Whitepaper

für eine

Blockchain-based Platform for Decentralized Autonomous Parties (DAP Platform)

Version 1.6

Autoren

Stephanie Tsomakaeva

Irakli Betchvaia

Markus Backfisch

Braunschweig, den 30.06.2024

Version 24.03.2025

Inhalt

Blockchain-based Platform for Decentralized Autonomous Parties (DAP Platform)

I. Introduction

The Problem: Public trust in associations, federations, political parties, and politics at large is in crisis worldwide. Boards, officials, and politicians frequently fail to adhere to the statutes they themselves have approved while in office. They make decisions behind closed doors. Minutes are either not published at all, published with delays, or made available in obscure locations that are difficult to access. In this way, board members accumulate privileged knowledge and secure their positions of power without being held accountable by the members beyond mere lip service.

In order to make decisions more controllable over the heads of members and citizens, direct democratic participation processes are seen as obstructive, while so-called "combat votes" (i.e., votes aimed at creating division) are encouraged to fragment the majority. As a result, necessary improvements are neglected, and organizations stagnate in outdated structures.

The Solution: The development of a blockchain-based platform for Decentralized Autonomous Parties (DAP Platform), designed to promote disclosure, liability of politicians, and direct democracy in all membership-based organizations worldwide. The platform is intended as a real-world application experiment aimed at replacing centuries-old, centralized hierarchical state models with a decentralized, direct democratic structure.

This whitepaper outlines the vision, structure, and functionalities of the DAP Platform, with the objective of creating a functioning technical framework that facilitates the evolution of representative democracy into a system of responsible democracy in practice.

1.1. Concept of Responsible Democracy

The DAP Platform sees itself as the "Bitcoin of Politics" and aims to be a quantum leap in the evolution of democratic structures. By utilizing blockchain technology, we aim to:

a) **Ensure disclosure:** All democratic processes and decisions will be documented in a traceable and publicly accessible manner.

b) **Guarantee liability:** Decision-makers and members must adhere to established rules and laws, as automatic sanctions will be imposed for violations.

c) **Self-organization:** Citizens and members actively inform themselves, make their own decisions, oversee their representatives, and have the right to veto decisions made by their representatives.

II. Structure of the DAP Platform (Republic)

The legal form of the DAP Platform is a membership organization (association). The DAP Platform is tasked with virtually representing and testing all principles of political decision-making for a future state in which the representative democracy model has evolved into a decentralized, citizen-controlled democracy. All levels listed below form the fundamental structures of a shared virtual democratic decision-making system, a "Respublika":

- "Constitution" (Statutes of the DAP Platform)
- "Public Sphere" (all users, including non-verified and non-eligible users)
- "Eligible Voters" (fully verified users of the DAP Platform)
- "Polis" (Virtual assembly of verified users)
- "DAPs" (Membership Organisations)
    - Statutes
    - Board
    - General Assembly
    - Members
- "Parliament" (General Assembly of the DAP Platform)
- "Public Servants" (Delegates from individual DAPs)
- "Government" (Board of the DAP Platform)
- "Judiciary" (Arbitration Tribunal)
    - e-Arbitrator
    - Elected Arbitrators
- "Audit Office" (Elected Auditors)

2.1. The Statutes of the DAP Platform (Constitution)

The statutes of the "DAP Platform" association serve as the first smart contract defining the voting and election processes governing decision-making concerning the development, administration, operational and community management of the DAP Platform. Additionally, the statutes outline all user rights and obligations as well as fundamental rights applicable to all smart contracts of the DAPs. They also regulate the principles of coexistence in the "Respublika." Therefore, the statutes of the DAP Platform are referred to be the Constitution. Constitutional amendments are decided in the Parliament through the "simple consensus procedure." The Constitution is publicly visible to all users. By registering on the platform, users accept the validity of the Constitution.

2.2. All Platform Users (Public Sphere)

All users share an anonymized, censorship-resistant forum, an open and for everyone accessible information platform (Public Sphere). Any user can publish contributions free of charge. The order

in which posts are displayed depends on their "weight." "Weight" can be purchased for Bitcoin at any time and in unlimited quantities. Each post loses 10% of its weight every 24 hours.

2.3. Fully Verified Users (Eligible Voters)

All fully verified users are citizens of the Republic and have the right to vote in the nomination of electoral lists for their DAPs and in parliamentary elections.

2.4. Virtual Assembly of verified users (Polis)

parliamentary elections, parliamentary debates, election of auditors

2.5. Membership Organizations (DAPs)

Each DAP is a membership organization consisting of at least three members. These organizations can be political parties, associations, or groups with entirely different objectives, purposes, and fields of activity.

Statutes as Smart Contract: The statutes of each DAP are implemented as a smart contract on the blockchain. These contracts regulate the internal processes and decision-making procedures of the DAP. Violations of the statutes trigger automatic sanctions.

Blockchain of Statutes: Each DAP has its own logical blockchain consisting of amendments to its statutes.

- **Versioning:** Each statute amendment references the previous version to ensure a complete history.
- **Rule-Based Amendments:** Amendments follow rules defined in the previous version and must be signed by authorized persons.

2.6. General Assembly of the DAP Platform (Parliament)

The Parliament is the general assembly of DAP-delegates. Various, yet equal, DAPs create electoral lists from which all verified users elect delegates to the Parliament.

Provisional Parliament: The founding Parliament, which initiates the smart contract of the DAP Platform, serves provisionally until the first parliamentary elections take place and consists of all founding members of the DAP Platform.

Parliamentary Elections: Once the tenth DAP board is constituted, all DAP members automatically receive a K-Token for candidacy for a government position, provided there are no restrictions on the user. The K-Token authorizes them to declare their candidacy for a government position in the Polis for 30 x 24 hours. After this period, the preliminary candidate list is closed,

and all verified users are notified that the first election round is open. Each election round lasts 3 x 24 hours.

The Parliament is elected for two years, and each public servant may serve for a maximum of two terms. Each DAP can nominate at most as many candidates as there are parliamentary seats. Delegates determine the objectives and tasks of the DAP Platform.

All decisions in Parliament follow the Systemic Consensus Process.

2.7. Public Servants (Delegates from individual DAPs)

Public servants are delegates of the DAPs, elected by all verified users collectively, and represent their interests in voting on tasks and changes to the rules of the DAP platform for a period of 2 years. They have a service-oriented mandate towards the entire community.

Delegation of W-Tokens: Public Servants may delegate their W-Tokens to others.

The first Parliament consists of the founding members. Once the 10th DAP has been established, all DAPs automatically receive as many K-Tokens as there are seats in Parliament for their candidate nomination assemblies.

Candidate Nomination: The election of candidates from a DAP follows the procedure of a board list election in the highest division (International Division) in a Platform_Nomination_Member_General_Meeting. No later than 3 months, the K-Tokens must be assigned to the candidates; unassigned K-Tokens will automatically expire after this period.

Number of Public Servants in Parliament:

Formula: Delegates = round(30 * LN(0.01 * AuthenticatedUsers + 1) + 7, 0)

Number of delegates in Parlament

Authenticated Users	Delegates
10	10
100	28
1.000	79
10.000	145
100.000	214
1.000.000	283
10.000.000	352
100.000.000	421
1.000.000.000	491
10.000.000.000	560
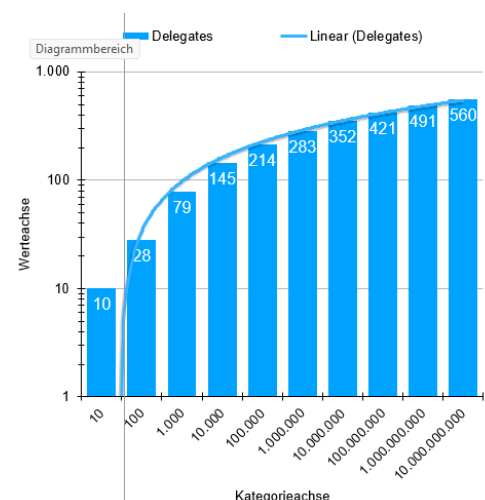
Formel: Delegates=round(30*LN(0,01*AuthenticatedUsers+1)+7;0)

Election Procedure: The election of Public Servants functions according to the municipal election principle. All verified users elect Public Servants from the DAP election lists by cumulative voting and cross-voting in a joint electoral process exactly 42 x 24 hours (campaign period) after the expiration of unassigned K-tokens. In this joint electoral process, all candidates, grouped by election lists, are up for election simultaneously. The election is conducted as follows:

a) **A-tokens for the electoral process:** Each verified user receives as many A-tokens (votes per election) as there are candidates to be elected. Each verified user can either dedicate their A-tokens entirely to one DAP election list or distribute them among individual candidates. Additionally, candidates can be struck from a DAP election list.

b) **Marking a list:** If a verified user wants to allocate all A-tokens to one election list, they simply select the election list. As a result, each candidate on this list receives exactly one A-token, and all allocated A-tokens are used up if the list contains the maximum number of candidates to be elected. If not, the verified user will be shown how many A-tokens they can still distribute.

c) **Cumulative voting:** The A-tokens can also be distributed among individual candidates. Each candidate can be assigned up to three A-tokens from a verified user (cumulative voting). Through such targeted vote distribution, certain candidates can receive more votes than others on the list, allowing them to advance to higher positions on the list.

d) **Striking candidates:** Conversely, candidates can also be struck from a DAP election list. If an A-token has been assigned to the entire list and simultaneously a zero has been placed behind a candidate's name, only the non-struck candidates on the list receive votes. The A-tokens remaining due to striking candidates are automatically distributed from top to bottom to the non-struck candidates on the marked list. Even in this case, no one may receive more than three A-tokens. Should more A-tokens remain and not be cross-voted (distributed to candidates from other election lists), they expire.

e) **Cross-voting:** It is possible to allocate A-tokens to candidates who are not on the preferred list. It is therefore permitted to distribute A-tokens across all election lists (cross-voting). Again, the rule applies that a maximum of three A-tokens per candidate may be allocated and the maximum number of A-tokens must not be exceeded.

2.8. The Board of the DAP Platform (Government)

The board of the association "DAP Platform" is the executive body of the DAP Platform and is referred to as the government. The task of the government is to fulfill the obligations set out in the articles of association, represent the DAP Platform externally, and implement the resolutions of the parliament and the general assembly of the association "DAP Platform." The executive board of the DAP Platform consists of: Chancellor, Vice-Chancellor, and Minister of Finance.

Whitepaper

Blockchain-based Platform for Decentralized Autonomous Parties (DAP Platform)

A provisional government is elected by the founding assembly of the DAP Platform from among the founding members. The founding assembly will decide on the initial number of advisory members.

The new chairman will invite the first constituent meeting within 14 x 24 hours. The government will make decisions through a consensus process.

Before triggering the re-election of the board, the government may again decide on the number of advisory members in the new board through systemic consensus. If the number of advisory members is changed, the term of the new board will begin only after the end of the user objection period through their veto right. Until then, the old board remains in office.

Once the 10th DAP board is constituted, all former and current members of the executive boards of the 10 DAPs will automatically receive a K-Token for personal candidacy for a government position, provided there are no blocks on that user. The K-Token authorizes them to use it for candidacy for a government position in the Polis for 30 x 24 hours. After this period, the provisional candidate list will be closed, and all verified users will be notified that the first round of voting has opened. Each voting round lasts 3 x 24 hours.

Once a candidate is elected, their K-Token expires, and running for an office is no longer possible. The elections take place in a publicly traceable manner for all users of the DAP platform. Only verified users are eligible to vote. The profiles of government candidates are publicly visible to all platform users. Each candidate must explicitly agree before the election begins that they are running for office, will accept the election if successful, and that they have had sufficient time to introduce themselves.

The executive board of the government is elected sequentially in secret and equal elections. First, the chairman, then a deputy, and a treasurer. For each of these three individual elections, each verified user will receive a new A-Token.

After that, the number of eligible board members at that time will be elected in a single election (simple list election). Each candidate who was not elected for the office in the previous election will automatically be asked, upon the conclusion of the election, if they wish to run again in the next election. They have 24 hours to respond, and if the answer is "Yes," they will automatically be added to the final candidate list for the next election, which will then be opened.

For the block election of board members, each verified user will receive as many new A-Tokens as there are positions to be filled. The A-Tokens can be distributed across all candidates in the final

candidate list, with each A-Token being assigned to only one candidate. All A-Tokens must be assigned at maximum, and at least one must be assigned. Unused A-Tokens will expire. The relative majority will decide. In case of a tie, a runoff election will automatically be triggered after the conclusion of the block election between the candidates who had a tie in the block election.

All users of the platform will be immediately notified of the final result of the government elections.

By-election of a government member: The moment an office becomes vacant during a term of office, the e-arbitrator will automatically trigger a by-election for this office for the remaining period of the term. The candidate nomination and individual election process will proceed in the same manner as the election for the executive board of the government

2.9. Arbitration Tribunal (Judiciary)

The compliance with platform-wide rules is guaranteed by the eArbitrator and elected arbitrators, both of whom decide on the basis of the constitution.

There is an arbitration tribunal for all DAPs and the constitution together, as well as a chamber of appeals. Both instances have at least one single judge.

Election of arbitrators: The founding parliament of the DAP platform elects 2 arbitrators from among its members, one for the arbitration tribunal and one for the chamber of appeals. All subsequent judges are elected by direct vote of all eligible voters. Any verified user can nominate themselves. All judges are elected for life but can be recalled at any time through a recall petition by referendum (only yes-no question). The rules are the same as for the veto right.

There is another judge election when:

a) All sitting judges of a chamber jointly decide, using the method of *Systemic Consensing*, that an additional *x* judges shall be elected. This decision must be communicated to all verified users. Verified users may lodge a veto against this decision. If, after the general deadlines applicable to the right of veto, no veto has been lodged by verified users, or if the veto has been rejected through the public objection procedure (*Volkseinwand*), Parliament shall elect the number of judges as determined by the sitting judges.

b) At the moment when the number of judges in office falls below the minimum number, all verified users are automatically informed by the e-arbitrator that the minimum number will be elected within 3 months.

Together with the notification about the necessity of the by-election, each verified user receives a K-Token, with which they can propose themselves as a candidate in the Polis. After 30 x 24 hours,

the candidate list is closed and the K-Tokens become invalid. Exactly 60 x 24 hours later the election takes place, for which all verified users receive as many A-Tokens as there are positions to fill. These A-Tokens are valid from the 61st x 24 hours to the 63rd x 24 hours.

All arbitrators are elected in a list election, sorted by last name. All candidates (arbitrators) who could unite the absolute majority of all cast A-Tokens are elected. If not all arbitrator positions are filled in the first ballot, a runoff election takes place among those candidates not elected in the first ballot from the 70th x 24 hours to the 73rd x 24 hours, in which the relative majority of cast A-Tokens is sufficient. If necessary, a further runoff election can be conducted in a third ballot from the 74th x 24 hours to the 74th x 24 hours. As soon as all arbitrators are elected or positions could not be filled, all verified users are informed.

2.10. Financial Audit (Court of Audit)

The Court of Audit consists of at least one auditor, who is elected in the Polis.

III. Cross-Platform Governance Rules

3.1. Fundamental Rights

The "Fundamental Rights, or User Rights" in the constitution limit the powers of the board and parliament in addition to the association's bylaws through the following immutable fundamental rights:

1. Disclosure may not be restricted (Disclosure)
2. The eArbitrator guarantees the liability principle for rule violations (Liability).
3. The veto right may not be restricted (Inviolability of dignity).
4. All users are equal before the arbitration tribunal and have, without distinction, equal claim to protection by the arbitration tribunal (Equality before the law).
5. Everyone has a right to verification (Citizenship).
6. The right to anonymity of the personal data of the original user, the transfer or temporary storage of data, and the destination in the IPFS network is inviolable (Secrecy of correspondence, posts and telecommunications).
7. The trust algorithm of the "Web of Trust" network of users is inviolable (Freedom of belief).
8. The censorship resistance of the IPFS network is inviolable (Freedom of expression).
9. The right to establish a DAP is inviolable (Freedom of association).
10. The possibility of creating a new user or excluding an existing user from the DAP platform may not be restricted (Right to life and integrity of the user).
11. I may do anything on the platform as long as I do not violate the rights of others (Individual freedom).

3.2. Systemic Consensing in the Polis

To minimize the conflict potential in controversial decisions between and against members and function holders, and to create more constructive work and satisfaction than "competitive voting," the following principle of consensing is used for decision-making in all cross-DAP platform decisions:

a) Consensing - Proposals: The discussion takes place for all users (publicly) in the Polis (Parliament). Only representatives of the DAPs can submit proposals according to the "Request For Comments" (RFC) principle in the Polis. Proposals for discussion must always include the current status quo along with the actual amendment proposal and may only contain open questions.

b) Consensing - Status Quo: It is the benchmark for any change. If there is more resistance to the change than to the status quo, the change is rejected. Therefore, in addition to the open questions, the passive option "what resistance do I have against changing nothing?" must always be asked.

c) Consensing - the procedure:

1. Each representative can submit a change proposal for voting. It costs x S-Tokens and must also include a status quo.
2. Each representative can add further change proposals for voting. Each proposal costs x S-Tokens.
3. Each representative can comment on all change proposals. Each comment costs y S-Tokens and loses 10% of its value every 24 hours. The order of comments is determined by their current weight in S-Tokens. Each representative can increase the weight of comments at any time by depositing additional S-Tokens (liking).
4. As soon as a 2nd solution proposal is added, a 24-hour countdown is triggered, after which voting begins. All representatives are informed about the start of the countdown.
5. Until the end of the countdown, each representative can add further change proposals for x S-Tokens for voting and comment on change proposals for y S-Tokens.
6. After the countdown expires, the voting round begins.
7. The voting round begins with an automatic distribution of 10x as many W-Tokens (resistance points) to each representative as there are change proposals including the status quo for voting.
8. At the same time, a new 24-hour countdown begins, within which all representatives can distribute their W-Tokens to the change proposals. Within the voting period, the W-Tokens can be delegated, added, changed, withdrawn, and/or added again.
9. If a representative has delegated their W-Tokens to another user, they can no longer use them themselves. The new holder of the W-Tokens is subject to the same rules as all other representatives. All W-Tokens are always only usable for a specific vote and lose their function afterward. They cannot be saved.
10. All solution proposals and the status quo must be rated with W-Tokens in the value range [0..10] during a vote. If a change proposal or the status quo has not been rated, all of the user's W-Tokens become invalid.
11. The solution proposal with the fewest W-Tokens is considered accepted. If the status quo has received the fewest resistance points, all change proposals are considered rejected.
12. If two or more solution proposals have received the fewest W-Tokens with a tie, a new 24-hour countdown with a new voting round is automatically triggered only with these solution proposals. Points 6-10 apply again for the round.
13. For the vote to become legally binding, at least z% (depending on the question, details regulated by the constitution) of the representatives must have participated.

3.3. Fraud Protection through Trust Network

Anyone can register as a user in the public network. Users maintain trust relationships with each other, resulting in a large trust network of users. Each user can assess other users in their trustworthiness with Veritas points from 0 to 1 (in tenths increments and inclusive) to exclude or

make content (fake news) and money fraud more difficult. If users do not have a direct trust relationship with each other, trust is calculated according to the following algorithm:

i.   find the shortest paths from user A to user B,
ii.   multiply all sections (segments) of the path from user A to user B with each other,
iii.   the obtained value is the trust value for the specific path,
iv.   find the maximum value, which is the trust value of user B for user A.
v.   If no paths exist from user A to user B, the trustworthiness = zero.
vi.   Trust can be built through personal acquaintance and/or publishing credible content.

3.4. Veto Right of Users

All verified users have a veto right against the decisions of the representatives as well as changes to the number of government (assessors) and arbitration court members (arbitrators).

Liability of the government: The members of the government are liable for damages to users if they implement the decisions of parliament before the period has expired within which users can exercise a veto.

Veto Right Procedure: Together with the notification about the publication of a parliament resolution in the Polis, all verified users automatically receive one V-Token each. The V-Token can be placed in a virtual "veto basket," which is automatically added to the veto-eligible publications in the Polis. These are valid for a maximum of 45 x 24 hours and all expire at the moment when 2.5% of the veto tokens issued for this publication have been received in the "veto basket" or after the expiry of the validity period (in case the 2.5% has not been reached).

As soon as 2.5% is reached, all verified users receive a notification together with an A-Token for a vote on a so-called "legislative objection," in which they can vote with "Yes, I am for the change" or "No, I am against the change" after another 45 x 24 hours. The notification must include the link to the full text of the amendment. The voting lasts 3 x 24 hours.

The amendment is rejected if at least 25% of the verified users have used their A-Token and a simple majority of them have chosen "No, I am against the change." After the end of the veto procedure, the decision is communicated to all users.

3.5. Verification Procedure of DAPs

a) Verification procedure: In the DAPs, there are four verification procedures that verify personal data of the members:

i.   The telephone number through a code via SMS,
ii.   Name through bank transfer to the foundation (fee),
iii.   Address through a TAN procedure by mail,

iv.   ID card/passport through Contact-WABEOor mandate examination commissions at general assemblies of individual DAPs.

v.   Election commission: The foundation manually checks all information of the candidates (their verification) for correctness before opening the candidate election to parliament in the Polis.

b) Sanction for verification fraud: Should it turn out that a DAP commits verification fraud, the case goes to the arbitration court to check culpability. The Contact persons who have verified incorrectly are marked (labeled) as "false verifiers" visible to all and are no longer allowed to sign for the one-time function "Contact-WABEO" or "mandate examination commission (verification iv)." Should the arbitration court determine systematic verification fraud, the sanction can lead to the forced closure of the DAP. Their governance tokens thereby become invalid/deleted.

3.6. Democratic Elections and Votes

In principle, all token holders can transfer their voting rights to others who then vote on their behalf. The DAPs have the option on the platform to adapt their elections and votes according to their own technical capabilities and the legal requirements of their country. They can choose from four voting procedures and three options for how to conduct their elections:

1) Type of voting procedure:
    a) Individual election,
    b) list election,
    c) consensing,
    d) cumulative voting and panachage
2) Type of election implementation:
    a) Online and On-Chain, where the assemblies are immediately stored on Rootstock
    b) Online, but Off-Chain with Lumino, where the assemblies are first stored in the Lumino system and at the end of the day stored on Rootstock together with other documents in one process;
    c) Offline sessions outside the blockchain, the results of which are recorded (documented) On-Chain.

3.7. Disclosure of Decisions and Their Traceability

All decisions and actions of users and function holders are stored immutably and indelibly. This data is retrievable at any time for authorized users and can optionally be signed by additional users. Data of the DAP that must be public or are marked as public by it, such as the bylaws, the names of board members, candidate lists, or press releases, are stored unencrypted on the file system of the P2P network and the hash to these on the blockchain to ensure an immutable history of changes. The signature of content ensures that all published information is authentic and immutable.

3.8. Automatic Sanctions (eArbitrator)

Rule-based processes that run automatically and can only be changed by following the rules ensure that violations of the bylaws are automatically sanctioned. Warnings and notifications are also sent automatically. The liability for breach of trust, i.e., the abuse of having the freedom to anonymously publish any opinion on the platform, is regulated by the trust network with its Veritas points. Abusers are punished with withdrawal of trust up to exclusion from the communication relationship (banning). In the decision-making processes, decisions are made on issues that affect everyone collectively, such as technical, economic, and organizational aspects of the platform.

IV. Special Guidelines for the Government

The exact rights and duties of the government arise from the current constitution of the Republic, but should include the following guidelines in the first version:

4.1. Working Committee

Government sessions: The government is obligated to convene for a session at least once a month and to promptly complete the incumbent tasks of management within the framework and spirit of the constitution.

4.2. Protocol Changes and Upgrades

Software upgrades: Decisions about updates and improvements of the underlying protocol to increase functionality, security, or efficiency. Bugs and security vulnerabilities: Measures to fix errors and security vulnerabilities in the code.

4.3. Economic Parameters

Fee structures: Determination of transaction fees for merge mining and the tax paid to the foundation. Inflation rates: Decisions about the issuance of new tokens and their distribution, which affects inflation within the platform.

4.4. Resource Management

Budgeting: Allocation of funds for development, marketing, community engagement, and other activities. Rewards and incentives: Determination of reward structures for DAPs and miners.

4.5. Rules and Guidelines

Terms of use: Creation and adaptation of terms of use and guidelines that govern the use of the platform. Compliance: Measures to comply with legal and regulatory requirements.

4.6. Marketplace

Decentralized applications (DApps): Approval of developers and support for new DApps to be developed and operated on the platform.

4.7. Community Management and Engagement

Community proposals: Organization of the decision-making process on proposals and initiatives from the DAP and nodes community concerning the further development of the platform. Disclosure and communication: Ensuring disclosed communication of the committee towards the

users. Community development: Funding of projects and initiatives that promote the platform's ecosystem.

V. Specific Technical Specifications

5.1. Architecture

The platform is based on Rootstock (RSK) for the implementation of smart contracts and uses IPFS for the decentralized storage of large data volumes. The means of payment within the platform is Bitcoin.

5.2. Implementation of Smart Contracts on Rootstock (RSK)

The platform is based on Rootstock (RSK), a smart contract platform built on the Bitcoin blockchain. RSK offers Turing-complete smart contracts written in Solidity and utilizes the security and stability of the Bitcoin blockchain.

RSK integration: The platform's smart contracts are executed on the RSK blockchain. RSK provides a Turing-complete environment for smart contracts written in Solidity. This environment is fully compatible with Ethereum, allowing developers to port existing Ethereum smart contracts to RSK with minimal changes.

5.3. RIF Lumino Network for Off-Chain Transactions

To accelerate transactions, they are processed offline with the RIF Lumino Network. The Lumino Network enables fast and cost-efficient off-chain transactions, which significantly improves the scalability and performance of the platform.

Off-chain scaling: The RIF Lumino Network is used to process transactions offline. This reduces the load on the main blockchain and allows for high transaction speed and low costs.

Functionality: The Lumino Network functions similarly to Bitcoin's Lightning Network. Users open payment channels in which they can conduct transactions without having to publish them immediately on the blockchain. Only the opening and closing of channels require an on-chain transaction.

Advantages: By using off-chain transactions in the Lumino Network, nearly instantaneous transactions can be conducted with minimal fees. This is particularly advantageous for microtransactions and frequent transactions within the DAPs.

5.4. Consensus Mechanism

The consensus mechanism of the platform is merge mining, where Bitcoin miners can simultaneously mine RSK blocks. This increases the security of the RSK blockchain by utilizing the hash rate of Bitcoin miners. Merge mining allows the same computational work to be used for

both the Bitcoin and RSK blockchains, thereby increasing efficiency and security. This means that smart contracts on RSK benefit from the robust and proven security of the Bitcoin blockchain.

On-chain voting: The votes of the parliament (Polis) and the government (management of the foundation) are always conducted directly on the Rootstock blockchain, using S-Tokens (tax points) and W-Tokens (resistance points). S-Tokens (tax points) are received by a DAP as a reward for paid tax, but not more than one token per day. They are necessary to trigger votes. W-Tokens (resistance points) are received by all representatives as soon as a vote is triggered.

Off-chain voting: The DAPs can choose between on-chain (Rootstock) and off-chain (Lumino) storage for their sessions, as well as the possibility to conduct sessions outside the blockchain and only store the documentation on-chain.

5.5. IPFS for Storing Large Data Volumes

Decentralized storage: Large files such as personal data, profile pictures, PDFs, and presentations are stored in a decentralized storage system like IPFS (InterPlanetary File System). IPFS stores data in small, distributed blocks and references them using cryptographic hashes.

Efficient storage and fast retrieval: By using IPFS, large data volumes can be efficiently stored and quickly retrieved. Each file is assigned a unique cryptographic hash that is stored in the blockchain.

Integrity verification: The blockchain stores only the hashes of the files, which can be used to verify the integrity and immutability of the data. Apart from the Bitcoin blockchain, only content that has been signed by a verified user as the author can be stored in IPFS.

5.6. Tokenomics

S-Tokens (tax points): DAPs receive S-Tokens when they pay taxes to the DAP platform. These tokens can only be used in the Polis and are communally available to the representatives. The DAPs independently regulate how the S-Tokens are distributed among the representatives. They can be saved, delegated, and used. Their transfer cannot be undone by the transferor.

W-Tokens (resistance points): W-Tokens are only made available to the representative for 24 hours for the voting process of systemic consensing and then expire. They cannot be saved.

A-Tokens (voting points): All verified members eligible to vote automatically receive A-Tokens with the opening of the respective election and they expire after the end of the election. For each election, there are new A-Tokens.

K-Tokens (candidate points): K-Tokens are received by all potential candidates, verified users with passive voting rights in the respective election procedure. The K-Tokens expire with the closing of the candidate list.

V-Tokens (veto points): All verified users automatically receive them after each amendment decision of the parliament and can be used for 3 months.

5.7. Security and Data Protection

The platform ensures the highest security standards to protect user data. Through the use of encryption technologies and secure communication protocols, the confidentiality and integrity of all data are ensured. Additionally, the platform uses optional timelocks in the smart contract, which sets a waiting time for transactions and informs members about them, so they can review or, if specified in the bylaws, decide about the execution themselves.

Personal data: All sensitive data is cryptographically encrypted and stored in the P2P network. The required access rights are ensured through the public keys of the corresponding users.

Large data volumes: For the publication of large data volumes, such as videos and other extensive content, there is a possibility for users to purchase storage space resources from other users of the platform.

5.8. Security and Verification Mechanisms

Verification through the blockchain: Despite the use of off-chain solutions like the Lumino Network, the final verification and settlement of all transactions are guaranteed by the Bitcoin blockchain and the RSK blockchain.

5.9 Network Latency and Global Distribution

Optimized consensus protocols: RSK uses optimized consensus protocols to minimize network delays and ensure fast transaction processing.

Global node distribution: The nodes in the RSK network are distributed worldwide, which leads to lower latency and better performance. A globally operating foundation supports the further development of the platform and the organization of sufficient nodes and data storage capacities for all DAPs.

VI. General Technical Specifications

6.1. Low Transaction Costs

Transaction costs should be kept as low as possible to ensure broad acceptance and use of the platform.

6.2. Real-time Requirements

The platform must ensure that transactions are stored no later than 10 minutes to meet real-time requirements.

6.3. Means of Payment

The means of payment within the DAP and on the platform is Bitcoin. This ensures a widely distributed and recognized digital currency that is accessible to all users. In the user interface, the current value is additionally displayed in various fiat currencies.

6.4. Communication Functions

The platform offers secure communication tools such as chat functions and video calls to enable seamless and secure interaction between users.

6.5. Support for Various Operating Systems

The platform must function on the following operating systems:

- Android,
- iOS
- SailfishOS
- Linux
- MacOS
- Windows

VII. Financing

7.1. Initial Development

The initial development shall take place through crowdfunding.

7.2. Revenue on the Platform

Tax: To ensure the further development and continued existence of the network, all users pay 1% of the transaction fees to the foundation in addition to the normal Rootstock transaction fees when storing data on the blockchain. This is called tax.

Data backup: The fees for securing data in the P2P network depend on the individual capabilities and prices of future private providers. Since the foundation has the task of securing the systems, it should, if possible, also be a provider of storage options and thereby generate revenue.

License fees: The foundation additionally earns from the fees for licensing providers on the marketplace.

VIII. Conclusion

The platform for Decentralized Autonomous Parties (DAPs) uses Rootstock (RSK) for the implementation of smart contracts and IPFS for the efficient storage of large data volumes. Bitcoin is used as the means of payment to enable transactions between participants.

The governance model of the platform encompasses a wide range of decisions concerning technical development, economic parameters, resource management, rules and guidelines, as well as community management. Through securing the fundamental rights of users, decentralization of decision-making through governance tokens, and the consensus mechanism, the platform becomes more democratic and the community of users becomes more strongly involved in the steering and further development. It guarantees freedom of expression, disclosure, liability, and the acceptance of self-imposed rules within the network.

Through the combination of these technologies, a secure, scalable, and efficient solution is created that meets the requirements of modern political organizations and can restore people's trust in politics.