Vlad Cristian
Bucharest, Romania
January, 2018

ChainRepublik

A peer to peer decentralized browser game

Table of contents

1 Introduction 3
1.1 Gameplay Overview 3

2 ChainRepublik Coin (CRC) 4
2.1 Default network address 4
2.2 Network fees 4
2.3 Distribution 5
2.4 Pre-mine and ICO 6

3 Rewards 7
3.1 Reward pools 7

3.2 Player rewards 7
3.2.1 Energy reward 7
3.2.2 Affiliates reward 8
3.2.3 Military reward 8
3.2.4 Political influence reward 8
3.2.5 Political endorsement reward 8
3.2.6 Press reward 9
3.2.6.1 Commenters reward 10
3.2.6.2 Voters reward 10

3.3 State budgets rewards 10
3.3.1 Citizens energy reward 11
3.3.2 Country area reward 11

3.4 Organizations rewards 11
3.4.1 Political parties reward 11
3.3.2 Military units reward 11

3.5 Nodes operators rewards 12
3.6 Conclusion 12

4 Economy 13
4.1 Companies 13
4.1.1 Raw materials and finite products 14
4.1.2 Workplaces 14
4.1.3 Production tools and buildings 15
4.1.4 Production process 15
4.1.5 Markets 15
4.1.6 Licenses 16
4.1.7 Shares and dividends 16
4.1.8 Autonomous Corporations 16

4.2 Energy 18

4.2.1 Energy boosters 18
4.2.2 Long term use products 18

4.3 Rental Market 19

5 Politics 19
5.1 Political influence 19
5.2 Political endorsement 20
5.3 Political parties 21
5.4 The Congress 21
5.5 Laws 22
5.6 Taxes 23
5.7 Bonuses 24
5.8 Traveling 24
5.9 Citizenship 24

6 Wars 26
6.1 Weapons....26
6.2 Military Units....26

7 Press 26
7.1 Followers 27

8 The Network 27
8.1 Addresses....28
8.1.1Addresses profiles 29

8.2 Transactions 29
8.2.1 Escrowed transactions 30

8.3 Messaging 31
8.4 User issued assets 31

8.5 Assets Exchanges....33
8.6 Consensus 33
8.6.1 Hashing algorithm 35

1 Introduction

ChainRepublik is new software. The game is running on its own blockchain. It was written from scratch in the past two years and is not fork of an existing software. It aims to create the first Massive Multiplayer Online Economic Strategy game with no need for a central administrator or central server, where players are rewarded for their achievements.

The distinguishing characteristic of ChainRepublik, which is absent in any 99.9% of existing online games, will be the possibility of monetizing the time spent in the game. In other words, players will be able to not only enjoy the game but also to earn from it, as well. It is and will always be **open source**.

ChainRepublik can be accessed through **web nodes (ex www.chainrepublik.com)**. A web node is a website that allows you to access all ChainRepublik features like sending transactions or securing addresses. A web node is the easiest method of using the network. Running a web node is a great way for players to spread the word about ChainRepublik and make money in the same time.

It's also important to realize the **difference** between the ChainRepublik Coin and the regular 'coins' being launched via initial offerings. 99% of ICO coins or tokens these days are **Ethereum-based ERC-20** tokens or similar. All these startups are still centralized businesses. They normally have an address, an advisory board, a team, CEOs and if the startup goes bankrupt, the value of the **'token'** will tend to zero in no time.

ChainRepublik is a decentralized p2p network of nodes with no company behind and no central server. This makes it impervious to regulation on a global scale. ChainRepublik Coin (CRC) is not a **'token'** but a real decentralized cryptocurrency, powering a virtual world impossible to stop. ChainRepublik **has its own blockchain** and has nothing to do with Ethereum tokens.

1.1 Gameplay Overview

The game is set in a mirror world where players, referred to as citizens, join in local

and national politics where they can help formulate national economic and social policies as well as initiating wars with their neighbours and/or tread the path of a private citizen working, fighting and voting for their state.

Players can participate in a variety of daily activities. They can be employees, own businesses, join political parties, vote in elections, become members of Congress or country presidents, write newspaper articles and even go to war as citizens of virtual versions of real life countries. The network rewards players for their achievements using ChainRepublik Coin (CRC), a limited-supply cryptocurrency.

Usually, upon joining using a web node, a citizen is assigned a virtual country where he / she will play. Each of these countries is named after an actual country in the real world, and is generally located similarly (warfare may cause certain regional displacements). The citizen then seeks employment at a company, join a political party or a military unit and is allowed the opportunity to train as a soldier for that country.

2 ChainRepublik Coin (CRC)

ChainRepublik Coin (CRC) is the cryptographic currency underlying the network. For any service or transaction, users will pay a small fee in MaskCoin. The number of coins is limited to **21,000,000** which will be slowly distributed to miners and content creators.

2.1 Default Network Address

Unlike other networks like Bitcoin, where a small amount of coins is created every day, in ChainRepublik all coins are created on the first block and stored in a special address called **Default Network Address**. This address does not have a private key and is entirely controlled by the software. Default Network Address receives all user-paid fees and distributes rewards to miners and players every day.

2.2 Network Fees

As mentioned for any transaction / service, users will pay a fee. Fees are essential to avoid spam attacks. Fees vary depending on the service used. Unlike other systems, in ChainRepublik, fees **do not go to miners** but go to Default Network Address. Miners will always be paid by network, not by users. Below are some examples of fees

• Sending coins to another address - 0.1% of amount sent

• Sending assets to another address - 0.0001 CRC for every unit of asset sent

• Running a company - 6 CRC / month

• Openig a workplace for your company - 3 CRC / day

On top of this, all addresses will pay a fee of 0.0001 CRC / day (~1440 blocks) if their balance is less than 0.1 CRC. Empty addresses will be removed from the distributed ledger and will be reincluded when they receive funds. This fee is essential to get rid of inactive addresses holding very small quantities of CRC. Scalability is the team number one priority.

2.3 Distribution

Every year, the network uses **5% of undistributed** coins to reward miners and players. This means **~ 0.013% / day** of the undistributed amount. The maximum annual inflation rate is 5%. Because in the first years the undistributed quantity will decrease every day, the rewards pool will be smaller and smaller each day.

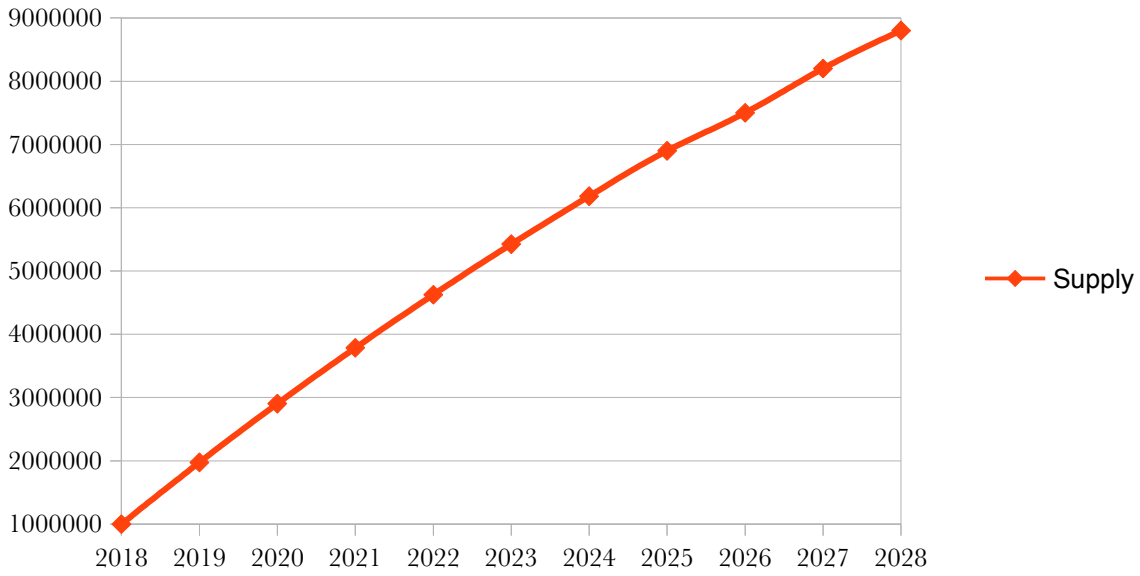
For example, block reward decreases 0.0001 CRC every two blocks. Undistributed coins are held by Default Network Address. This address' balance will never reach 0 CRC because it will distribute fewer and fewer coins. Sooner or later, the earnings of this address (from the fees) will be higher than the rewards paid to users. There are 3 scenarios:

- The default address spends more coins that receives from fees - rewards decrease each day
- The default address receives the same amount of coins it spends - the rewards tend to remain unchanged
- The default address receives from fees more than it spends on rewards - rewards tend to increase every day

In the long run, the revenue / spending of Default Network Address ratio will tend to 1. Initially, the default network address will hold 20.000.000 coins (1.000.000 reserved

for ICO, bounties and the developers). In the first year, a maximum of 975.477 coins will be distributed. This quantity will gradually decrease, and in 2027 only 621.972 coins will be distributed. This is the extreme case where the default address has no revenue. Depending on the revenue received, the amounts distributed will be slightly higher. But never more than 5% of the default network address balance will be distributed per year.

Below is a chart showing the **maximum available supply** of coins in the next 10 years (in case the default network address has no income which is impossible). In case fees amount become really high due to increased adoption the total supply will tend to remain unchanged from year to year.



2.4 Premine and ICO

At block 0, **1.000.000** coins (**3%** of total number of coins) will be deposited in ICO participants addresses / bounty participants / developers address. ICO will be launched in June, 2017. The funds received will help the team develop the project and ChainRepublik ecosystem in the following years. Our target is to sell 800.000 coins during ICO. **All unsold coins will be deposited in developer's address.** Also 100.000 coins will be used to reward testnet players depending on their final CRC balance. Another 10.000 coins will be used for bounty campaign.

3 Rewards

Unlike other decentralized networks like Bitcoin where **all** newly created coins are used to reward miners, in ChainRepublik miners **receive only 10%** of the newly created coins. The rest of 90% are used **to reward players**, or other entities such as state budgets or political parties. A regular player receive **6 types of rewards**. State budgets, political parties or military units are also rewarded.

Miners are rewarded after each block created. The rest of the users are rewarded every 1440 blocks (~ 24 hours). Payment of rewards is hard-coded in the network code and is done automatically based on clear rules without any outside intervention.

3.1 Rewards Pool

Every 24 hours, the network rewards players for their performance. Every year 5% of the remaining undistributed coins goes to players and miners. The total daily reward pool is calculated by formula DailyPool=U/20/365, where U is the amount of undistributed coins. Each reward has its own pool. Because the ChainRepublik Coins number is limited to 21 milions and the amount of undistributed coins decreases each day, total reward pool become smaller every day. In the first years the total reward pool will be ~2650 CRC / day. In 2028 the daily reward pool will decrease to around ~1500 CRC / day.

3.2 Players rewards

Regular players receive six types of rewards based on their character performance like energy, political influence and so on. Each reward has its own pool calculated as a percent from total daily reward pool.

3.2.1 Energy reward

Energy is the main users indicator. Players increase their energy level by consuming instant energy boosters like food or drinks or by using items like clothes, jewelry or cars. Players automatically loose 4% of their energy every hour but they also loose energy when working, fighting, traveling or doing other activities. The energy reward pool is **10% of total daily reward pool or ~265 CRC / day.** Players will receive a small amount coresponding to their energy level. For example if the total players energy is 340.000 points, a player having an energy of 23 (at distribution time) will receive 0.015 CRC.

3.2.2 Affiliates Reward

An affiliate is a player who has used the link of another player to sign up. In order to motivate users to bring their friends / other players into the game, we implemented a network level affiliate program. This means that the network will automatically reward players based on the energy of the affiliates they own. The affiliate reward pool is **10% of total daily reward pool or ~265 CRC / day.** Let's say the total players energy is 340.000 and your 40 affiliates have a total of 900 energy. You will receive 0.66 CRC each day from network. This is why we motivate players not only to bring new players to ChainRepublik but to **help them increase** their energy as much as possible.

3.2.3 Military reward

Countries will go to war from time to time. When players fight in wars they increase their war points (military influence). Depending on war points players are assigned a military rank. There are 10 military ranks from Private to General. The network rewards players depending on their military rank. The war reward pool is **10% of total daily reward pool or ~265 CRC / day, each ranks having a 10% stake.**

To better understand how this reward is calculated we will give you a simple example. Let's say the there are 230 players having the Private rank and only 41 Sergeants First Class. The Privates allocated pool will be 26.5 CRC so each private will receive 0.11 CRC daily. The sergeants pool is also 26.5 but each sergeant will receive 0.64 CRC daily.

The military reward is reset when players change citizenship.

3.2.4 Political Influence Reward

When players work their political influence increases depending on the energy spent working. For each point of energy they spend working, their political influence increases 1 point. Political influence decreases automatically 1% / day. The network rewards players by their political influence. The political influence reward pool is **10% of total daily reward pool or ~265 CRC / day.**

Political influence in reset if a player changes citizenship or moves to another political party.

3.2.5 Political Endorsement Reward

Each country has a 25-member congress. Members of the congress are regular players. The top 25 players by political endorsement form the congress. When a player endorses you to become a congressman, your political endorsement increases depending on the player's political influence. The network rewards players by their political influence. The political endorsement reward pool is **5% of total daily reward pool or ~132 CRC / day.** To better understand how this reward is distributed, we will analyze an example. Let's say 20 players having a total political influence of 3500 endorse you to become a congressman and the total player's political endorsement is 540.000 points. You will receive 0.84 CRC daily.

3.2.6 Press Rewards

Players can write articles and articles can be voted by community. The network rewards content creators depending on how many votes their content received. Not only the number of votes but the vote's power count also. A vote's power depends on voter's energy and time of vote. The votes power formula is

$$P = E-(0.07 * T * E/100)$$

P=Final vote power

E=Voters's energy

T=Number of blocks since the content was created

Basically a vote's power decreases 0.07% / block. If you vote on an article the first hour after it is published, the voting power is higher than if you voted the same article 5 hours later. It's a little complicated concept so we need a good example to better understand the the logic behind the above formula.

Let's say you write an article that's voted by 3 players :

- Player 1, has 10 points of energy and voted your article after 30 minutes. His vote's power is 9.79

- Player 2, has 20 points of energy and voted your article after 10 hours. His vote's power is 11.6
- Player 3, has 100 points of energy and voted your article after 23 hours. His vote's power is 3.4

As you can see a player having 100 points of energy will have a lower voting power than a much smaller player, because he voted much later. Overall your article was received 24.79 voting points. This is important because the network rewards content creators based on how much voting points their content received. The press reward pool is **10% of total daily reward pool or ~265 CRC / day.**

To better understand how this reward is distributed, we will analyze an example. Let's say 200 articles were published in the last 24 hours. The total voting points received was 8900 points. Your 24.79 article will be rewarded 0.71 CRC. But you will receive only 50% or 0.35 CRC. The rest will be used to reward voters that helped the article win this amount.

3.2.6.1 Commenters Rewards

The same rules applied to articles apply to comments. Players can comment not only on articles but on many other categories of content like the laws proposed in the congress. Comments are voted by other players and the votes cast will be rewarded. They have their own reward pool, of **5% of total daily reward pool or ~132 CRC / day.** Just as with articles, half the bonus goes to the voters.

3.2.6.2 Voters (curators) Rewards

As explained above, voters are also rewarded by the network. They earn half the amount received by the voted content. For example, if an article wins 1 CRC, half will go to voters depending on each vote power. Above we explained how the vote power is calculated.

Voters can also down vote content. Those who down vote an article / comment are also rewarded based on their vote power.

3.3 State Budget Rewards

Not only citizens are rewarded by the network but also state budgets. State budgets

receive two reward. The first is the citizens energy bonus and the second is the area reward.

3.3.1 Citizens Energy Reward

This bonus is paid to the state budgets according to the total energy of the citizens in the country. The country area reward pool is **5% of total daily reward pool or ~132 CRC / day.**

In case a country is under **occupation**, this bonus will be received by the attacker. For example, if Canada is occupied by Columbia, this bonus will be paid to Columbia State Budget, instead of Canada.

3.3.2 Country Area Reward

This is the only fixed reward and depends on the real world area of a country. The country area reward pool is **5% of total daily reward pool or ~132 CRC / day.** For example, virtual Russia will receive the biggest reward because it has the largest surface in the real world. The total area of countries in ChainRepublik is ~134.000.000 km2. Russia has 17.000.000 so it will receive ~16 CRC daily.

In case a country is under **occupation**, this bonus will be received **by the attacker**. In our example, if Russia is occupied by China, this bonus will be paid to China State Budget.

3.4 Organizations Rewards

Organizations are also rewarded by network. There are two types of organizations : political parties and military units. Each of them receive **5% of total daily reward pool or ~132 CRC / day.** The reward depends on organization size.

3.4.1 Political Parties Reward

Political parties receive **5% of total daily reward pool or ~132 CRC / day.** The reward depends on total political influence of party members. A big party having influent members will always receive more than a small party.

3.4.2 Military Units Reward

Military units receive **5% of total daily reward pool or ~132 CRC / day.** The reward depends on total military influence of unit members.

3.5 Network Nodes Reward

Those who run network nodes are also rewarded by network depending on users total energy. Network nodes operators units receive 10**% of total daily reward pool or ~265 CRC / day.** To better understand how this bonus is obtained, below are the steps performed by a network node when a new citizen registers

1. A new address is generated. It determines the country where the player lives based on the IP.
2. The node software checks if the player has used a referrer link of another player and retains the referrer address.
3. The node registers the address with the data obtained above, namely the citizenship, the location and the referrer address. **The node also sets the address as being registered under its own address** in order to receive the daily bonus from the network.
4. Finally, if the node offers any bonus to the new members then that bonus will be paid to the newly registered address.

Node operators have all the interest to maintain a high level of energy for everyone who plays ChainRepublik using their server because a high level of users energy means a bigger network reward.

3.6 Conclusion

In conclusion, a wide range of players and other entities are rewarded daily by the network. This money is extremely important because it provides a constant source of income for the players and a breath of air for the game economy. From our experience, without constant rewards, the economy would have been blocked sooner or later. Rewards are automatically paid by the network without anyone's intervention and except for the miners bonus, they are paid every 1440 blocks.

4 Economy

The economy of ChainRepublik simulates a real economy. There are companies, jobs, raw materials, production equipment and, of course, workers. Absolutely all

items in the game are produced by decentralized virtual companies. The role of the economy is to deliver products that maintain the energy of the players.

4.1 Companies

Companies are the most important aspect of the economy. Companies use raw materials, labor and machinery to deliver finished goods and pay taxes to state budgets. Most finished goods are used as raw materials by other companies. A paper-producing company needs cotton, while cotton-producing companies use electricity, and so on. There are over 40 types of companies selling from basic utilities such as electricity to companies that self-administer as autonomous corporations.

Anyone can open a company if they have a small amount to make the initial investments. The registration of a company costs 6 CRC / month, but the investment is not limited to this fee. A company needs raw materials, production licenses, machinery, and a building in which to operate.

Companies belong to a country and pay the taxes imposed by the country congress. A player may hold companies in more countries.

4.1.1 Raw materials and finite products

There are over 200 types of products that companies can produce in the game. Companies use between 1 and 8 raw materials and generally produce a single final product which is usually a raw material for another company. There are exceptions such as electricity that does not need raw materials to be produced, or clothing companies producing 18 kinds of products.

That is why many companies can not exist without others. A cloth-producing company needs material, and a material-producing company needs cotton and so on. There is a very close link between companies. Because investments to own more companies are large enough, an entire community of entrepreneurs is needed to fully support the economy.

The products are divided into 4 categories. Raw materials, production machinery, production buildings and consumer goods. Consumer goods such as cigarettes directly increase the players' energy.

Consumer goods are also of two types. Those that increase energy on the spot and can only be used once, such as cigarettes, beaters or beverages, or durable goods that provide players with small amounts of energy each day for at least 30 days. Long-term use goods can also be leased by players to other players.

Another important rule is that only companies are allowed to sell products. Players can not sell products but can only rent their consumer goods.

4.1.2 Workplaces

To operate a company needs workplaces. A company can have an unlimited number of workplaces but the maintaining fee of a new workplace costs 3 CRC / day. This fee, like other network fees, goes to the default address, not to the miners. A workplace has a finite product associated and a single worker can use it at some point. Company manager must set a wage for each workplace. Minimum wage was set to 0.0001 CRC / hour. Workplaces can not be manually closed. They will automatically be removed by network when they expire if they are not renewed by the administrator.

4.1.3 Production Tools and Buildings

Companies also need production equipment. Each type of company needs another type of production equipment. There are over 40 types of machines. The production equipment has a limited life span and expire after a certain number of finished products delivered by the company.

For example, the utilities for energy production expire after 10,000 kw while the construction companies' tools expires after only 10 apartments built. Production tools are also produced by the game companies.

Companies also need factories (buildings) to function. The factories are built by construction companies. As with production tools, there are over 40 types of factories for each type of company. All factories have a fixed life span of 100 days, regardless of the production delivered during this period of the company. As with tools, factories are automatically removed from the company inventory when they expire.

4.1.4 Production process

When a company has raw materials, production tools, factory building, workplaces

and money for salaries, the production process can begin. Production processes are initiated by workers (other players) who decide to work at a particular firm.

Depending on the energy, a player can work between 5 minutes and 8 hours. During this time, the workplace is busy and can no longer be used. It is released automatically after the work process ends. Players will loose 1 point of energy for every 5 minutes of work. A 60 minutes work process will consume 12 points of energy.

When the work process is initiated, several actions take place simultaneously. First, determine the amount of finished product that will be created. This quantity depends exclusively on the duration of the work process.

Then a certain amount of raw materials are consumed and taken from the company inventory. Also the production equipments are used in accordance with the production delivered, the worker is paid the appropriate salary and finally the finished products enter the company inventory.

All these processes take place one after the other and last for a fraction of a second, but the workplace will remain stuck for up to eight hours after the process can resume.

4.1.5 Markets

In order to buy raw materials and machinery, companies need markets. For each type of product there is a decentralized marketplace where companies / players can trade that product. At present over 200 markets are active. On all those markets, the default currency is ChainRepublik (CRC), meaning traders will need CRC to participate.

Not all types of traders can trade on a particular market. For example, only clothing companies can sell on the pants market and only citizens can buy pants from this market. An exception is made by autonomous companies that can buy or sell any product.

To trade, market participants place orders to buy or sell at different prices. The network will match these orders, and automatically transfer products / coins between participants. Placing an order costs 0.0001 CRC / day.

4.1.6 Licenses

To start producing a particular product, companies also need production licenses. Most companies can only produce one type of good, but others such as clothing companies can produce over 15 types of items and will need a production license for each one.

Production licenses cost 3 CRC / month and are leased from the network for at least one month after which they must be renewed or the company will lose the right to produce the product associated with the license.

4.1.7 Shares and dividends

When a company is born, 10,000 shares are created and transferred to the company's administrator. Also, a decentralized market is created where company shares can be traded.

Company shares are in fact simple assets and can be transferred exactly as regular assets or coins. When the company expires, the shares are removed along with the associated market.

When the company's manager withdraws money from the company, the withdrawn amount is distributed to all those who hold shares based on their percentage of ownership. Revenue from dividends is taxed by state budgets.

4.1.8 Autonomous Corporations

Autonomous corporations are companies driven by software. They can be programmed to be anything from organizations with special rules to banks or casinos. You can program these companies using JavaScript, one of the most popular programming languages.

In order to completely isolate the corporation's custom code from the network and local computer, we developed a virtual machine called the ChainRepublik Virtual Machine (CVM) that runs the code contained by the autonomous companies in a 100% secure and isolated way.

Autonomous companies have extended rights compared to a normal company. They can access any market, initiate transactions with any product or asset, send messages or even emails in the real world (they use the node services where they run for this function). Another feature of autonomous corporations is that they do not require production tools, buildings or workplaces. They also don't need production licenses because they produce nothing. They are the perfect equivalent of services companies in real world After all, developed real world economies are largely based on services not on agriculture or industrial mammoths.

The corporations code can be set to run at regular intervals or when an event occurs such as receiving a transaction or message. To avoid situations where the code rolls into an infinite loop or consumes CPU resources that would endanger the machine that runs it, every virtual machine instruction has attached a cost, paid in electricity. Basically, after each run, a autonomous corporation will pay more or less energy depending on code complexity. A simple assign instruction like 'a=5' for example consumes only 0.0001 kw of electricity while sending a message consumes 1kw. In case the company runs out of electricity the network will deactivate the code and refuse to run it until the company buy more energy.

Programming and testing of the code executed by an autonomous company can be done online using any web node. Normally, the code of an autonomous company can be changed at any time by the administrator, which is a serious security risk. Imagine a virtual bank where citizens deposit their precious coins or assets. If the administrator has full access to the code, he can change it at any time to send all funds to an external address and then “disappear”.

Fortunately, this problem of trust can be avoided by **sealing** the company's address. The administrator can seal the company address and from that moment he will completely lose access to the company. He will not be able to make any changes to the code. Also any other action such as company name change or raw materials acquisition will also be rejected by the network. An autonomous corporation with a sealed address operates 100% independent and it's code once reviewed by a specialist can be fully trusted by any player.

This is a brief presentation of autonomous companies. Things in reality are much more complex, and the documentation on autonomous companies is quite large.Almost 25% of ChainRepublik code deals with autonomous corporations impementation. Autonomous companies will be launched in July after being extensively tested.

4.2 Energy

Energy is the most important indicator of a citizen. A zero-energy citizen can not do anything. Maintaining a high level of energy is essential for any player. Without energy ChainRepublik can not be played. Energy is obtained from the consumption of products that immediately give you energy such as cigarettes, food or beverages (the so called energy boosters). It can also be obtained by using goods such as clothes, cars or homes. At the same time, energy decreases after almost any action such as work, writing an article or simply voting the content. Also the energy decreases by 4% / hour, even if the citizen has no activity. A relatively cheap way to get more energy is to rent products such as clothes or cars.

4.2.1 Energy boosters

Products that provide instant energy after being consumed are called energy boosters. There are 3 categories of energy boosters. Cigarettes, beverage and food. A player can consume only one type of booster energy per day. For example, you can earn a single pizza every 24 hours (1440 blocks). Immediately after consumption, the product is removed from the inventory. Energy boosters are perfect when you need fast energy, like in wars.

A special product is wine. Once it's bought wine increases its energy supply by 0.7 points / day. A bottle of wine that is consumed immediately will provide 5 points of energy. A bottle of wine consumed after 10 days will provide over 12 energy points. After 3 months, it will provide over 70 points.

4.2.2 Long term use products

Another category of products are the products that provide small amounts of energy every day, such as clothes. There are 5 categories of such products. Clothes, belts, cars, homes and gifts. After a while, those items expire and will be removed from the citizens' inventory. For example clothes expire after 30 days, while homes after 6 months.

These products provide fixed amounts of energy after each block. For example, a coat provides 0.0040 energy points after each block (~ 1 minute). Another advantage of long-time products is that they can be leased to other players and as energy boosters can be donated. Renting products such as homes could be a serious source of profit for the players.

A special type of product is the gift. Gifts provides 10 points of energy / day and increases the energy of owner to 25 points when first received. Gifts were designed as a perfect welcome product for new players and can be donated only to new addresses.

4.3 Rental Market

As mentioned, players can't sell products. They can only donate or rent them. To allow players to rent their products, we have created a special rental market. On this market, any owner can rent out long-lasting products such as homes or cars. When they are rented, the products do not disappear from the player's inventory but the owner can not use them for the duration of the rental. The products can be rented for a maximum of 6 months. In case they expire sooner, the maximum rental period will be reduced. Rental income is taxed on state budgets.

5. Politics

The political module allows any player to participate in political life, become a member of a political party or even be elected congressman. In ChainRepublik there are no elections, the members of the congress being elected according to the support received from the citizens. Citizens can grant / withdraw the support of a candidate whenever they wish. The political module offers equal chances to all players. The only condition to enter politics is to become a member of a political party.

5.1 Political Influence

Political influence is a particularly important indicator. When citizens endorse another players to the congressman position, they do so on the basis of political influence. For example, if your political influence is 1000 and endorse a single player he /she will increase their political endorsement points by 1000. If you endorse 3 players, each of them will receive 333 political endorsement points.

Players are also rewarded on the basis of the political influence they have every day. Increasing political influence takes place when you work. After each work process, the political influence of a player increases depending on the energy consumed to work. For example, if the player loses 12 points of energy working, then his / her political influence increases by 12.

Also, the political influence decreases daily by 1%. As it gets higher and higher,

players will have to work more and more to grow it. Because a player can not work more than 8 hours a day, up to 96 points of energy can be consumed by working. This means that the maximum value of this indicator is 9600. At 9600 points, the indicator decreases by 96 points / day and can no longer be raised, and in order to maintain this level a player has to work every day for 8 hours without a break - just like in real life :).

To avoid the situation where a group of players with high political influence move from one party to another in order to execute a PTO (political take over), the political influence is reset to zero if a player moves to another political party. For the same reason, political influence is reset to zero when a player changes his / her citizenship.

5.2 Political Endorsement

Political endorsement is another very important indicator. Based on it the congress is formed. The top 25 players according to political endorsement enter the congress and have the right to propose / vote laws. The network also rewards players according to political endorsement. Political endorsement is recalculated to every 1440 blocks for all players.

This indicator increases when a player supports another player at the congress. As a general rule, players can only support players who are members of the same party as they are. For example, if you are a member of the US Democratic Party, you can only support members of the Democratic Party.

Players can endorse a maximum of 5 other players and have the option to reject a particular player (negative vote). As explained above, political endorsement points rise / decrease depending on the political influence of endorsers. For example, if a player with a political influence of 1000 votes 4 candidates, then each candidate receives 250 extra political endorsement points. When a player moves to another political party, his / her political endorsement is reset to zero. Also, all votes given to other players are deleted. The same happens when a player changes his / her citizenship.

5.3 Political Parties

Political parties are the core of political life. Political parties are predefined and bear the names of real-life parties. We have Democrats and Conservatives in the US, the Liberal Party plus 5 more parties in Canada and so on. Political parties can be created / removed / changed only by a network hard fork.

Political parties are rewarded by the network every 24 hours based on political influence of members. The political parties are managed through the vote of the members. Not all votes are equal. Members vote power depends on voter's political influence. Proposals are adopted by a majority of 51%. The voting process takes 24 hours. If a proposal is approved, the network will immediately execute the requested changes.

Members can propose four types of changes.

- ✔ Members can propose the change of party's description or avatar image.
- ✔ Members can propose the transfer of funds / assets from the party's address in any other address.
- ✔ Members can vote on the distribution of a certain amount of CRC from the party's address to all members. Distribution is based on political influence.
- ✔ Members may also propose that a particular article become an official political statement of the party.

These above proposals can only be initiated by the top 10 political party members by their political endorsement. The member with the highest political endorsement becomes the party's official president. All political parties are disabled by default. In order for a party to become active, it need at least 100 members having a total of at least 100.000 political influence points.

In case a party is disabled, no changes can be proposed.

5.4 The Congress

Congress is the most important organization in a country and has the complete power over state budget, taxes and bonuses. Congress can also start wars. As we have already mentioned, a country's congress is made up of the top 25 players by political endorsement points. All congresses are initially disabled.

Congress is only active in countries with at least 500 citizens and a minimum of 1,000,000 total political influence points. For example if a country has 400 members having 2.000.000 total political influence points, the congress will be disabled. Same will happen if a country has 2000 citizens having a total of just 800.000 political influence points.

Congressmen have the right to propose / vote for a wide range of laws. The vote is based on political support. In order to avoid monopoly situations, at the time of voting the political support of a congressman is limited to 20% of total congress voting power. To better understand this concept we will analyze an example. Suppose the 25 members of a congress together have a political support of 1,000,000 points, and one congressman has 400,000 by himself. His vote's power is limited to 200.000 (20%) so he will vote with 200.000 points instead of 400,000.

5.5 Laws

As we mentioned the congress can vote for a wide range of laws. Laws are approved when 51% of voters approve the law. The votes are not equal but depend on the voter's political endorsement. The voting process takes 24 hours but if the law is approved by at least 51% of total congress voting power, it will be considered approved even if the law was proposed less than 24 hours.

For example, if a country's congress members have a total voting power of 1,000,000 points and a law receives approval 510,000 points, it is considered approved and the network will immediately implement the changes even if the law was proposed just one hour ago. Such a law is called emergency ordinance.

Below are the types of laws that can be proposed

- ✔ Change of taxes. Congress may propose to change any tax. Changes are expressed as a percentage. The minimum tax is 0% and the maximum is set to 25%.
- ✔ Change bonuses. Congress may propose the change of any bonus. Bonuses are expressed in absolute value and paid only in CRC.
- ✔ Honorary citizens. Congress can make a honorary citizens any citizen of the country. In general, the congressman will proposes a list of citizens to be included in this category. Only honorary citizens are eligible to receive government bonuses. Do not confuse the bonuses granted by the government with the bonuses granted by the network. The congress can also vote to withdraw the title of honorary citizen to any citizen.
- ✔ Rewards. Congress can give a fixed one time reward to all honorary citizens. Every citizen will receive the same fixed amount. Payments are made in CRC

only.

- ✔ Purchase of military equipment. Congress may propose the acquisition of military equipment such as bombers, missiles or warships.
- ✔ Deploying military equipment to various areas. Congress may order moving military equipment such as warships to various conflict zones. Moving military equipment is because the majority have a limited range of action.
- ✔ Order an attack. Congress can order attacks during wars, such as air attacks, or missile attacks.
- ✔ Start a war. Congress can start wars against any country.
- ✔ Movement of funds. Congress may order a payment from the state budget of any sum to any other address.

5.6 Taxes

In ChainRepublik there is a wide range of taxes. Citizens pay 4 types of different taxes. Companies pay only a sales tax. Taxes are paid in the CRC when citizens / businesses collect money. The money are deposited into the state budget automatically by the network. Charges are expressed as a percentage of the collected amount and can be set between 0% and 25%. Congress is the only one to change fees. Below are the types of taxes.

- Wage tax - the wage tax is paid by all citizens when they receive their salary.
- Rental tax - the tax is paid when a citizen rents a good and receives the money.
- Rewards tax - this tax is paid by all citizens when they receive a network reward. Government bonuses are not taxed.
- Dividends tax - the tax is paid by citizens holding shares in companies that receive dividends.
- Sales tax - this tax is paid only by companies when they make a sale. The tax can be set for each product separately.

5.7 Bonuses

Government bonuses are granted to citizens / companies when making product purchases in the form of a fixed amount discount. For example, congress could subsidize the price of electricity for companies with 0.01 CRC or the price of cars with 0.1 CRC.

There is a bonus for each product (over 200). Congress may also grant government bonuses in the form of a fixed amount paid to honorary citizens once. By using autonomous companies, however, any bonus type can be implemented.

The most important aspect of government bonuses is that they can only be received by honorary citizens or companies. All bonuses are expressed as a fixed amount in CRC. If the state budget runs out of funds, all bonuses are reduced to zero by network.

5.8 Traveling

Citizens can travel freely from one country to another, especially when they have to fight. Traveling to other countries is different from changing citizenship and does not imply any change in the status of the citizen. To travel to another country citizens need travel tickets. Travel tickets have 5 levels of quality depending on the distance you can travel with. In ChainRepublik the countries have a fixed position on the map and the distances between them are similar to those in real life. For example, traveling from the USA to France will take longer than if you travel from the USA to Mexico.

5.9 Citizenship

Every player has a certain nationality and will pay the taxes corresponding to the country where he / she is a citizen. Players get their citizenship at signup, but they can change it whenever they want. Network nodes will determine a new user country based on user's signup IP and will register the address accordingly.

A very important aspect is that the change of citizenship comes with some serious changes in the status of the citizen. Mainly, if a player changes his / her citizenship, the following changes are made by network

- ✔ Political influence is reset to zero
- ✔ Political endorsement is reset to zero
- ✔ The citizen is no longer member of any political party
- ✔ The citizen is no longer member of any military unit
- ✔ The citizen loose the honorary citizen status

- ✔ All political endorsements votes are removed

Basically, a player who changes his or her citizenship loses almost all of the progress, except for energy. This decision must be carefully considered by old players.

6. Wars

This section is work in progress. We will update it soon.

6.1 Weapons

This section is work in progress. We will update it soon.

6.2 Military Units

This section is work in progress. We will update it soon.

7 Press

A blog is a frequently updated online personal journal or diary. It is a place to express yourself to the world. A place to share your thoughts and your passions. Really, it's anything you want it to be. For our purposes we'll say that a blog is your own website that you are going to update on an ongoing basis. Blog is a short form for the word weblog and the two words are used interchangeably.

ChainRepublik allows users to create and manage their own anonymous blog. If other users feel that a post is original and informative they can up vote it. Depending on the number / strength of votes received every 24 hours, bloggers are rewarded in MaskCoins.

15% of total daily reward pool is reserved for bloggers, commenters and voters. The reward is shared with those who voted the post. Only 50% of the reward will be received by blogger. The rest will be distributed to voters.

Users can also down vote a blog post. The total votes power a blog posts receives is calculated using the formula

TVP=UP-DP

VP = votes power

UP = up votes power

DP = down votes power

The blog post will be rewarded depending on the total votes power received. Both up voters and down voters are rewarded even if the down voters can significantly reduce the reward amount.

Users can vote a blog post or comment only once and only in the first 24 hours from publication. A blog post can't be voted multiple times

Users can maintain their blog using the tools provided by web wallets. Posting a blog post cost 0.0001 CRC / day. Users can publish a post blog for at least 30 days but may extend this period if they so wish. After this period expires, the post is removed from the distributed ledger and can't be voted anymore.

Users can also comment on a post. Just like blog posts, comments can be up voted / down voted and the authors rewarded. Commentators have their own reward pool. Every 1440 blocks (~24 hours) 5% of total daily reward pool is used to reward comments. Commentators will split this reward with voters just like bloggers do.

7.1 Following

Following someone means you've chosen to subscribe to their ChainRepublik updates. When you follow an address, every time they post a new blog post, it will appear on your home timeline. Following an address costs 0.0001 CRC / day. You can follow an unlimited number of addresses. If you think an address's post has become worthless, you can unfollow that address by paying a fee of 0.0001 CRC.

Just like any other action, following / unfollowing an address can be made using a web wallet.

8. The Network

ChainRepublik is a global and revolutionary peer-to-peer, decentralized cryptographic network which enables censorship resistant value transfer and delivers a new and innovative type of gaming experience.

Just like Bitcoin is a peer to peer network that operates on a cryptographic protocol. Unlike Bitcoin network where users can only send and receive bitcoins, ChainRepublik network allows users to execute a large set of actions from writing articles to managing virtual companies. Transactions are recorded into a distributed, replicated public database known as the blockchain, with consensus achieved by a proof of work system called mining.

The network requires minimal structure to share transactions. An ad hoc decentralized network of volunteers is sufficient. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will. Upon reconnection, a node downloads and verifies new blocks from other nodes to complete its local copy of the blockchain.

8.1 Addresses

A ChainRepublik address, or simply address, is an identifier of 108 alphanumeric characters, that represents a possible destination for a ChainRepublik Coin or other assets. Addresses can be generated at no cost by any user of ChainRepublik. It is also possible to get a ChainRepublik address using an account at an exchange. Each player has only one address associated. Basically a ChainRepublik player is a registered network address.

There are two types of addresses. Registered addresses that are actively participating in the game and the usual unregistered addresses. Registered addresses have a profile, have a name, belong to a country, and can do anything from fighting to working. Unregistered addresses can only send /receive coins or assets. They are generally used by users who do not want to participate in the game but they still need to store / transfer coins or other assets. A good example are the exchanges. The registration of an address costs 0.0001 CRC / day and is usually done automatically by the network nodes without any intervention by ordinary users.

The most important aspect of ChainRepublik addresses is that an address is actually the concatenation, in Base58 format, of the public key. That means you can send encrypted messages / data to any address with no additional info required even if the address was never used before. The built in messaging system provides exactly this function of sending secure, encrypted messages between addresses.

Creating addresses can be done without an Internet connection and does not require any contact or registration with the ChainRepublik network. It is possible to create large batches of addresses offline using freely available software tools like the official paper wallet generator. Generating batches of addresses is useful in several scenarios, such as e-commerce websites where a unique pre-generated address is dispensed to each customer who chooses a "pay with ChainRepublik" option.

ChainRepublik addresses are case-sensitiveand should be copied and pasted using the computer's clipboard wherever possible. If you hand-key a ChainRepublik address, and each character is not transcribed exactly - including capitalization the funds could never be recovered.

This is the reason the network provides and alias system, that allows users to name an **address** like marry or casino and those who want to send others funds can use this alias. Manually typing a raw network address is not recommended.

8.1.1 Addresses Profiles

The Alias System is one of ChainRepublik simplest but most powerful features. ChainRepublik Alias System essentially allows you to associate a name (up to 2-30 alphanumeric characters) to an address. The address name is also the player username. This means that a long, complicated or impossible-to-remember string of data like a network raw address ID can be replaced by a shorter one.

The main advantage of this is the convenience it offers. You can use a single word to represent something far more complex: your address details.

Each address has also a public profile. Address profiles are exactly like facebook profiles. Users can provide contact information, a brief description, a profile picture or other details. An address can have only one active profile.

8.2 Transactions

A transaction is a transfer of ChainRepublik / asset value that is broadcast to the network and collected into blocks just like any other packet type. A transaction moves funds or assets from an address to another.

Transactions may have only **one** source and one destination. Transactions with multiple sources / recipients are not supported. Transactions are not encrypted, so it

is possible to browse and view every transaction ever collected into a block.

All transactions are **visible** in the block chain. Any web wallet includes a block chain browser where every transaction included within the block chain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments.

If the transaction is denominated in ChainRepublik, the sender will pay a fee of **0.1%** the transacted value. The fee goes to the default network address and is the **main revenue source** of the network. Transactions can also move assets between addresses. If the transaction transfers an asset, then the fee will be **0.0001 CRC / asset** transferred. The fee will also be paid by sender.

Asset issuers can specify a **transfer fee and an address** where this transfer fee will be received. This transfer fee will be paid by the recipient of an asset transaction. The fee is denominated in that asset and will be sent to the address indicated by the asset issuer and **not** to the default network address. As a general rule, default network address can **only receive CRC.** In case no transfer fees are specified by issuer, the recipient will not pay anything.

In order to be able to receive an asset, users have to '**trust**' an asset first. Trusting an asset is an easy process that can be made using a web wallet. Once an asset is trusted, the user is able to **receive** transactions denominated in that asset.

Messages can be attached to any ChainRepublik transaction, making bookkeeping easy, as you can tag all your transactions with a description. Project developers can use the Messaging system to embed machine-readable data within an ChainRepublik transaction. This allows automated functions by reading the data sent to you on the blockchain. All messages are securely encrypted and only the receiver can decrypt it.

8.2.1 Escrowed Transactions

Users can also send escrowed transactions where a trusted third party securely holds buyer's coins in escrow until the terms of the sale are met and as a result the buyer or the escrow address release payment to the seller. Escrow transactions are built-in the ChainRepublik protocol.

Sending an escrow transaction is a trivial process especially if all the parties involved use a web wallet. All the sender has to do to initiate an escrow transaction is to specify an escrow address. If such an address is specified, the funds will leave the sender but will not reach the recipient.

The escrow address does not own the funds so the risk of fraud is completely eliminated. Funds are blocked by the network for a maximum of one month, until one party makes a decision.

The sender can only **release** the funds to the recipient.

The recipient may only **remit** the sender's funds back.

The escrow address can **release** the funds to the recipient or **remit** the funds back to the sender.

An escrow transaction costs **0.0030 CRC** more than a regular one. When an escrow transaction is initiated, all parties are informed and can make a decision within 30 days. Decision means a signed package that once included in a block will release the funds.

8.3 Messaging

The ChainRepublik Messaging system allows you to send and receive data on the ChainRepublik Blockchain, thus allowing any network address holder to communicate directly with any other addresses. All messages are securely encrypted and only the receiver can decrypt it even if it traverse the whole network. Because a ChainRepublik address is a Base64 coded public key, the sender doesn't need additional info in order to send a message to an address even if that address was never used before.

Sending a message can be done easily using any web wallet. Messages are delivered instantly even if they were not included in a block. This makes it possible in the future to create p2p encrypted instant messaging applications.

Sending a message cost 0.0001 CRC.

8.4 User Issued Assets

An asset is a digital token that can be transferred between addresses in the same way that ChainRepublik are transferred. The main difference between an user issued asset and ChainRepublik is that an asset is issued by a user and not by the network as a whole.

ChainRepublik assets are a convenient way to represent anything fungible and tradeable. An asset token could represent a bar of silver, a pizza redemption coupon, a share in a company, even a portion of a portfolio of other assets. By representing these things digitally on the blockchain, they can be publicly verified and easily traded.

The ChainRepublik assets are based on the concept of the 'colored coin'. More specifically, ChainRepublik assets are based on the ability of the blockchain to recognise and therefore trace the origin of transactions involving a coin or a set of coins which have been designated to represent any type of asset you can imagine, whether digital (for example, stocks, bonds, smart property) or tangible (for example, cars, houses, precious metals etc).

An asset is under the full **control** of the person who created it. Those who issue assets can **increase** the available supply whenever they want. Assets issued by users do not have a limited amount. Once the asset is issued, the whole qty belongs to the creator.

The value of an asset depends on issuer. For example, if someone issues an asset representing 1 gram of virtual gold that can be bought or sold for 1 gr of real gold, its value depends exclusively on the the person who issued it. If the issuer disappears, or refuses to give you one gr. of real gold for 1 asset, the value of that asset will become zero in no time.

Any user can issue his / her own asset. Issuing an asset can be done very easily using a web wallet. The creator has to provide a few details such as asset name, symbol, brief description and eventually a transfer fee.

The issuer may charge a transfer fee that will be paid by the beneficiary of an asset transaction. The fee will be denominated in the asset and represents a maximum of 5% of the amount received. The fee is sent to an address specified by the issuer. For example if the transfer fee of asset TESTTE is 1%, and a user receives 10 TESTTE, he / she will pay a fee of 0.1 TESTTE. The fee will be transferred to an address

owned by the issuer.

Another difference from MaskCoins is that an asset can not be sent to an address if the address does not **trust** the asset. We have introduced this rule to limit spam. In order for an address to be able to receive an asset, the address must first **trust** that asset. It is a simple process that can be done from the asset presentation page.

8.5 Assets Exchanges

The ChainRepublik Assets Exchange is a peer-to-peer exchange built directly into the ChainRepublik software, allowing secure and fast decentralized trading in ChainRepublik Assets. This eliminates the need to transfer assets or to put trust in an outside agency or business, and as ChainRepublik Assets can be used to represent literally anything (from Bitcoin to coffee beans) there are a wide range of potential investments or trades to be made on the Asset Exchange.

The ChainRepublik Asset Exchange matches asset buyers and sellers, it works in a similar way to cryptocurrency exchanges. All asset exchange operations can be accessed using a web wallet.

Any user can launch an asset exchange. An exchange is used to buy / sell an asset for a currency. The currency may be CRC or another asset. Once launched, users can start trading. Markets allow placing buy / sell orders as well as a mechanism by which buy orders are matched with sales orders. Trading on such a market does not involve fees, except for the transaction fees paid to the asset issuer.

Because an asset exchange can be use to trade any asset for any other asset, exchanges have to be manually created by users. Those exchanges are not automatically created when an asset is issued. The fees for starting a new exchange is 0.0001 CRC / day. Also, those who place buy / sell orders will pay a CRC 0.0001 fee for their pending orders.

8.6 Consensus

The consensus algorithm implemented by ChainRepublik is called Variable Proof of Work (VPOW) and is derived from the classic POW used by Bitcoin and hundreds of other clones.

A **proof of work** is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.

Bitcoin for example uses the hashcash proof of work system.

Hashcash proofs of work are used in Bitcoin for block generation. In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The **difficulty** of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

For a block to be valid it must hash to a value less than the **current target**; this means that each block indicates that work has been done generating it.

Under Bitcoin consensus algorithm the current target is the same for all miners. Under ChainRepublik VPOW, the target is higher or lower depending on the votes a miner address received from stake holders. Basically miners can be up voted / down voted just like content is and depending on a miner popularity, the target at which the miner works is bigger / lower.

A bigger target means less work for a miner to find a solution. The target for a miner that has no votes is called **default mining target** and corresponds to the highest difficulty. To better understand how VPOW works, let's take a few examples. Let’s suppose the default mining target is 1000 (mining targets are usually much bigger numbers).

- A miner was not up voted. The has to find a nonce that after PX16 hashing generates a number less than **1000**.
- A miner was up voted by 5 addresses with a total power of 50. The miner has to find a nonce that after PX16 hashing **generates a number less than 50.000**. Basically the miner will have to work on average 50 times less in order to find a block than a miner who was not been voted at all.

- A miner was up voted by 10 addresses with a total power of 350 and down voted by 3 addresses with a total power of 100. The miner has to find a nonce that after PX16 hashing generates a **number less than 250.000**.

  Any address holding at least **10 CRC** can up vote / down vote miners. A vote becomes active after ~200 blocks. Miner's target levels are recalculated after each block. Voting a miner implies a 0.1 CRC fee. **The vote never expire** but it will be **removed** if the voter balance is less than 10 CRC.

The voting power decreases according to the number of votes given to miners by the formula :

$$P = B / N$$

P = vote power B = voter address balance in CRC N = number of miner's votes

Both miners and those who voted for it are rewarded by the network after each block. Miners reward pool is the largest. 30% of the daily reward pool goes to the miners. Miners will share rewards with their voters. Only 75% of the reward is kept by the miner. The rest goes to the voters.

8.6.1 Hashing algorithm

The hash algorithm is called Polymorphic X16 (PX16) and was developed by Vlad Cristian back in 2016. The algorithm represents an improvement of the X11 algorithm implemented by Dash and other networks.

The first difference from X11 is the number of hash functions used. In PX16, 16 hash functions are used to verify POW nonce instead of 11. This is the list of used hash functions used

Blake512, BMW512, CubeHash512, ECHO512, Fugue512, Groestl512, Hamsi512, JH512, Keccak512, Luffa512, SHAvite512, SIMD512, Shaba512, Skein512, SHA256, SHA512

Another important difference is that the algorithm **changes** after each block, hence the name **polymorphic**. More specifically, in X11 the order of hash functions is the same. In PX16, the hash function is **different** depending on the previous block.

For example if the last block hash is

000012cb4ff317be3cd200329ab87625af83108643197603238b6244f0ef e175

the POW check will be made based on formula

Hamsi512 (Hamsi512 (Hamsi512 (Hamsi512 (JH512 (Keccak512 (CubeHash512 (……..(nonce))))))…)))

Basically for each hexadecimal letter / number (there are 16 in total 0, 1, 2, ...a,b,c,d,e,f) a different hash function is linked. Because block hashes are unique, the exact hashing algorithm used **changes after each block and it's also unique.**

Variable Proof of Work / Polymorphic X16 was developed in order to overcome some significant drawbacks associated with previously used cryptocurrency mining algorithms / consensus such as SHA256 (Bitcoin) or Script (Litecoin). The biggest of these drawbacks was the fact that electronics companies had developed specialist hardware, called ASICs, for mining coins which used the SHA-256 and Scrypt mining algorithms. This had the effect of making the networks more centralized – controlled by a small group of powerful miners, whereas the original vision for cryptocurrency was for ordinary users to be able to take part in securing the network and earning rewards through mining.

By designing the PX16 algorithm to be well suited to use with general purposes CPU processors and commonly used GPU graphics cards, and by cycling through many different algorithms in a different order after each block, rather than using a single algorithm, it makes it difficult for manufacturers to develop ASICs for coins which use this algorithm. Although it is possible that ASICs will eventually be produced, PX16 coins are expected to remain ASIC-resistant for at least the short and medium term future.

The use of 16 different algorithms also increases the security of coins using this method against brute force attacks. Brute force attacks against coins, such as Bitcoin, which use other algorithms are not currently possible, but may conceivably be possible at some point in the future.

Mining centralization reducing network security, reduces the number of people with a stake in running the netwok who naturally become its advocates, and may increase the likelihood of mined coins being instantly 'dumped' as businesses need to cover costs and take profits whereas individuals may not have to.

Mining centralization is also serious problem because miners can not be held accountable by shareholders. They 51% attack the network with no shareholders consent.

The best example is Bitcoin block size debate where 100% is up to miners to change the maximum block size and fork the network. Bitcoin holders are completely ignored by miners. Under VPOW, that would not have been possible.

Under the ChainRepublik algorithm (even if we talk about a POW consensus), miners can be **drastically penalized** by shareholders. If they are down voted, the difficulty they work on will explode and the number of blocks found will be **significantly lower**. Also, the miner's revenues will be drastically **reduced**. Since miners rely on hardware-intensive hardware (such as GPUs), a negative vote on the part of shareholders may mean the **death of miner's business** due to the cost associated with maintaining equipment / income from mining.

Variable POW combined with PX16 significantly reduces the chances of mining centralisation / miners's influence on the network while preserving the security of a POW consensus.