Foin

# The decentralized peer to peer cryptocurrency for the finance sector

**WHITEPAPER**

Version 1.0.1

Created on: May 14TH 2018

Last revised: December 17th 2018

# LEGAL CONSIDERATIONS, RISKS AND DISCLAIMER

**IMPORTANT NOTICE: PLEASE READ THE ENTIRETY OF THE "Legal Considerations, Risks and Disclaimer" SECTION CAREFULLY. WE RECOMMEND YOU CONSULT A LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) OR EXPERTS FOR FURTHER GUIDANCE PRIOR TO PARTICIPATING IN CRYPTOCURRENCY INVESTMENTS (SUCH AS THE ONE DESCRIBED IN THIS WHITEPAPER). YOU ARE STRONGLY ADVISED TO TAKE INDEPENDENT LEGAL ADVICE IN RESPECT OF THE LEGALITY IN YOUR JURISDICTION.**

Please note that this is a summary of the legal considerations, risks and disclaimers document which can be found online on the FOIN website and which you must read in full, making use of this White Paper and any and all information available on the website(s). This summary should not be relied on in place of reading the "Legal Considerations, Risks and Disclaimer" section in full.

The "Legal Considerations, Risks and Disclaimer" section the full version of which can be found at https://www.foin.io/legal applies to this White Paper and any and all information available on the Website. The contents of the "Legal Considerations, Risks and Disclaimer" section outlines the terms and conditions applicable to you in connection with your use of this White Paper and of any and all information available on the Website.

The information set forth in the "Legal Considerations, Risks and Disclaimer" section may not be exhaustive and does not imply any elements of a contractual relationship. While we make every reasonable effort to ensure that all information: (i) in this White Paper; and (ii) available on the Website (all the information in the White Paper and all information available on the Website hereinafter referred to as the "Available Information") is accurate and up to date, such material in no way constitutes professional advice.

Ownership of FOIN cryptocurrency do not entitle you to any equity, governance, voting or similar right or entitlement in the Company or in any of its affiliated companies. FOIN cryptocurrency coins are considered as digital assets, similar to downloadable software, digital music and the like. It is highly recommended that you don't invest in cryptocurrency unless you have prior experience with cryptographic tokens, blockchain-based software and distributed ledger technology and unless you have taken independent professional advice.

The technology outlined in this whitepaper does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in the Available

Information. You should carefully consider and evaluate each of the risk factors and all other information contained in the Terms before deciding to invest in cryptocurrencies of any kind.

# Abstract

In today’s day and age, blockchain-based technology and its applications have advanced the innovation in many fields, such as the electronic money transfers, personal banking, online payments, Internet of Things, distributed storage, digital voting and others. While most of the cryptocurrencies have a dystopian future in vision, in which the end-user is 100% disconnected from the finance industry, some new players have started to fill in this gap (Ripple, Populous, etc.) by becoming a bridge between financial institutions or companies and the cryptocurrency adopters. In the same fashion, FOIN aims to be the cryptocurrency for the finance sector, enabling the coin holders to gain from its inherent cryptographical model (Proof of Stake) and from the range of financial instruments made available through the FOIN ecosystem.

# Definitions

P2P = Peer to peer

ICO = Initial Coin Offering

PoS = Proof of Stake

PoW = Proof of Work

ASIC = Application-Specific Integrated Circuit

CPU = Central Processing Unit

GPU = Graphics Processing Unit

FSP = Financial Service Provider

ROI = Return on Investment

# Table of Contents

## State of the art

Since the dawn of the modern age, all major currencies have been issued and controlled by central authorities. The ancient Greek philosopher and scientist Aristotle once said about the creation of money as a new element in society: "When the inhabitants of one country became more dependent on those of another, and they imported what they needed, and exported what they had too much of, money necessarily came into use" (1). Until recently, societies have depended exclusively on central authorities and financial institutions to process payments and to offer financial services. While this is satisfactory for most actors in the scene, this centralized approach suffers from the inherent weaknesses of the trust-based model (2). With the advent of cryptography, financial transactions had been redefined forever. The first and most popular finance-related cryptography application has been Bitcoin, the first P2P (peer to peer) network that can prevent forgery in a trustless environment by solving the "Byzantine Generals Problem" (3). While digital currencies have been known for quite some time now, only recently real progress has been made regarding the actual implementation of trustless, decentralized, distributed cryptocurrencies.

However, in spite of all this, the only way of gaining wealth through cryptocurrency investments has been to speculate on the future value of the cryptocurrency when valued against fiat currency and holding on to the electronic token. Unfortunately, this has paved the way for countless cryptocurrencies and initial-coin-offerings (ICOs) taking advantage of the inexperience and uneducated investors who, out of the fear of missing out on potential returns, have jumped on any opportunity they might have had in their way, regardless of the potential utility of the coin or token. Because of these and its unregulated nature, cryptocurrencies have been either forbidden or strictly regulated in several jurisdictions, including some very highly populated ones, such as China, Singapore or United States. It is expected for this trend to refract on other jurisdictions in the coming years.

Today’s investment scene, at a global level, is highly prohibitive and limiting. An investment services provider, defined as a set of connected funnels forming a complex whole, does not describe the currently siloed payments networks and financial instruments that lack effective inter-connectivity to deliver on the demands of today’s investors. As for its global reach, due to the high costs, legal jurisdiction issues and inefficiencies of cross-border payments, many investors are missing out from potential investment opportunities, instead having to rely on the highly volatile nature of cryptocurrencies.

# Introduction to FOIN

Currently addressing the issue of the global siloed investment scene, but not limiting itself to this sector for the future, FOIN aims to be the cryptocurrency bridging the finance sector with the personal investors by acting as a highly curated investment medium. FOIN will act as the de-facto cryptocurrency coin within this ecosystem made of financial services providers, blockchain applications and A.I. (artificial intelligence) modules.

From a technological point of view, the FOIN network uses the PoS (Proof of Stake) mathematical model to reach network consensus. Proof of Stake is a novel consensus mechanism for cryptocurrencies that is an alternative to PoW (Proof of Work), which is the most widely used consensus mechanism implemented in Bitcoin, Ethereum and the majority of cryptocurrencies. From a technical point of view, FOIN is a hybrid cryptocurrency, meaning it uses Proof of Work for the initial distribution of coins (which is what the majority of cryptocurrencies use) but then switches to fully Proof of Stake to provide the network security. Under this hybrid design, after the initial mining using Proof of Work is complete, the Proof of Work consensus mechanism is irrelevant for the long run. From the user's point of view, Proof of Stake is the only consensus mechanism available, thus providing a more secure, environmentally friendly and more cost-competitive peer to peer cryptocurrency. In FOIN, Proof of Stake is the core consensus mechanism used to settle transactions.

# Brief history of cryptocurrencies

## 1998 – 2009 Pre-Bitcoin

Although Bitcoin was the first established cryptocurrency, there had been previous attempts at creating online currencies with ledgers secured by encryption. The first proposals for distributed digital scarcity-based cryptocurrencies were Wei Dai's b-money (4) and Nick Szabo's bit gold (5).

## 2008 – Satoshi Nakamoto

A paper called "Bitcoin: A Peer-To-Peer Electronic Cash System" (2), authored by Satoshi Nakamoto, was posted to a cryptography mailing list. The paper described methods of using a peer to peer network to sustain a trustless system for electronic transactions.

### 2009 – Bitcoin begins

On January 3rd, 2009, the bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of Bitcoin. Embedded in the coinbase of this block was the text: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

### 2010 – First Bitcoin transaction

Because it had never been exchanged for goods or services before, it was impossible to assign a monetary value to the bitcoin units of the emerging cryptocurrency. The value of the first bitcoin transactions were negotiated by individuals on the bitcoin forum with one notable transaction of 10,000 BTC used to indirectly purchase two pizzas. If the buyer had hung onto those Bitcoins, at today's prices they would be worth more than $100 million.

### 2011 – Altcoins

As interest in Bitcoin increases and the idea of decentralized and encrypted currencies appeal to a wider audience, the first alternative cryptocurrencies appear. These are sometimes known as altcoins and while the majority of them are based on Bitcoin's source code, they try to improve on the original Bitcoin design by offering greater speed, anonymity or some other feature. Among the first to emerge were Namecoin and Litecoin. Currently there are over 1,000 cryptocurrencies in circulation with new ones frequently appearing.

### 2012 – The Bitcoin Foundation

In September 2012, the Bitcoin Foundation was launched to "accelerate the global growth of bitcoin through standardization, protection, and promotion of the open source protocol". The founders were Gavin Andresen, Jon Matonis, Patrick Murck, Charlie Shrem, and Peter Vessenes (6). 2012 was also the year that Bitcoin saw wider acceptance, with merchants such as BitPay reported having over 1,000 merchants accepting Bitcoin and even big services such as Wordpress.com starting to accept Bitcoin.

### 2013 – Bitcoin price crash

In February 2013, Coinbase reported selling US $1 million worth of bitcoins in a single month. Towards the end of the year, shortly after the price of one Bitcoin reaches $1,000 for the first time, the price quickly begins to decline, following a ban from the People's Bank of China. On 5 December 2013, the People's Bank of China prohibited Chinese financial institutions from using Bitcoin. After the announcement, the value of bitcoins plummeted to around $300.

### 2014 – Mt. Gox

While the Bitcoin network continued to grow, exceeding 10 petahash/second for the first time in 2014, in early February 2014, one of the largest Bitcoin exchanges, Mt. Gox, suspended withdrawals citing technical issues. By the end of the month, Mt. Gox had filed for bankruptcy protection in Japan amid reports that 744,000 bitcoins had been stolen.

### 2016 – Ethereum and ICOs

This is the year Bitcoin's dominance had been diluted with altcoins gaining more traction. The platform called Ethereum uses cryptocurrency known as Ether to facilitate blockchain-based smart contracts and apps. This also enabled the emergence of ICOs (Initial Coin Offering), a term specifically chosen to resemble the financial acronym IPO (Initial Public Offering). However, in spite of the technical advances made by the Ethereum platform, there had been multiple instances where the ICOs failed to deliver on their promises.

### 2017 – The Bitcoin ecosystem

As more and more businesses and services started to accept Bitcoin as an alternative payment method to legacy payment methods, the Bitcoin ecosystem gradually widened and legitimized the blockchain applications and cryptocurrencies themselves. This, in turn, has attracted more and more investors of various sizes, 2017 being the year where some of the big players in the US finance sectors joined the Bitcoin game. During this year the cryptocurrencies landscape had witnessed tremendous growth, from a total market cap of 17 billion dollars in January 2017 to almost 800 billion dollars in late December (and eventually crossing the 800 billion dollars mark in early January).

## PoS vs PoW

### Introduction

In broad terms, a blockchain application can be viewed as a distributed database, keeping track of the users' balances. But instead of a traditional database, where it's kept on a single server (therefore vulnerable to hacking), a blockchain application such as a cryptocurrency is distributed, with replicas of the database scattered across the world, forming a large network accessible by everyone. This eliminates the hacking problem because an attacker would have to hack all the participants of the network, which is statistically and technically not feasible.

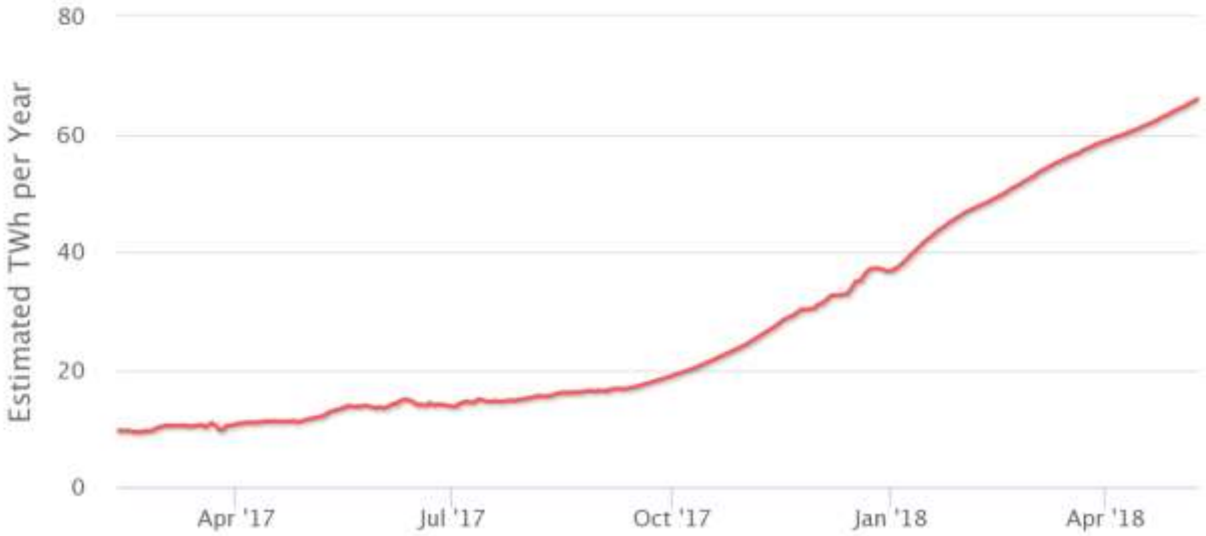
In theoretical computer science, the CAP theorem (7) presents the problem of a distributed data store being unable to simultaneously provide more than two out of the following three guarantees: Consistency, Availability, Partition tolerance. Cryptocurrencies are available (every request receives a (non-error) response) and partition-tolerant (the system continues to operate despite an arbitrary number of messages being dropped or delayed by the network between nodes). To satisfy the consistency condition (albeit weak consistency because of the confirmation blocks), a reliable consensus algorithm had to be developed that could reliably work in a large network of trustless nodes susceptible to partition.

Considered to be Satoshi Nakamoto’s major breakthrough, the PoW (Proof of Work) consensus algorithm tries to solve the consistency problem of the CAP theorem. It relies on the processing power of the computing devices taking part in the network, without any central authority. However, because of the algorithm's computationally intensive nature, which is dependent on energy consumption, a new-age gold rush phenomenon had been observed. Because of Bitcoin's deflationary nature, the race for more efficient computing devices and mining installations had started. Unfortunately, the technical innovation in computing efficiency cannot keep up with the demand for Bitcoin mining, meaning the Bitcoin network consumes more and more electricity as it grows. This is kept profitable for the participants in the Bitcoin network (miners) by a combination of market price inflation and transaction fees, but it is obviously harmful to the environment and inefficient with the computational resources.

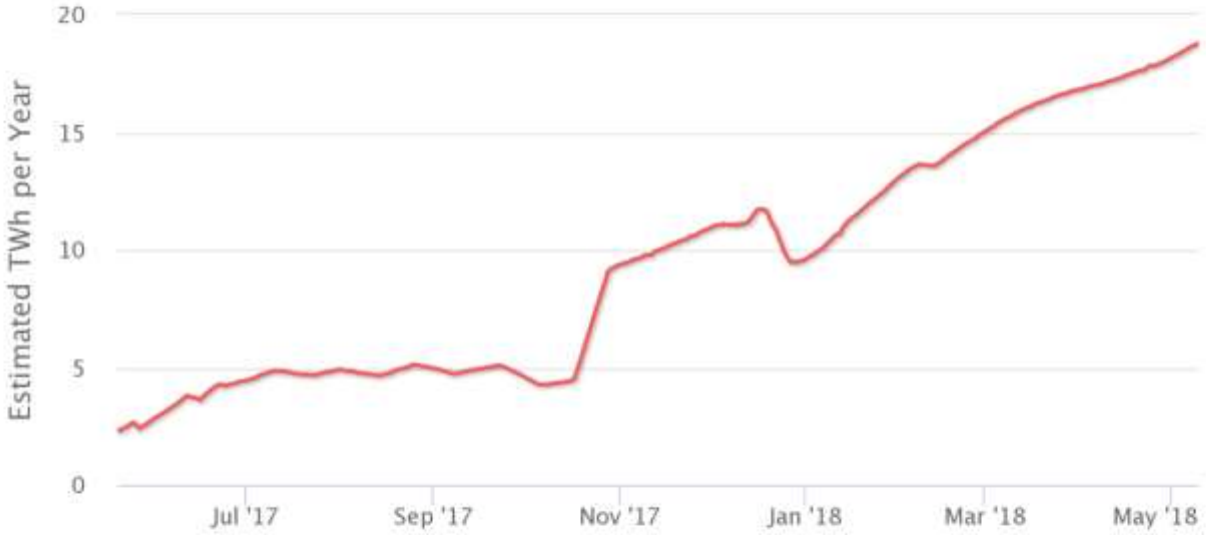
The security of the Bitcoin network relies on the PoW (Proof of Work) consensus algorithm in the form of block mining. Each participant of the network is given a computationally intensive puzzle to verify the validity of the block. The first node to successfully solve the puzzle is rewarded with a fixed number of coins (block reward) and a variable number of coins (transaction fees). The network is considered fair because the odds of a participant node to solve the computational puzzle first are directly proportional with its computing power relative to the total network computing power.

This network fairness aspect of Proof of Work introduces a theoretical vulnerability, the so called "51% attack" (8), where an attacker with at least 51% processing power of the total network power could forge transactions and verify them on behalf of the network. However, because of the current network size and because coin mining uses physically scarce resources (specialized hardware and electricity), it is cost prohibitive, if not impossible, for an attacker to launch and sustain such an attack on the Bitcoin network or any other large Proof of Work network.

The nature of Proof of Work rewards the first node that solves the puzzle. This translates in an arms race to deploy more and more resources in crypto mining that consumes a proportional amount of energy, without stop, 24/7. While there are other computationally intensive tasks that also consume a lot of energy (3D rendering, video processing, weather simulations, physics simulations, etc.), these tasks are computed incrementally and are intensive because of the complex problems they need to solve. In Proof of Work, only the first node's work is taken into consideration and the work done by the rest of the nodes is discarded. This inefficiency is a severe downside of the Proof of Work consensus algorithm and it is one of the main reasons that triggered the search for alternative solutions.



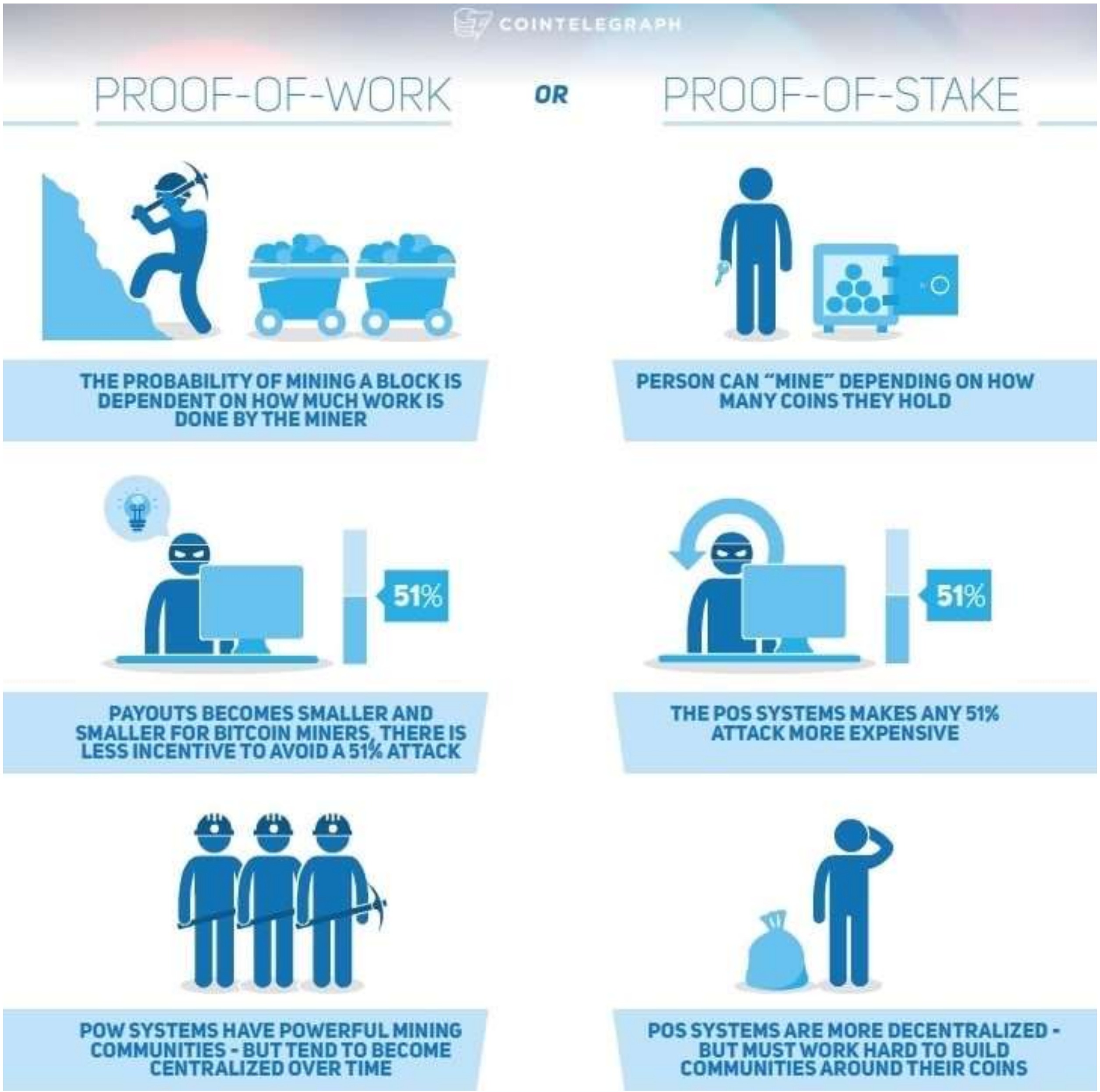
Bitcoin Energy Consumption Index Chart (9)



Ethereum Energy Consumption Index Chart (10)

One of these alternative solutions whose security is not based on expensive computations relies on PoS (Proof of Stake) algorithms. If in the PoW (Proof of Work) consensus algorithm the participant node is likely to be the first to create a new block and collect the block rewards based on his computing power compared to the total network computing power, in PoS (Proof of Stake), instead of computational resources, the probability to create a new block and receive the associated reward and fees is proportional to a user's ownership (stake) in the system. An individual stakeholder who has *X* fraction of the total number of coins in circulation has a *X* probability to be the first to create a new block.

The rationale behind this consensus algorithm is the following: users with the highest stakes in the system have the most interest to maintain a secure network, as they will suffer the most if the reputation and price of the cryptocurrency would diminish because of the attacks. To mount a successful attack, an outside attacker would need to acquire most of the currency, which would be prohibitively expensive for a popular system.


COINTELEGRAPH
PROOF-OF-WORK
OR
PROOF-OF-STAKE
THE PROBABILITY OF MINING A BLOCK IS DEPENDENT ON HOW MUCH WORK IS DONE BY THE MINER
PERSON CAN "MINE" DEPENDING ON HOW MANY COINS THEY HOLD
51%
51%
PAYOUTS BECOMES SMALLER AND SMALLER FOR BITCOIN MINERS, THERE IS LESS INCENTIVE TO AVOID A 51% ATTACK
THE POS SYSTEMS MAKES ANY 51% ATTACK MORE EXPENSIVE
POW SYSTEMS HAVE POWERFUL MINING COMMUNITIES - BUT TEND TO BECOME CENTRALIZED OVER TIME
POS SYSTEMS ARE MORE DECENTRALIZED - BUT MUST WORK HARD TO BUILD COMMUNITIES AROUND THEIR COINS

Proof of Work vs Proof of Stake (11)

## Proof of Work

In order to fully understand Proof of Stake consensus mechanism, one must understand the mechanism from which it derived, Proof of Work. Because Bitcoin is the most popular real-world use case for Proof of Work, we will use it as our example in order to better understand how the consensus algorithm works. The transaction data of the Bitcoin network is stored as a linked-list of blocks. They are secured by mathematical functions and the older a block is, the harder it is to alter or remove, which is what makes all transactions irreversible. Among other metadata, the main data stored in a block are:

- block header (version number, hash of the previous block, Merkle tree root hash (9), timestamp, target difficulty, block nonce)
- list of transactions.

The hash of the block is calculated by hashing twice the block header with the SHA-256 (10) function:

$$hash_{block} = SHA256(SHA256(header_{block}))$$

In order to simplify the notation and to account for various hashing functions used in Proof of Work algorithms, we'll consider a generic hashing function

$$hash(B) \in [0, M]$$

where

- $\mathrm{B}$ is the block header of the current block
- $\mathrm{M}$ is the upper boundary of the hashing function

To successfully embed this block in the blockchain, the resulting block hash must be smaller than the current difficulty target, which is given by the inequality:

$$hash(B) \leq \frac{M}{D} (1)$$

where:

- $\mathrm{hash(B)}$ is the hashing function
- $\mathrm{B}$ is the block header of the current block
- $\mathrm{M}$ is the maximum value of the hashing function (upper boundary)
- $\mathrm{D}$ is the target difficulty

It is important to note that the Proof of Work mining process is not a constructive process, where you calculate upon the results of the previous calculations. Instead, it is more similar to a lottery, where the first miner to find the block hash to fit the criteria submits it to the blockchain and ultimately gains the fees and reward that comes with the block. As you can see in equation (1), the bigger the difficulty, the smaller the interval in which the hash must reside. Because the hashing function's output is unpredictable, it outputs a completely different hash for even slightly different inputs. Therefore, miners must race to find a variant of the block header (in practice they increase the nonce from the block header starting from 0) that completely changes the block hash, hoping that they will be the first to collect the reward and the fees.

## Proof of Stake

According to Proof of Work's inherent rules, all participants in the network (miners) have a fair chance of discovering the next block and being rewarded. The only thing they can change is how fast they iterate through the possible block header variations by using advanced hardware and consuming more power.

In comparison, Proof of Stake's rules are changed to account for the user's stake in the blockchain network. Once the coins are "mature" enough, meaning they have a specific number of confirmations, they can be staked. The equation from (1) is changed as follows:

$$hash(B) \leq balance(U) \times \frac{M}{D} \, (2)$$

where

- $\mathrm{hash(B)}$ is the hashing function
- $\mathrm{B}$ is the block header of the current block
- $\mathrm{balance(U)}$ is a function that returns the balance of address $\mathrm{U}$
- $\mathrm{M}$ is the maximum value of the hashing function (upper boundary)
- $\mathrm{D}$ is the target difficulty

Unlike the Proof of Work inequality, the Proof of Stake inequality inserts an easily changeable factor, the user's balance, which offsets the need for specialized hardware and power consumption. In short terms, the higher the balance of a miner, the easier the difficulty for him. This results in the need for expensive computation being eliminated. This also enforces a fairness to the network: the statistical probability to mint a new block is directly proportional to the miner's balance of coins when compared to the current amount of coins being actively staked.

In order for the miner to collect the reward and fees, he must provide a valid proof of ownership of the address being staked. In order to achieve this, he can sign the newly minted block with the private key corresponding to the staking address. This ensure that only the owner of the coins (holding the private key used to unlock them) can stake them, and no other miners can hijack their address to stake the coins and collect the rewards for themselves.

## Consensus in FOIN

The FOIN cryptocurrency, the cryptocurrency for the finance sector, uses a hybrid of PoS (Proof of Stake) / PoW (Proof of Work) consensus algorithm. The proof of work algorithm is used for the initial distribution of wealth and now relies solely on proof of stake. Therefore, we shall consider that the FOIN network is secured by a more secure Proof of Stake algorithm, since this is the algorithm the great majority of the coin owners will use. FOIN is among the only cryptocurrencies that uses the unmodified proof of stake approach, according to which the user's stake is computed as his share of total coin supply (more on this in the Coin Minting topic).

The main advantages of Proof of Stake over other consensus algorithms are:

- Proof of Stake is eco-friendlier, as it is more efficient and does not require massive amounts of electricity. It is estimated that the combined total electricity costs required to run the Bitcoin and Ethereum networks amount to over 5 billion dollars in 2018 (14) (10);
- Proof of Stake discourages the forming of cartels that could present a threat to the decentralization aspect of the network, therefore giving everyone a fair chance at staking. 1 million dollars worth of coins will get you exactly 2 times higher returns than $500,000 worth of coins, without any advantages a better funded PoW miner would have by being able to acquire more expensive and more efficient specialized hardware;
- There is no need for specialized mining hardware at all, so the barrier to entry is dictated by how many coins a potential investor would want to buy. As opposed to Proof of Work, where the mining hardware is mandatory in order to gain a marginal profit, you need to accommodate the specialized hardware in a secure, temperature-controlled facility. The mining operation would also have to have access to a sufficiently advanced electrical grid infrastructure capable of delivering the required electrical load;

- An extra channel of wealth creation (besides the value appreciation on partner exchanges) by the PoS algorithm which rewards miners with a variable percentage of their total staking coins, similar to how a bank deposit would function;
- Enhanced security for the "51% attack" vector that enforces a vastly discouraging financial barrier to even attempt such an attack.

It is regarded by the crypto community as a whole, with even prominent figures from Ethereum such as Vitalik Buterin (11) declaring that Proof of Stake is the most probable direction for the future because it is truly decentralized, distributed, secure and ASIC-resistant. Because it is resistant to mining using specialized hardware, thus rendering null the incentive for mass-mining the cryptocurrency, the coin will remain in the control of the cryptocurrency owners, regardless of any exterior efforts to hijack or manipulate the blockchain.

## Coin minting

While in the Proof of Work consensus algorithm the generation of new coins is called “coin mining”, for Proof of Stake algorithms the process is called “coin minting”. The FOIN network is set to generate a new block in average every 90 seconds with a reward per block of 3 FOIN. That translates to roughly 1.16% inflation per annum. This approach ensures that the new coins issued in circulation are kept in tight check as to not affect the existing coin owners and to preserve the stability of the network. The total number of coins mined in the Proof of Work initial distribution phase is 90 million and will be distributed to future coin owners according to internal rules.

Coin minting works by “locking” your coins in your wallet and using these locked up coins as a trust indicator that you are trustworthy. The more coins you are actively staking, the bigger your weight in the network, the more coins you are earning from staking.

Because the FOIN network has a fixed reward per block, this open the door for competition among the cryptocurrency owners to stake the longest. For example, if 100% of the coin owners are actively staking the coin, all of them combined will receive 1.16% from the total supply, distributed proportionally according to their share in the network.

The share in the network is calculated with the following formula:

$$share(A) = \frac{coins_{total}}{coins_A} \quad (3)$$

where

- $\mathrm{share(A)}$ is a function resulting the share of address $\mathrm{A}$ in accordance to the total FOIN in circulation
- $coins_{total}$ is the total number of coins in circulation at any given time
- $coins_A$ is the total number of coins of address $\mathrm{A}$

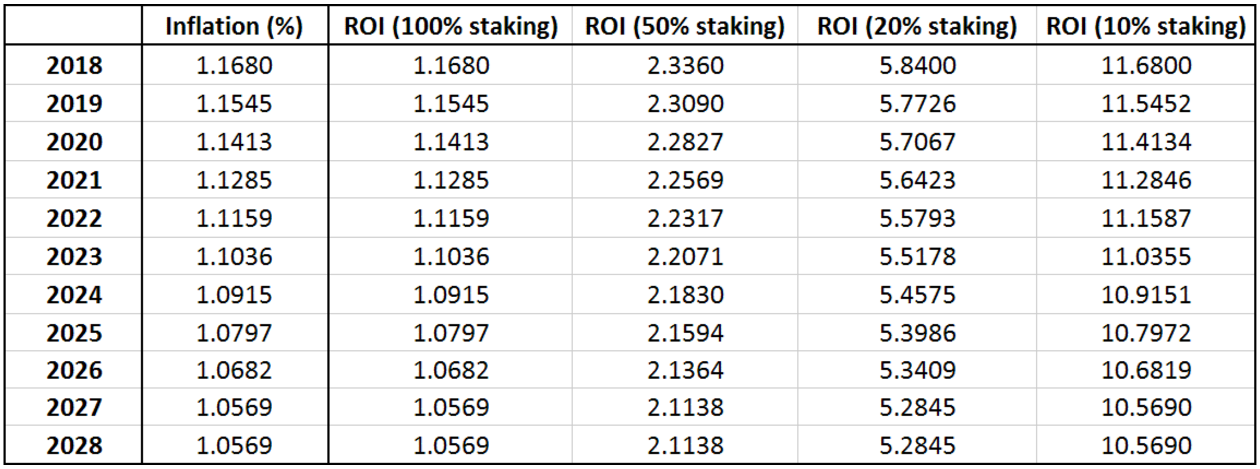
However, if only 20% of the coin owners are actively staking, they will be the only ones to receive the block rewards to a combined total of 1.16% from the total supply, distributed proportionally according to the following formula:

$$share(A) = \frac{coins_{staking}}{coins_A} \quad (4)$$

where

- $\mathrm{share(A)}$ is a function resulting the share of address $\mathrm{A}$ in accordance to the total FOIN actively staking
- $coins_{staking}$ is the total number of actively staking coins at any given time
- $coins_A$ is the total number of coins of address $\mathrm{A}$

As one can see, the difference between the two formulas, (3) and (4), is the base from which the share is calculated. The smaller the base, the bigger the rewards. The fewer people actively staking, the bigger the rewards for those few coin owners. Continuing the example above, where only 20% of the coin owners are actively staking, that would translate in 5 times as many coins according to their weight in the network. Based on industry data from similar Proof of Stake cryptocurrencies, we estimate that there will be between 5% - 6% increase in coins each year if a client is actively staking all year round. So, for a coin owner with 100,000 FOIN actively staking since January 1st 2019, he will have around 105,000-106,000 FOIN or more on January 1st, 2020.



| | Inflation (%) | ROI (100% staking) | ROI (50% staking) | ROI (20% staking) | ROI (10% staking) |
|---|---|---|---|---|---|
| **2018** | 1.1680 | 1.1680 | 2.3360 | 5.8400 | 11.6800 |
| **2019** | 1.1545 | 1.1545 | 2.3090 | 5.7726 | 11.5452 |
| **2020** | 1.1413 | 1.1413 | 2.2827 | 5.7067 | 11.4134 |
| **2021** | 1.1285 | 1.1285 | 2.2569 | 5.6423 | 11.2846 |
| **2022** | 1.1159 | 1.1159 | 2.2317 | 5.5793 | 11.1587 |
| **2023** | 1.1036 | 1.1036 | 2.2071 | 5.5178 | 11.0355 |
| **2024** | 1.0915 | 1.0915 | 2.1830 | 5.4575 | 10.9151 |
| **2025** | 1.0797 | 1.0797 | 2.1594 | 5.3986 | 10.7972 |
| **2026** | 1.0682 | 1.0682 | 2.1364 | 5.3409 | 10.6819 |
| **2027** | 1.0569 | 1.0569 | 2.1138 | 5.2845 | 10.5690 |
| **2028** | 1.0569 | 1.0569 | 2.1138 | 5.2845 | 10.5690 |

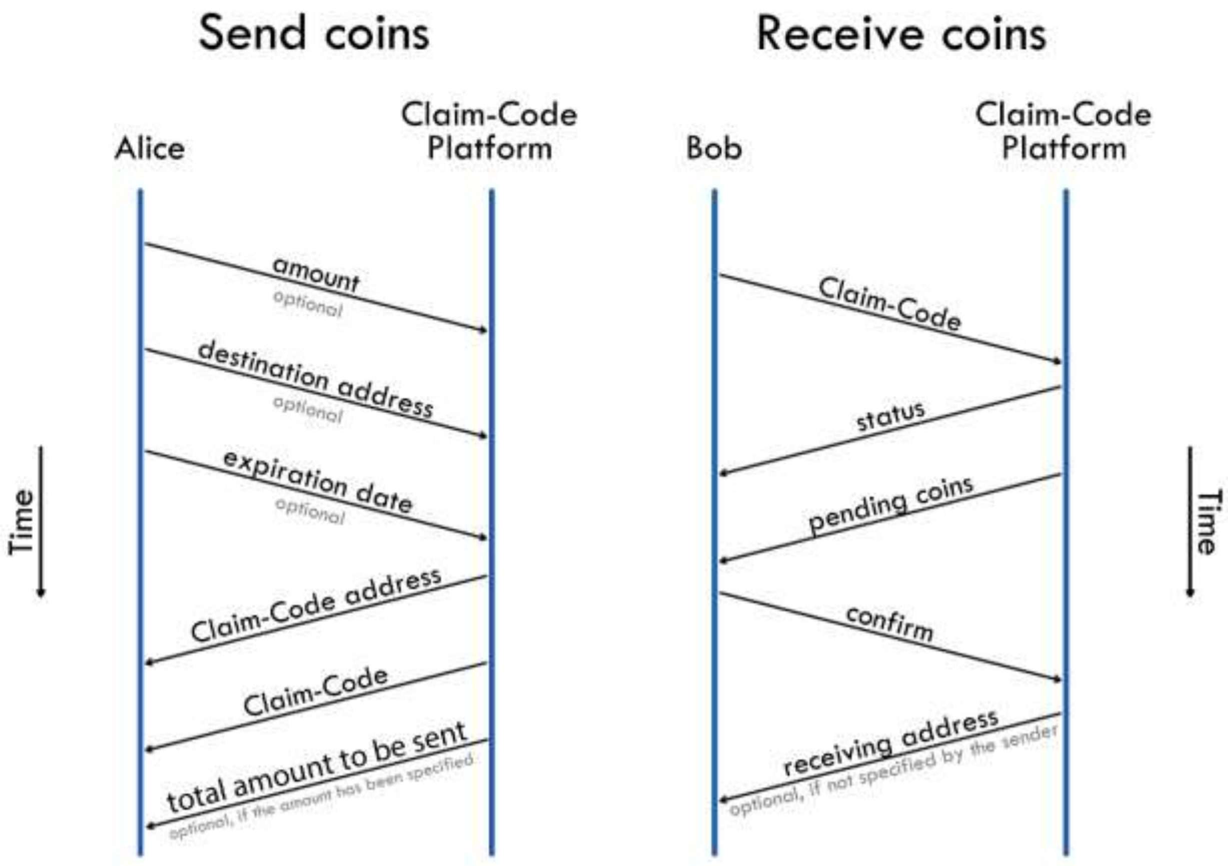
## Claim-Code

Because of its applications in the real world, a need for a more secure way of transferring coins from one party to another had risen. Our approach to this need is a multi-stage payments software solution, similar to an automated escrow system. This solution uses an additional "Claim Code" that must be communicated to the intended recipient so that he can gain possession of the funds. This solution will not be available at launch, but instead will be deployed in stages. While the initial stage will be similar to a centralized solution, in the long term, our focus will be on a fully decentralized solution.

For example, if Alice wants to send Bob funds in a secure way, Alice would opt for the Claim-Code transfer instead of the regular blockchain transfer. The transfer would follow these steps:

1. Alice visits the official portal for the Claim-Code and initiates a new sending transaction. She can input the exact amount she would like Bob to receive (optional), Bob's address (optional) and an expiration date (optional) on period for this transaction.
2. Alice will be given an address where to send funds along with a Claim-Code. At this moment, the Claim-Code is considered private. Without it, Bob cannot receive the coins.
    a. If she entered the exact amount she wants Bob to receive, she will also be shown the total amount to be sent (what Bob will receive + Claim-Code fees). In this case, she will pay the Claim-Code fees.
    b. If she didn't specify a specific amount to be received by Bob, she will be shown just the address where she needs to send as many coins as she wants. In this case, the Claim-Code fees will be deducted from the total coins sent.

3. Alice sends the funds from her FOIN wallet to the address generated by the Claim-Code portal.
4. Alice then tells Bob that she has initiated a Claim-Code transaction and gives him the Claim-Code.
5. Bob visits the Claim-Code portal and enters his Claim-Code.
   a. If the Claim-Code transaction has not expired, Bob will see that there is a transaction pending from Alice. He will be shown the transaction status and the funds available for him. If Alice has chosen to send a variable amount of coins, he will be shown the fees deducted from the total amount and how much he will receive. If Alice had not specified a destination address, he must enter his receiving address.
   b. If an expiration date is specified and it is past, he will not be able to receive the funds.



Claim-Code transactions protocol

This approach also brings with it an added privacy layer. Because all blockchain transaction are public, anyone can see the direct transactions between Alice and Bob. However, using the Claim-Code solution, the platform acts as a third party and all transactions between Alice and Bob will be private. Also, by using this approach, any transaction is guaranteed to arrive at its intended recipient. This translates to:

- no more lost funds sent to invalid addresses
- no more lost funds sent to addresses where the recipient doesn't have the private key to
- no more lost funds to MITM (man-in-the-middle) scams, where ICO websites were hijacked and the crowd sale address swapped with the attacker's
- ability to cancel a transaction before redeeming it by the recipient
- ability to send coins without knowing the destination address

## AI integration

Artificial intelligence (AI) dates back to 1956 when it was introduced as a subdivision of computer science, which was expected to operate intelligently and respond as efficiently as humans. In computer science AI research is defined as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. Colloquially, the term "artificial intelligence" is applied when a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving".

In today's fast-moving finance sector, FSPs (financial services providers) need to balance automation and personal analysis to work more efficiently and effectively. Along with FOIN's deep implications in the finance sector comes a responsibility to offer a safe financial medium for coin owner. This infers the problem of tailoring the investment channel for each individual coin owner, ensuring both minimum risk and maximum ROI, which are at the opposite sides of the spectrum. While on a small scale this problem is easily solved by a human specialist (financial advisor, investment banker, etc.), when applied at a global scale, it becomes much more difficult. Thanks to the recent strides in artificial intelligence research and technologies, AI represents the perfect solution for making the problem more manageable.

The AI (artificial intelligence) integration will consist of multiple independent modules and will be deployed in stages. The main modules of the AI integration will be: Fraud Prevention, Risk Analysis and Portfolio Recommendation.

### Fraud Prevention

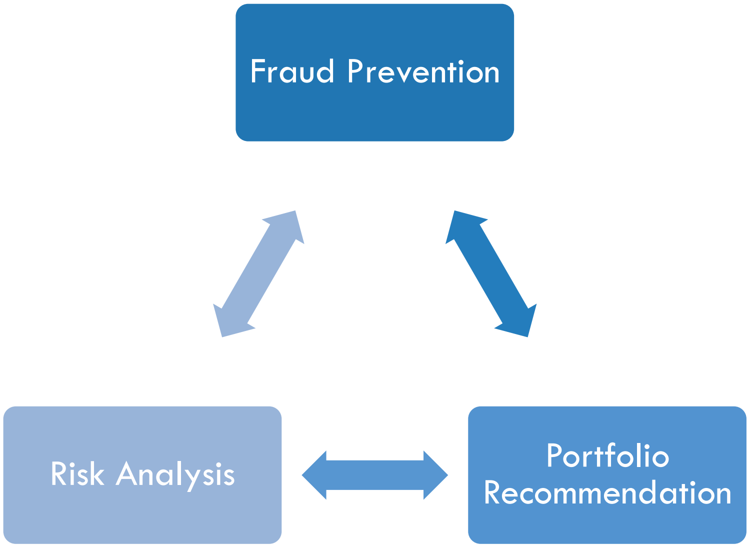
This module will ensure that the coin owners' funds will remain safe throughout the entire investment process, by safeguarding the deposit and withdrawal processes as well as the investment analysis. This will make sure that all investments carried through the FOIN ecosystem will be protected against malicious actors.

### Risk Analysis

The RA (Risk Analysis) is mainly responsible for risk management and compliance. AI has already been proven impactful in real-world applications regarding how financial service providers manage their risk. It will use publicly and privately available data from FSPs and their investment vehicles to score the risk behavior for a specific investment option.

### Portfolio Recommendation

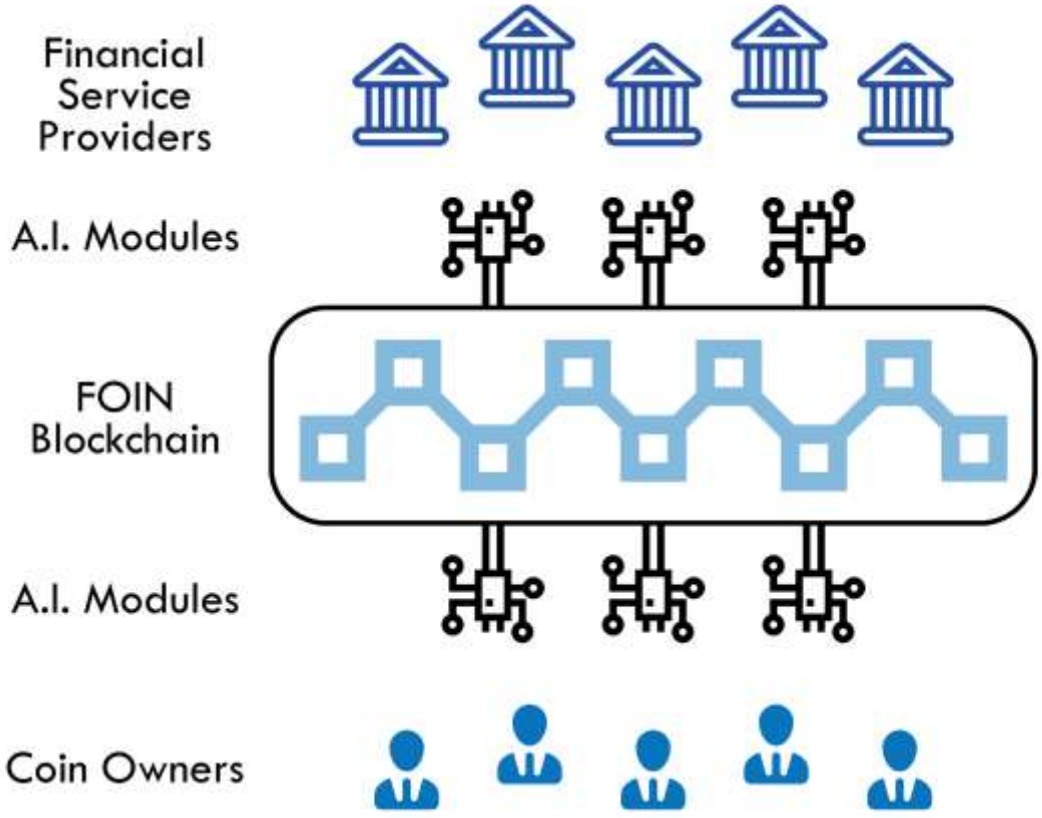
This module will use data from various other AI modules, including the Fraud Prevention module and the Risk Analysis module. Combined with various datapoint specific to each investor (e.g. country of residence, gender, age, marital status, household size, education, income, monthly expenses, debt, savings, other data from social media profiles, etc.), the analysis will output the investor's risk profile that will grade one's aversion to risk. Ultimately, the investor risk profile will be matched with an appropriate FSP based on the FSP's risk analysis (see previous module). This will enhance the security of the invested funds, in such a way that all investors, regardless of their size, will benefit from maximum ROI while exposing them to the minimum risk, as computed by the machine learning algorithms.



## Finance ecosystem

Because the FOIN cryptocurrency will address individual investors, it will act as the de-facto cryptocurrency connecting them to various financial services around the globe. To begin with, the built-in mechanism of value increase made possible by the Proof of Stake consensus algorithm will offer returns on their investment guaranteed by the blockchain technology. The theoretical minimum is 1.168% per annum, the best-case scenario is around 11-12%, but using staking data from other PoS cryptocurrencies, the real-world ROI is expected to hover around 5-6% per annum.

Furthermore, coin holders will have the ability to opt-in to invest their coins into financial service providers who have registered beforehand to become part of the FOIN ecosystem. Coin owners will be screened by an A.I. risk-assessment module, also part of the FOIN ecosystem, which will output a risk profile and recommend zero or more financial service providers within the ecosystem. With the rising pool of participants in FOIN, this will create an incentive for financial service providers to join the FOIN ecosystem. Because of the liquidity of the FOIN network, it is expected to generate interest to both well-established financial service providers, as well as to other startups in the blockchain - fintech region as well.



## Conclusion

In conclusion, FOIN is a cryptocurrency that aims to bridge the gap between financial service providers and individual investors, at a global scale. It uses a state-of-the-art consensus algorithm which has been industry-proven to be future proof, Proof of Stake. This enables coin holders to participate in the staking process, receiving between 1.16-12% per annum of their staking capital (current data points to a 5-6% range), guaranteed by the blockchain. Furthermore, by developing an ecosystem revolving around fintech and FOIN, the coin owners will have the ability to opt-in to investment opportunities, according to their risk profiles. The development and investments in the FOIN ecosystem along with an innovative marketing strategy will inevitably increase the coin value on the partner exchanges, resulting in a wealth increase for all FOIN cryptocurrency owners.

# Bibliography

1. **Kinley, D.** *Money: A Study of the Theory of the Medium of Exchange.* s.l. : Simon Publications LLC, 2003.

2. **Nakamoto, Satoshi.** Bitcoin Foundation. [Online] 2008. https://bitcoin.org/bitcoin.pdf.

3. *The Byzantine Generals Problem.* **Lamport, Leslie B.** 3, s.l. : ACM Transactions on Programming Languages and Systems, 1982, Vol. 4.

4. **Dai, Wei.** b-money proposal. [Online] http://www.weidai.com/bmoney.txt.

5. **Szabo, Nick.** Bit-Gold proposal. [Online] http://unenumerated.blogspot.com/2005/12/bit-gold.html.

6. **Matonis, Jon.** Forbes, Inc. [Online] https://www.forbes.com/sites/jonmatonis/2012/09/27/bitcoin-foundation-launches-to-drive-bitcoins-advancement/.

7. **Brewer, Eric.** CAP Theorem (Brewer's Theorem). *Wikipedia.* [Online] https://en.wikipedia.org/wiki/CAP_theorem.

8. **Majority attack.** *Bitcoin Wiki.* [Online] https://en.bitcoin.it/wiki/Majority_attack.

9. **Bitcoin Energy Consumption Index.** [Online] https://digiconomist.net/bitcoin-energy-consumption.

10. **Ethereum Energy Consumption Index.** *Digiconomist.* [Online] https://digiconomist.net/ethereum-energy-consumption.

11. **Making Sense of Proof of Work vs. Proof of Stake.** *CoinTelegraph.* [Online] https://coincentral.com/making-sense-of-proof-of-work-vs-proof-of-stake/.

12. **Merkle Tree.** *Wikipedia.* [Online] https://en.wikipedia.org/wiki/Merkle_tree.

13. **SHA-2.** *Wikipedia.* [Online] https://en.wikipedia.org/wiki/SHA-2.

14. **Bitcoin Energy Consumption Index.** *Digiconomist.* [Online] https://digiconomist.net/bitcoin-energy-consumption.

15. **Buterin, Vitalik.** A Proof of Stake Design Philosophy. *Medium.* [Online] https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.

16. **Vogels, Werner**. Eventually consistent. [Online] https://www.allthingsdistributed.com/2008/12/eventually_consistent.html.

17. **Sunny King, Scott Nadal**. PPCoin: peer-to-peer crypto-currency with proof-of-stake. *PeerCoin*. [Online] https://peercoin.net/assets/paper/peercoin-paper.pdf.

18. **Vasin, Pavel**. BlackCoin's proof-of-stake protocol v2. [Online] http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf.

19. **Zamfir, Vlad**. Introducing Casper "the friendly ghost". *Ethereum Blog*. [Online] https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.

20. **Proof of stake**. *Novacoin Project Wiki*. [Online] https://github.com/novacoin-project/novacoin/wiki/Proof-of-stake.

21. **Buterin, Vitalik**. On stake. *Ethereum Blog*. [Online] https://blog.ethereum.org/2014/07/05/stake/.

22. **Buterin, Vitalik**. Slasher: a punitive proof-of-stake algorithm. *Ethereum Blog*. [Online] https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/.

23. **Buterin, Vitalik**. Ethereum Whitepaper. *Ethereum Github Wiki*. [Online] https://github.com/ethereum/wiki/wiki/White-Paper.

24. **Proof of Stake versus Proof of Work**. [Online] BitFury Group, 2015. http://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf.

25. **Karl J. O'Dwyer, David Malone**. Bitcoin Mining and its Energy Footprint. [Online] http://eprints.maynoothuniversity.ie/6009/1/DM-Bitcoin.pdf.

# Notes and further reading

**Eyal Hertzog, Guy Benartzi, Galia Benartzi**. Bancor Protocol - Continuous Liquidity for Cryptographic Tokens through their Smart Contracts. [Online] 2018. https://about.bancor.network/static/bancor_protocol_whitepaper_en.pdf

**Serguei Popov**. The Tangle. Version 1.4.3. [Online] 2018. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

**Stox Platform for Prediction Markets**. Stox Whitepaper. Version 03. [Online] 2018. https://resources.stox.com/stox-whitepaper.pdf

**David Mazieres**. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. Stellar Development Foundation. [Online] 2018. https://www.stellar.org/papers/stellar-consensus-protocol.pdf