for interaction with A.
- The operation is free-of-charge for A (if placed in a block at the cost of time).
- The fee for changing the deposit status to ownership is paid by B.
- A cannot deposit more cryptocurrency than the amount available to it.
- Unconditional depositing, i.e. A cannot get the cryptocurrency back.
- Even if A becomes insolvent, B will receive the cryptocurrency.
- When depositing the cryptocurrency, A may enter arbitrary data into the transaction.

The combination of deposited cryptocurrency properties forms an economic basis for motivating the system participants.

13.2. Motivation of System Participants

13.2.1. User Motivation

Users are motivated to use the platform services by getting the maximum amount of cryptocurrency for every minute of their time.

When a service distributes a reward from the deposited cryptocurrency, a user is motivated to keep his/her money in the deposit, extracting the cryptocurrency into his/her wallet as and when necessary.

In earning cryptocurrency, users are influenced by their circadian rhythms, qualifications, spheres of activity and offers from competing services.

Users are rewarded by the same cryptocurrency irrespective of the service and thereby don't have to accumulate scores and bonuses by participating in hundreds of loyalty programs offered by miscellaneous services.

Users are motivated to interact with plenty of services and other users as it enhances their reputation in **mytime**.

13.2.2. Services Motivation

Services participating in the system can be, for instance, B2C applications for broad market, or corporate applications, or any other businesses that integrate the protocol into their products.

The **mytime** platform may serve to improve the overall efficiency of ongoing businesses. Also, fundamentally new models can be created, impracticable outside of the **mytime** platform.

The advantages for services using the **mytime** platform:

- Micropayment opportunities for users.
- An alternative to banking for most business operations.
- Reward based on the Proof-of-Time algorithm - in analogy to accruing interest on a bank deposit.
- Automated business operations through smart contracts.
- Security and depersonalized data.
- Automatic accrual of bonuses for achieving time-related KPI.
- Competitive advantages over businesses not using **mytime** opportunities.
- Advance payments for attracting new users to the service in exchange for marketing research data, cpc, new customers profile ID, etc.
- Possibility to deliver content to resources regularly visited by users.
- Reducing rewards for users making use of several services at the same time (conditional fine for split attention).

13.2.3. Validator's Motivation

One of the problems faced by B2C services is bots emulating the actions of real users. Another problem is validation of performed work, actions, results followed by cryptocurrency depositing.

To eliminate these problems, we introduce the role of a validator. A validator is a service variation different from other services because it verifies user identity, their actions and results, rather than attracts user attention.

A validator is motivated by receiving a reward for the work performed by services or users.

The basic software for validators will be developed and released by the Chronos Foundation. Special software for validators can be created by third-party developers interested in gaining profits.

13.2.4. Nodes Motivation

As in any other blockchain project, nodes are motivated by receiving rewards for block packing, and transaction fees. In Proof-of-Time, nodes receive only part of the reward for block packing, the remaining portion goes to applications/users that have voted for the node.

Given that **mytime** can process millions of transactions per minute, the nodes will come in the form of computing clusters, including those deployed in Google/Amazon cloud services. Thus, we ensure fast balancing of the required number of nodes.

In the case of a negative scenario caused by rapid depreciation or other factors, the **mytime** network will be supported by nodes run by the Chronos Foundation. After stabilization the Chronos Foundation nodes will be withdrawn from the network, making room for other participants.

13.2.5. Data Storage Motivation

The volumes of metadata related to user-service interaction can be massive since there are virtually no limitations for services as far as the recording format is concerned. We offer decentralized data storage in analog with Storj, FileCoin, Maidsafe, Siacoin, and EOS. Whether we make a fork for one of the developed solutions and customize it for our needs, or use one of the ready-made functioning services, will be decided in the course of **mytime** development.

Services on metadata storage will be paid by the interested service.

14. Conclusion

The economic and social features of the **mytime** platform can set a new level of blockchain technology adoption in various spheres of our daily lives, restructuring economic relationships between businesses and users.

The **mytime** software will help reduce the costs arising from the interaction of businesses and users.

As a result, we'll be able to build a new economy wherein any person can benefit from his/her time invested into any interaction, and any economic relationship can be expressed through the cost of time.

15. Disclaimer

The information contained in this Technical Paper may be incomplete. The contents hereof do not suggest any contractual relations, nor are binding to the Company, and may be further changed as the **mytime** ecosystem is developing.

This Technical Paper does not contain any investment, legal, tax, regulatory, or other financial recommendations.

This Technical Paper should not be considered as the only correct, comprehensive information for use in evaluating MYTC transactions.

Nothing in this Technical Paper should be regarded as a request for investment, nor should it in any way be regarded as an offer to purchase securities in any state jurisdiction.

This document is not subject to any state jurisdiction that prohibits or otherwise restricts cryptocurrency transactions.

Certain statements, assessments, and financial data contained in this Technical Paper constitute hypotheses, rather than factual information.

Given unidentified risks and other uncertainties associated with the project, its actual performance may differ materially from the forecasts reflected herein.

The Company neither offers nor distributes MYTC nor conducts business in the United States of America, People's Republic of China, Republic of Korea, the State of Israel, the UK, Singapore, or other countries and territories where digital token and currency transactions are prohibited or subject to special regulations or restrictions.

MYTC are not offered, distributed, or otherwise disposed to legal residents or citizens of the United States of America (including all states and the District of Columbia), People's Republic of China, Republic of Korea, the State of Israel,

the UK, Singapore or other countries or territories where cryptocurrency is prohibited or in any way restricted.

Actions taken by such people to acquire MYTC will be regarded as illegal, unauthorized, and fraudulent. Such actions may lead to negative consequences in accordance with laws applicable in a particular jurisdiction.

Every potential MYTC holder shall note that this Technical Paper is presented on the grounds that the reader is authorized to read the document.

Each potential holder may independently assess the legality of acquiring and carrying out other operations with MYTC based on the laws and codes applicable in a given jurisdiction, both in the case of buying them from the Company and in the case of reselling them, and carrying out other operations with them.

This English Technical Paper is the official source of information about the MYTC project. In translating this document into other languages, some information may be lost, damaged, or distorted.

The accuracy of the translation is not guaranteed. In the event of any inconsistencies or collisions between Technical Paper translations, this official English version shall prevail.

Before participating in the project it is strongly recommended that each prospective participant/holder consult with legal, investment, tax, financial and other advisors in order to gain a better understanding of the risks and to calculate the potential benefits and effects. It is also strongly recommended to read the information below.

16. Project Risks

Acquiring MYTC comes with a high degree of risk. Multiple factors can have a significant negative impact on the cost of these digital assets, as well as on the entire **mytime** platform.

The following is a list of risks and uncertainties that may become reality for MYTC holders, and it is not exhaustive.

16.1 Risks associated with MYTC value

16.1.1. Absence of rights, application areas, functionality and other attributes

MYTC does not grant any rights, has no scope, functionality or features, other attributes, explicit or implied, including any spheres of use, purpose, functionality, attributes, or features of **mytime**.

MYTC is not a tool for owning any assets of the Company, nor can it be considered as an intangible asset.

The Company makes no commitments and provides no guarantee to the holders on acquiring any rights through MYTC, or on their application, functionality, attributes, or features.

16.1.2. MYTC market failure

Since there was previously no open market for MYTC, the launch of the project may not lead to the formation of an active or liquid market of MYTC. The market price of MYTC may be volatile.

Despite the proposed demand for MYTC, the active market may not form after trading begins, or may cease to develop. As a result, the owner would not be able to perform MYTC operations in a timely fashion.

In the worst-case scenario, the market will not form or will cease to exist, and MYTC holders will lose the opportunity to sell them.

16.1.3. Speculative risks

The evaluation of cryptocurrencies in the secondary market often lacks transparency. The cost of MYTC can fluctuate greatly within a short period of time.

16.1.4. Risk of loss of value

There is a significant risk that a holder of MYTC may lose all his or her contribution because of depreciation.

The Company does not guarantee the value of MYTC, nor predicts their liquidity. The Company is not and shall not be held liable for the market value of MYTC, or their liquidity.

16.1.5. No refund

The Company is not obliged to redeem MYTC, or to otherwise refund their holders, for whatever reason.

MYTC value is not and will not be guaranteed, including their inherent value. Therefore, the refund of contributions may not be possible. Apart from that, it may be limited by laws and regulations that differ from the laws and regulations applicable to MYTC holder.

16.2. Blockchain and software risks

16.2.1. Untimely processing of smart contracts

In Bitcoin and Ethereum blockchains, block production can occur at arbitrary times, so there is a risk of untimely performance of smart contracts. The holder should be aware of this and consider its probability.

Bitcoin and Ethereum-blockchains may not process a transaction at the exact moment the buyer expects it, and the buyer might not receive MYTC on the same day that it completes the necessary action.

16.2.2. Network overload

Bitcoin and Ethereum networks are subject to congestion, when transactions can be lost or delayed. Individuals and groups can deliberately congest entire networks, trying to gain an advantage.

16.2.3. Development risks

None of the properties or the forecasts for the **mytime** ecosystem set out in this Technical Paper have been tested in practice. Their development may face insurmountable technical obstacles.

The **mytime** platform may fail to operate or may operate in a way different from the initial concept. MYTC may not get their intended functionality.

In addition, the **mytime** platform may become obsolete or lose relevance in the development process or right after launching due to the fast pace of innovations.

16.3. Security Risks

16.3.1. Risk of losing private keys

MYTC may be stored in a digital wallet or other storage requiring a digital key (or combination of keys).

The loss of keys associated with a digital wallet or vault will result in the loss of access to their balances. Additionally, a third party may get access to the private keys from the holder's wallet and, consequently, access to the MYTC they contain. The Company is not liable for the losses that this may entail.

16.3.2. mytime infrastructure security

Hackers or other bad actors may try to intervene in a smart contract, or otherwise interfere with aspects of how **mytime** functions. These may include malware attacks, denial-of-service attacks, and other digital disruptions.

16.3.3. Failure to connect open cryptographic keys to the holder's account

In the event that the MYTC holder does not provide access to connect open cryptographic keys to his or her account, it may cause a third party to incorrectly recognize its MYTC balance in the Ethereum blockchain when initial balances of a new **mytime** blockchain are formed.

16.3.4. Incompatibility of a cryptocurrency wallet

A wallet or cryptocurrency storage system used by the holder must be technically compatible with MYTC. Failure to use compatible technology may result in the MYTC holder not gaining access to their MYTC.

16.4. Development risks of mytime

16.4.1. Third party dependency

Even after the launch, **mytime** will rely wholly or partially on third parties for the adoption and implementation of certain functions, as well as for continuing the development, maintenance and support of the platform. There is no guarantee that these third parties will do their job properly.

16.4.2. Development team dependency

This project exists as the result of effort by the **mytime** team, who are responsible for maintaining the competitiveness of the ecosystem overall. To lose members of the management team (or to fail to attract and retain additional staff) could have a significant adverse impact on **mytime**.

The competition for staff with relevant experience is high due to the small number of qualified specialists. This shortage of personnel seriously affects the ability to attract additional qualified management, which can have a significant negative impact on the platform.

16.4.3. Lack of interest in the platform

Even if the platform is completed and launched, the success of the platform depends on the interest and participation of third parties. Their interest cannot be guaranteed.

16.4.4. Risk associated with other projects

The platform can prompt creation of alternative projects promoted by unaffiliated third parties.

16.4.5. Other factors

The development of the platform can terminate due to lack of funding, loss of key personnel, lack of commercial success, and other factors.

16.5. Risks associated with business of the company

16.5.1. Conflict of interest

Company units may be involved in transactions with affiliated entities. Conflicts of interest may arise within the Company or between the Company and affiliated parties. Transactions with related parties may fail to comply with the arm's length principle.

16.5.2. Emerging markets risks

The Company (or some of its units) can operate in emerging markets countries subject to high risks, including significant legal, economic and political risks.

16.6. GOVERNMENT RISKS

16.6.1. Inadequacy of regulatory framework

The legal status of cryptographic tokens, cryptocurrencies, and other digital assets remains unidentified in many countries. Predicting how quickly and how public authorities will regulate these assets, as well as the blockchain technology that facilitates it, is not possible.

Changes in legislation may adversely affect the Company and the prospects for the technologies developed by it.

The Company may stop distributing coins, developing a platform, or its activities in a specific jurisdiction in the event that such actions are found to be illegal, or legislative changes will make them economically impractical.

16.6.2. Failure to obtain, maintain, or renew licenses and permissions

Although there are no statutory requirements for the MYTC Company or holders to receive any licenses or permits, there is a risk that such requirements will be introduced in the future.

Regulatory authorities may establish requirements for cryptocurrency traders, including requirements for compliance with various standards, getting licenses, and the like.

In this case, an exchange trading MYTC could be suspended for an indefinite period.

16.6.3. Risk from state regulation

The Company operates in a new industry and may be subject to increased supervision and control.

The Company's property and operations are regulated by various state authorities and are subject to annual inspections.

The inspection bodies may conclude that the Company has violated laws, decrees, or regulations if it cannot refute these findings or rectify the violations in a timely manner.

Failure to comply with the applicable laws can lead to significant penalties, ranging from fines to criminal prosecution.

Any toughening in state regulation of the Company's activities may increase the Company's expenses and adversely affect its operations.

16.6.4. Illegal or arbitrary actions by state bodies

Sometimes public authorities show a high degree of freedom. Under the influence of commercial or political considerations, they act selectively, arbitrarily, without prior notice, or in a manner contrary to the law.

This creates risks for the Company's operations. Additionally, such conditions allow competitors to gain various privileges and preferences from state bodies, equating to direct competitive advantage.