From the Swarm-App to the Proxy-Party (draft)

Abstract

The proxy-party is controlled by its members via an app and offers them direct political participation in a secure manner. The voting process is transparent and all activities are secured by blockchain technology. At the same time, data protection is ensured, because all activities are stored without reference to underlying identity. Before every formal vote (in parliament), a pre-vote is performed by the party members. Representatives are required to follow the results of the pre-vote and also document their voting behavior. There is no overarching party program in which initiatives have to fit consistently. Therefore subsidiarity is maximized and each proposal stands for itself. The voters do not choose the proxy party primarily because of their current programmatic goals, but for the fact that their opinion and voice have weight in the party.

The proxy-party rewards the work of its members through mechanisms that are anchored in the blockchain network. The rewarding and inciting of participation is achieved through an internal currency. This currency is tradable on an exchange and the party uses a large portion of its income to buy it back from the users. As a consequence, a large part of the party's assets are managed transparently on the blockchain. The leitmotifs of the proxy-party are: security, transparency, data protection, equality, openness, subsidiarity, rewarded participation and simplicity.

** If the masculine form was chosen in this document, it was made solely for reasons of better legibility.*

p.cypher@protonmail.com

Table of Contents

Note: This sketch describes the swarm-app in connection with a political party (proxy-party), because this application requires the full range of functionality. However, the use is not limited to political parties and can also be used independently from an organization and without representatives or functionaries. Some of functions described in this document are therefore optional. In order to better illustrate the concept and the functionality, aspects are also named here that go beyond the pure functionality of the software. These aspects should later be anchored in the statutes of the proxy-party. A technical specification for the software is to be developed from this document later on. The internal currency is referred to as a "coin" here, but it is also possible to use a "token" (e.g. according to the IRC20 standard).

Introduction

Currently, most people cannot identify themselves with all program points in the agenda of a political party and are therefore forced to choose “the lesser evil”. In practice, the influence of the voters and the party rank on political decisions is small and participation is made more difficult by technical hurdles (e.g. party congresses in distant cities). Decisions with far-reaching social consequences are not or rarely discussed in public. The voters have to trust that MPs will decide as promised during their term. The lack of transparency encourages corruption and political disaffection. Citizens lose faith in the “democratic” system. Digitization offers new opportunities for grassroots democracy even within the representative democracy. With the approach outlined here, party members can influence or determine the political content as well as the voting behavior of their representatives directly via an app (proxy party). The voting process is divided into two subsequent steps: Before every formal vote by the representatives a pre-vote is performed by the party members. The elected officials follow the voting results of the members, provided this does not violate the respective legal framework (and in Germany: provided the elected officials can reconcile the will of the base with their conscience). In addition, the elected representatives continuously log their actual voting behavior voluntarily via the app. The actual decision-making process therefore does not take place between officials, but is carried out by the members directly. The base expresses its will transparently and continuously through votes and evaluations.

In the software, a domain represents a grouping and does not necessarily correspond to an organization. The members of a domain manage themselves and also determine their functionaries and representatives. The users (including functionaries of the proxy party) interact anonymously via an alias name. Thus, arguments receive greater significance in the competition of ideas and activities can not be assigned to the identities. A domain can also be open to all citizens, e.g. if it is only about the presentation of opinions (transparency tool). In the context of the proxy-party, the domain is an instance at an administrative level. The name of the domain could be, for example, "Chapter Musterhausen" or "National Party". The respective domain is self-governed. Quorums and other details are built-in as variables and can be adjusted by the members of the domain. All data and properties of the domain (ratings, functions and lists) are stored on the blockchain by the node network. All activities (= changes to this data) must be signed (authorized) by the respective member before an entry can be made. The programmatic content on a domain is freely defined by its members. Technically, there are no interdependencies between domains, enabling maximum subsidiarity on the different administration levels. Therefore, the demands on municipal, country and federal level can be completely different or even contrarily. There is no overarching framework program and no whip. Every initiative stands for itself. Members pay a contribution to the organization (party) and thus acquire participation rights. The political work is done by common party members and not by the officials in parliament. The party honors this by rewarding the members for their participation. The same applies to node operators, which validate block entries for the blockchain and thus protect the activities of the members from manipulations. The members of the proxy party are united by the respect for the opinions of others as well as the faith in democracy.

1. Opening an initiative and decision

Initiatives may relate to own legislative suggestions, reactions on initiatives of other parties or self-government matters. Each member can only have one initiative "in process" at the same time. This serves the limitation of power, protects the community against overload and keeps the quality of the applications high. If an initiative is rejected, the member has to wait 14 days before starting a new initiative. If another rejection follows in a row, the period doubles. This mechanism should protect the community against a flood of insufficient applications. There is a distinction between two different voting types: directional decisions and representative decisions. For directional decisions alternative initiatives are evaluated (optionally also via the procedure **"Systemic Consensing"**). If only one proposal is available for choice, it can be accepted or rejected. In the case of a representative decision, the result of the pre-voting (yes, no, neutral) is taken into account accordingly by the representatives during the formal vote (see page 4).

<u>Steps and hurdles in the decision process:</u>

•Formal hurdle (optional)

The initiative is formally 9 parts that must be available for the online submission:

- Title (max 5 words)
- Short version (max 7 sentences)
- Impact assessment (max 5 sentences)
- Legal conflicts (optional)
- Explanation text (max 10 pages)
- Two questions (multiple-choice): later used to check whether short version (1 question) and explanation (1 question) has been read by members before the rating.
- Details on the classification: new initiative or counter proposal for existing initiative, topic etc. ?
- Domain the initiative should be finally forwarded to (final destination)
- Voting type (directional or representative decisions).

The list of requirements can be extended or shortened by the admin of the domain. In general, new initiatives (without reference to existing initiatives) should always be started at the lowest level of administration. However, this “rule” is not implemented in the software, but in the statute of the proxy party.

•Aleatory hurdle

For this process a number (10-100) of users (Random Member = RM) are randomly chosen by the software from the pool of RMs. Every member of the domain has the right to take part in the pool of RMs. At least 60% of chosen RMs must consider the initiative as "voting worthy", otherwise the initiative is rejected. The decision is based on the following criteria:

- Is the initiative formally sufficient (see formal hurdle above)?
- Are targets, short version, multiple-choice questions and wording of the initiative consistent?
- Is there “sufficient seriousness” in the proposal (free beer for all citizens?)

The RMs make the final classifications (voting type, “systemic consensing”, administrative level). Thereby, RMs don’t necessary have to follow the suggestions of the initiators. RMs are paid for their work.

•**Approval hurdle (vote)**

i. Defense of the initiative: If the aleatory hurdle was passed, questions about the initiative are collected and evaluated by the members. Each member is allowed to ask only one question, but can up- or down-vote questions of other members. The 10 questions with the highest ratings must be answered by the initiators of the proposal. The answer must be submitted at the latest 1 week before the end of the voting process. If these questions are not answered in time, the process is paused and the initiative remains in suspension until the answers are present. The process is than extended accordingly, but not beyond the maximum length for voting processes (8 weeks). If the maximum duration passes without results, the initiative is rejected. During the decision process, all users on the domain can view and rate the questions and answers. The function of the questioning is to reveal weak points and possible risks or flaws in the proposal. It gives members the opportunity to reconsider their opinion and voting. Bad rated answers indicate that the concerns could not be clarified by the answer coming from the initiators. The rating of questions and answers is also rewarded. Ratings and votes can be changed during the process, but this will result in no additional rewards (see section 4).

ii. Voting and discussion: In parallel to the questioning, the initiative is placed for voting. The process is terminated after a defined time. As a rule, these are at least 3 weeks. If a majority decides accordingly, the period can be extended for another week. There is a minimum period to avoid "cloak-and-dagger votings" and a maximum period. It should also offer the possibility to contribute counter-proposals.

Any member of the domain may vote positively (in favor), negatively (against) or neutral. For a directional decision, an application is accepted if it has more positive than negative votes (positive voting difference). Representatives take into account (follow) the results of the pre-voting, the negative and neutral voices are also represented. If counter-proposals are submitted, the deadline extends one week, the initiative (proposal) with the highest number of net-positive votes (positive minus negative) wins. Optional the algorithm for “systemic consensing” can be applied if activated during aleatory hurdle.

Before the vote users have to answer the 2 questions (multiple choice, see formal hurdle) correctly. This ensures that the initiative has been read properly. Users can change their vote as long as the process has not yet been closed (otherwise the questions would be meaningless). The voting is rewarded.

At the beginning of the voting process, a forum thread will be opened to each initiative. User of the domain can discuss the proposal anonymously.

2. Representatives document their voting (formal vote in parliament or committees)

i. Documentation: The representatives Vote in parliaments and bodies according to the pre-voting of the members. If the party has 10 members in parliament and the initiative received 40% approval, 10% rejection and 50% abstentions (neutral) in the pre-voting, then 5 MPs will abstain from voting, 1 will vote against and 4 MPs will vote for the initiative. The app calculates the distribution of votes so that the deviation to the will of the members is minimized. The representatives are registered on the app through a separate account (representative account = RA). Each RA receives a suggestion for its vote (in favor, against or abstention). After voting, the representatives document their voting behavior and a statistic is led accordingly. The statistic indicates whether RA has participated in the voting (participation rate) and whether the voting was in accordance to the voting suggestion of the app (matching rate). This statistic is later used as a quality criterion for the compilation of the list of candidates for the next legislative period. The documentation work of the representatives is also rewarded.

ii. Verification of the voting results by the members: Users can enter the actual voting results (as far as publicly known) into the swarm-app (human oracle network analogous to ChainLink). That way, inconsistencies regarding the documentation of the representatives become transparent. Users can revise their input data, but without additional rewarding. The system accepts the results with most confirmations as "true". If there is a contradiction between the documentation of the representatives and the revision carried out by the users, representatives receive "slash points" (downgrade of the matching rate). This automatically has an impact on the ranking when lists are compiled.

3. Onboarding (identification, security) and self-administration

i. Accession of members and identity verification

The user can create themselves a wallet for the blockchain via the client-software. The wallet consists of Public and Private Key. The public key represents the user in the network. The private key is only known to the user. With their private keys users can authorize their activities on the blockchain. Technically, the activities are equipped with signatures that can only be generated if the private key is known. The immutable data of the person (identity) is stored encrypted and separate from the activities in a blockchain database. The entries in both databases are maintained by a node network. In the database with the personal data, the public key is not saved. On the blockchain with public visible activities, the personal data is not stored. There are no dependencies between the data in the two databases. This ensures data protection, so that the activities on the blockchain cannot be linked to the identity.

However, in order to perform activities, the public key must be activated periodically (once a year). The public key address is activated by assigning a postal code and optionally an association to an organization on the blockchain. This allows activities to take place on all domains that are related to the postal code area.

<u>**Steps (figure 1):**</u>

1. The user transmits his personal data to the node network, which manages the person register (register of members). Here is distinguished between immutable data (personal data: birth name, date of birth, birthplace) and the private data (passport id, name, biometric data etc.). The postal code is transmitted as well. The private data is not stored, but will later serve for the verification of the identity by an external service provider (id-service). The personal data is encrypted and can only be read by the id-service. The immutable data can also be decrypted (optional) from a organization (client organization, e.g. Party). In addition, the signed public key is also transmitted, the signature serves as proof that the user also has the private key and is thus the owner of wallet. However, the public key is not stored in the database and is transmitted to the node-network encrypted! A PGP solution could be used for data encryption **2-5**. The personal data is transmitted to the id-service. The immutable data will be additionally transmitted to the organization (political party) to confirm the membership.

6. If identity and membership have been confirmed, the network is checking in the register of members whether a activation already exists for this dataset (identity). **7.** Only if this is not the case, does the register network sign~~s~~ the prompt for the activation of the public key on the blockchain with the activities. **8.** For this purpose, the encrypted and signed public key is transmitted to the node network, together with the postal code.

9. The node network checks the signature and links the postal code to the public key address on the blockchain. Optionally, the membership of the organization is also linked to the public key address. The user can now perform activities on all domains belonging to the postal code and/or organization.

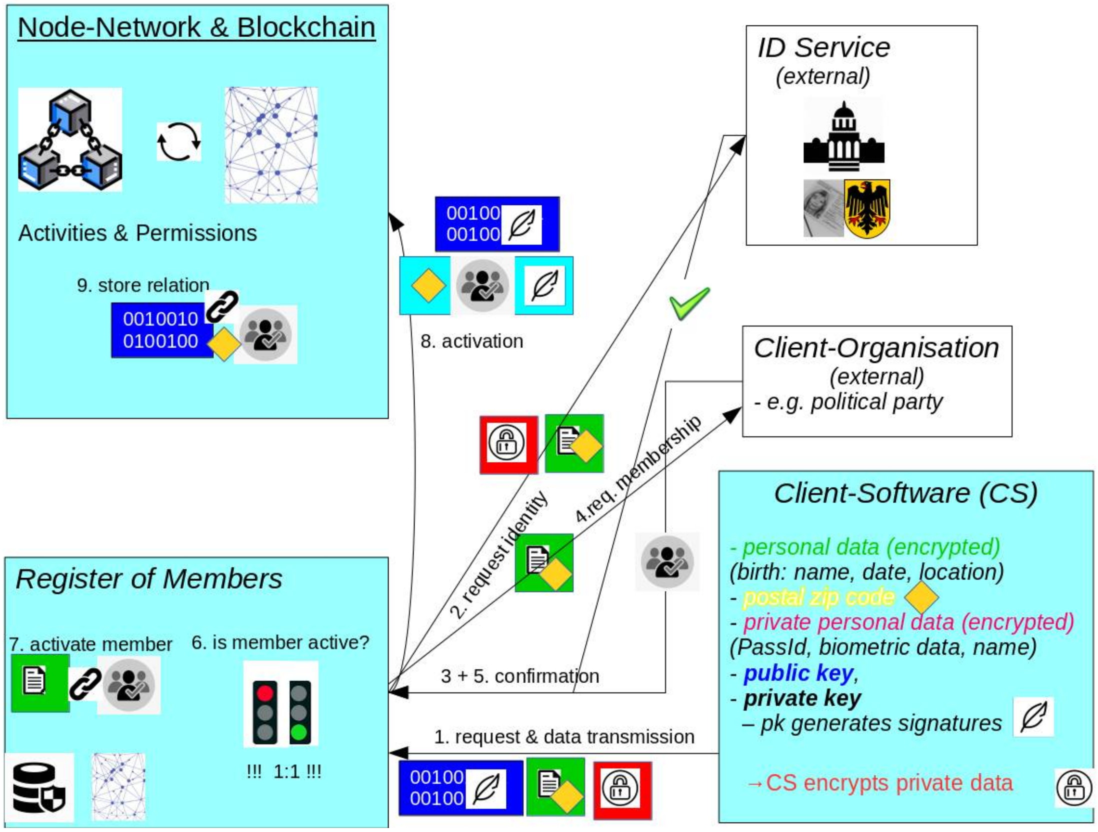


Figure 1: Information flow when activating an account (schematic sketch)

ii. Election of the domain-admins

If a new domain is created, the initial user becomes an admin automatically. Therefore, he must be listed on the “admin list”. All members of the domain (assignment via postal code, membership) have the right to register or unsubscribe on the admin-list at any time. They can also up- or down-vote other members on this list. When new members enter the domain, each member must make an assessment (voting) on the admin list. This measure aims to consolidate the admin position. If the admin unscribes, the next member on the list inherrits the admin privileges instantly.

All member can change their voting at any time. Voting on this list is not rewarded (no incentive for admin change).

iii. Rights and duties of the admin

The admin can create and delete predefined offices/functions and lists, except the admin list itself. In addition, he can put offices or functions for elections. He defines the domain (name, organization, postcode belonging), but has no influence on the rights of users and cannot exclude, add or authorize them. He can choose moderators to help him with his work. The moderators have all the rights of the admin except the right to nominate (or withdraw) moderators. There is a ticket-system for user requests, the admin and his moderators work through. All activities of the admin and his moderators are rewarded.

iv. Compilation of lists for functionaries and mandate holders

Members can specify whether they want to be electable in regard of for functions in the proxy party (board, mandate carrier, press spokesman, ..) or in the tool (e.g., admin, participation in the alimentary procedures) on the domain concerned. Since mandate carriers normally follow the preliminary decision of the base, no special prior knowledge is required for this office. All mandate carriers and officials are basically selected randomly. Therefore, in principle, all party members are in question for all functions, unless they have explained. For this purpose, all candidates appear on the corresponding list (e.g., list of treasurer candidates) with their public key or alias name. In a second step, the lists are then automatically sorted so that the members are with the best statistics (match quota, participation rate) above. When sorting, the principle applies: no statistics are better than bad statistics. So the good work of representatives should be rewarded. Members can change sorting through their evaluation, each member has a review (positive, negative) that can be changed at any time. This activity will not be rewarded (no incentives to change the lists).

4. Rewarding of voting activity and network services

Goals:

i. The users should be rewarded for democracy work (incentive for participation).

ii. Drawing attention to the organisation (party) and decision-making processes.

iii. Transparency regarding the usage of income in the organization.

Overview and motivation

Grasroot democracy means that the party reflects the current opinion of its members. For this, a constant exchange and coordination process between the members is necessary. This political work should be rewarded in a monetary form. The same applies to the administrative work. Today we have information and communication techniques that were not in existence a few years ago, which open completely new possibilities. This includes blockchain and distributed ledger technology. These innovations have the potential to enable consensus formation safely and transparent and at the same time, data protection can be ensured. These technologies also offer the opportunity to reward the productive work of the participants (votes, reviews and tasks of self-government) via an internal currency. Therefore, a large proportion of the organizations revenue is used to buy the internal currency back from the members. This creates demand and the internal currency gets fiat- nominated price (€). Members can exchange their "coins" against fiat on a market. At the same time, a large part of the assets of the organization (party) is managed on the blockchain transparent. Each member can also operate a node through software to make the network safer. This work is also rewarded. Since the concept presented does not use the method "Prof of Work" but "Prof of Stake", energy consumption is extremely low.

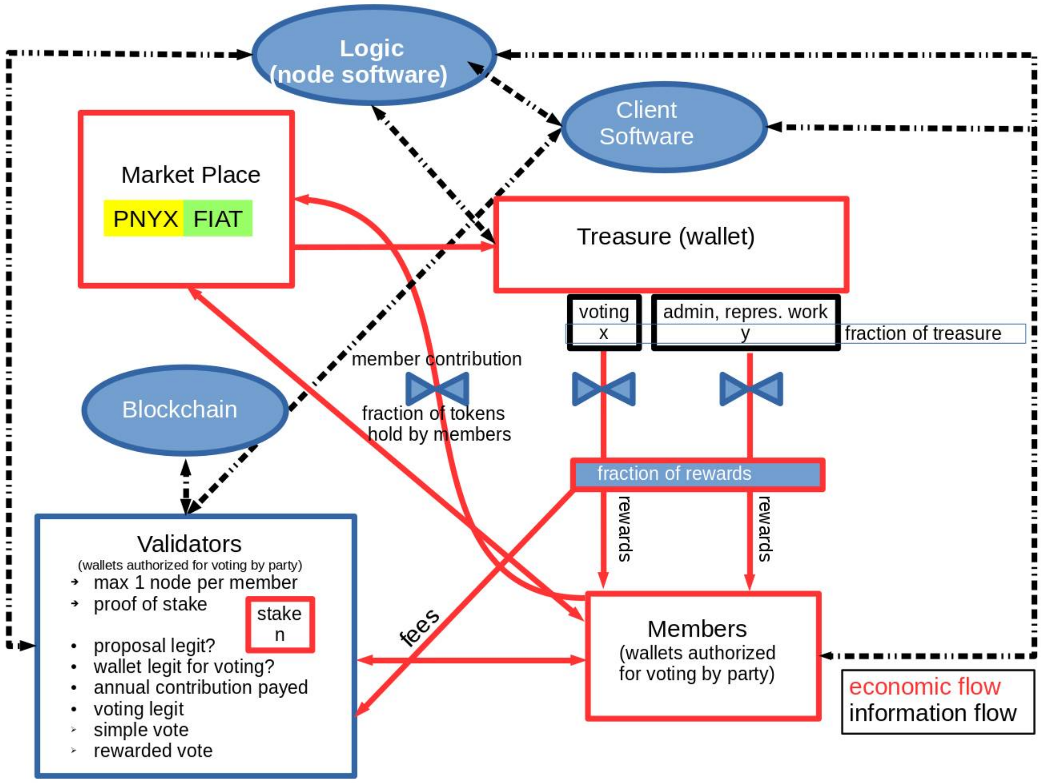


Figure 2: Schematic view of the "tokenomics"

Roles (figure 2):

- Members of the domain

Activities related to votes are signed with the help of the private key for authorization. All activities are documented on the blockchain. Members are rewarded with coins (arbitrarily divisible) when they participate in voting, evaluations, administrative or monitoring tasks. The amount of the rewards is based on the amount of deposits in the domain wallet (treasure wallet) multiplied by a ratio (x, y). For example, 0.001% from the treasure wallet per vote or 0.005% for administrative tasks. Each day a fraction of the deposits of the user wallets (all none treasure wallets) is transferred to the wallet of the marketplace (Figure 2). The amount of these contributions sums up to 0.5% of the total value over a month (0.017% per day). As a result, only active participants are net accumulators, but without activity and rewards the balance shrinks (**sell pressure**).

Node owners must freeze a part of their coins as collateral in order to operate a node. The collateral (stake) does not shrink as long as the node operates (**node pressure**). Thus, the stake functions as a ‘safe haven’ and this creates an incentive for users to provide a node. Members can therefore "stake", sell or just send their coins.

- Validators

Validators are members of the network (no domain membership is required) who operate a node-server. In order to do this, a fixed number of coins has to be staked (e.g. 12 coins in the stake), similar to Ethereum 2.0. In order to run the node-software, a computer has be provided. For providing collateral (taking risk) and the provision of the computing power, the validators participate in the remuneration of the other members (e.g. 0.3% of the rewards). Each node is checking whether activities are legitimate (following the rules), thereby protecting the logic in the software. For example, it is checked whether the member has already cast his vote for a specific ballot, if he is a member of the domain, etc.. Another activity is transferring credits (coins) from one wallet to another. The necessary information for the verification can be derived from the blockchain and the signatures of the activities. All activities are documented on the blockchain. In order to prevent incorrect entries in the blockchain, nodes check each other via a special consensus mechanism. If the software on a node-server is faulty or "malicious" (e.g. a member is allowed to give more than one vote), incorrect entries are rejected by the other nodes. In order to compromise the blockchain, 51% of all nodes would have to be manipulated at the same time, which is practically impossible in a decentralized network. A random mechanism is used to decide which node receives the fees for the respective block entry. If the majority of the nodes decide that a certain node is "malicious", their credit will expire (coin burning). This means that the node can no longer operate and disrupt the network. Node-server works globally for all domains (administration level). In this way, the number of coins required when opening a new domain remains low (no own stake required). Node also charges a very low fee for every transaction (crypto transfer) in order to prevent an attacker ~~to~~/from troubling the network with fake transactions. The origin of the funds in the stake-wallets is transparent. To prevent an attacker from undercutting the node-network, the network does only accept coins mined at ‘legit’ domains for the stake. Therefore, it is not possible to simple buy coins on the market and run a node. Node owners have to have earned their node via political work. Domains are considered as legit (for “node mining”), if the number of active members (members with funds) is large. The threshold for a large domain is defined by largest the domain. A legit domain must have at least 25% the number of members than the biggest domain in the network. The examination of the stake only takes place if a new node wants to register. Thus, operating nodes are not affected, if the domain from where the coins originated close.

•The organization (proxy-party)

Each domain has its own treasure-wallet. The proxy-party uses a large proportion of its fiat income (€) to buy coins into the treasure-wallets of its domains. The funds (coins) are used to reward the members of the domain. The price discovery depends on supply and demand and takes place on an internal marketplace, operated by the network. It is not allowed to exchange (dump) the coins back into fiat-money, because this would be at the expense of the members (devaluation of their coins). In order to strengthen trust in the internal currency, transfers from the treasure wallet are possible only via the rewarding-mechanism. The buying program ensures that a large fraction of the party assets are managed transparently on the blockchain.

A domain can also operate without a party or organization. However, in order to enable rewarding, coins for the respective treasure wallet must be purchased (e.g. via crowd funding).

•Treasure-Wallet and Marketplace (price discovery)

There is only one global marketplace accessible to all user- and treasure-wallets. Members (sellers) can deposit their coins into an escrow wallet on the marketplace. Organizations can deposit fait-money into the marketplace's escrow checking account. Once a day there is a market clearing and price discovery takes place. Thereby, the price for a coin is determined by the quotient of N_f / N_c, where N_f stands for the fiat volume (€) and N_c the coin volume supplied by the users plus automated member contribution (figure2). The fiat sales proceeds of the seller result from the number of deposited coins multiplied by the coin price.

Initialization:

Total number of coins:

The number of coins must be high enough to theoretically operate 100k nodes (1,200,000 coins with a stake size of 12). The number of coins is fixed and the distribution~~s~~ is technically controlled by a team of core-developers (multi-sig wallet). However, the process of bringing coins into circulation should be coordinated with the development association. In order to run the first test-domain, enough users have to agree to operate a node. Therefore, supporters, developers and trustworthy investors (ICO) get coins to run a node (first 100 nodes program). The remaining coins are distributed as follows:

First airdrop:

At start, 20% of the coins are distributed to all existing treasure wallets in the network. The distribution among domains is weighted by the number of active participants in the respective domain.

Core-Team:

Another 20% of the coins are reserved to fund the future maintenance and development of the software (after launch phase).

ICO:

Through an Initial Coin Offering (ICO) program 20% of the coins will be sold to trustworthy investors (one node option per investor) by the development association. The revenue serves to promote the tool and its development. The development association can also support domains with coins in order to promote grassroots democracy.

Bug-Bounty program:

Another 20% is deposited on a separate multi-sig wallet for the bug bounty program. This account is controlled by the core developers, but funds are preserved for external hackers only.

Second Airdrop:

When the number of active users (wallets with funds) reached 20k, the remaining 20% of the coins are distributed to all treasure-wallets in the network, weighted by the number of active participants in the respective domain.

Price:

It is not the aim of the tokenomics to drive the price up as quickly as possible. However, there is no inflation and the price will go up over time under the following circumstances:

- New members accumulate
- New nodes reduce~~s~~ the supply
- Coin burning due to faulty or malicious nodes
- Wallets are lost and the funds can no longer be accessed
- Increases buy-up rate (buy program of organizations)

5. Some remarks on security

Code

At the latest after completion of the beta version, the source code should be disclosed so that errors can be discovered externally. First, a test network with 2 domains is to be set up and money is to be made available for external code audits. In addition, the bug-bounty program should be actively promoted by the development association. The bug bounties are intended for external hackers who expose relevant security flaws. Rewarding must be transparent and the core-team has to develop error categories.

Transparency and data comparison

Through the front end, every user must be able to view and check their history of activities on the blockchain. For a domain, the number of members and their spatial distribution as well as distribution of coins must also be transparent.

Separation between identity and activity

So there is no connection between activities and personal data. If the register of members was hacked, the personal data is protected by the encryption. Even if this encryption can be overcome, the public key is not stored there. The activities on the blockchain are public, but these activities are only assigned a zip code and a public key, which means that no identification of the person is possible. It is important that only the unchangeable personal data is stored in the register so that a user cannot activate a second address by changing his name or place of residence. If the user manipulates this data in order to activate a second address, this will be recognized by the ID service (e.g. wrong name at birth or wrong place of birth).

Activity window and periodic activation

If the activity-window expires, technically the link between postcode (optionally also membership) and public key is deleted. The user can still dispose of his credit, but the domain will no longer accept him without activation, so the user has to repeat the activation process. It is irrelevant whether the user generates a new wallet (address) or has the same one activated again. The private personal data (passport number, biometric data etc.) is not stored anywhere in the system, not even by client software. It is only transferred to the id-service for the activation process (e.g. photo from ID card, etc.). The periodic activation ensures that stolen or lost wallets do not remain active forever. After activity-period, the user can activate a new wallet (e.g. if the old wallet has been lost or he wants to better protect his identity). The activation must be confirmed by the node network, so there is no central point of attack (apart from the provider of the identity check).

Protection of the node network (single node rule, nominated proof of stake, slash points)

There is a risk that attackers could buy coins to operate nodes in order to gain control of the network (51% attack). However, the larger the node network, the less likely this scenario becomes. Therefore, there must always be a strong incentive for users to operate a node. However, some restrictions seem helpful, as they only slightly reduce these incentives but make it more difficult or even prevent the takeover of the network:

i. Single node rule: Since each natural person only has one active entity on the network, the risk of a takeover can be limited by only allowing one node to be operated on the same address. This no strict one person one node rule, but a measure against centralization and the limitation of power to individuals.

ii. Nominated Proof of Stake: When a new node is opened, the network can also check the origin of the coins. The following rules can prevent the "buying together" of nodes:

a) The coins must have been generated by the node address: The coins for staking must therefore have been transferred directly from a treasure-wallet of a legit domain. This ensures that the coins were earned and not bought.

b) The domains on which the coins were generated must be of sufficient size. This can prevent an attacker from opening a dummy domain in order to "earn" coins more easily. The minimum size for a “legit” domain could be based on the size of the largest domain (n_max): n = n_max * 0.5.

iii. Slash points: If a node is not working correctly or is not available, slash points are awarded. These can be compensated with rewards. If a certain threshold of slash points is exceeded, the credit on the node address (stake) is deleted (coin burning). As a result, minor "offenses" (node is offline, software update forgotten) are punished in monetary terms, while serious offenses (malicious nodes) are punished by the network with loss of the stake and exclusion.

Potential benefits of a newly developed node software compared to using an existing blockchain

There are many examples that can be used for developing new node software, but the development effort would be significantly greater compared to implementing the logic via smart contracts on an existing blockchain such as Ethereum 2.0. Using smart contracts is probably the fastest way, but some disadvantages have to be taken into account:

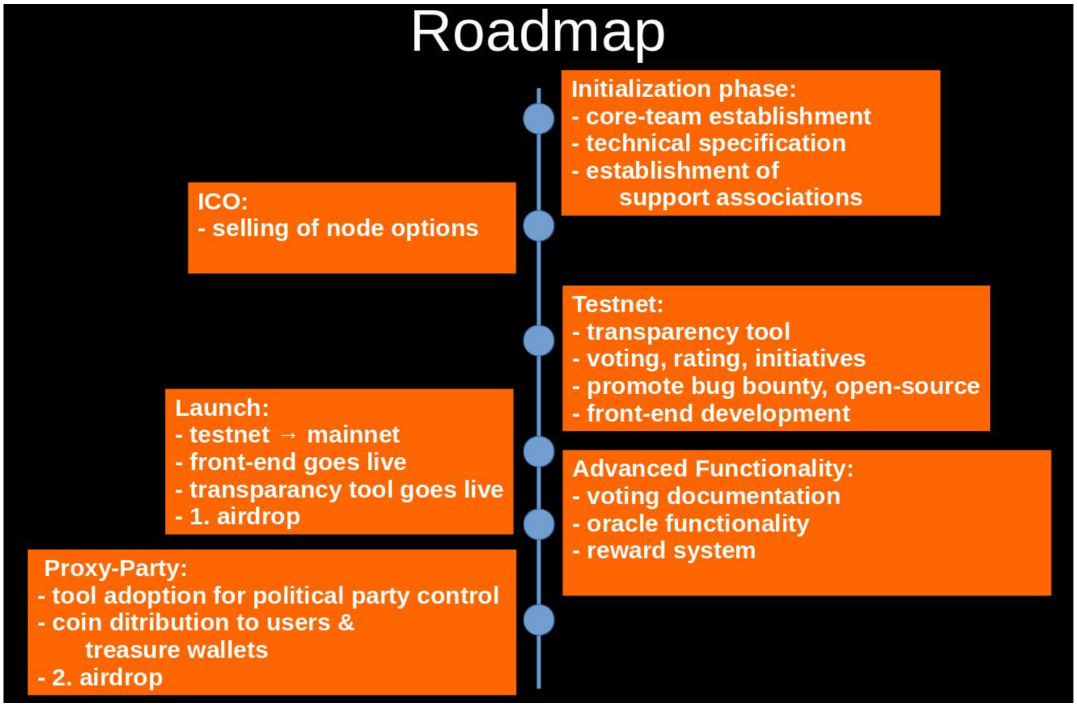
1. The source code of the base chain is extremely large and confusing as many functionalities are supported, most of which are not required for the tool. This increases the surface area for attack vectors.

2. The software must be kept permanently updated and synchronized with the original code base in order to close security gaps. Code divergence has therefore to be prevented (wherever possible), what hinders flexibility in development. If the software is "forked", it is extremely time-consuming to enter all updates of the original implementation later on. In the case of a fork, security gaps are always closed with a delay, which gives attackers a permanent head.

3. Software platforms such as the Ethereum virtual machine (EVM) are “turing-complete” and therefore offer space for further attack vectors (currently more than 16 attack vectors are known for Solidity only).

Conclusion: It is likely that a new development of the node software (in C ++?) makes sense.

6. Roadmap



Roadmap

Initialization phase:
- core-team establishment
- technical specification
- establishment of
  support associations

ICO:
- selling of node options

Testnet:
- transparency tool
- voting, rating, initiatives
- promote bug bounty, open-source
- front-end development

Launch:
- testnet → mainnet
- front-end goes live
- transparancy tool goes live
- 1. airdrop

Advanced Functionality:
- voting documentation
- oracle functionality
- reward system

Proxy-Party:
- tool adoption for political party control
- coin ditribution to users &
  treasure wallets
- 2. airdrop