White Paper

Pool of Stake

Version 10.1

25 June 2018

1. Table of Contents

2. Abstract

Pool of Stake is creating a safe pool for Proof of Stake coins, the future of blockchain. Qtum, Stratis, Universa and soon Ethereum holders can unite in the Pool of Stake and start staking together. Pool of Stake aims to operate in all types of PoS blockchains- Smart Contract platforms or blockchains with a delegated mechanism. The main goal for Pool of Stake is to increase the profits for small coin holders by enabling a trusted environment to pool funds together. For this purpose, two tokens are used. First, the ERC-20 PSK token that gives discounts an rewards withdrawal fees. Second, a KEY token that acknowledges the user's initial investment. The PSK platform will provide an analytics tool via a smart i.o. database that will allow members to track, control and optimize their investments. In this white paper, we explain the implementation of Pool of Stake and its services. We elaborate the governance vision which will be developed in the coming months to ensure that the PSK community remains fair and agile. We then present detailed information relevant for the upcoming ICO starting 20 July 2018. We conclude the white paper with a review of our current accomplishments and an overview of projected milestones.

3. List of Abbreviations and Definitions

PoW
Proof of Work
Consensus algorithm used by first- generation cryptocurrencies, e.g. Bitcoin

PoS
Proof of Stake
Consensus algorithm used by second-generation cryptocurrencies, e.g. Peercoin

dPoS
Delegated Proof of Stake
PoS in which coin holders vote for delegates

PSK
Pool of Stake token

DLT
Distributed Ledger Technology
Technologies such as blockchain

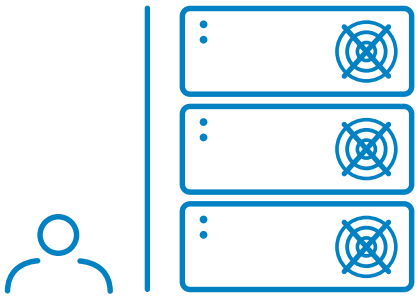
4. Introduction

Moving into the Future - From PoW to PoS

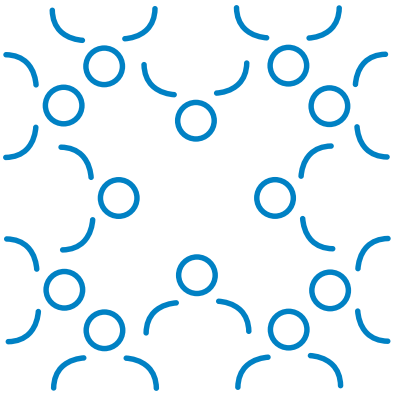
Proof of Work has been the state of the art of consensus algorithms for first-generation blockchains. Proof of Stake is the new kid on the block and 2018/2019 will be the years in which PoS will be fully adopted by major players in the blockchain field. When PoS becomes the new gold standard of blockchain, Pool of Stake will be ready to become the biggest staking pool for PoS. The core value of cryptocurrencies lies in fully trustless, permissionless protocols and decentralization. PoW is not ecologically sustainable and exhibits fundamental problems that compromise decentralization. First-generation cryptocurrencies, e.g. Bitcoin, create new coins via mining, that is, by using computational power to solve mathematical puzzles based on blockchain rules. Due to significant growth rate of the network over time, Bitcoin's PoW algorithm is facing fundamental problems. With the current block size, Bitcoin has a maximum transaction capacity of 7 transactions per second, with peak transaction costs of around $50 and an annual energy consumption of 42 TWh (the same amount as New Zealand). These facts demonstrate that the first-generation digital cryptocurrency network Bitcoin has fundamental limits for scalability and problems with efficiency that cause it to that stray from its core philosophy. While the Bitcoin community was fighting and becoming divided over Bitcoin and Bitcoin Cash, in 2012 other parts of the community took a step into the future by inventing a new consensus algorithm: Proof of Stake (PoS). In 2018/2019 Ethereum will switch from PoW to PoS. PoS is the future of blockchain and Pool of Stake is already here to bring PoS coin holders together and make the greatest profit possible.

4.1 PoW Mining

At the beginning, all you needed to mine in Bitcoin was a home computer, an application, and the will to do it.



As the Bitcoin network grew, more powerful and expensive hardware became necessary, rendering it impossible for small miners to continue mining.



This led to the formation of highly professional and centralized mining pools in Bitcoin.

4.2 Staking

The core difference between PoW and PoS lies in the model concerning how the next block is mined or forged within the blockchain. In PoW the only way to mine is by using computational power derived from CPU (Bitcoin, but also non-exhaustive: 21Coin, Bytecoin, Betacoin) and from GPU (Ethereum, Ethereum Classic, Dash, Startcoin, Karmacoin). In the initial phase, home PCs had sufficient hardware for mining with the same Bitcoin Core client, which also served as a peer-to-peer communication protocol. With the expansion of the overall hashing power of the network, the difficulty of computing the SHA algorithm -3 (SHA-256) increased as well. Home PCs were no longer sufficient, so miners had to buy new, expensive electronic components with more graphics power in order to better mine new Bitcoins. However, the growth of the network made it increasingly difficult for individual miners to find mathematical puzzles and accordingly to mine more coins. This led to the development of highly professionalized mining pools with mining farms, outcompeting the regular small miner. The image below shows that the 5 biggest mining pools (BTC.com, AntPool, ViaBTC, BTC.Top and SlushPool) are responsible for 77.1% of hashing power within the entire Bitcoin network. A study from Cornell University shows that 56% of Bitcoin nodes reside in data centers[1]. This shows that decentralization, the core value of blockchain technology, is highly compromised with current PoW protocols. These centralized mining pools in PoW pose dangers to the community, e.g. via selfish mining. The fundamentally different structure of PoS solves many of these problems.

1 “Decentralization in Bitcoin and Ethereum Networks” by Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, Emin Gün Sirer, submitted January 2018

Hash Power Per Mining Pool in PoW

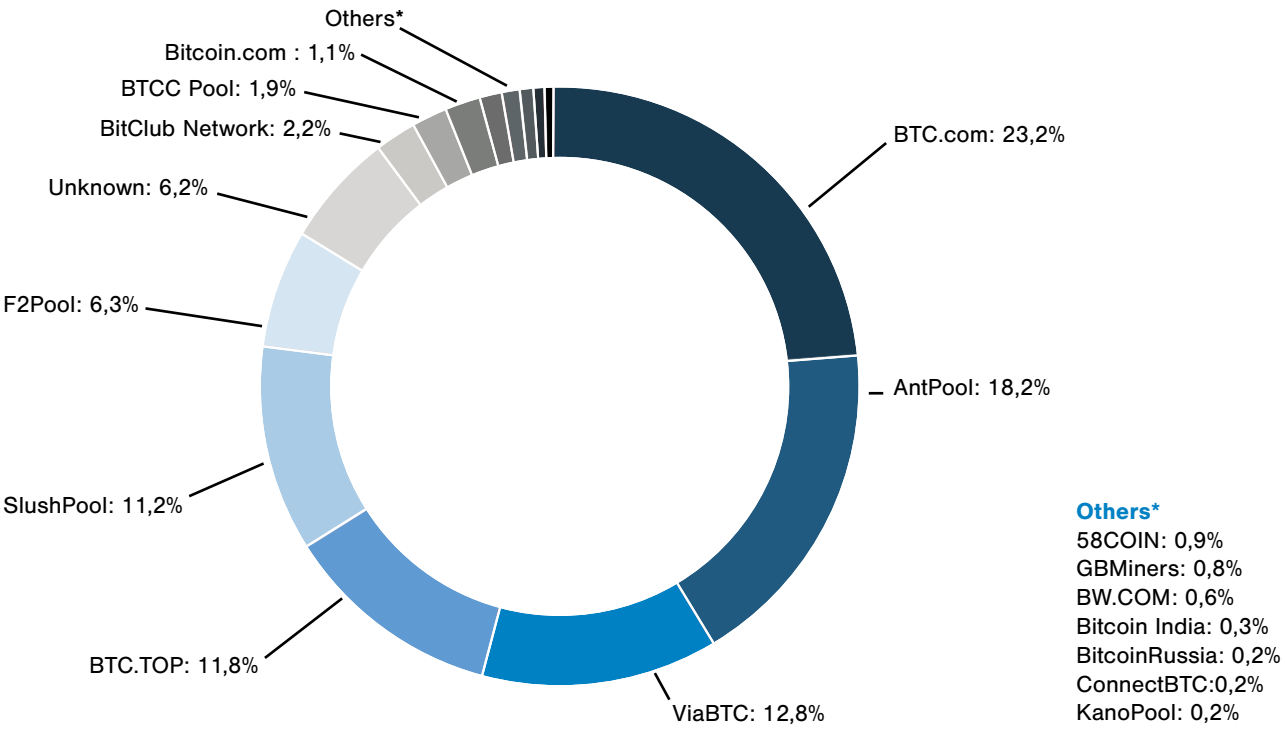
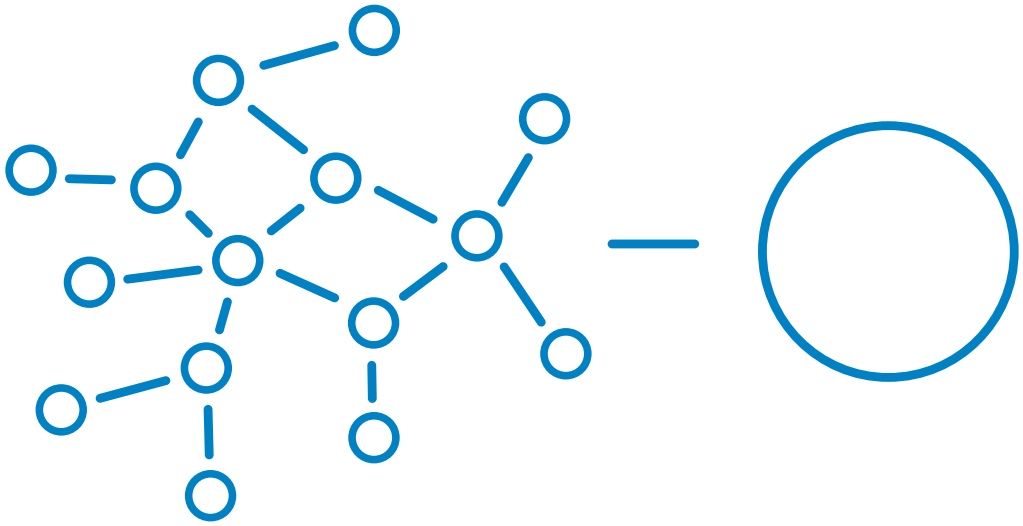


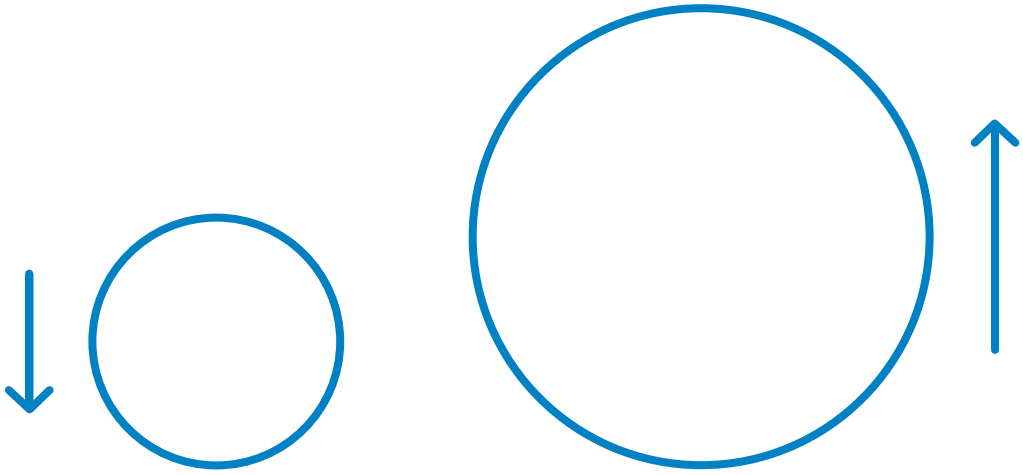
Image 1: Hash Power Per Mining Pool, https://blockchain.info/de/pools retrieved 18.01.2018

In PoS, there are no miners as such. Instead, there are validators or stakers. The next block is proposed and voted on by a set of randomly chosen validators. The voting power of each validator depends on his or her weight (amount of staked coins). This means that stakers do not necessarily create new coins (it varies among different blockchains) but instead mainly validate transactions. Hence, they receive transaction fees instead of mining rewards. As Vitalik Buterin, the founder of Ethereum, claims: "The [s]ignificant advantages of PoS include **security, reduced risk of centralization, and energy efficiency."**[2] This means that small miners can earn money by validating transactions in PoS. However, there are still two challenges for small stakers and that is what Pool of Stake is meant to solve. First, the node (or validator) has to be online 24/7 in order to be able to forge a new block at some point. In a home environment very few people can accomplish this. Second, the chance of getting to validate a transaction depends on individual weight. This means that a validator with high stakes gets unproportionally more chances to forge a new block and validate new transactions, thereby earning transaction fees. These are the reasons for the creation of Pool of Stake. It acts as one node which enables small stakers to join together, collectively creating a much higher network weight and collecting more forging rewards. By using Pool of Stake services, pool members can stake their coins generate a passive income for themselves. A significant security advantage of PoS over PoW is that there are much fewer economic incentives for pools and individuals to be harmful to the network. Some PoS blockchains, such as Ethereums Casper FFG have a built in mechanism that slashes malicious actors, causing them to lose their own staked investment. This makes attacks unprofitable.

2 https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, retrieved 18.01.2018



Pool of Stake allows small coin holders to build a staking pool.
By joining together, they regain their lost edge.
Now they can stake together and collect higher forging rewards.

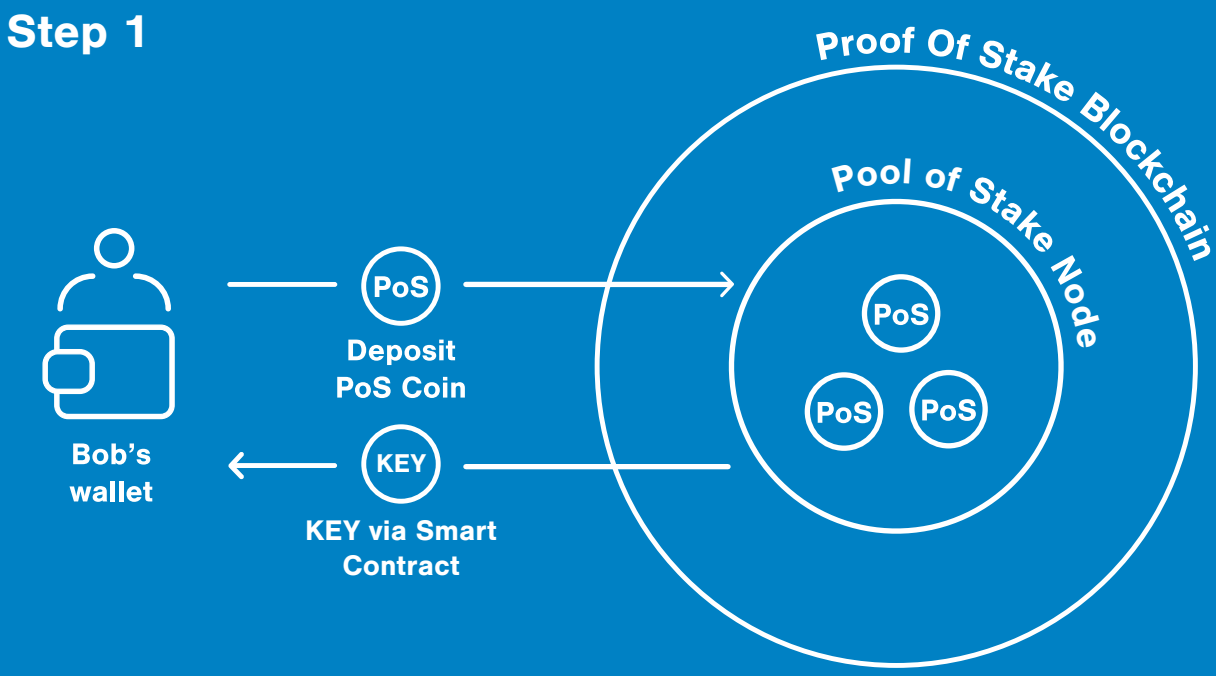


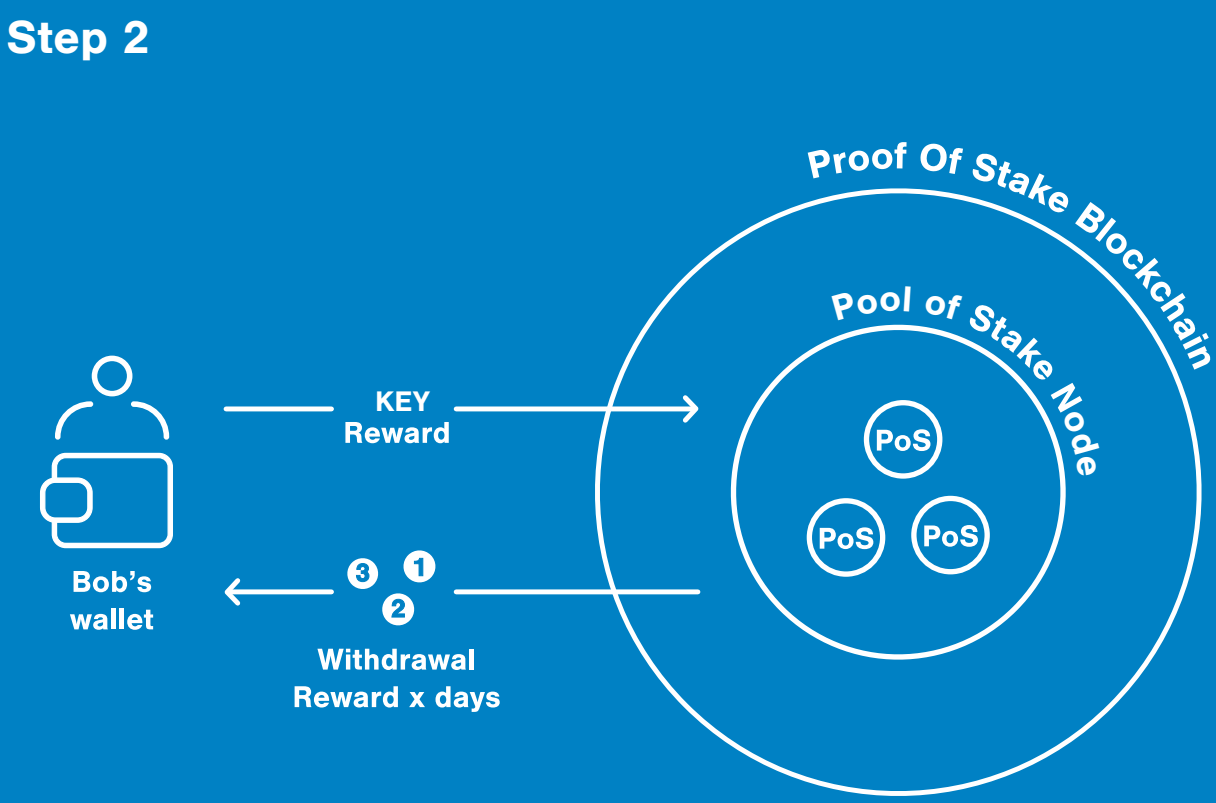
Proof of work

Proof of stake

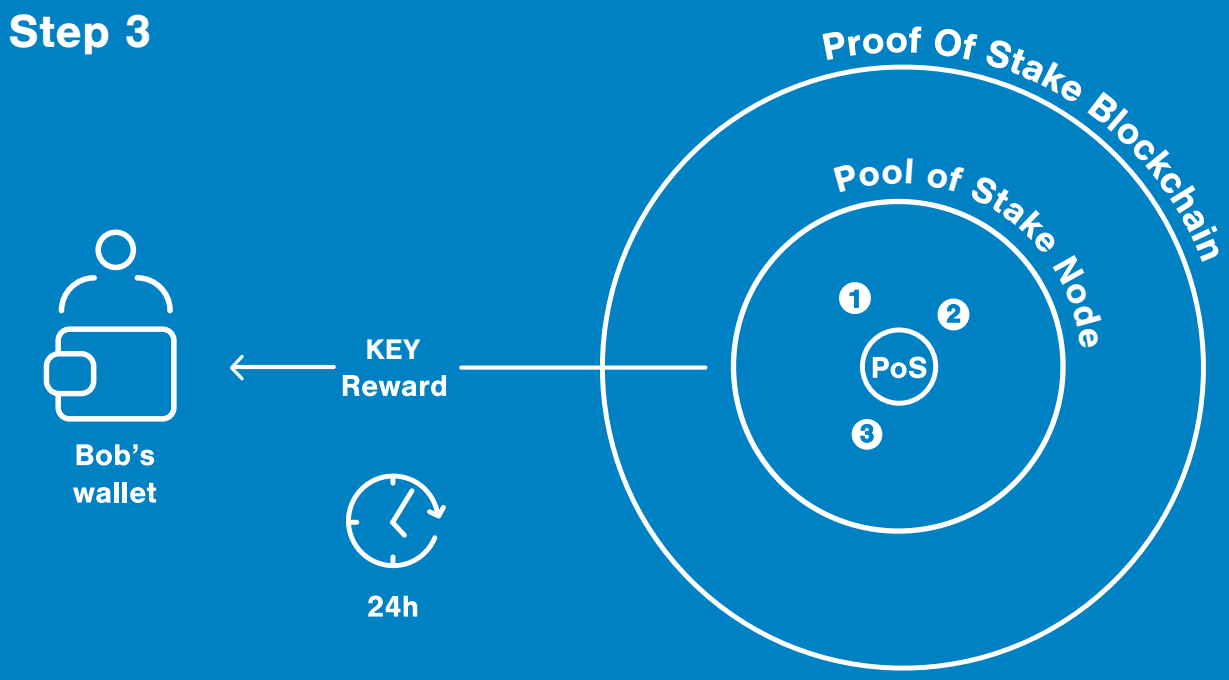
The future of blockchain is Proof of Stake.

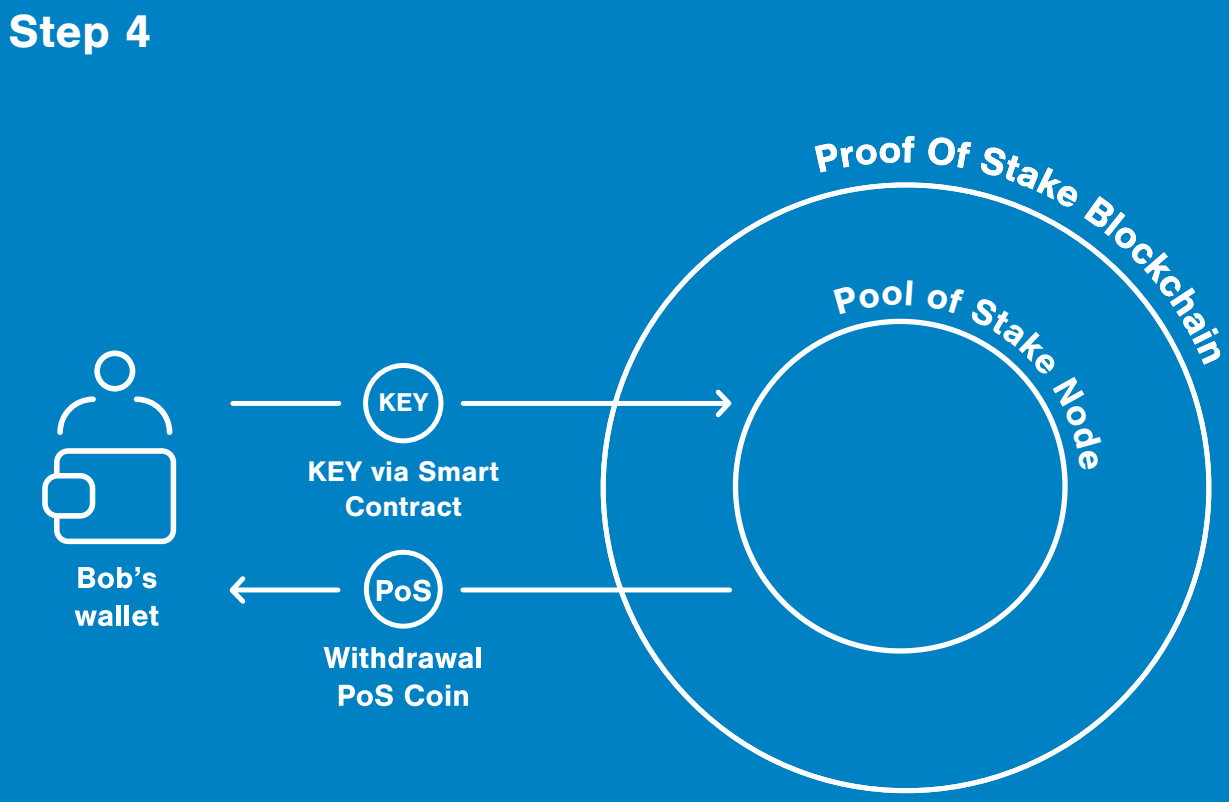
5. Pool of Stake Implementation





5. Pool of Stake Implementation





5.1 PSK and KEY Token Explanation

Users can buy their PoS coins such as Qtum, Stratis or Ether in their preferred exchanges. In order to increase forging profits, they can participate in Pool of Stake. They need to transfer their PoS coins into the Pool of Stake full node and via a Smart Contract they get back a KEY token. On the one hand it acknowledges their initial investment and on the other hand it enables users to withdraw their funds. The exact daily reward is calculated every night at 23:59:59 CE(S)T. This way users are generating passive income for themselves with their staked PoS coins on the basis of the collected rewards of the Pool of Stake community. The legal and the tech team are currently working on a multisignature solution in order to decrease the level of trust needed in this process.

PSK is a utility token sold during the ICO, enabling users to get discounts on withdrawal fees. The PSK utility token is on the Ethereum blockchain so users can keep PSK tokens in their favorite Ethereum wallet. KEY tokens exclusively serve the purpose of declaring initial PoS coin ownership. Thus KEY tokens cannot be traded, not even among PSK community members. Pool of Stake will act as a regular node on PoS coins. The vision for the near future is to be able to stake on Smart Contracts which would make Pool of Stake fully trustless and decentralized. In the MVP, Pool of Stake will cooperate with delegates for dPoS coins. The vision in the long run is for PSK to put up its own delegates for dPoS coins as Ark or Waves.

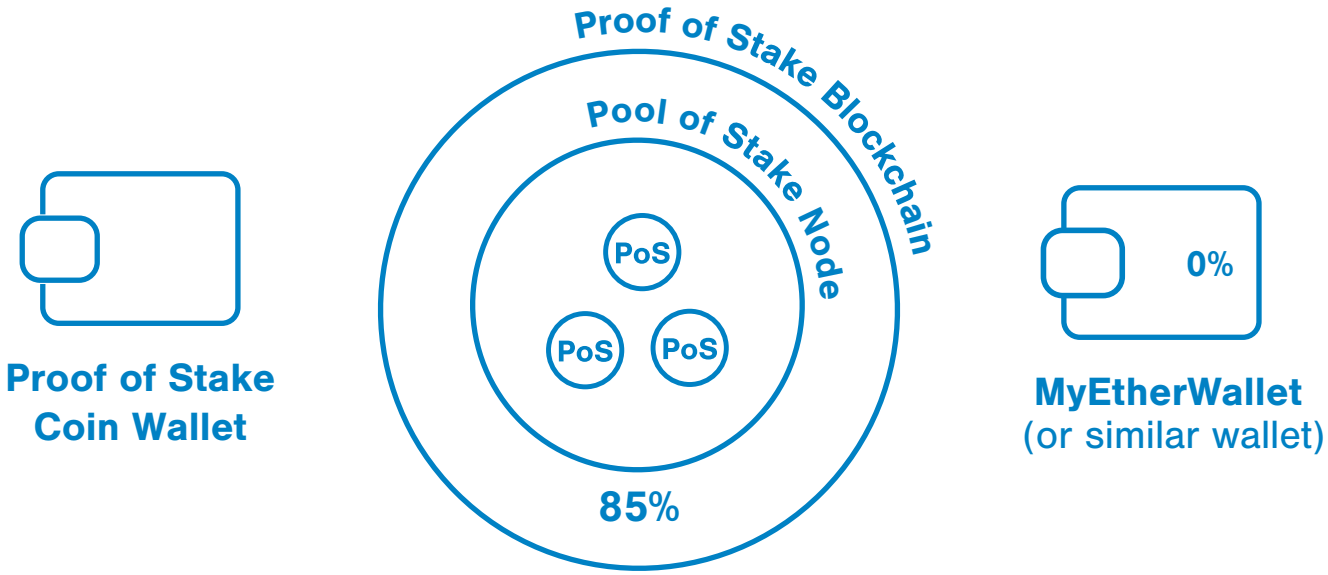
5.2 Reward System

The reward for each Pool of Stake community member is calculated every night at 23:59:59 CE(S)T and is proportional to the amount of staked coins. Along with this, corresponding KEY tokens are distributed to each member accordingly. The bigger the pool, the greater the total rewards and hence the proportion for every Pool of Stake member. Withdrawing the amount of initially staked PoS coins (in whole or part) is free of charge. The withdrawal of rewards, however, will imply a fee. In order for the Pool of Stake community members to obtain maximum gain on rewards, the correlation between held PSK tokens and value of the daily reward (*) is important. For example, if Bob wants to obtain the maximum value (95 %) of his rewards (thus paying only 5 % for GAS), he needs to have, at 23:59:59 CE(S)T, a value of PSK tokens greater or equal to 200 % of the daily reward value. An overview with exact calculations is found in the table below. The PSK platform and apps will suggest to PSK members individual strategies for obtaining the maximum amount of rewards.

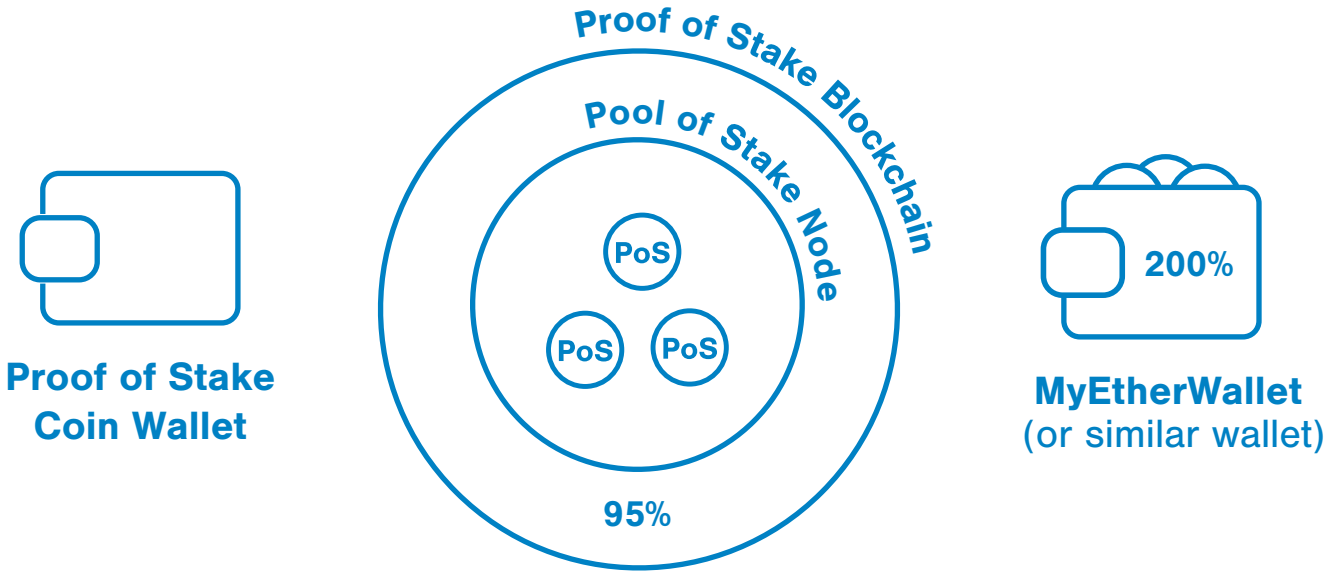
The reward will be redistributed as following:
- a variable percentage between 85% and 95% subdivided among members

- a variable percentage between 0% and 10% for Pool of Stake to reinvest in management, business development and innovation

Reward for Pool of Stake member	Reward for Pool of Stake	PSK to reward value proportion*
85 %	10 %	0 %
86 %	9 %	20 %
87 %	8 %	40 %
88 %	7 %	60 %
89 %	6 %	80 %
90 %	5 %	100 %
91 %	4 %	120 %
92 %	3 %	140 %
93 %	2 %	160 %
94 %	1 %	180 %
95 %	0 %	PSK > = 200% of reward value



Bob gets a share between 85% and 95% of his reward.



Burning mechanism

PSK will allocate 5% of the rewards to pay the GAS utilized to send the KRY back to the user and to rebuy PSK tokens on the market. PSK will include a burning mechanism. Burning means that coins are sent to an address which can never again be accessed or used. Burning is a deflation mechanism. In order to prove to Pool of Stake members that PSKs have been burned, a method called Proof of Burn is used. This method employs the same logic as blockchain technology, namely that trust is established by the system without the need for third parties to verify actions and transactions. Proof of Burn provides anyone interested with empirical and untampered evidence that the tokens have really been burned.

5.3 Platform Services - Smart i.o. database

The platform is going to be account based and protected by all common security measures, e.g. 2FA. Transparency and trustless services are central to Pool of Stake. The vision for the platform is to give users the possibility to check at any time the state of the pool and collected rewards, while also protecting users' privacy. The PSK platform will use a smart i.o. database. Pool members will be able to check the total amount of coins held by the entire pool and the generated rewards in total so that they can verify the correctness of their individual rewards. This means that members do not have to trust the Pool of Stake daily rewards calculations. They can check for themselves. Additionally, the analytics of the smart i.o. database will show the performance of the different PoS coins. This will enable pool members to easily track which coin has generated the most rewards in the last day, last week, last month and last year so that they can make informed decisions for their future investments. PoS coin performance will be measured for pool reward performance and individual PSK members. The PSK platform will include a communication tool so that PSK members can communicate with each other, make proposals to the community and vote on important decisions. A more precise vision for the communication tool will be developed in the coming weeks and months. Any updates will be communicated promptly to the community. Closely related to the communication platform is the vision for the Pool of Stake governance model, which will be discussed next.

6. Governance

The permissionless, distributed ledger technology of blockchain makes the need for third-parties obsolete on a technological level. This distribution can be (but does not necessarily have to be) reflected in the social governance model and provide true decentralization. Every token or coin poses different demands on the governance model. For the most part, a clear and simple governance model gives users the possibility to voice their preferences and hence ensures the loyalty of the community (and with it the success of the token/coin). First-generation PoW blockchains that strictly reject a governance model fall into a “Tyranny of Structurelessness” which leads to informal governance practices. This in turn creates a concentration of power in two (usually mutually conflicting) interest groups, namely core development teams and miners, despite the potential that blockchain as a DLT offers. This creates unjust oligarchies/cartels, bribing and other undesired effects compromising blockchain’s core value of decentralization. As already discussed in the introduction, PoS redistributes power back to stakeholders. Governance systems in PoS need to decentralize power among all community members and keep it agile for any changes in the system while also keeping the community loyal.

From a technical perspective, Pool of Stake may appear to be a centralized pool, but decentralization lies at the heart of the project. The mechanism of decentralization is provided by the governance system. There are internal and external governance mechanisms. One instance of internal governance is the Coin Community Vote. With it, users vote on the next PoS coin to be integrated into the pool. It will takes place in regular time intervals and the nominated coins can be suggested by the community to the Pool of Stake team. The coin with the most transactions is the next to be integrated into the Pool of Stake. As for the external governance, Pool of Stake depends on the cooperation with native blockchains so that Pool of Stake members can continue to participate in voting processes of the native blockchains. Pool of Stake will create a universal voting mechanism on the PSK platform and represent the community on the respective native PoS blockchain.

Staking in dPoS coins, such as Ark, which will take place at a later stage and will pose special requirements to the governance system. In the future, Pool of Stake will establish its own delegate representing the community. A special set of regulations will be developed to ensure that the delegate is fully accountable to the community. Any updates on the governance system will be promptly communicated to community members and input and feedback are always welcome.

7. Security Services

The key to success is security in both, software and hardware. As for the software- the PSK token is based on the Ethereum blockchain. PSK is a ERC-20 token and the KEY token is code-wise close to the ERC-20 standard. The PSK Smart Contracts are based on the native PoS blockchain, thus for staking qtums, the Smart Contract is based on the Qtum blockchain. All Smart Contracts are open-source and have been audited by Maveric SA in order to guarantee maximum possible security. Concerning the hardware for running the node, the tech team of Pool of Stake is doing in depth research for the best and most secure server solution. The current plan is to have a physical server in a data farm close to Zurich. This would allow the tech team to quickly react to any form of impairment (see table below). A very substantial point of Pool of Stake success is to be online 24/7 to keep the forging of the community ongoing. Hence additional virtual servers will be used in the USA, Hong Kong and other locations. Here the importance is to be spread globally, in order to lower substantially the chances of a DDOS attack. The exact solution is subject to ongoing research. Any updates will be communicated to the PSK community promptly.

	Level 1	Level 2	Level 3
Event	Critical - forging program - withdrawal process - network line not available	- poor response time - critical module impaired - deposit function not available	Non-Critical - non-critical function (e.g. forging statistic) not available or impaired
Solution	Highest Priority! - immediate and full attention of entire tech team until resolution or workaround	- immediate and full attention of tech team until resolution or workaround	- quick reaction for resolution and remedy of impairment for PSK
Response time	30 min	2 h	4 h
Resolution time	4 h	24 h	3 working days

8. Token Sale

8.1 ICO

Pool of Stake AS will accept donations in €, $, CHF and ETH, in accordance to the Swiss regulations. In case a donation is equal or more than 50.000CHF, a KYC process is obligatory. Pool of Stake ran a seed funding during which early adopters invested 750 000 €. This enabled the team to reach fundamental milestones and prepare for the ICO. There will be a private and a public presale at a discounted price (less than ICO price) using reservation contracts. The official start of the ICO is 20 July 2018 and is scheduled to run for one month until 30 September 2018. Pool of Stake has established a hard cap of 8 Mio € and a soft cap of 2 Mio €. In case the hard cap of 8 Mio € is reached prior to the official end, the ICO will be closed at that point in time. If the soft cap of 2 Mio € is not reached, all invested ETH will be reallocated back to the investors. In order to protect the project from market fluctuations, once the ICO is closed the collected ETH will be reallocated to few and selected currencies. The tokens will be distributed 10 days after the end of the ICO. Strategy updates will be published on our blog, and any public key for the redistribution will be shared on our website. This allows every member of the community to verify the actions that are taking place. Citizens from the following countries may **not** partake in the ICO: USA, China, Canada, Israel, South Korea and Vietnam. In the online procedure, investors themselves are responsible for determining their eligibility to invest. The ETH/PSK conversion will be announced 1 week prior the sale. After the end of the ICO, the collected amount of donations will be distributed between CHF, €, BTC and ETH in order to guarantee the correct delivery of the project respecting the timeline.

The total amount of tokens on the market will be 70 Million, the distribution will be the following:

PSK unlocked	39.839.624	56,9%
PSK 3 months locked	8.881.772	12,7%
PSK 6 months locked	12.470.937	17,8%
PSK 1 year locked	1.807.667	2,6%
PSK 2 years locked	7.000.000	10,0%
	70.000.000	

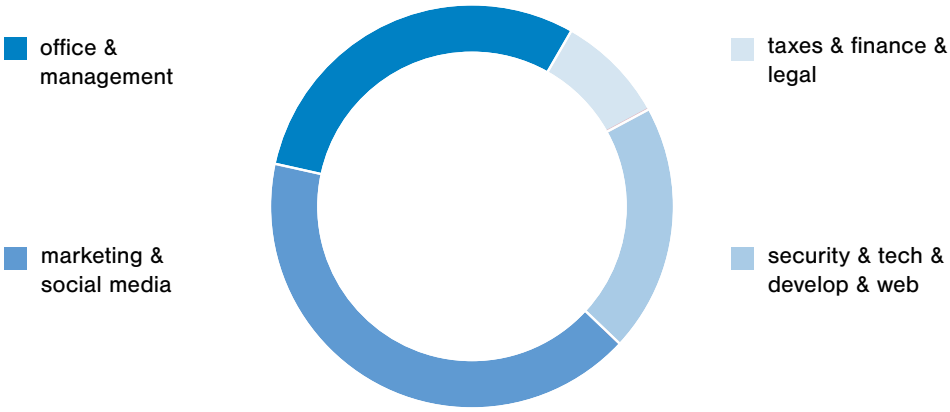
Tokens will be distributed 10 days after the ICO closes in order to ensure correct distribution to our investors.

IMPORTANT:
If the hard cap is not reached during the ICO, the amount of tokens (circulating and non-circulating) will be distributed accordingly. The idea is to achieve a fair relationship between the donors, the developers, the advisors and the 3 founders. Hence the total amount will be divided according to the current %.

8.2 Budget Plan

In case the hard cap of 8 Mio € is reached during the ICO, the crowd sale distribution will look as follows.

Budget Plan 2018



	2018	2018	2019	2018
taxes & finance & legal	160.000 €	9%	200.000 €	12%
security & tech & develop & web	362.000 €	20%	184.000 €	11%
marketing & social media	758.067 €	42%	440.800 €	27%
office & management	546.000 €	30%	824.000 €	50%
TOTAL	**1.826.067 €**		**1.648.800 €**	

Based on future projections and current calculations, we expect to reach the break-even point (BEP) in 2020-Q3. Of course, this outcome may vary, depending on market fluctuations and other events outside our influence. To the best of our ability we have developed a realistic future projection, which is also in line with the future projections of other Swiss blockchain companies. In the initial phase, **tech developments and security** will be very important. The budget for tech development will decrease over time. Nonetheless, we are working with a team of the best developers in order to stay flexible for changes in the blockchain ecosystem. **Marketing** is an important step in our plan, with a community target growth of 40% every quarter. The right marketing strategy will ensure that Pool of Stake core ideas are easily accessible and understandable. The core of our marketing strategy is devoted to raising awareness for the ICO, business development and milestone achievements. **Office and management** implies a strong back office, capable of supporting PSK members on any inquiry or issue. This includes project managers and a governance mentor in order to ensure smooth daily operations. Our dedicated team is following, discussing and lobbying for PoS and dPoS blockchains supported by Pool of Stake. The core team wants to support the correct creation of new blockchains, helping new projects interact directly with our pool and supporting the interconnection at the project level. With **tax, finance and legal** support Pool of Stake wants to ensure compliance with tax regulations and legal requirements.

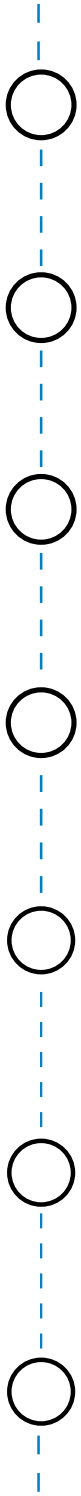
Timing of ICO

The initial sale will begin on 20 July 2018 (at a specific block) at around 12:00 CE(S)T and will run until 30 September 2018 at 20:00 CE(S)T or until the hard cap of 8 Mio € is reached.

9. Milestones

Major Achievements so far:

- Seed Funding of 750.000 €
- Cooperations with great advisors!
  - Patrick Lowry
  - Ian Scarffe
  - Daniil Morozov
- Strong core team
- Establishing a Swiss Company



21 March 2018
Announcement of the ICO day & press release

April 2018
KEY mechanism prototype on Qtum testnet

20 July 2018
The initial sale will begin on 20 July 2018
(at a specific block) at around 12:00 CE(S)T

30 September 2018
The sale period will run until 30 September 2018
at 20:00 CE(S)T

Q3 2018
1st platform release PoS
- Adoptation of coins depending on results from Coin Community Vote
- Implementation of direct governance via platform

Q4 2018
2nd platform release DPoS
- Platform open for dPoS blockchains - Ark
- Liquid democracy for governance via delegation mechanism or direct vote

TBD
3rd platform release
- Platform open for PoS blockchains - Ethereum
- Platform open for dPos blockchains - TBD

The plan will be reshaped according to dependencies on other projects outside our control.

Legal

Pool of Stake SA (from now on only “PSK SA”) is operating as a company selling tokens that will be used within the PSK SA platform. PSK Token is considered to be a hybrid token since it is possible to use it either as a payment token or as a utility token, in line with the provisions of the FINMA guidelines published on 16 February 2018. Contributor has no rights attached to the PSK Token, outside of participation access provided by ownership of the PSK Token and limited rights provided under this Agreement.

I. The PSK Token or its related sale is not considered a security. PSK SA is operating as a company selling tokens that will be used within the PSK SA Platform. PSK Token is not a security since it is simply a form of payment which PSK SA will accept on the PSK SA Platform. Contributor has no rights attached to the PSK Token, outside of participation access provided by ownership of the PSK Token and limited rights provided under this Agreement. PSK SA intends to offer a service through the PSK SA Platform and is now accepting prepayment for the PSK SA Services in the usage of PSK Tokens; however, the PSK Token sale and the PSK SA Platform features are separate for all intents and purposes.
II. This is not an investment product. This document does not constitute investment advice or counsel or solicitation for investment in any security and shall not be construed in that way.
III. This document does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or any invitation to offer to buy or subscribe for, any securities, nor for the PSK Tokens.
IV. This is not a company share stock/derivative. It is a sale of a digital asset.
V. The purchase price of the PSK Token is quoted in cryptocurrencies only and no determination of value in terms of fiat currency will be made.
VI. The PSK Tokens may or may not be listed on various secondary markets for trading. However, such trading is incidental and non-consequential to the primary purpose and the actual utility of the PSK Token as specified in this Agreement.

Legal Miscellaneous

I. If any court determines that any provision of this Agreement is invalid or unenforceable, any invalidity or unenforceability will affect only that provision and will not make any other provision of this Agreement invalid or unenforceable and this Agreement shall be modified, amended, or limited only to the extent necessary to render it valid and enforceable. The same applies if this Agreement is incomplete because a necessary provision is missing.
II. Nothing contained in the Agreement shall be deemed to constitute either Party a partner, joint venture or employee of the other Party for any purpose.
III. This Agreement shall be governed by material Swiss Law without the conflict of law provisions. Any dispute, controversy or claim arising out of, or in connection with, this Agreement or the breach, termination or invalidity thereof, shall be exclusively settled by the courts of Zurich 1, Switzerland.

10. Conclusion

In this white paper we first elaborate the fundamental problems that first-generation PoW blockchains experience in terms of scalability, inefficiency, centralization and most urgently, unsustainability. We then present the consensus algorithm Proof of Stake and argue that it solves most PoW problems and will likely replace PoW in the future. We discuss staking and how PoS makes stakeholders central players again. PoS reduces the risk of centralization and has built-in incentives for users to behave in a way beneficial to the community. For small coin hoders it is hard to stay online 24/7 and obtain the necessary weight in order to experience profitable forging. This is where Pool of Stake plays a crucial role – in uniting small PoS coin holders and helping the community generate greater rewards. The PSK platform will provide an analytics tool via a smart i.o. database that will allow members to track, control and optimize their investments in a fully trustless way. Through the governance model, members will have direct influence on the pool via voting mechanisms. Users that stake their PoS coins in Pool of Stake automatically receive a KEY token in return via Smart Contracts. Pool of Stake envisions to become a fully trustless and decentralized pool as soon as Smart Contracts make this possible. To achieve this, we are preparing for an ICO 20 July 2018. This will enable the team to develop in the first half of 2018 the platform for selected PoS coins, the governance model and later the platform for dPoS coins.

This whitepaper that has been written by the 3 co-founders and the governance researcher: Delia Hallberg, Andrea Luigi Guido Balzini, Davide Luigi Borella and Dario Calderoni.