Practical BFT Governance

By Mitja Goroshevsky

Second Edition

DRAFT V

“All government officials,” Melith explained, “wear the badge of office, which contains a traditional amount of tessium, an explosive you may have heard of. The charge is radio-controlled from the Citizens Booth. Any citizen has access to the Booth, for the purpose of expressing his disapproval of the government.” Melith sighed. “This will go down as a permanent black mark against poor Borg’s record.”

“You let the people express their disapproval by blowing up officials?” Goodman croaked, appalled.

“It’s the only way that means anything,” said Melith “Check and balance. Just as the people are in our hands, so we are in the people’s hands”.

“And that’s why he wanted me to take over his term. Why didn’t anyone tell me?”

“You didn’t ask,” Melith said, with the suspicion of a smile, “Don’t look so horrified. Assassination is always possible, you know, on any planet, under any government. We try to make it a constructive thing. Under this system, the people never lose touch with the government, and the government never tries to assume dictatorial powers. And, since everyone knows he can turn to the Citizens Booth, you’d be surprised how sparingly it’s used. Of course, there are always hotheads…”

Goodman got to his feet and started to the door, not looking at Borg’s body.

“Don’t you still want the Presidency?” asked Melith.

“No!”

“That’s so like you Terrans,” Melith remarked sadly. “You want responsibility only if it doesn’t incur risk. That’s the wrong attitude for running a government.”

— Robert Sheckley. A Ticket to Tranai

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 Fault Tolerant Governance protocol for Free TON and some discussion about it.

The Governance

Let's think of the governance of a blockchain as a higher level social blockchain. One may also think about it as a virtual shard, a workchain[1], taking the analogy from the existing Free TON blockchain. 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) may be used[2] to make sure a representative decision is reached within the community with even low turnaround 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 system 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 funding[3]. The problem with quadratic funding 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.

---

[1] Telegram Open Network, by Dr. Nikolai Durov, https://ton.org/ton.pdf, p.5
[2] As described in Free TON Declaration of Decentralization
[3] Quadratic Payments: A Primer, Vitalik Buterin, https://vitalik.ca/general/2019/12/07/quadratic.html

Meritocratic Token Distribution

One of the problems of POS design[4] 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[5].

Usually POS blockchains begin with selling their tokens to future validators to create a starting point of this game. 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 tokens in such a way that the game theory of Proof of Stake allows.

Free TON has found a 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.

The Sub-Governance

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. Let's think of it as a sort of sharding.

To achieve further scalability of MTD the community can form Groups (also called sub-governances) which apply for a broader scope of contests. In this case the community votes not for a one particular contest but for a budgetary framework for a series of contests to be run by the Group.

For the purpose of this proposal sub-governance is a group of participants to which the Community allocates some public funds. But similar to how sharding is organized in a multi sharded blockchain today and for exactly the same reasons, the Jury selection should never be handled by the sub-governance. The group Jury, like a validator set in the proof-of-stake blockchain, should be selected from the broader community in order to reduce the risk of fraud. The Jury should also rotate from contest to contest in a random fashion exactly like shards' validator set is rotated.

---

[4] https://www.peercoin.net/whitepapers/peercoin-paper.pdf
[5] https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

Instead of public funding a group can receive private funding. In fact once all Free TON community tokens will be exhausted the public funding should be naturally replaced with the private one. Yet the Jury selection for the private funding could remain the same. The private contest would therefore be judged by the same public jury consensus improving the security of the sub-governance voting, helping to ensure the investor of the fair distribution of their funds, if of course such distribution is desired.

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 cancelling a membership could be set up by the sub-governance voting.

Contests are the only type of proposals which may receive Public Funding from the Community. 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.[6]

In any event we now have another mechanism in addition to the SMV. We can distribute tokens based on merit by the decision of all participants, i.e. the community, to provide funding for a Contest or a set of Contests in a Group and then by the Jury to select winners.

The Jury

With the introduction of Groups which can create their own contests we have added an additional vector of attack on our governance system. If Jury is selected from within the Group it might clearly lead to Jury corruption and Group collusion. Now we need to decide how we select the Jury and most importantly how do we keep them honest.

This problem is very similar to a problem of selecting a set of validators in a sharded blockchain and has been addressed in this context before.

Let’s think of a contest as a block, a submission as a 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.

[6] The main argument against other methods of token allocation is that it is not aligned with 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 it’s rotting to the community, but it is going against the principle of decentralization.

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 the jury if they fail.

In blockchain the proof of block correctness or therefore blame of its incorrectness could be verified[7]. When we judge a contest the results are most of the time subjective. Therefore a somewhat more complicated mechanism will probably be required, 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, therefore we need to introduce a sort of governance sharding. Think of different block structures requiring different sets of validators, yet bound by the same token and consensus rules.

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. Let's call it a zero state problem. Since we already have the first set of jury and first contest winners in the Free TON community, it could be used to create such a zero state. Generalizing, to start such a governance system one would probably need to run a series of dedicated contests with trusted Jury to choose more qualified jury members.

When a contest is finished every winner is proposed to become a jury member. If they agree, a portion of their contest prize automatically goes to their jury stake into a special Governance DePool[8] with a Tag attached, 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.[9]

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.

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 in the upper 90 pct. of all jury stakes which currently are not participating in any other contest judgements (jury threshold) and which has the Tag “JavaScript” attached are drawn into Jury Elections for a random[10] selection. Number of Jury

[7] https://computersciencewiki.org/index.php/Merkle_proof
[8] https://docs.ton.dev/86757ecb2/p/45d6eb-depool-specifications
[9] Special “request for withdrawal” mechanism for Jury Members should be provided.
[10] Random means pseudo random function available in Free TON Virtual Machine from F810–F81F instructions range.

stakes *NJS* selected by random pulling of Jury members until the total available stakes of the Jury reaches the pool prize.

Tag indicates the Contest domain. It must be part of a contest's smart contract meta-data. The Contest can have several Tags if several domains of expertise are required. In which case only a Jury group which has all the Tags listed will be selected. If the available Jury group is less than 5 members the contest can not be submitted for Voting. Since Jury is selected by Tag, the Tag manipulation is a potential threat. Therefore the community or sub-governance group should discuss the Tag selection of a particular contest. The Jury can reject the contest based on its Tag selection, i.e. the particular contest does not fit into a particular jury group domain of expertise.

The Jury Vote

The jury vote is taking place in which every Jury member has 1-10 points to allocate to each submission.

The Jury Selection as well as Jury vote are pseudo anonymous using any kind of suitable commit-reveal scheme. At the end of the voting the Jury will send an open vote into a JMVC which will compare hashes of all scores and comments and send a message to Jury Root. Jury Root will verify that the JMVC is original and accept the Vote. The Jury key is accepted only after the voting period ends.

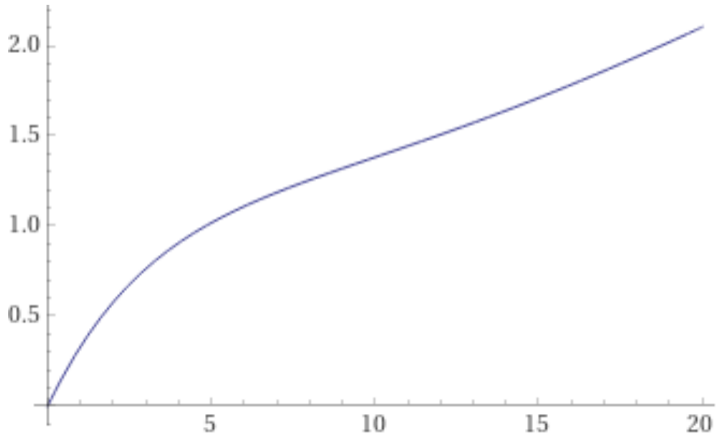
Every Jury member must provide a written justification for their score. The justification should not be limited in size.

The jury voting time *VT* is set automatically based on its prize pool *PP* and number of submissions *NS* received $VT \sim PP \times NS$. The minimum Jury Voting time is 1 week for all contests and proposals.

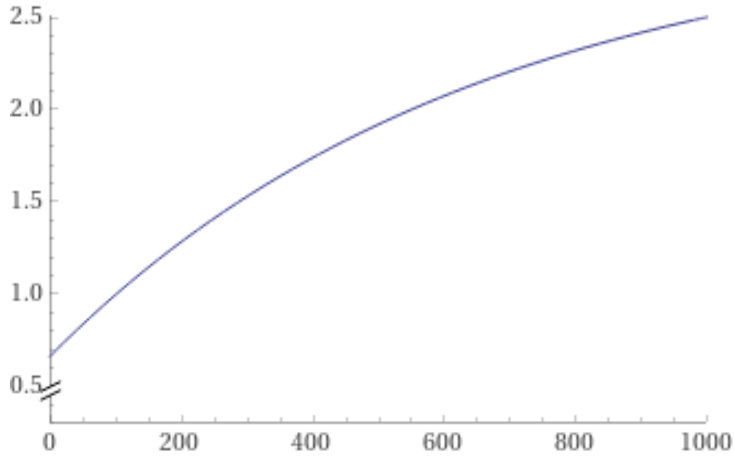
To estimate the time period for the judgement process let's suggest that we need 33% of total contest duration *CD* for the case if we have only one submission, and 10% of total contest duration for each "infinite" submission. So that we propose the relation

VT' (TS) = CD*F(PP)*TS*(10%+23%*exp((1-TS)/5))
VT (TS) = max [*VT'* (TS) , 1 week]

with PP0 normalization factor set to 100,000 TON F(PP) = 3 - 7/3*(6/7)^(PP/PP0). so that F(0) = 66%, F(PP0) = 1, F(∞) = 3.



Plot of VT'(TS) with PP = PP0 and CD = 1.



Plot of F(PP) with PP0 = 100.

The Jury is expected to vote monotonically over a voting period. The Voting period is then divided by the number of submissions and it is expected from the Jury members to vote for at least one submission in each of these periods. If a Jury member is missing 33% of its slots their reward is reduced by 5% each time until it reaches 50% of the Jury reward which is slashed if not all the submissions are scored proportionally.

The Jury can reject the contest proposed by sub-governance if general governance rules described throughout this document are broken. If 66% of jury member stakes have rejected a contest, a special committee is randomly formed from all jury members. Such a rejection will automatically create an SMV Proposal for Community voting to block the public funds in that 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.

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.

The Jury member can not abstain from the vote for any reason.

The Jury and Administrative Compensation

The Jury should be well compensated for their work as we should expect high quality judgement over even most complicated contests.
The jury compensation *JC* should be a proportion of Voting Time VT to the total prize pool *PP* of the contest:

$$JP = (VT/CD)*PP/F(PP)$$

The administrative support is everything that relates to the contest creation, preparation, promotion and discussion. The administrative support is up to 2% and should be indicated in the contest submission with community members wallets together with the portion of the administrative support. Whenever the community accepts the Contest it automatically accepts the payment of the administration fees therefor.

The Slashing

Before Jury receive their compensation the blame period of ⅓ of a jury voting time is set during which time Fishermen have the possibility to review the jury voting and their justifications. If no action is taking place the Fishermen stake is returned to the Fisherman minus commissions.

In order to prove jury fault fishermen need to use a blame method of the contest smart contract to submit a blame and attach some TON Crystals to it. Once the value in TONs of total blames reaches a total price of Blame Jury necessary to conduct investigation plus some commission (say 5%), 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 33% 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 proximity to other tags associated with the

selected jury set. If the whole available jury pool is exhausted the SMV voting is used in the last round to determine the outcome.

The Blame Jury is judging all contest submissions again. If the blame is confirmed by the difference in new score from the original score with deviation described below, the jury contest voting is recalculated.

We suggest that every submission is to have some fair score and define it in the following way. We suggest that a certain neighborhood of the mean score value corresponds to the honest judgement and outlying values correspond to incorrect (or malicious) jury behaviour. The honesty interval we define as [m - 33% M, m + 33% M], where m is the calculated mean value and M is the max score (currently 10). So, for example if the mean value is 4, the honesty interval is [1;7].

The malicious rank is determined as follows: r' = r*(1-a) + a*rc , where r' is new rank, a - some rate constant which should be defined further base on the convergence ability of the rank on real network data, rc - current blaming rank which is given by the relation

rc = 0, for v in honesty interval ;
rc = | v - m | / M.

That is, rc goes to 1 e.g. when v = 0 (the submission is rejected) for the blaming jury while the mean value is set to M.

Then with the current rank *r* the stake of the jury is reduced by the *r* as a factor. Every correct jury can improve the rank due to the given algorithm.

The convicted Jury Member is deprived of its jury reward which the Blame Jury receives instead. The convicted Jury Member is slashed. The Fisherman receives the slashed value.

"No show" — a portion Equivalent to getting ⅓ as a current rc rank of Jury stake is slashed if a Jury Member did not vote for a contest they have been selected for.

The Prize

Another problem regarding MTD our community faces is determining the contest prize pool. There have been many proposals to somehow make this determination algorithmic. Indeed while the community can judge if in general some funds should or should not be directed

somewhere, it is very hard for a person which does not possess specific expertees to judge if a particular prize pool is adequate for a particular field.

Let's remember that the main purpose of the Contest is to encourage as many people as possible to contribute value to the Free TON in exchange for tokens. Therefore it is the quantity and the quality of the submissions that we are after. Simply speaking we could create a mechanism by which the prize pool will be a function of how many quality submissions have been made. It is quite easy to obtain these parameters. The quantity is obviously a simple submissions count method of a contest smart contract and the quality is judged by the jury as described above.

The community or sub-governance for that matter only needs to provide a prize for the winning solution (1st place) and contest duration. -> PP (to be used in previous formulas), and prizes for each winning place

For the given Contest Prize Pool PP the jury point value is calculated as:

$$PV = PP/\left(NS\left[Highest\ score - \left((Highest\ score * 2/3/10)\ \hat{}\ 2\right)\right] \times 10\right)$$

where NS is any number of submissions above the threshold. Then the final prize for every submission is calculated as the number of points received multiplied by the point value PV.

Note that the ballpark budget provided by the sub governance won't be distributed in full most of the time.

Unfortunately, the contribution to one contest does not equal economically to a contribution to another with a similar score. Therefore in the future a mechanism may be developed that would determine the rough ballpark figure of economical value of the contest score depending on the contest domain.

In blockchain we have only one mechanism which determines the economic value of a system. It is gas fees such a system pays. Therefore it is quite easy to calculate the economic value of a Contest. For that we need to take a hash of every contract that was produced by this contest and sum up all the gas all of existing contracts with this hash paid up to a particular date.

Of course for the first contests this figure has to be guessed by the organisers. But as time progresses this figure will be automatically adjusted.

Now, knowing the value we can predict what ballpark value of the prize pool certain tags can have.

What about contests that do not create smart contracts? Such as social contests, mem contests, media and PR contests and so on. I believe all these contests must have at least one smart contract as an output. Otherwise they do not contribute to the blockchain.

Let's consider a contest for a social meme. If the use of the meme promotes a project it must be reflected somewhere on-chain. If we can not track the on-chain effect of this contest it can not be funded by the community public funds. The contest designers must therefore create a way to measure the contest outcome. A backlink to the smart contract, a hidden "treasure" inside some wallet qr-code and so on. It is possible to write a book "the art of contest design" on that subject, but this is outside of the scope of this work.

Any contest winnings should be distributed automatically after the Blame period is ended[11]

The Vote

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's 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 is imposing a participation on somebody else. 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 tied to the amount of tokens a person stakes.

But doesn't it create a problem of oligarchy? Yes and No.

[11] In order to be useful, sometimes contest winning solutions require active development and support by its authors. Currently this is done by all sorts of vesting schemes but it is tedious to manually control the payments and the required level of participants support. In our opinion any kind of vesting schemes should be avoided as they add extreme amounts of bureaucracy. Instead a Decentralized Git solution should be considered which creates Contest proposals out of Issues and Feature requests. In general large contests should be avoided as much as possible and smaller, focused contests should be preferred instead.

“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*.”[12]

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, something that should not be subject to public funding distribution mechanism anyways.

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 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.

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

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. It is 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.

Acknowledgments

Special thanks to Andrey Lyashin for his review and important additions to this work.

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, including inventing the word “serverless”; 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 (DePools), Decentralized Bots (DeBots) and Decentralized Name Service (DeNS) 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 the 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 were involved in the design and implementation of key protocol changes which is quite a substantial departure from the original design of Dr. Nikolai Durov. The key reasons behind those changes on top of protocol security and performance improvements are the decentralization aspects of the network governance.