Practical Byzantin Governance

Mitja Goroshevsky

November 23, 2020

Abstract

Problem of governance of a decentralized community is a consensus problem. Since the goal of any community governance is to reach a consensus about its decisions, the protocol must be proposed with some consensus rules, to which the community agrees including the rules of the protocol upgrades. If every part of the community starts creating its own rules for every decision they want to take consensus with other parties won't be reached in time of a conflict. Below I present informal specifications for a Practical Byzantin Governance protocol for Free TON and some discussion about it.

I

Let's think of a governance of a blockchain as a higher level social blockchain. One may also think about it as a virtual shard, a workchain of the existing Free TON blockchain. Let's call it "Governance Workchain". In order to participate in the decision making process a Participant must possess a token of such a workchain. Since the Utility of said token will be in its Voting power, the more such tokens the Participant has the more their Voting power is.

To be a community driven blockchain, decisions of its decentralized governance should be widely discussed. Without such discussion they lose their community status. After discussion every token holder should execute a direct vote for such a decision. There should be no delegation of votes. The Soft Majority Voting (SMV) should be used to make sure a representative decision is reached within the community with even low turn around or is not reached if no consensus exists.

There are many types of Proposals the Global Community should vote for. For example the partnership proposals, allocation of Funds to sub-governances, proposals to remove funding from a sub-governance, proposals to change the system itself by

adjusting its parameters or introducing new smart contracts. Let's agree that SMV should be the main decision mechanism on the consensus layer of our Governance Workchain, when all the community members need to vote (Community Voting). Unfortunately it is not always the case.

The problem of public funding has been discussed many times at length in the blockchain space but the best solution so far that the community came about is quadratic voting. The problem with the quadratic voting is that it solves something obscure. The real problem is not how to reach the decision on funding, but how to reach the decision on funding results. Community does not have a particular problem identifying areas where a solution is needed, but how to effectively judge those solutions once presented.

Let's presume our Blockchain needs to improve a protocol for which a deep knowledge of the technical aspects of our blockchain is needed and a set of mathematical and programming skills are necessary. Since these skills are quite rare we should assume that not many members of our community would possess such skills. It is clear that if we use an SMV for taking these decisions at best no decisions will be ever taken, at worst the community will be prone to manipulations, misrepresentations or altogether fraud. Therefore some other mechanism of reaching such decisions is needed. Fortunately Free TON already has part of the answer.

II

One of the problems of POS design is that it requires validators to have material stake in the network which they would be afraid of losing. This assumption provides a basic ground for Game Theory behind Proof of Stake. Participants are motivated to ensure the correctness of the blockchain by a possibility to lose their stakes if they don't. Usually POS blockchains begin with selling their tokens to future validators to create a starting point of this game economy. At Free TON it was very clear to everybody from the very beginning that we are not going to sell any tokens to nobody. The puzzle that we had to solve is how to distribute the tokens in such a way that the game theory of Proof of Stake allows. Free TON has found a revolutionary solution to that problem in the Meritocratic Token Distribution model (MTD). It starts from the community proposing a Contest in which all other members of the community can participate. The contest is discussed and if the community agrees that the end result of this Contest will benefit the community and the network as a whole, the budget to this contest is voted for via an SMV. Any member of the community can now participate by submitting their work to the contests. At the end the Jury votes for contest submissions and tokens are distributed to the winners. So now we have

another mechanism in addition to the SMV. We can distribute tokens based on Merit by the decision of all Participants (the Community) to provide funding for a Contest and then by the Jury to select winners. All is good except for now we face another problem: how do we select the Jury and most importantly how do we keep them honest. This problem is fundamental to our model and has never been addressed so far. But it was fundamental to blockchain sharding and has been addressed many times. Let's think of Contest as a block, a Submission as transaction and Jury as validators. It is quite clear that in order to preserve security we need the Jury to have skin in the game (i.e. stake), they should rotate as fast as possible between contests and finally the Fishermen should be there to verify the correctness of their judgement and punish Jury if they fail.

In blockchain the proof of block correctness or therefore blame of its incorrectness could be calculated. When we judge a Contest the results are most of the time subjective. Therefore a somewhat more complicated mechanism should be provided as described below.

To add some complexity on top, not all Contests are of the same domain of Merit and therefore could not be judged by the same Jury members, we need to introduce... sharding. Think different block structures requiring different sets of validators, yet bound by the same token and consensus rules.

III

It seems only logical if we choose a Jury from other winners of Free TON contests. Of course there is a problem of chicken and the egg but we already have the first set of jury and first contest winners in the community, which is a good starting point.

When a Contest is finished every winner is proposed to become a Jury Member. If they agree, 33% of their Contest Prize automatically goes to their Jury Stake in a special Governance DePool with a special Tag, indicating their domain of Merit, taken from the Contest Domain. Jury members are fully entitled to all rewards Governance DePool will generate but their Jury Stake will be used to guarantee the correctness of their judgement of the contests they judge. Jury members can always withdraw their stake from the Governance DePool as long as there are no active contests they participate in.[1]

Subsequently stakes in the Governance DePool are used to choose the Jury members for any particular Contest. For example a Contest with a Tag "JavaScript" takes place. All Governance DePool members whose Jury Stake is no less than a Jury Threshold and which has the Tag "JavaScript" attached are drawn into Jury

[1]Special "request for withdrawal" mechanism for Jury Members should be provided.

Elections for a random selection. Number of Jury members selected depends on the amount of Funding attached to the Contest. The amount should be adjustable by the Community Voting. Let's assume it is a 1 Jury member for every 100,000 TON Crystals of the Contest Prize Pool but no less than 3 Jury members.

The Jury Vote is taking place in which every Jury member has 1-10 points to allocate to each submission. They also must provide a written justification for their score. The justification should not be limited in size. 66% should vote to Reject the Submission altogether and must provide a ground for rejection. The Jury Voting time is set automatically based on its prize pool and number of submissions received. The minimum Jury Voting time is 1 week for all contests and proposals.

The Jury can Reject the Contest proposed by sub-governance if general governance rules described throughout this document are broken. If 66% of Jury members has Rejected a Contest a special committee is randomly formed from all Jury members. Such a Committee can initiate an SMV Proposal for Community voting to block the public funds in any sub-governance.

Once the Jury has voted for the submissions they are entitled for a portion of the Contest Prize Pool proportionally to their Jury Stake. The Jury compensation should be no less than 5% of the total prize pool of the contest and increase automatically with the number of submissions received.

Important to mention that a Rejection of submission or a Contest will not affect the total prize pool for the purpose of Jury compensation. Even if all submissions or a Contest are rejected the Jury should receive their part of the contest prize pool.

Before Jury receive their compensation the Blame Period of 1/3 of a Jury Voting time is set during which time Fishermen have the possibility to review the Jury Voting and their justifications.

In order to prove Jury fault Fishermen need to fill out the Blame form and attach a Value in TON Crystals to it. Once the value of total blames reaches a 66% of Jury Stake, the Blame is taken into consideration. The second round of Jury Election is taking place. The new Blame Jury is randomly selected this time having more Jury members than in the first attempt. The number of Blame Jury members increases by 66% every time. If there are no more Jury Members in the Governance DePool under selected Tag the selection includes similar tags, where similarity is measured as a simple proximity of other tags associated with the selected Jury set.

The Blame Jury is judging all contest submissions again. If the Blame is confirmed by the difference in score with the blamed Jury member, the Jury Contest Voting is recalculated, the Fishermen receives the blamed Jury Member Slashing amount minus a set fee for Blame Checking which Blame Jury receives.

If the Blame is not confirmed the Fishermen loses its Blame Value.

Jury Stake will be slashed for the following: "No show" — a portion of Jury stake is slashed if a Jury Member did not vote for a Contest they have been selected for. "Blame" — a portion of a stake is slashed If a Fishermen proves the judgement fraudulent or incompetent. Fishermen are then entitled to the portion of the Jury Stake that has been slashed.

If the Jury Stake is reduced below threshold they are losing the chance to be elected. The Jury can increase their stake by submitting more of their Contest Prizes into Governance DePool, but they can not transfer any other tokens to increase the Jury Stake.

IV

Following this logic we will have a structure where Community Voting would allocate funds to all Contests. This has been proved impractical. If all participants need to vote for every Contest there won't be enough contests approved. To correct this we need to introduce... multi governance blockchains. There is a similar structure in Free TON, it's called sub-governance. Sub-governance today is a manually created informal structure to which some funds are allocated based on the roadmap this sub-governance has proposed. The Jury is selected based on the internal Contest this sub-governance runs. For the purpose of this proposal sub-governance is a group of participants to which Community allocates some public funds. But the Jury selection is not handled by the sub-governance, the Jury from the Governance DePool is used instead greatly reducing the risk of fraud. Instead of the public funding a group can receive Private Funding. In fact once all Free TON givers will be exhausted the public funding should be naturally replaced with the private one. The sub-governance is a closed group where change of member status is voted for by an SMV voting. The group can have different settings for SMV voting, for example the Super Majority thresholds for inviting a new member or cancel a membership could be set up by the sub-governance voting.

Contests are the only type of proposals which should receive Public Funding from a sun-governance. If the Funding is provided to the sub-governance, it should only be used to fund Contests and no other type of funding distribution. Abuse of the system, by introducing types of Contests for which no competition is possible (such as "contractual or salary payments" in disguise) should be rejected by a Jury. [2]

[2]The main argument against other methods of token allocation is that it is going against the main value of Free TON — Meritocratic Token Distribution. As such it should be out of the scope of community funding. Second argument is that any such distribution outside of the Contest method will inevitably introduce more bureaucracy. Bureaucracy is not only ineffective, not only

V

Let's finish with a question we probably should be starting with: who can vote? In today's democracy the "one person — one vote" is almost universally used. It has been criticized over and over again but for real life democracy where every person's life depends on their country government decisions it is probably the only solution. The main argument about this is that the person can not voluntarily (meaning just upon the free will) leave. We can criticize this part as much as we want. The reality is that we are not yet living in a society where a person chooses a place to live. Fortunately Free TON is a digital reality. Everybody can come or exit at any time. Nobody imposing a participation on nobody. This by itself is a form of freedom every blockchain governance and consensus rely upon. As discussed above, in Proof-of-Stake it is a stake of native blockchain tokens which guarantees a participant its share in the protocol. Therefore it is obvious that participation in the governance of such a protocol must be directly tight to the amount of tokens a person stakes. But doesn't it create a problem of oligarchy?

Yes and No. "Marginal utility of money is the amount by which an individual's utility would be increased if given a small quantity of additional money, per unit of the increase. Additional money can increase utility in two ways. First, it is an addition to the wealth that a consumer can allocate to consumption. The marginal utility of money is then derived through the additional consumption it finances. Second, some models of money demand assume that consumers derive utility directly from holding money. The quantity of money held then enters as an argument of the utility function and the marginal utility of money arises from an increase in this argument." [3]

The latter in Free TON is achieved through staking. The former is a direct function of MTD. If the Token distribution would not be Meritocratic it must be something else — services, products or other value equivalent — something we do not have at the start.

Once an open market is established and the token is freely tradable such services and products start to appear and marginal utility of the token starts to be derived

it's rotting to the community, but it is going against the principle of decentralization. Last but not least it makes TON Crystal a financial security and as such a subject to potential evaluation by regulators. Any sub-governance that violates this rule is subject to security law violation in many jurisdictions. Tokens can only be distributed for the work that has been done where utility has been already established and can not be promised to be paid before such utility is created. The difference between an "investor", a "subcontractor" and an "entrepreneur" should always be clearly defined.

[3] https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100133871

from its power of consumption. At the same time the Givers that empowers MTD naturally dries out. Should we then claim that the MTD is over and forget about it?

If that is the case, then it is no longer the question of Oligarchy but of the need for network Governance altogether. The protection mechanisms then should be created to peacefully disband all governance and strip the network out of any possibility to change anything in a take-it or live-it kinda fashion. Oligarchy control over the Meritocratic network is only possible once Meritocracy is not providing any marginal utility. For clarity, it means, at that stage, Free TON no longer provides any more technical or business innovation on the protocol level. Similar to Bitcoin it is simply good at what it does.

If that is the network we want to build we do not need to start thinking now about how we build a sustainable decentralized governance but rather how we peacefully disband one, not how we create a framework for innovation, rather how we get the network into as stable a state as possible restricting any further changes. Not how we create a dynamic platform driving more developer entrepreneurs in, but how we accommodate speculators and exchanges that could use this blockchain for trading.

For me this scenario represents a departure from all Free TON values stated in its Declaration of Decentralization. Soft Majority Voting as a principle decision reaching algorithm is specified there. The community driven network simply implies there is a sustainable community driven decentralized governance. Only through such governance can we build a decentralized platform for massive use cases and therefore a marginal utility of its token.

In order to achieve that we need not only to think how tokens from initial supply will be distributed, but how we continue to support MTD even after the initial givers dry out. Only through such mechanisms can we ensure that the only oligarchy we create is the Oligarchy of Merit. Such Oligarchy would never become a problem as long as distribution is more or less balanced across many domains of merit.

About the Author

I am Mitja Goroshevsky co-founder and CTO of TON Labs. I am Israeli, I have more than 25 years experience in building IT projects, have co-founded and led Delta Three Corporation, Internet Telecom, Popular Telephony; have patents in distributed computing, developed first serverless concept back in 2004, has been following Bitcoin from 2009, started chat based crypto messenger based on Ripple, was an architect for several projects on Ethereum blockchain before joining TON Labs. I am the Author of first draft of the original Declaration of Decentralization of Free TON, I am one of the authors behind Free TON key Improvement Proposals, such as Free Software License TON VM Opcode, Distributed Token architecture, Practical Byzantine Dynamic Slashing, Decentralized Pools and Decentralized Bots which are part of End-to-end Decentralization concept I have introduced. TON Labs is a core developer of Free TON, we have been implementing independently TON protocol in Rust computer language for 2.5 years now, based solely on blockchain specifications available then. In total TON Labs has contributed more than 2 m. lines of Free Software Code to the Free TON ecosystem which formed the basis for Free TON network software stack, we call TON OS. When Free TON was launched we have been involved in design and implementation of key protocol changes which is quite a substantial departure from the original design of Dr. Durov. The key reasons behind those changes on top of general protocol improvements relates to the decentralization aspect of the network.