AERUM PROTOCOL - FREQUENTLY ASKED QUESTIONS

Q: *Since the transactions will not have fees, how will the network be maintained? And how exchanges will deal with rates, since they charge network fees for withdrawal?*

A: Aerum features a fee subsidizing model where fees (which exists) are subsidized by a dApp operator in order to simplify process of purchase/engagement for service/goods consumer. It features s a Proof of Stake with unique cross-chain consensus created by us, called ATMOS. It allows having a noninflationary token model, while providing enough incentive to stake the network and earn coins. We are 30-50x faster than Ethereum already and we have a clear scalability solution that can bring us to 100,000+ tps.

At the same time, since we are running a dxPoS consensus, coins are minted and distributed to token holders, effectively dApp operator can be a token holder who stakes tokens or even become a Delegate (validator) and receive a part of block reward. There is a minting cliff built in and at certain point rewards will come from transaction processing during the block creation.

Our model is noninflationary as we have a separate EIP20 token on Ethereum blockchain that secures the consensus and a coin that fuels transactions on Aerum.

Q: What is blockchain 3.0?

Bitcoin appeared in 2009 and was the first blockchain ever created. Many other blockchains were derived or "forked" from its code, like Litecoin or Dogecoin. They commonly referred as Blockchains 1.0 or the first generation of blockchains. They are primarily targeting financial functions and are not suitable of providing a complex set of decentralized utilities. Blockchain 2.0 was created with the arrival of Ethereum in 2014. Ethereum has provided with versatile and not specialized approach to decentralized computing on a blockchain. One of the very defining characteristics of Ethereum was ability to conveniently create a custom cryptocurrency by anyone. It's commonly referred as "tokens" now. Within a year or two other blockchain projects were created that took that "token" idea to a heart such as BitShares, NXT, and others. These solutions were still isolated in a sense that they did not support interconnectedness with other blockchains and their security was solely based on their own hash power (in case of PoW consensus) or their internal perceived value (in case of PoS). They also had limited performance and often high transaction fees once network adoption grows. Blockchain 3.0 in our opinion should provide with a mechanism to enable users to transact for free or very inexpensively, have high throughput and short transaction time, be interconnected to provide users with ability to transfer value (tokens, cryptocurrency) between blockchains and to enhance security by collaborating with other blockchains. Another very important aspect is to boost user experiences and make it accessible not only for geeks but broader audiences. We believe Aerum delivers on all of these fronts.

Q: What is actually meant by “value”?

A: By value we assume anything that can provide a quantifiable utility to the user, such as cryptocurrency coins or tokens.

Q: Where are transactions recorded?

A: Transactions are recorded in a decentralized ledger shared by all nodes on the network. Anybody who wants to run a blockchain software will get a copy of all the data.

Q: What is the main “fuel” of Aerum?

A: Aerum uses XRM tokens on Ethereum mainnet to provide with a way to access Aerum utility and become stakeholders for the users. Any stakeholder can participate in regular Aerum native cryptocurrency distributions which is used to pay transaction fees on Aerum. Token is not getting spent and distributions happen regularly which gives access to "free" transactions on Aerum. SME and Apps operators can sponsor users transactions by holding a balance of XRM tokens in a staking contract and share received coins with their users.

Q: How is it technically possible to have such a little time to complete transactions?

A: Aerum runs unique consensus delegated cross chain consensus algorithm called ATMOS that helps to improve transaction speed while battling centralization. In short, by having smart contracts to select a Committee of voted in business participants (delegates) to sign blocks using professional setup for a short while we are able to boost performance and reduce centralization same time.

Q: Can we compare Aerum with BitTorrent? In a sense the more people use it, the higher speed is achieved.

A: In a sense - yes. As network grows, more participants are adding nodes on the network and improving accessibility and availability of the services, removing dependency on singular gateways and access points.

Q: Are there mechanisms to protect against system failure and data loss?

A: Public blockchain is a permissionless ledger, while we strive to maintain decentralization and censorship-free environment, in case of a serious abuse decentralized governance mechanism may decide on best course of action through the token-based voting in a liquid democracy manner.

Q: What consensus model does Aerum use?

A: Aerum uses delegated cross chain Proof of Stake. It is powered by XRM tokens on Ethereum which users can use to give or remove voting power from certain Delegates who form network consensus for Aerum blockchain.

Q: Can you “hide” a transaction?

A: The blockchain itself is a public ledger, meaning all operations are open to public. However in specific cases certain measures might be applied to make transactions private by means of encryption or technologies like ZK-Snarks and ZK-Starks. These technologies are in active development and Aerum will implement them on system-wide level as soon as they will be ready for practical use.

Q: Is the XRM supply infinite?

A: Yes, XRM supply is finite and is set to 1 Billion (1,000,000,000) tokens without the possibility to create (mint) more tokens.

Q: How do I mine XRM?

A: Tokens are not minable, however, through owning tokens and staking them anybody can participate in Aerum blockchain cryptocurrency minting process. As network use growth we believe a certain market will be established for that cryptocurrency.

Q: Where value is derived from in Aerum ecosystem?

A: Value of Aerum network as a whole and its XRM token is derived from its utility - ability to provide with fast, free, decentralized transactions over the public ledger while having access to cross-chain atomic swaps, decentralized exchange and end-user designed set of tools users and business owners need to transact on blockchain. Participants can generate value by holding and staking XRM token, establish a Liquidity Provider entity, become a Delegate, offer services and dApps.

Q: What is the difference between account and “wallet contract”?

A: On Aerum, wallet contract is a smart contract which can hold cryptocurrency or tokens while user needs to have access to designated account in order to operate that wallet contract. It can be a multi-signature wallets, DAO wallets, vesting wallets and as such. Account is always needed to access contract-based wallets, meaning user need to possess account's private key.

Q: Can a transaction be sent by a third party? i.e can transaction broadcasting be outsourced?

A: Yes, transaction can be sent by any third party (relaying or broadcasting) as long as it is signed by originator's private key and contains digital signature. Then it can even be created offline on "airgapped" computer and loaded to the blockchain software using a flash card or usd drive to be broadcasted to the network.

Q: Can AERUM contracts pull data using third- party APIs?

A: Contracts cannot poll external sources of data, however, external data providers can feed contracts with outside data, operating as "Oracles". Aerum is well-capable of using any oraclization technologies and is actively working towards bringing most prominent of them to the users.

Q: Is the content of the data and contracts sent over the Aerum network encrypted?

A: The blockchain data itself is not encrypted, however, it's authenticity is protected by digital signatures created when transaction is being prepared which uses asymmetric key elliptic curve cryptography. However, users can chose to encrypt the data for storage on blockchain or for peer-to-peer transmission.

Q: Can i store secrets or passwords on the Aerum network?

A: It is possible if encryption or zero-knowledge proof technologies are used.

Q: How will Aerum deal with ever increasing blockchain size?

A: We honestly don't believe this to be a big problem. Most nodes excluding archival nodes can use pruning to get rid of very old information. As network use grows we envision that most active Delegates will utilize our PlasmaBIT software package to run their own child networks on top of Aerum reducing the load on Aerum significantly. And last but not the least - computer memory and drive capacity increases much faster than blockchain grows and cost of that capacity constantly declines. We don't see it as a big problem since we don't see future of blockchain with most of the users running their own full nodes and having to deal with large data sets. We believe node operatorship will be professionalized.

Q: Where do contracts reside?

A: Smart contracts code and data set is stored in blockchain and distributed among all nodes just like any other data. Every node has a copy of it and executes all the code while verifying incoming blocks.

Q: Is it possible to cancel or overwrite a transaction?

A: It is possible to replace a transaction while it is waiting to be mined in the transaction pool. Usually it is done when the gas price is set too low, which is a regular problem on Ethereum. On Aerum usually transaction will go through so fast there will be no reason to reset the gas price.

Q: Does Aerum support scripting? If so, what types of scripting?

A: Aerum supports scripting. The main language supported is Solidity, however it is very likely that more languages will be added in future.

Q: Is it possible to call contract function from another contract without consuming Gas?

A: It is not possible by the design - to prevent network spamming and clogging. However, Aerum is designed in such a way that gas will cost no money to users while operating for legitimate reasons, as it will be sponsored by application operator or user can received as a result of staking their XRM tokens.

Q: How do I prevent further theft from my compromised Aerum address?

A: In short - by having a good security hygiene, not writing your private keys or recovery phrases on post-it notes, using hardware keys. If you feel like your account might be compromised - immediately create a new account (for example using AerumWallet) and transfer all tokens and then remaining cryptocurrency to a new account.

Q: Ethereum 2.0 is a proposal I look forward to seeing in action. In what way would you say it would be better than Ethereum classic?

A: Aerum has up to 500 tps without employing scaling, ETC has same throughput as Ethereum. These are key differences:
- Aerum has tx time of ~5 seconds, ETC ~20s
- Aerum has tx finality in about ~10 sec, ETC ~60 blocks
- Aerum is secured by dxPoS, uses staking mechanism, governance is secured by Ethereum mainnet hash power, ETC uses PoW and has low hash power (easy to manipulate and take over)

Q: How do you deal with Spam problem? There is enough Spam being sent to Ethereum mainnet even with high transaction costs.

A: Spam is possible but this is why we do not remove gas completely but instead distribute it through block rewards to stakeholders who are airdropping it to their customers on need to have basis we believe it is a better solution than EOS with their RAM purchase and price manipulations. Our governance mechanism will have ability to slash wrongdoers stake via a vote, and outsiders should never have too much gas to generate a lot of spam. In essence our governance is based on similar ideas as Casper, and in essence we use Ethereum mainnet as our beacon chain

Q: Ethereum mainnet have a scalability problem. How does Aerum prepare to face a similar situation?

A: - It's a totally new network, not a hard fork, based on delegated cross-chain Proof of Stake, token distribution and purchasing will actually speed up adoption. Network is fully compatible with Ethereum, and is linked to it via atomic swaps and collateral bridge allowing users to transfer their tokens from and to Ethereum from day 1. We are not trying to replace Ethereum, rather to enhance it with a practical solution that can mitigate multiple performance and cost issues right away, not sometimes.
Aerum has a scalability solution from the get-go, utilizing its unique consensus algorithm, that will allow Aerum ecosystem to scale up to 100,000+ tps and beyond on demand.

Q: I am aware of some other projects which have the same angle to speed up Ethereum with some kind of side chain. What makes your solution better than these?

A: Aerum has already a functional prototype, well tested network and a set of tools to get both developers and users up to speed. Right from the start users and dApp operators can use and integrate with our functional wallet for both desktop and mobile platforms, supporting atomic swaps, decentralized atomic token transfer between Ethereum and Aerum in both directions, name-based addressing system and many more features already implemented. Aerum is based on a new kind of consensus mechanism connecting two blockchains: Aerum and Ethereum allowing to provide both superior security and outstanding decentralization through application of liquid democracy principles.

Q: With a game like ETH Town just released I can really feel the need for a quick solution again. The gas cost are getting higher and i'm afraid it will scare of new users of the project. How much work would such a project have switch over to your chain for the gas-free environment? Is that a lot of work or just some adjustments?

A: It has virtually no costs. Contracts and dApps can be migrated without any code changes except checking for the network id. In order to provide your users with free gas, you will need to get some Aerum tokens (XRM) and stake it to participate in coin distribution. Then our mechanisms will allow you to generate paper wallets containing coins on the fly and automatically deliver it to user's wallets.

Q: A necessary and very relevant project. Can you explain in more detail what it means for end users free of charge? If I want to transfer tokens from one address to another, will this operation be free?

A: In order to provide protection from Spam and DDOS attacks, some sort of stake in the system is required. Aerum uses delegated cross chain Proof of Stake consensus mechanism to secure the network. It requires users to own XRM token on Ethereum network and stake it to participate in Aerum network native cryptocurrency distribution. This cryptocurrency is used to pay transaction fees. However it comes at no cost to token holders as tokens are not getting spent and distributions happen regularly. Owning 100 XRM staked tokens gives you a possibility to get enough cryptocurrency on Aerum to execute 1 transfer transaction per day every day.