FIREBIRD

Artificial Intelligence
for Monetary Systems

WHITE PAPER

Table of contents

Introduction

Up to a few years ago, an idea of an alternative monetary system to existing, fiat, money would be a far-fetched one. The emergence of blockchain expanded our understanding of monetary systems and allowed us to examine the advantages and disadvantages of various ways of organizing them.

This document describes the rationale and modus operandi of a system, capable of revolutionizing the financial world whilst also balancing the socio- economic inequalities.

Justification of validity

FIREBIRD is being created as an alternative to existing instruments characterized by non-transparent emissions and to deflationary crypto-currencies models that can lead to economic slowdown whilst widening the gap in participants' savings.

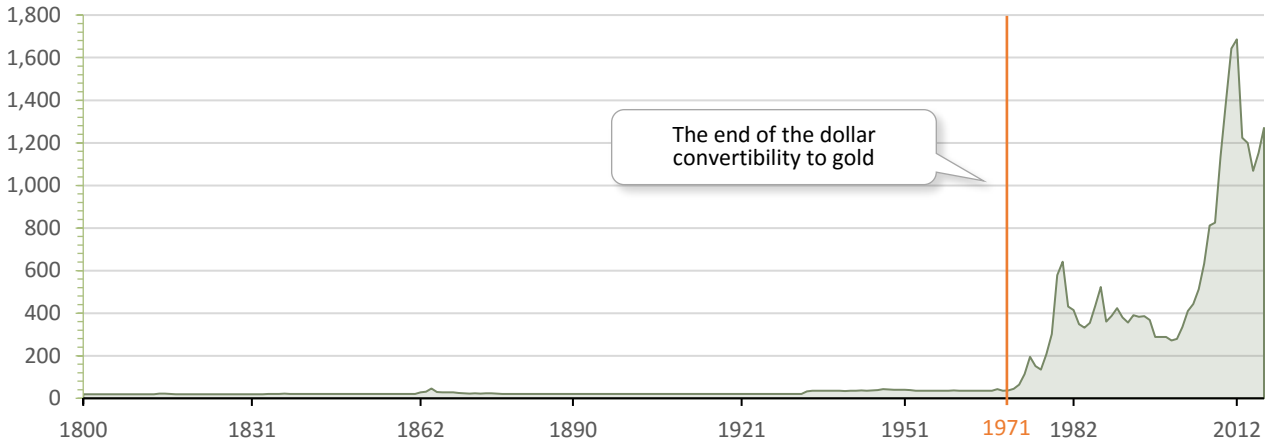
Problems of the modern currency system and its challenges

The Jamaica Accords, which exists since 1976, is a system of mutual settlements and relations, based on a freely floating rate, or in other words exchange rates which are set not by the state, but by the market. Now, 40 years later, what valuable lessons can we learn?

Money Standard

After moving away from the Bretton Woods system in 1971, the USD was completely de-pegged from Gold removing the guarantees to exchange the world reserve currency for any value. Gold is rapidly becoming more expensive, and gradually increasing effort is spent by Economy scholars to find the answer to what should be the best monetary standard in the modern world.

Figure 1. Cost of troy ounce of gold (USD)



Underwriting monetary value by government level debt is often scrutinized whereas the return to the gold standard is also impossible due to the deviation of global gold production from the growth rate of the global economy.

Other proposed options, in particular the electricity peg create discrimination favoring certain countries and industries over others.

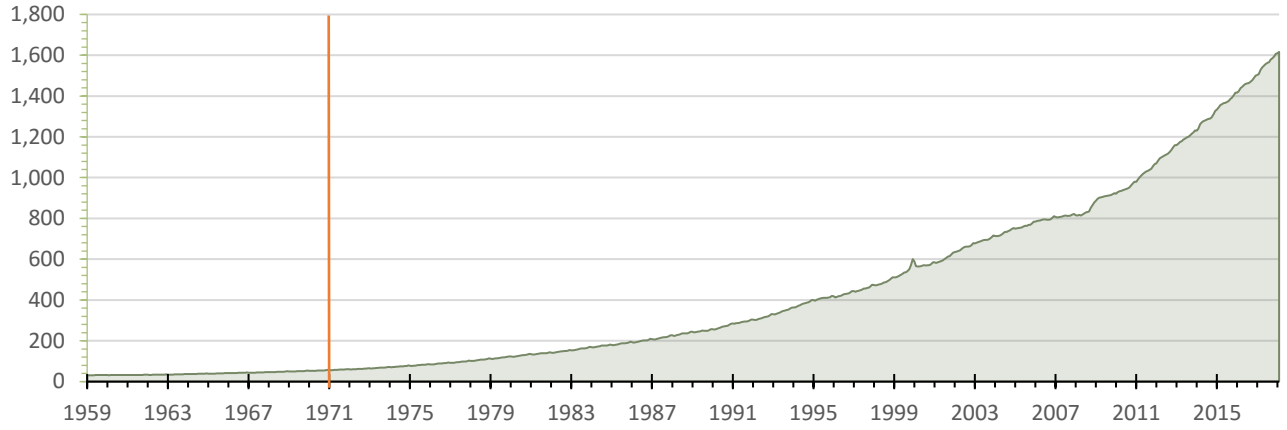
Vagueness of supply principles

The question of how much money should be in the system, on first examination, seems simple. Let's say that holders of a certain currency have 2 cars and 2 coins. If they created a third car, they release a third coin. Thus, one coin is still linked to exactly one car. The system, however, becomes stronger, because with the same number of people they have more money.

A more effective method of development is when, in order to make a third car, the participants agree to issue a third coin in advance. The balance remains the same if this coin is utilized in the creation of that, third, car.

In real life, linking emissions to gross domestic product is not simple nor transparent. Nowadays, it seems, there are no objective and/or automatic methods for calculating GDP growth. This is due to the rise of intangible elements as a percentage of total led by the disproportionate growth in: services, digital products and derivative financial instruments as compared to real goods. Consequently, there are no guarantees for an effective growth in money supply.

Figure 2. The amount of money in circulation (billion USD)



According to the study by Credit Suisse, 85 world's wealthiest people now own the same amount of total world wealth (1%) as 3.5 billion of the "poorest" people. Taking into account the fact that most of the money in the system since 1971 is "new", such a situation can be partly attributed to the distribution mechanism of incremental money supply.

Currency speculation

A key function of money is providing a measurement of value. Existing monetary systems, however, do not have any built-in protection against being used as a speculation tool in currency markets. Consequently, as their value can be influenced by profit seeking speculators, they cannot, on a standalone basis be a universal measure of the value of all existing goods and services. External regulation is required.

Problems of existing crypto currencies

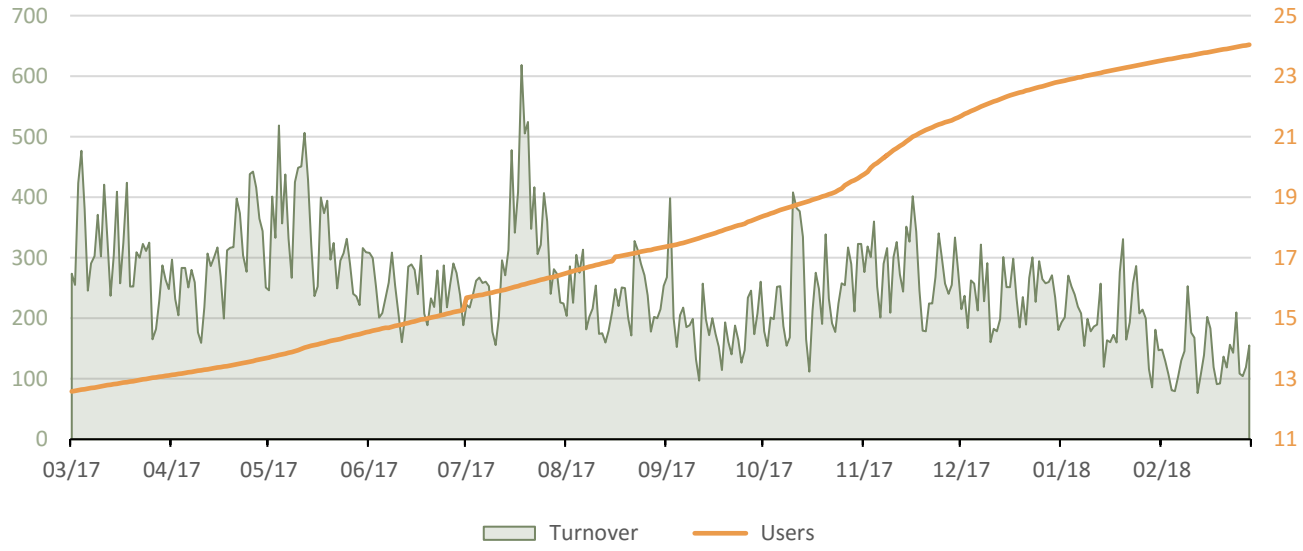
Bitcoin, underpinned by nothing else baring a fascinating idea of a limited coins supply, was proven so popular that, despite its significant price volatility, has outperformed all quoted convertible currencies. This outperformance and the urge to own it, resembled the gold rush to some extent making us second guess whether BTC is actually made of gold. So what might be the problem here, disregarding of course issues, such as; speed of transactions, commissions and price corrections?

Limited Supply

Turnover Reduction

On the one hand, the value of crypto currencies is underpinned by its limited supply and by the progressively increasing complexity of mining. On the other hand, however, the same restriction of supply immediately raises a major issue. The inevitable expectation of deflation (appreciation of the crypto asset against other assets) caused by the increase in mass adoption will in the future lead to a decrease in turnover and cooling of the overall activity. This as the appreciating value of the crypto asset incentivizes saving rather than expenditure or utilization.

Figure 3. Turnover (thousand BTC) and users (million)



Example: if an entrepreneur has $ 1 million and knows that the purchasing power of this asset will decline over time, he/she will invest this money in real estate or another business in order to preserve and/or grow the real value. And if he/she owns 100 bitcoins, which are expected to grow in the long run, he/she will be dis-incentivized to invest them as they risk significant exposure to opportunity cost.

Increasing the gap in the level of savings

The aforementioned, in-built, deflation mechanism of the crypto currencies will inevitably lead to an increase of the socio-economic gap relating to accumulated savings. This will happen as the mathematics of the transaction will keep the proportional deviation constant therefore leading to an ever increasing gap in absolute dollar terms as the assets appreciate.

> *Example: 2 Users bought tokens at rate of 1 USD / token. User 1 bought tokens for 200 USD, and user 2 for 100 USD. If token appreciates 1000% the difference in assets will still be at a ratio of two-to-one but the absolute delta will grow to 1000 USD from 100*

Concentrating wealth in the hands of the few

In currency systems with limited supply, widening of the savings gap leads to concentration of money in the hands of a small group of its most successful members. And, over time, the weight of this group increases with increasing speed. There is, therefore, a risk of a loss of interest of other participants to a specific monetary unit and, as a consequence, the risk of a depreciation of this currency (participants begin to look for other ways of mutual settlements). In order to balance such a system, loans and credits are needed (returns some money back to the system).

Anonymity

On the one hand, the world is moving towards full transparency of processes and transactions. On the other, disputes continue regarding the anonymity of popular crypto-currencies. It goes without saying that preservation of anonymity prevents proper regulation. This means that such a currency will either always be in direct conflict with prevailing Government issued currencies, or will need to find a way to simulate these.

It is also important to note that despite the anonymity of crypto-currency wallets, account verification is necessary for trading on exchanges, and companies conducting ICO's now collect full information about investors (KYC). Thus, owners of such wallets needs to repeatedly re-confirm their identities, as opposed to having one fully verified multi-purpose account / wallet.

Volatility

Limited number of market participants and lack of regulation leads to significant volatility of the conversion rate. Whilst not a problem in terms of long-term investments or short term speculation, this becomes a major issue when the adopting the currency to be used **as a medium of for exchange of goods or services**. How can one effectively set prices in crypto currencies when conducting its trade if prevailing volatility makes it virtually impossible to predict the expected income and or cost?

Consensus

Due to their decentralized nature, blockchain based systems do not have a clear answer regarding rights of data administration. The situation gets ever more complicated by the fact that in an anonymous systems there is no clear connection between the user and the physical person or company.

Consequently, a large mining pool has the ability to take full control of the system running on the most popular consensus today, «***proof of work***». And if it happens, it will not be even possible to identify the invaders.

Possible Solutions

Is it possible to create a currency based on mathematical laws, rather than basing it on a subjective trust in the issuer?

Fixed Supply

There are known suggestions to create a monetary system with fixed, periodic supply. The problem with this approach is that if even the approved supply does correctly reflect the true growth of the underlying economy, the future is still very much uncertain. And as the quantitative coefficient of supply needs to adapt to changes, its triggers and sped (lead, or lag) are very difficult to estimate.

Token withdrawal

As discussed above, the deflation of such crypto-currencies with limited supply can reduce the number of transactions. A known method of systematic withdrawal of tokens from the wallet holders can stimulate activity. Users, however, react negatively to such measures, as in this case tokens do not fulfill another important function of money – **means of saving and accumulation**.

Control of the money supply

If transactions cannot be stimulated by the withdrawal of tokens, there remains the option of a programmed emission that has a decreasing effect on the purchasing power of each individual token. Since it is not possible to monitor the average level of profitability within the blockchain system to identify the optimal level of emissions, it is worthwhile to consider the way of linking emissions to the structure of transactions. This due to the blockchain system's full transactional transparency. The simplest version of this supply mechanism is to release a small number of tokens for each transaction. Thus, the more transactions in the system, the more intensive is the issuance.

Such a system is counter intuitive as monetary stimulation is generally used in economic slowdowns rather than periods of growth. This traditional approach, however, only considers velocity of supply. But when another variable, such as the distribution mechanism, is added this method makes complete sense.

Distribution mechanism

Let's consider an automatic supply algorithm in combination with an intelligent system for its distribution among participants. Thus, new supply, despite reducing the purchasing power of each individual token, does not reduce the value of the aggregate token holding. And, on the contrary, increases it. Which means it is token withdrawal – in reverse.

Example: User 1 has 1000 tokens at 1 $, user 2 has 500 tokens at same price. The system released another 1,500 tokens, but distributed them in proportion to user portfolios. Thus, token value has depreciated by 50%, as supply has doubled, but the value of both user 1 and 2 portfolios had remained the same at $ 1,000 and $ 500, respectively. If the entire issue went to user 1, then he would have 2500 tokens for $ 1250, and User 2 would have be left with $ 250. In other words, user one would have an increase of $250 , whilst user 2 would have seen its wallet value decline by $250. This despite no physical withdrawal of any tokens.

Balancing the savings gap

The simplest version of the proportional distribution between users relative to current balances on their accounts would not change anything, except for the token value.

Consider a method that distributes the new, transactional, issuance in a way that is inversely proportionate to the outstanding balance on user accounts. This solution has several advantages:

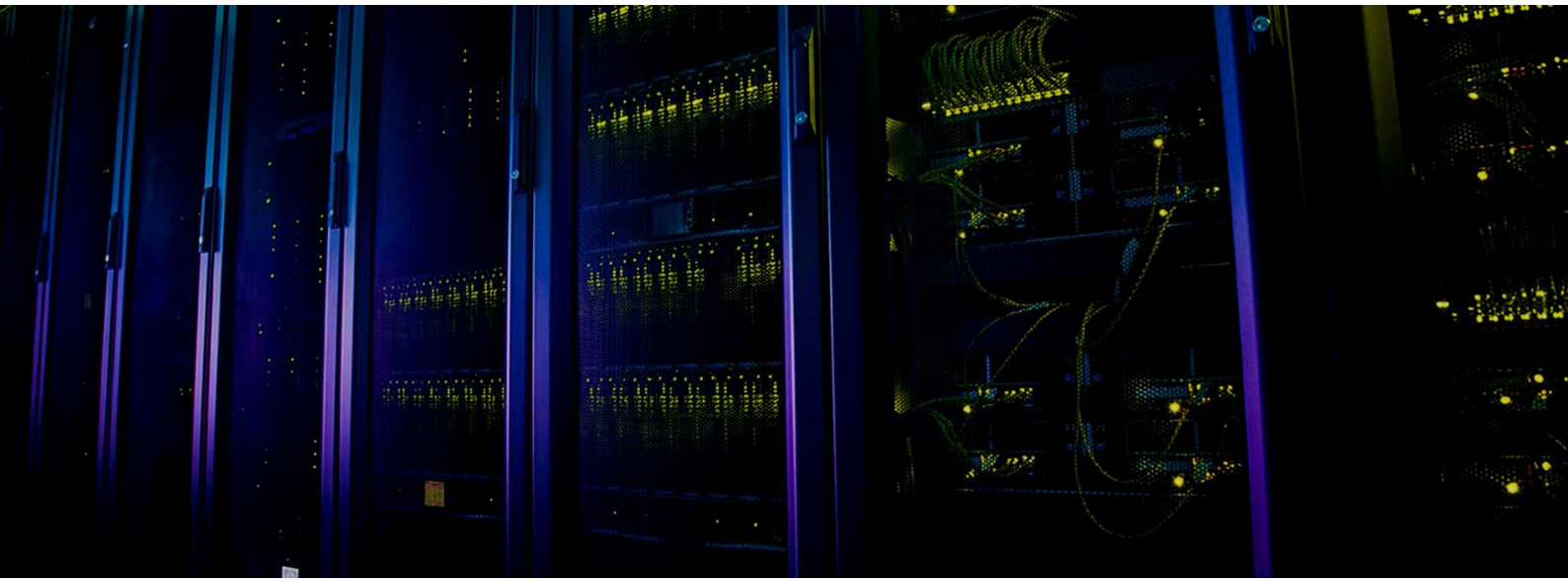
1. Balances the gap in the level of user savings
2. Eliminates the possibility of token concentration
3. Guarantees a certain minimum level of tokens in each wallet
4. Maintains stable demand and solvency of participants in the system

If user's serial number is also written into the mechanism, one can get some similarities to a pension type of payoff, in which early users gain time value advantages over late joiners.

*See «Transaction related supply», **3.1.2***

FIREBIRD platform

FIREBIRD – it is a personalized blockchain monetary system with instant free transactions and the ability to create collective wallets. The main feature of the system is its intelligent, crisis resistant, supply of tokens, revolutionizing our views about structuring of money.



Each FIREBIRD user is verified and can have only one account. Instead of energy-intensive mining farms and heavy nodes with terabytes of information, a small number of high-tech master nodes and storage facilities are used, and the nodes are lightweight applications that can work on any smartphone. Initially "empty", the system is then gradually filled with tokens automatically. The released tokens are distributed among all participants according to an algorithm that takes into account the speed of new users involvement and the specifics of transactions in the system.

Token supply and distribution

As mentioned above, in order to maintain the exchange rate of tokens, supply is needed when the system grows and becomes stronger. So, in FIREBIRD there are 2 emission mechanisms:

1. For when new participant is added
2. For when a transaction is made

Token supply when adding a participant

New token issuance calculated from the average balance on existing accounts occurs with the verification of each new user and is distributed among all participants, including the new user, evenly.

Thus, the number of "E_x" tokens that are emitted per each purse when verifying the next user is described by the formula:

$$E_x = \frac{S_p}{U_k \times (U_k - 1)},$$

where:

S_p – the sum of all already issued tokens

U_k – the number of the user to add

Example: There are 2 accounts in the system. Each account has 75 tokens. When a third user is connected, the system will release 75 tokens (average per person) and distribute them to three participants. As a result, the first and second will have 100 tokens, and the third will get 25 tokens. The more users will be in the system, the less impact will be felt from connecting new members.

Without considering the effect of emissions from transactions, the remainder of «S_x» on a particular wallet at any time is generated in accordance with the following numerical series:

$$S_x = \sum_{U_x}^{U_n} \frac{S_i}{U_x},$$

where:

U_n – number of verified users at a particular time,

U_x – ordinal number of the user,

S_i – starting balance of the first wallet

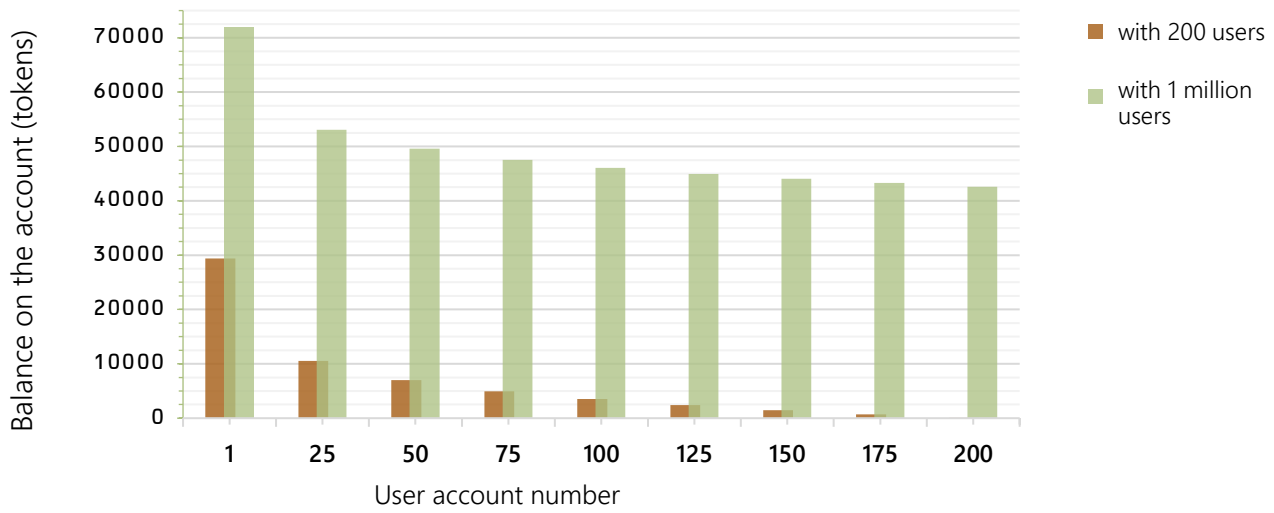
Below is a table of changes in wallet (account) balances with an increase in the number of users, provided that the initial balance of the first wallet is 5000 tokens:

Table 1. Issue of tokens when adding users

Account number	Number of participants in the system								
	1 →	2 →	3 →	4 →	5 →	6 →	7 →	8 →	9
1	**5000**	**7500**	**9166**	**10416**	**11416**	**12250**	**12964**	**13589**	**14144**
2		**2500**	**4166**	**5416**	**6416**	**7250**	**7964**	**8589**	**9144**
3			**1666**	**2916**	**3916**	**4750**	**5464**	**6089**	**6644**
4				**1250**	**2250**	**3083**	**3797**	**4422**	**4978**
5					**1000**	**1833**	**2547**	**3172**	**3728**
6						**833**	**1547**	**2172**	**2728**
7							**714**	**1339**	**1894**
8								**625**	**1180**
9									**555**

The earlier the user has connected to the system, the more tokens they will receive over time. The distribution of tokens by wallets is shown in the following diagram:

Figure 4. Balance of the cohort of the 200 first users



As evident from the formula, the incremental supply relating to new participant addition, exponentially reduces with every new participant and tends infinitely to zero. Here it should be noted that despite a seemingly converging numerical series, especially as viewed from incremental supply for existing users, participant related supply represents a diverging harmonic series.

The aforementioned supply process is similar to the payment of pensions. That is, early users have certain advantages over late users throughout the life cycle of the project, no matter how long it is expected to last. In deflationary systems, this mechanism is implemented by increasing the cost of savings, but, as mentioned earlier, deflation slows down the general economy.

Transaction related supply

Supply related to each incremental transaction is distributed between users who have confirmed the transaction. The system allocates the transaction confirmation to users, according to the balances on their accounts. The distribution, however, is linked to the serial number of the user's main wallet. Thus, the earlier the user connected to the system and the less the balance on his account – the more transactions he gets to confirm and the more tokens he consequently receives from the confirmation of these transactions.

On average, the amount of emission from transactions «$\boldsymbol{E_x}$» for each user will correspond to the following expression:

$$E_x = E_{cp} \times \left(1 + \frac{1}{U_n} - \frac{S_x}{S_p}\right)^{\frac{U_n}{5}} \times \left(1.5 - \frac{U_x}{U_n}\right),$$

where:

E_{cp} – average supply per user in the system,

S_x – number of tokens on the account of user

S_p – number of tokens in the system,

U_x – serial number of the user,

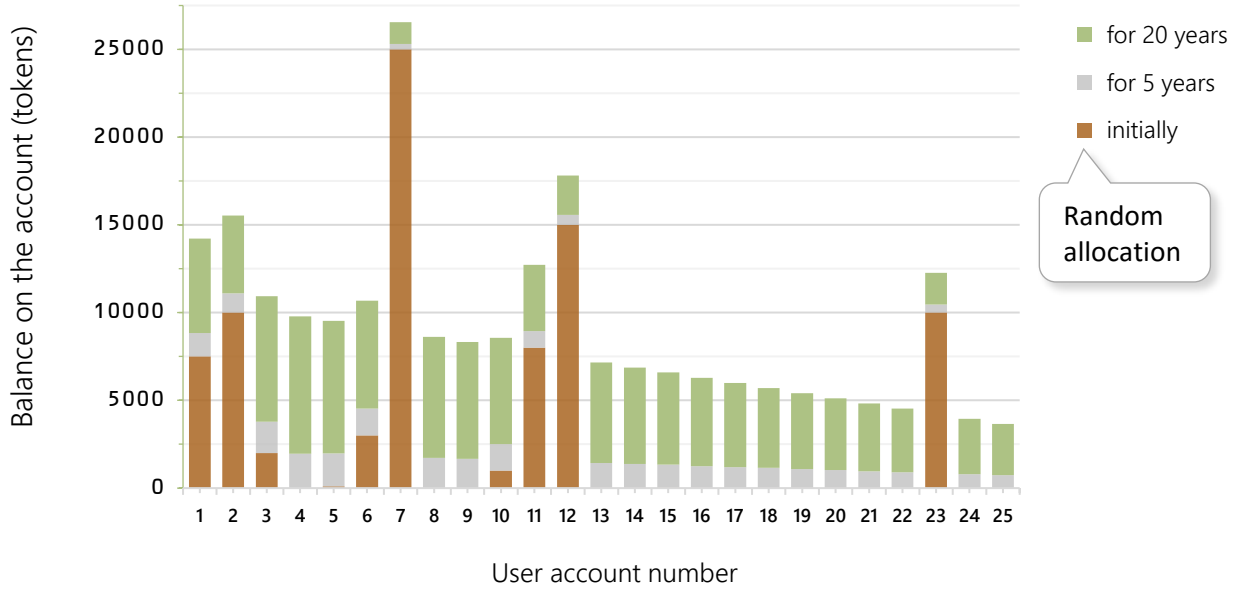
U_n – number of verified users in the system

The average supply of «$\boldsymbol{E}_{\mathrm{cp}}$» is calculated as 0.5% of the total transaction amount divided by the number of users in the system at the time of its execution. Thus, with system turnover at the current crypto-currency market levels, annual supply is expected to amount to 4% of the total.

So, for a system with equal account balances and circular transactions, the gap in the distribution ratio will tend to the number 3.

Chart below visualizes the transaction driven supply mechanism through an example of the first 25 wallets with random balances:

Figure 5. The impact of transactions driven supply on the amount of savings



Periodic decimal fractions

Since the results of calculations can be periodic decimals or transcendental numbers, the system provides rounding up to four digits after the point. This is introduced to simplify the human perception relative to bitcoin and many other crypto-currencies with 6 or more decimal digits. The system will then aggregate transactions and calculate new supply on an aggregated level in order to minimize the rounding error. Aggregation of transactions might take a few hours or up to a month, depending on the turnover.

Price Stability

At first it may seem that FIREBIRD is susceptible to manipulation by users engaging in harmful transactions between their accounts. Back-testing, however, shows that in order to stimulate overall system inflation, these accounts need to operate with very significant amounts of tokens. Moreover, such an activity is strictly uneconomic for the users themselves as the transaction driven supply of tokens will not be sufficient to keep their asset value at previous levels.

Servicing and Development

20% of new token supply is proposed to be directed to master-nodes and storage nodes as incentivisation for system maintenance. For the purpose of making this project easier to comprehend, such calculations are not presented in the current paper.

Wallets and user accounts

Individual user accounts

FIREBIRD Platform token supply / issuance is driven by addition of participants and the volume of transactions between them. For that reason, full verification of users is needed in order to enable the system to function.

This is, however, a double edged sword. On one hand, without verification, the system would not , because of possible manipulations with the number of wallets and harmful transactions. On the other hand, it infringes the crypto-community's quest for anonymity. Having said that, the world does constantly move towards maximum transparency the with many crypto users contributing to this themselves as businesses and personal lives of many people are now almost completely public. Finally, full user verification will allow FIREBIRD to be better integrated into the global economic system.

Either way when connecting to FIREBIRD, each user receives their unique registered account without transfer rights. FIREBIRD maintains confidentiality and does not disclose ownership.

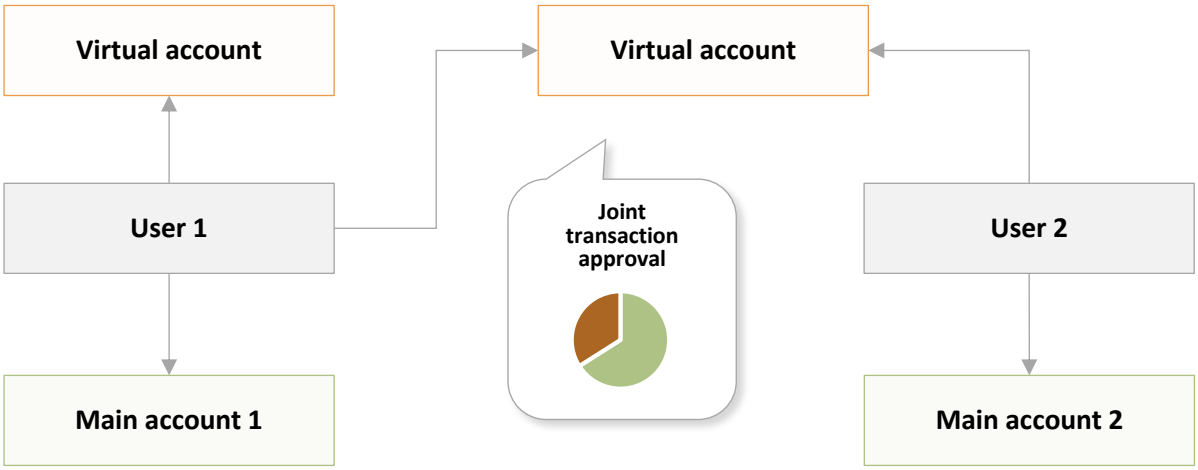
Virtual and shared accounts

For convenience, FIREBIRD platform allows users to create additional wallets besides the main one.

In addition to personal virtual accounts, a mechanism for creating collective ones is also provided. It is convenient for organizing a business partnerships. On the FIREBIRD platform, 2 or more users can create a joint account, specifying share of ownership and legal access and operational rights.

Token supply, in this case, will be calculated based on the total balance of all user accounts, taking into account the share of ownership of these accounts.

Figure 6. Ownership structure of virtual accounts



Example: Users 1 and 2 create a collective account with 50% / 50%. Ownership. At the same time, the account can be configured so that all payments from this account are carried out only upon approval by both users.

Structure of the blockchain

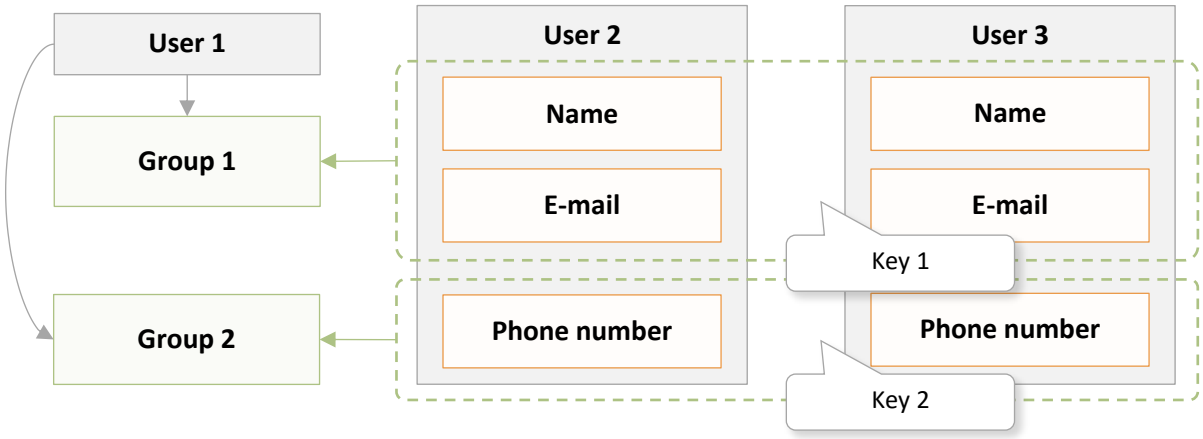
FIREBIRD consists of 3 distributed networks - one user and two transactional networks. Blocks in the system are formed by the forging method every 5 seconds.

User Network

The user network stores information about account holders. A separate block of up to 5 MB allocated for each user. The data in the block is encrypted using an algorithm based on McAliece keys, corresponding to the groups to which the user belongs, as well as the user's own key.

Each group has its own set of user data, which it is able to accesses with its key with the user's permission. The owners of the groups are the users of the platform. Thus, users do not see information about each other by default, but they can provide and access to it by agreement.

Figure 7. Data and groups in the FIREBIRD user network



Transactional networks

2 transactional networks operate on general principles, one of which is public and the other private. Information about transactions in the private network is encrypted, and in the public ne it is available to all users.

In FIREBIRD's transactional networks, master nodes are used for both task allocation and data storage. Thus, the work of the node does not require significant disk space. In fact, every FIREBIRD

user application for smartphones or desktops is a node, which provides the network with significant computing power.

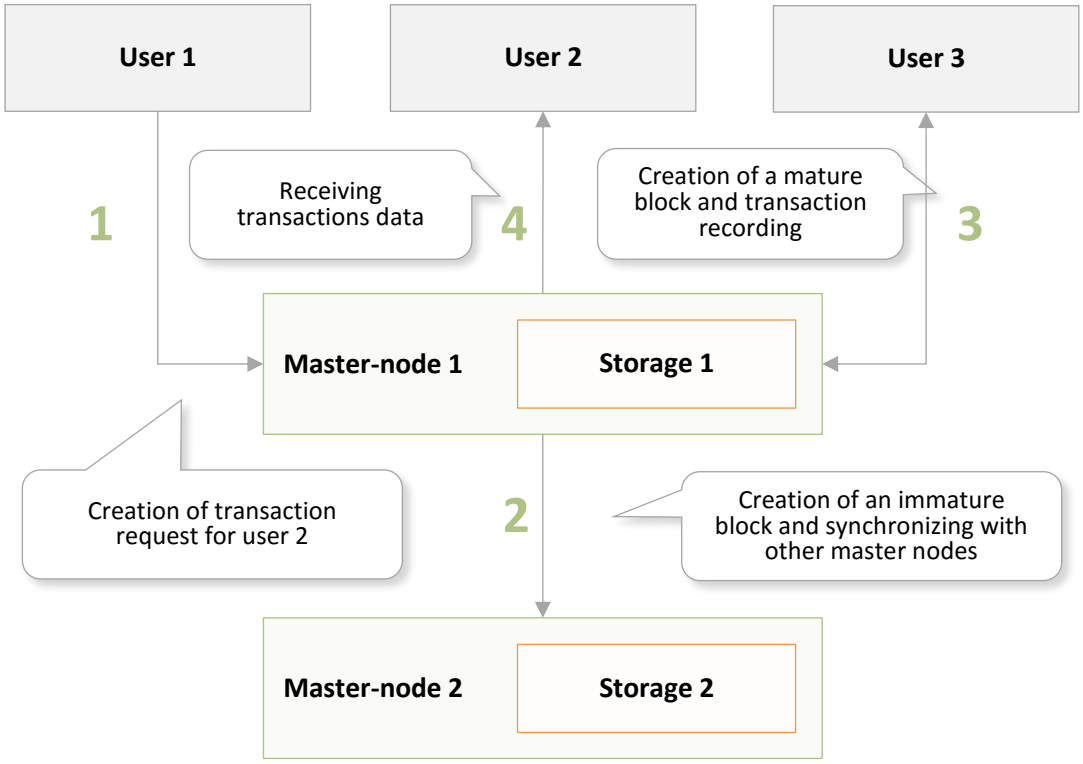
To sign transactions, the ECDSA algorithm is used. Consensus is PoS («***proof of stake***»).

Distribution and appropriation of tasks between the nodes is done by generating a pseudorandom sequence every 300 seconds in such a way that the load on the nodes corresponds to the principles of transactions based token supply.

*See. «Transaction related supply», **3.1.2***

It is important to note that the personification of the FIREBIRD system makes it possible to minimize the risks of data manipulation by its users, and the algorithms used in the networks will be resistant to attacks from quantum computers.

Figure 8. Scheme of the FIREBIRD transactional blockchain



Own tokens and Integration

FIREBIRD provides for the possibility of issuing its tokens by each participant. Moreover, FIREBIRD provides the infrastructure for working with verified users. It is possible to create an isolated system with its own master nodes and storages, as well as integrate it into an existing network.

Roadmap

Q2 2011	Concept formation
Q2 2014	Basic principles for token supply
Q4 2017	General documentation
Q1 2018	Testing of mathematical models
Q1 2018	White paper preparation
Q2 2018	Launching the electronic auction site
Q4 2018	Presale
Q1 2020	**Opening of the public auction**
Q1 2021	**End of the auction and launch of the test network**
Q2 2021	Connection to exchanges and public network
Q3 2021	Launch of transaction based token supply
Q4 2021	Infrastructure for master node connections
Q1 2022	Managing user groups
Q2 2022	Implementation of the mechanism for creating own tokens

Public auction of user accounts

It is widely known that the reason ICO's are able to attract significant user interest is because of time value. In other words users buy at presale or ICO point in anticipation of price appreciation as the token is listed on exchanges. Thus, the ICO mechanism is a perfect example of deflationary expectations in the crypto-currency market. After all, if tokens do not appreciate in price, what would be the reason to buy them early.

As stated earlier, a token that will truly reflect all monetary functions, must overtime, lose its purchasing power. Put simply, it becomes cheaper, and not more expensive.

*The negative impact of deflation on transactions see «Turnover reduction», **2.2.1.1***

How can FIREBIRD attract investments if its tokens do not offer price appreciation? Since, once launched, the main source of value in the system will be a serial number of the user's main account, we have developed a new mechanism of the initial offer – **Open Account Auction (hereinafter, the Auction)**.

The Auction is essentially a process whereby for a limited amount of time, early users get allocated a certain amount of wallets as dictated by the chronological order of their verification and the size of their bids. Bid sizes are not limited. Bids can be increased at any time and through an unlimited number of attempts during the Auction's duration. At the end of the Auction, the system will sort all participants according to the size of their investment and the serial number of their registration.

Auction procedure

1. **In the first quarter of 2020, 1 million FIREBIRD accounts with registered number of 1 – 1,000,000 will be auctioned**
2. **Auction's duration is 1 year**
3. Auction is held on Coordinated Universal Time (UTC±00:00) and is taking place on the electronic platform https://firebird.auction
4. Only first 1,000,000 registered users who have undergone full verification will be allowed to participate
5. Bids are accepted in ETH and in Firebird Auction token (FAT) of which 10,000 were issued and distributed during the pre-sale (contract number 0x2746025ae2eba10c91d1c70393ffb23a58f05911). For the period of the Auction FAT value is set at the following rate: 1FAT = 1ETH.
6. FAT tokens which were acquired by investors during the pre-sale and not utilized for bidding purposes during the Auction, will seize to represent any value immediately post the completion of the Auction. FAT would not be converted to FBD.
7. Auction increment is 0.3 ETH or 1 FAT (FAT tokens don't have any decimals)

8. Assignment of serial numbers of wallets according to the results of the Auction occurs on the basis of primary sorting of participants by the size of the bid and secondary by the registration number. If no bet was made, but the account is verified, it is included in the register with a bid of "0".
9. At the end of the Auction, the system records the total number of wallets, enables their access to the system, calculates and distributes the tokens onto them. Distribution happens such that serial wallet numbers of participants are assumed as from the moment of registration and basing the calculation on the fact, that wallet No. 1 was issued with 5000 tokens.

   *See «Token supply when adding a participant», **3.1.1***

10. If a certain user has used more than one wallet during the Auction to make bids, upon completion, the system will automatically transfer all tokens to the wallet with the lowest serial number. All other tokens are to be distributed (by means of commercial sale of gifting) by these users to third parties who have underwent full verification.
11. Non verified user who has made a bid during the Auction, has 3 months to undergo full verification, but no later than the last day of the auction
12. To pass the verification users will need to provide the following KYC documents: Proof of ID and Proof of Address
13. During the first 11 months of the Auction, bidding users will benefit from a bonus system which adds to the bids according to the schedule provided in the table below

Table 2. Calculation of bonuses based on the results of each month

Month	1	2	3	4	5	6	7	8	9	10	11
Bonus (ETH)	**+ 100%**	**+90%**	**+80%**	**+70%**	**+60%**	**+50%**	**+40%**	**+30%**	**+20%**	**+10%**	**+5%**

Estimates and the total number of tokens

Each “lot” in the Auction represents a wallet with a unique serial number. Thereafter, each lot’s estimate implies the estimated value of the aggregate FBD tokens which would be distributed to that particular wallet immediately post the completion of the Auction.

Planned starting price of the FIREBIRD token as it lists on the first exchange - **$1**.

Below is a table displaying token distribution at the end of the auction as driven by serial wallet numbers and the number of participants:

Table 3. Accounts estimate

	Sequence number of the participant								
	1	10	100	1 000	10 000	100 000	500 000	750 000	950 000
Number of participants	**Balance on the account at the time of auction completion**								
100 000	**60 450**	**46 305**	**34 563**	**23 028**	**11 513**	**0**			
500 000	**68 497**	**54 353**	**42 611**	**31 075**	**19 560**	**8 047**	**0**		
1 млн	**71 963**	**57 818**	**46 076**	**34 541**	**23 026**	**11 512**	**3 465**	**1 438**	**256**

The table above shows that being early reduces financial risk, as early wallets will receive high token distribution even in a case of a meaningful shortfall in the number of participants.

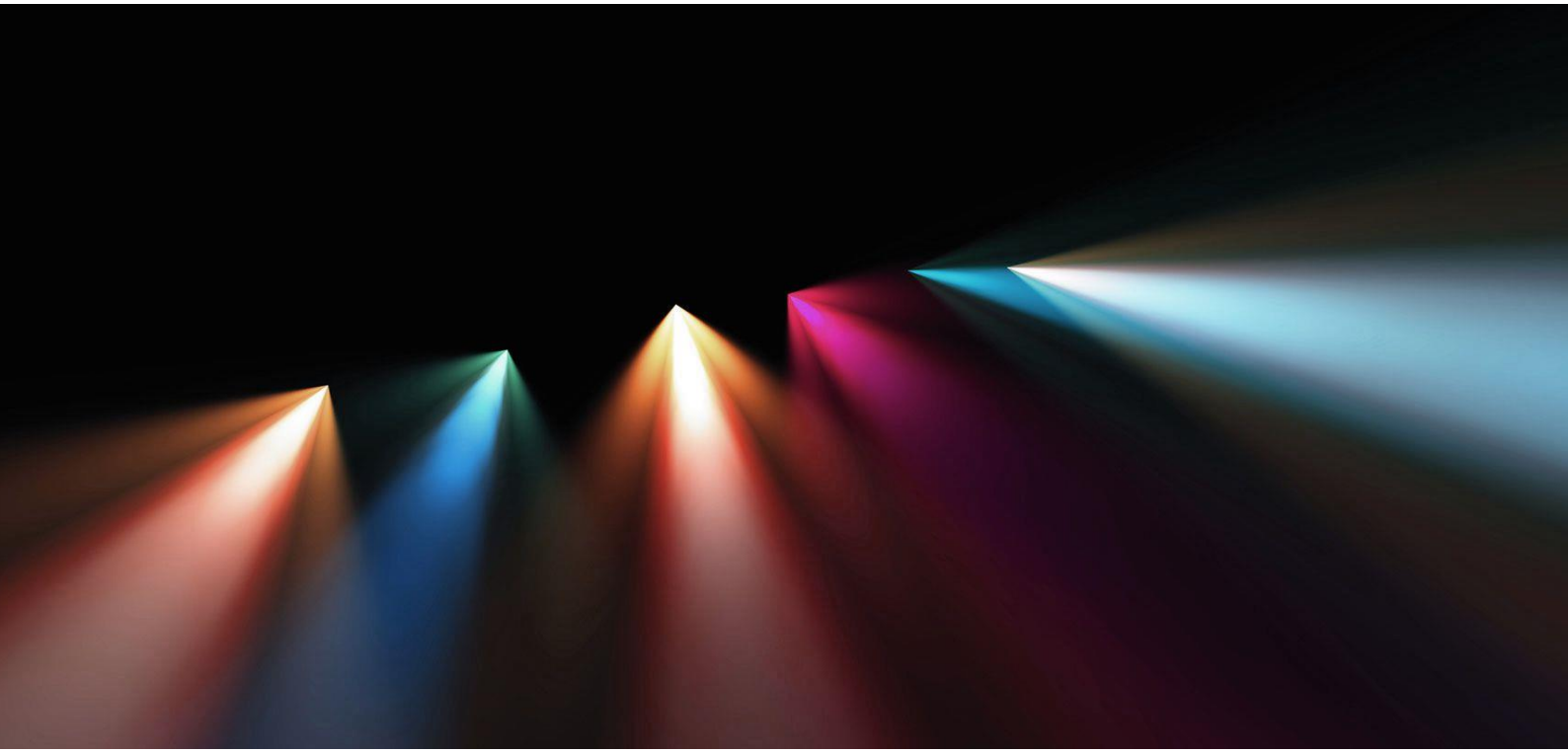
3 Scenarios are taken under consideration:

1. The average of bids for the wallets exceed the estimate. This might mean that participants see themselves as long term users of the Firebird platform. This as the serial number of the wallet will keep its meaningful effect even after the auction and as the system grows.
2. The average bid is on par with the estimate. This might imply that users optimize their risk/reward. Confidence in project success matched by the need to minimize participation risk.
3. The average bid being lower than the estimate. This would mean that the lot is undervalued given that the value of the tokens which will be distributed on that wallet would exceed the value of the bid.

Regardless of the final outcome. The Auction should be considered normal if the distribution of bids is both above and below the estimate.

The Organization

FIREBIRD is headquartered in Switzerland. The organizational structure is formed from users on the basis of a recommendation from at least two active members.



At the time of writing this document, the team consists of 30 professionals with substantial experience in the following areas:

- **Cybersecurity**
- **Mathematical analysis**
- **Accountancy and finance**
- **Web programming**
- **Development of decentralized applications**
- **Management of Internet projects**

Given our prudent approach to the protection of personal data, we do not publish such information about team members until a unanimous decision is taken.

Contacts:

press@firebird.auction – press releases
marketing@firebird.auction – events, events and promotions
team@firebird.auction – questions of participation in the project team
support@firebird.auction – user support