Technical Lightpaper
LUKSO Blockchain

FABIAN VOGELSTELLER
Author ERC 20, ERC 725
Blockchain Architect, LUKSO Blockchain GmbH
Berlin, Germany

fabian@lukso.network

February 10th, 2020
Version 3

Abstract

This paper presents the basic technical components, and the direction of research and development of the *LUKSO Blockchain*. The *LUKSO Blockchain* is dedicated to the lifestyle industries with the goal to bring together industry players, consumers, creatives, developers and innovators to build and run use cases by leveraging a common Blockchain infrastructure. The *LUKSO Blockchain* will be based on the *Ethereum Virtual Machine (EVM)*, as the most advanced and developed smart contract Blockchain protocol. The *LUKSO Blockchain Foundation* (currently registered under the name Lukso Blockchain GmbH) will be innovating and researching on aspects of the consensus layer of the network, and around smart contract standards to fit the needs of a domain specific Blockchain. The LYX coin will be the networks native cryptocurrency, which is required for transaction fees to run smart contracts and LYX transfers itself, as well as staking for block producers. Ownership of LYX will be partly distributed through a public ICO executed in a novel way as a "Reversible ICO" or rICO. This system balances control between participants and receivers of the ICO Funds and is described in detail in this Paper further down.

1 Introduction

Blockchain is a revolutionary technology that creates a level playing field for unknown ACTORS to participate in an ecosystem. In this new ecosystem participants can create new form of interactions, as well as port current economic and business interactions, and give it a never before seen level of automation and trustworthiness. This technology benefits especially the lifestyle industries, as it struggles to create verifiable authenticity and uniqueness. This becomes even more important when we realize that the world is moving towards inherently global, strongly digitized and soon virtualized world in which uniqueness and ownership not only in the physical, but also digital world is becoming absolutely important.

Creating a dedicated specific Blockchain will allow for all lifestyle industries and creatives to come together on their own network and create an unforeseen compatibility and interaction between services and the customers they interact with. It is also the platform for new experimental forms of interactions and future business models.

There are already existing public Blockchain platforms that largely function as an open experimentation ground for a new kind of decentralized applications. One of the most widely used Blockchain is the Ethereum public main net. It would be ideal to have all global activity on a shared Blockchain network, as it creates unprecedented forms of interaction and interoperability. The reality is that it will take multiple years and a lot of technological improvements until the technology will be a level to process multiple billions of transactions with the same or a higher security than we have today.

This is where *Domain Specific Blockchains (DSB)* come into play. They allow for sufficient transaction throughput for the next few years of innovation within a specific domain, given that not all players will equally join the network at the same time. With a possible transaction throughput of 1-10 million transaction per second, there is enough room for this domain to innovate and explore first production use cases for years to come. As the *LUKSO Blockchain* will be based on the EVM it will greatly profit from any innovation done around the Ethereum protocol, which is the most widely used Blockchain protocol in the world today. The Ethereum Foundation is currently working on sharding, which is a way to multiply the transaction throughput by splitting the Blockchain in multiple "shards". This innovation will greatly benefit all EVM based Blockchains and would increase the transaction throughput (not equally) by a factor of 1000. This would still not be enough for the whole planet, hence why domain specific Blockchains will be a must.

The second argument for domain specific Blockchains is that it will be easier to bring the advantages of this technology to new user groups and industries, if they are given their *own space* to innovate and experiment with like minded participants. The growth of the network in terms of interoperability - through the standards created, and the value increase through the native cryptocurrency will additionally increase the interest and activity on the network. This value growth will come through the limited supply of the native cryptocurrency, which is necessary to keep the network secure. The security is generated as there will be a cost to using the decentralized infrastructure, preventing spamming and other attacks.

2 The Blockchain Architecture

The LUKSO Blockchain will be an EVM based smart contract Blockchain, initially with a HoneyBadger BFT consensus algorithm and a fluctuating VALIDATOR set based on smart contract based delegated PoS. It will be open-source, publicly accessible, and verifiable network of computers specifically tailored through common standards and use cases to the lifestyle industries.

A Blockchain is a software that creates a network, which is able to reach a consensus about its current last state, without the oversight of humans and without the possibility of data manipulation, or inconsistency. Thereby it provides trust in the correctness and validity of the data from different actors in the network.

The Blockchain uses cryptography, such as, hashing functions, and Merkle Patricia Tries to calculate data integrity and validity. A consensus algorithm is used to determine which proposed latest block of transactions is deemed valid by all nodes of the network.

Public Blockchain networks commonly use Proof of Work (PoW) as the consensus algorithm, which is a form of competition between all mining nodes in the network to find the next valid block hash, which is a compressed information unit that is unambiguously assignable to the data contained in a block. To find the right block hash a nonce is altered and the hash recomputed until it meets the conditions given by the protocol. All other nodes in the network can validate this created PoW and thus determine the validity of a proposed block. The drawback of such algorithm is that finality can never be reached, but only assumed, as a MINER could propose a block with a higher PoW than the one currently accepted and therefore invalidate the current one. Commonly a number of blocks after the current block is used to determine finality of the current block. E.g., If a block is valid and has five blocks created on top of it, it can be assumed that it will not change.

The *LUKSO Blockchain* will be based on the Ethereum Virtual Machine and will largely function as described in the Yellow Paper of Dr. Gavin Wood [Woo18]. Changes will be done to the consensus algorithm to improve speed, add finality and reduce the energy consumption of the network.

Smart Contracts are programs that are stored on a Blockchain. A smart contract can describe business logic and the rules of interaction, thereby giving participants (ACTORS) in a Blockchain ecosystem a way to interact reliable with each other. The most powerful feature of the smart contract technology is

immutability and composability. Smart contracts can be deployed in such a way that neither the deployer nor any external person or institution can change its functionality.

Smart contracts are also able to interact with other smart contracts on the same Blockchain, allowing for chains of logic to be executed from one single transaction. In this chain all smart contracts that are touched will run as programmed, meaning they will adhere to the rules and ownership of its code. This feature allows for complex economical interactions with many known and unknown participants in a way that protects the security of all participants.

2.1 Consensus Algorithm

The LUKSO Blockchain deviates from the Proof of Work (PoW) consensus algorithm that is currently used on the Ethereum main net and will be utilizing a Proof of STAKE (PoS) consensus instead. PoS has advantages and drawbacks compared to PoW and is discussed in the following section:

So called VALIDATORS have an important role in PoS systems. These VALIDATORS are nodes in the network that are entitled to produce (seal) the next block on the Blockchain. In contrast to PoW where any MINER is allowed to solve a difficult problem and thereby prove work done. In PoS anyone who wants to become a VALIDATOR needs provide a STAKE that could be confiscated if the VALIDATOR acts maliciously.

Delegated Proof of STAKE (dPoS) is intended to be used for initial network, together with the HoneyBadger BFT (HBBFT)[al16] consensus algorithm which is by design censorship resistant as VALIDATORS produce blocks using threshold signatures and the content of a block is only revealed to all VALIDATORS *after* it is finalized. HBBFT will work in conjunction with a delegated Proof of STAKE governance build in smart contracts called POSDAO[al19]. dPoS means that anybody is able to delegate its STAKE to a specifc VALIDATOR, from which a set of VALIDATORS is randomly chosen to become block producers for a period of time (EPOCH) based on the weight of their STAKE.

A later *LUKSO Blockchain* stage is intended to use pure PoS. Pure PoS allows for any address with a locked STAKE to become a VALIDATOR, increasing the decentralization through the amount of possible VALIDATORS. Currently there are a few option we consider for this switch, the most promissingis PoS consensus algorithm being developed within the Ethereum community and is called "Casper" (https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide).

The following is a comparison of dPoS vs PoS:

Key advantages of using a dPoS-algorithm:

- Its easier to implement and faster to execute with little message overhead, as the VALIDATOR set is mostly small.

Potential drawbacks of using a dPoS-algorithm:

- VALIDATORS could group together with malicious intend and stall the network, making a user soft fork necessary;
- Delegation processes requires the use of EPOCHs, time slots that VALIDATORS are chosen to produce blocks.

Key advantages of using a pure PoS-algorithm:

- Higher network decentralization;
- Larger STAKEs in LYX coins that were bought by early adopters will likely be sold over time, which leads to a natural buy and decentralization of the system. This can naturally increase the overall trust in the network by all parties;

Potential drawbacks of using a PoS-algorithm:

- While the PoS consensus algorithm is being developed by major thought leaders in the Blockchain space, its use is not fully tested yet at this point of time;

2.2 Transactions

Transactions are the basic form of interaction on the network, through which ACTORS instruct the network to transfer LYX and instruct smart contracts to execute functions.

ACTORS (users, computers, machines) interact with the network by sending a transaction that contains instructions to what the ACTOR wants to do. These transactions are digitally signed by the ACTORS private key, and can, therefore, be verified by the network. Transactions contain information about the value being transferred, the functions to execute and its given parameters, or the code of a smart contract to be deployed on the network. The data structure of a transaction looks as follows:

```
{
    from: // the ACTORS address,
    to: // the receiving of the transaction,
        // if empty out, the transactions deploys a smart contract,
    value: // the amount of LYX to transfer to the to address,
    gasPrice: // the ACTORS proposed GAS PRICE,
    gasLimit: // the maximal amount of GAS allowed by the ACTOR
    data: // the data to be transferred to a smart contract,
          // if the to address is a smart contract.
          // Includes function name and given parameters.
    nonce: // an increasing number
           // to prevent the replay of transactions.
    r, s, v: // the signature of this transaction,
             // so the network can verify its validity.
}
```

Listing 1: Transaction format example

2.3 Native LYX coin

The native LYX coin will be the native cryptocurrency of the Blockchain and used as transaction fee for the networks VALIDATORS and is required to be STAKEd when becoming a VALIDATOR. It prevents spam, Denial of Service and other attacks, as there is an increasing cost to such attacks. VALIDATORS will be rewarded with LYX coin for securing the network and incentived to construct blocks that include transactions.

The native coin of the *LUKSO Blockchain* is called LYX. It is a so-called cryptocurrency. The native coin will be required to pay for executions on the network. This transaction fee is necessary to prevent spam on the network and incentive VALIDATORS to secure the network.

Each transaction from an ACTOR will contain a request to the network to either:

- Move an amount of LYX from the address of the ACTOR to another address.

AND / OR

- Execute or deploy code at a specific address.

The executions and value transfers are accounted for atomically in a unit called GAS, which is pure measurement unit not a token or coin itself. Each atomic computation has a hard-coded GAS amount required. The sum of all atomic computations executed by the transaction forms the total GAS amount required for a transaction.

When multiplied by the provided GAS PRICE given by the ACTOR in the transaction, it results in the fee the transaction will consume in LYX. The GAS PRICE, which is denominated in LYX, is determined by the ACTOR, while the VALIDATORS will set a MINIMUM GAS PRICE they require to forward and mine transactions. This creates an equilibrium, where ACTORS will set a not-too-low GAS PRICE to be included in a block, and VALIDATORS will set a not-too-high MINIMUM GAS PRICE requirement, to mine blocks with transactions. The total transaction fees of the blocks transactions goes to the VALIDATOR which created the block, if the block is accepted as valid by the network. An example transaction fee for a simple value transfer could look as follows:

$$21000\,\text{GAS} \times 0.0000002\ \text{GAS PRICE in LYX} = 0,0042\,\text{LYX}$$

2.4 Block Reward

Block rewards are incentives given to the VALIDATOR by the protocol for successfully sealing a block. The Block reward is a yet to be determined number of LYX.

The Block reward incentives VALIDATORS to secure the Blockchain by producing blocks and providing a STAKE to do so. As the final consensus algorithm is part of the research for the *LUKSO Blockchain* a final Block reward is not yet determined.

The chosen Block reward should not exceed 5% of the initial LYX buy per year.

3 LYX Pre-Sales

The LUKSO Blockchain Foundation will raise capital to develop and improve the LUKSO Blockchain core, smart contract components and standards, as well as fund research around governance, consensus algorithms, and IoT devices connected to the Blockchain. It will also seed the Blockchain by giving grants to projects that enhance and develop the ecosystem. Capital will furthermore be used to create Events, Workshops, Education and Marketing to raise awareness for the LUKSO Blockchain within the lifestyle industries.

The LYX coins (LYX) sold will be added to the genesis block when the *LUKSO Blockchain* launches, giving every LYX buyer control over their LYX right from the start of the Blockchain. The LYX buyers from the public ICO (Initial Coin Offering), that do not provide an *LUKSO Blockchain* address before the network starts, will have the ability to migrate at a later date and gain access to their LYX when migrating their *LYX on Ethereum*.

The reasons for generating and buy LYX at the start of the *LUKSO Blockchain* are twofold: First it will distribute ownership and participation in the network while giving relevant parties, like established businesses, start-ups and customers of the lifestyle industries a STAKE in the network. This makes it more valuable and more attractive for participants, which in return increases the network effect substantially as seen in past Blockchain networks. And secondly it provides initial funding for the network initiators to build and improve the platforms technology and raise awareness within this Industry.

The funding phase and LYX buy by *LUKSO Blockchain Foundation* will multiple stages:

1. 1.5% sold in the seed phase or given as compensation to collaborators. Those are people and groups are relevant to, or help with technical and structural issues and improve the network. This percentage contains also the compensation for advisors.

2. 3.5% sold to the founding team in the seed phase.
3. 5% will be held by the *LUKSO Blockchain Foundation* to fund future development.
4. 10% sold in a *Private Sale* with selected buyers.
5. 20% sold in a public ICO (Likely 1% IEO, 20% rICO) to increase public ownership and buy.
6. 59% sold over time to brands, institutions and given to projects and start-ups as grants to accelerate the ecosystem.

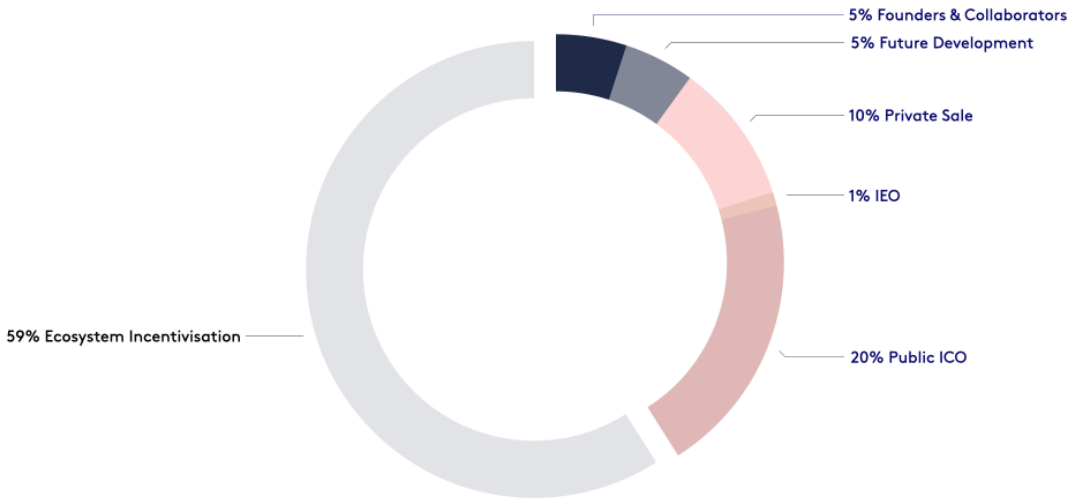

Figure 3.1: LYX coin buy

3.1 Seed phase

Early supporters, collaborators, founders and potential team members will initially be able to buy up to 5% of the LYX to secure seed capital for the project.

3.2 *Private Sale*

The *Private Sale* will sell to selected buyers to secure initial funding of the project. Those collected funds were used as a base funding and also allow for a Reversible ICO (rICO), as fluctuations in the committed funds from the rICO have a less critical effect on the projects funding.

Buyers in the seed phase and private sale, are not able to reverse their committed fund, like buyers in the public rICO, they will simply receive their LYX in the genesis block.

3.3 Public ICO

The public ICO will allow the public to buy up to 20% of the total amount of LYX initially in existence when the network starts. This offer is mainly for users, start ups and companies interested in using LYX at a later time on the *LUKSO Blockchain*. At the same time by distributing the ownership of LYX to as many people as possible, the interest and viability of the network grows significantly. When this network is adopted by the industry there will be a significant crowd ownership and benefit to early adopters and users of the network, making it more likely to succeed.

Participation in the Public ICO will only be possible through sending Ether (ETH) and possibly DAI - a programatic stable coin, to a smart contract. For simplicity reasons we will use only ETH as example in the further descriptions. The price for the public ICO will be based and fixed rate of ETH at the beginning of the ICO and determined by the price of ETH and the traction of the *LUKSO Initiative* at the time. The public ICO will be done in the format of an Reversible ICO.

3.3.1 Reversible ICO

To increase fairness and responsibility in the ICO space, we propose a new model for an ICO, which we call a "Reversible ICO" (rICO). This type of ICO improves the power balance between coin buyer and project by flowing funds slowly to the project and allowing coin buyers to withdraw their funds at any point in time.

The ERC 20 Token Standard [Fab] spurred a new era of projects that run ICOs on the Ethereum Blockchain. This is mainly due to the flexibility of a smart contract interface standard, meaning it only defines how to interact with it, but not how it should internally work. This flexibility allows ERC 20 tokens to be used in all kind of smart contract based protocol, and be issued by other smart contracts, like an ICO smart contract.

Current ICOs deploy a smart contract that receives ETH and return tokens (cryptocurrencies, assets, utility tokens, protocol tokens, access tokens, etc.) based on a set ratio. This ratio is sometimes changing over time while the ICO is running, and many models like dutch auction systems [Net] and others [Wat] have been used to improve the fairness and the price finding of the initial token price. After or during the ICO period, which lasts between some days to multiple months, funds were immediately passed to the project. This in combination with the extreme traction ICO projects got in the last years has lead to founders receiving more funds than expected, shifting of interest from finalizing the project to personal wealth and enrichment. It also lead to outright scams, where projects promised a project outcome and disappeared with the collected funds after the ICO.

The biggest problems of current ICOs is the trust between the project team and the initial coin buyers. Even if the result is a decentralized project, there is some upfront trust required to get the project started. The rICO system addresses this by holding founding teams accountable to deliver on their promise, by *committing* money rather than *transferring* it directly to the project.

The Reversible ICO is improving this, by shifting the power balance between the buyer and the project. This is done by controlling the flow of funds to the project. Rather than giving the funds directly to the project after the ICO, the funds are given over time, meaning that a coin buyer controls at all times the not-yet-given funds and can stop the flow to the project any time. The individuality is of strong importance here, as no consensus has to be reached between coin buyers, while everybody can individually decide to not trust in the project anymore.

This power is what makes a rICO so trustworthy and will likely usher in a new era of fairer ICOs.

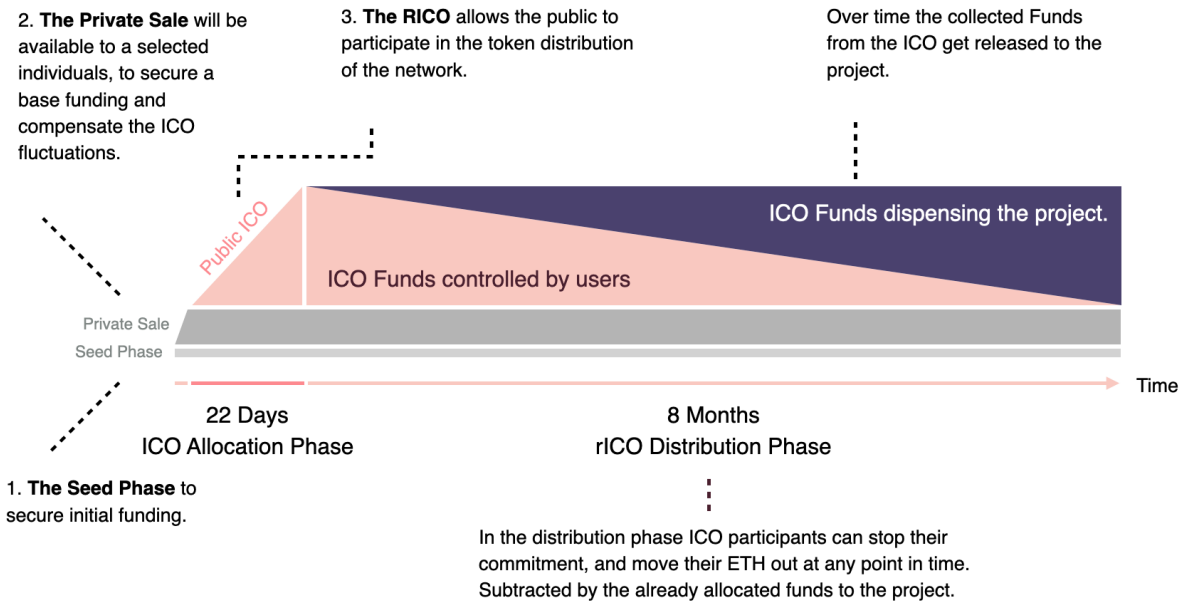

Figure 3.2: Reversible ICO model.

In a rICO the ICO phase is divided into two stages. The *Allocation phase* and the *buy phase*.

In the allocation phase ETH are committed to the project by sending them into the rICO smart contract, which sets up a ”vault” controlled by the SENDER. The SENDER receives *LYX on Ethereum* (*LYXe*) in return to prove ownership of the committed ETH.

The *LYX on Ethereum* (*LYXe*) fulfills two purposes:

1. They account for the amount of LYX reserved in the *LUKSO Blockchain*,
2. They give access to the users wallet and its corresponding ETH in the rICO, which can be withdrawn at any point in time.

   The total amount of *LYXe* will be equal to the total amount of LYX sold in the Public ICO.

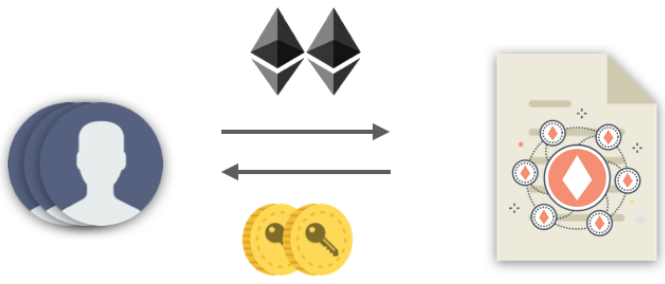

Figure 3.3: Participation in the Public ICO, and allocation of *LYX on Ethereum*.

In this first phase the coin buyer can send at any time *LYXe* back to the rICO smart contract and will receive the equivalent in ETH back. He can also decide to send parts of the *LYXe* as they are fungible. Depending on the amount of *LYXe* send back to the rICO smart contract, future LYX will be available for sale again, meaning ETH can be send again to the rICO smart contract in return for *LYX on Ethereum*. The ratio of ETH to LYX \ *LYXe* will be set at the start of the ICO and will increase by a set ETH amount every month. The *allocation phase* will run for 22 days.

$$n\,\text{ETH} = x\ \text{LYX} = x\ \text{LIA}$$

In the buy phase ETH committed will flow to the *LUKSO Blockchain Foundation*, over a period of approximately 8 months based in blocks on the Ethereum Blockchain. The *LUKSO Blockchain Foundation* can then withdraw their already received share of ETH at any point in time. The flow quotient x will change based on the amount of ETH in the coin buyers "vaults" n divided by the blocks left until the end of the rICO, where t is the total amount of blocks for the buy phase and k the last block since any withdraw from either buyers or *LUKSO Blockchain Foundation*.

$$x = \frac{n}{(t-k)}$$

This transition from the ownership of the buyer who committed ETH, to the ownership of the *LUKSO Blockchain Foundation* per block on Ethereum marks the final buy of LYX. The buyer can not withdraw this part of the ETH anymore, and will keep *LYXe* as a receipt for future LYX.

The *LUKSO Blockchain Foundation* can withdraw any already allocated amount of ETH, which will be re-calculated before any withdraw from either buyers or the *LUKSO Blockchain Foundation*. The allocation x is calculated as below, where b is the current block number at which the calculation takes place, k is the last block at which the allocation was recalculated, and a the current flow quotient.

$$x = (b-k) \times a$$

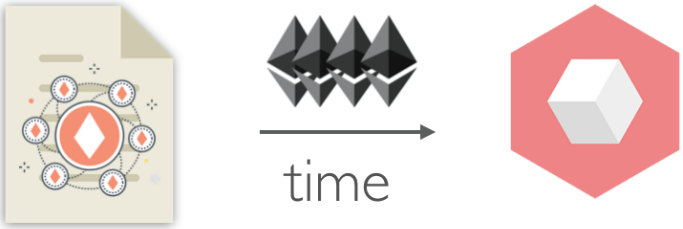

Figure 3.4: ETH can be withdrawn over time from the LUKSO project, based on the above formula.

The buyer can withdraw ETH fully or partly at any point in time during the *buy phase*. To do so they send *LYXe* back to the rICO smart contract which will return the the equivalent in ETH, subtracted by the already allocated part for the *LUKSO Blockchain Foundation*. The *LYXe* work like a key to access their wallets funds in the rICO smart contract.

For the part is already allocated to the *LUKSO Blockchain Foundation*, buyers will keep the equivalent of *locked LYXe*, as a receipt of their future LYX allocation.

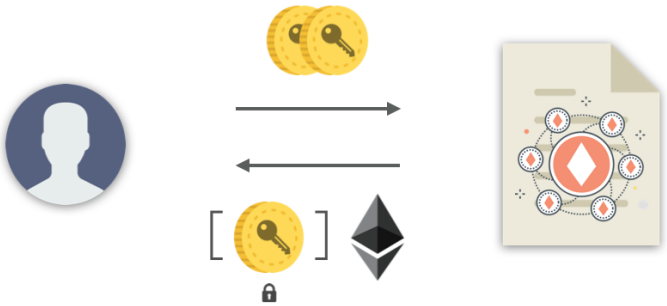

Figure 3.5: Withdrawing of ETH using the *LYX on Ethereum*.

If a buyer has multiple contributions at different price stages, the average price needs to be calculated, due to the restricted calculation capability of smart contracts. The amount of ETH returned x is calculated by multiplying the currently committed ETH r times the division of the returned token amount n by the buyers total reserved tokens t.

$$x = r \times (\frac{n}{t})$$

Committing during the buy phase is possible after another buyer has withdrawn his ETH and returned his *LYXe*, or *LYXe* are still available in the rICO. Those returned *LYXe* provide availability for future LYX again and allow any buyer to participate as well. The main difference is that if a buyer commits during the buy phase his buy phase is shorter as the buy phase is already in progress.

After the buy time is over all ETH are fully allocated to the *LUKSO Blockchain Foundation* and buyers keep the receipts in form of *LYXe*, which will allow the migration to real LYX once the *LUKSO Blockchain* genesis block is created.

3.4 Ecosystem Incentivisation

The main portion of 59% of the initially created LYX, will be used to grow the ecosystem. Planned are a grant program (5%) a community DAO (5%) and for future sales, mainly focused on enterprise and larger companies (40%). This will give the largest STAKE in the network to the players who will help define this ecosystem and increase their interest in the network significantly. A large portion of this could be burned should the ecosystem have matured enough, currently 9% is to be determined.

The price will be determined on the current market value with an additional discount that will be determined by the *LUKSO Blockchain Foundation* and will variate over time.

4 Road map

The *LUKSO Blockchain Foundation* is a larger undertaking and requires multiple stages to be successful. The funding phase from the public sale in 2020 will help the project to gain the resources necessary to initiate the network and bring stakeholders and industry leaders together. The initial phase is determined by Brand eduction around the *LUKSO Initiative*. The team behind LUKSO has built a large network and advisory board consisting of Brands and Industry leaders. Talks with multiple large Brands are in late stages and some partnerships are formed that can not yet be announced.

The technical development around the consensus algorithm and dPoS smart contracts is in full progress, and will result in a HBBFT test network soon.

Round tables around standardization have already started in September 2019 and fostered the first examples of digital certificate standards, which make LUKSO currently well received withing the lifestyle industries.

the *LUKSO Blockchain Foundation* aims to start the public network in Spring 2021 with production lifestyle use-cases and projects from start-ups alike. This phase and the time after will be defined by technological improvements, open source contribution from the *LUKSO Blockchain Foundation*, as well as eduction events and tool building to accelerate an ever growing ecosystem around the *LUKSO Blockchain*.

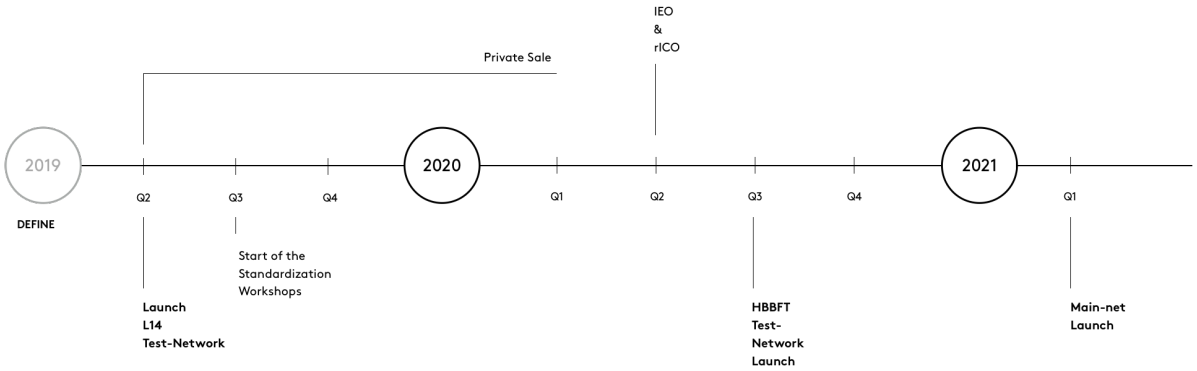

Figure 4.1: Road map

References

[al16] Miller et al. “The Honey Badger of BFT Protocols”. In: (2016). URL: https://eprint.iacr.org/2016/199.pdf.

[Woo18] Dr. Gavin Wood. “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, BYZANTIUM VERSION”. In: (2018). URL: https://ethereum.github.io/yellowpaper/paper.pdf.

[al19] Igor Barinov et al. “POSDAO: Proof of Stake Decentralized Autonomous Organization”. In: (2019). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3368483.

[Fab] Vitalik Buterin Fabian Vogelsteller. *ERC 20 Token Standard*. URL: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md. (accessed: 15.06.2018).

[Net] Raiden Network. *The Raiden Network Token Auction Explained*. URL: https://medium.com/@raiden_network/the-raiden-token-auction-explained-1cc0c7946b26. (accessed: 10.06.2018).

[Wat] Aaron Watts. *Types of ICO Auctions*. URL: https://coincodex.com/article/60/types-of-ico-auctions/. (accessed: 09.06.2018).