atbcoin

ALTERNATIVE TECHNOLOGY BASE

Powered by SEGWIT

WHITEPAPER

Revision 1 / June 8, 2017

Contents

1. Abstract

A sharp rise in price and usage of Bitcoin as well and other cryptocyrrencies as Ethereum, Ripple, NEM, Litecoin, Dash, Monero, and others—has shown the world that the global financial system is more than prepared for a change that will take it to another level where transparency and decentralization will become the main pillars of its growth.

However, such a rapid upward trend in popularity of cryptocurrencies came with its drawbacks that may hinder further development of the digital decentralized currencies: increasing number of attacks and forks that cause double spending and jeopardize the network security, limited number of available coins and complexity of coin mining, higher transaction processing time and transaction fees, price fluctuations and plunges[1], centralization concerns, lack of malleability within the network and so on.

ATB Coin is a balanced DPOS cryptocurrency that successfully tackles the abovementioned issues by leveraging the most helpful features of Proof-of-stake algorithm and makes it even more efficient, flexible, and agile due to the use of SegWit technology.

[1] http://www.businessinsider.com/bitcoin-price-blows-past-2500-2600-and-2700-2017-5

"Imagine a technology that could preserve our freedom to choose for ourselves and our families, to express these choices in the world, and to control our own destiny, no matter where we lived or were born. What new tools and new jobs could we create with those capabilities? What new business and services? How should we think about the opportunities? The answers were right in front of us, compliments of Satoshi Nakamoto."

From Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World by Don Tapscott and Alex Tapscott[2]

[2] https://www.amazon.com/Blockchain-Revolution-Technology-Changing-Business/dp/1101980133

2. Key technologies

ATB Coin incorporates the (best/ most popular)features of DPOS based cryptocurrencies together with the advantages of SegWit technology capabilities

In ATB Coin users will be able to obtain decentralization, transparency, privacy, cost-efficiency and low energy consumption, ease of use, and network participation incentives work in line with enhanced security, doubling of the network capacity, smart contracts, lightweight wallet, and cloud mining in order to provide people from all over the world a worthwhile, stable, and more pliable way of handling their financial needs.

2.1. DPOS

The first cryptocurrencies based on Proof-of-stake algorithm, or POS, appeared in 2012 with Peercoin, followed by Emercoin in 2013, and Nxt and BlackCoin in 2014. Just like in every other cryptocurrency blockchain algorithm. The main aim(objective) of cryptocurrency blockchain algorithm as well as POS is to achieve the distributed consensus within the network that is comprised of a massive number of nodes.

POS algorithm was developed as a more eco-friendly, resource efficient, and secure alternative to cryptocurrencies based on Proof-of-work algorithm, or POW, that require massive amounts of energy in order to maintain the proper functioning and growth of the network.

Coin of cryptocurrencies which are based on POS are created through staking, or simply forged. In other words, all nodes in the network that possess any amount of coins in their wallet and keep the node online are automatically included in the coin forging pool and are therefore eligible to create and sign blocks, ensuring that the distributed consensus is achieved.

In May 2017 the world's second largest cryptocurrency, Ethereum, announced[3] that it will make a transition to Proof-of-stake algorithm by the end of 2017.

2.1.1. Comparison between POW and DPOS

As it has been mentioned above, the only thing that nodes within a POS cryptocurrency need to do to maintain the security of the network and be eligible to earn is to have a certain amount of coins in their wallet and keep their PC online.

This mechanism—which both excludes the human factor so notable in POW and DPOS from the mining/forging process and helps avoid spending massive amounts of electricity on creating coins—is the backbone and the most laconic property of Proof-of-stake algorithm.

But apart from Proof-of-stake, there are two other algorithms that are used in cryptocurrency blockchains, Proof-of-work and Delegated Proof-of-stake, which are both meant to help blockchain reach

[3] http://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake/

a distributed consensus and this way maintain the integrity of the network.

Distributed consensus, is a term which is used in computer science and cryptocurrencies, should be interpreted as a mutual consensus between all members of a cryptocurrency, or its users, on whether the data about transaction in the last block is valid. If this is the case, the distributed consensus will be achieved and the block will be successfully signed, ensuring proper functioning of the network.

If the data in the last block is false, is a term a distributed consensus between all active members of the network will not be reached and this block will not be signed, therefore avoiding the possibility of various kinds of attacks that jeopardize the system integrity or result in double spending.

In cryptocurrencies that use POW the distributed consensus in the network is reached between its active members, or miners, who need to continuously keep their PCs running and use real energy produced by the GPUs to hash blocks and mine coins.

Though this may look as the although, it may seem as the most robust and true-to-life method of reaching the distributed consensus, actually it leads to several serious problems.

Firstly, it requires massive amounts of energy due to the increasing difficulty to mine coins.
Secondly, in order to survive in the evergrowing mining market, miners are required to purchase expensive equipment which gets outdated in a short period of time and eventually ends up at a landfill site, harming the environment even more.
Thirdly, such system leads to appearance of miner monopolies that tend to negatively influence the commission fees and transaction processing times because of corruption, let alone the possibility of carrying out a 51% attack.

Delegated Proof-of-stake, or DPOS, is the latest blockchain algorithm which is currently used only scarcely (e.g. BitShares). In its essence, it’s very similar to POS, but it still has a few changes that make it different from Proof-of-stake algorithm.

Network nodes in DPOS cryptocurrencies, or users, create coins in exactly the same way as it's done in POS cryptocurrencies, by storing a small amount of currency in their wallet. However, all important decisions within the network in DPOS cryptocurrencies are made via the results of elections organized between all active members of the network as well as by the consensus of the delegates or witnesses who are appointed by the active members in order to carry out tasks associated with ensuring security of the network.

At first sight this mechanism may look more democratic and transparent, but in practice it overcomplicates the system, makes it more corrupt and less secure due to the human factor, and decreases the user participation rate, in this way causing centralization concerns.

2.1.2. Encryption

ATB Coin uses several cryptographic algorithms for purposes of ensuring the blockchain integrity and safety of its users' coins.

The first one is ECDSA, a public key cryptography algorithm, which is associated with every coin in the system by means of employing a public key, private key, and signature so that every node of the blockchain can verify the coin ownership.

The second one is a robust one-way SHA-256 encryption algorithm, which is included in SHA-2 family of cryptographic hash functions, and is considered to be classic in the majority of the world's cryptocurrencies.

SHA-256 hash function is used to turn input data of any size in the blockchain into a string of 32 bytes that is impossible to reverse or predict. In case of an attack upon which some or all of such input data is changed, the hash associated with these data will be changed too, making it impossible to create a different block of data with the same hash.

These two cryptographic algorithms ensure stable functioning of the ATB Coin blockchain network where the ownership of coins can be easily verified and distributed consensus is achieved without possibilities of double spending.

2.1.3. Blocks and block creation

Since ATB Coin is a cryptocurrency based on DPOS algorithm, creation of blocks is carried out through provision of a proof that the active network node possesses a certain amount of coins and therefore can participate in generation of blocks.

If the active network node—meaning that it is a user who keeps their wallet open—possesses a certain amount of coins, it will be eligible to enter the block creation process by sending the coins to itself and proving their ownership.

Selection of the creator of the next valid block is made by using deterministic randomization formulas that take both the stake size and the lowest hash value into account, therefore avoiding centralization of the cryptocurrency by not letting the richest members of the network accumulate their wealth.

2.1.4. Coins and forging process

Based on the POS algorithm, active node of the blockchain network in ATB Coin randomly selected, based on their stake size and hash value will receive a daily reward, or ROI, for their contribution to achieving the distributed consensus.

As a means of combating the inflation and the market glut, two years after the ICO and creation of the genesis block the daily ROI will decrease twofold. The decrease of the daily reward by two times will be repeated every two years until the daily reward rate reaches almost zero.

As a POS cryptocurrency, ATB Coin will start with an open ICO that will last one month during which anyone will be able to purchase ATB Coins and receive a certain number of ATB Coins as a bonus. The total number of coins that will be offered to the public during ICO equals the quantity of coins in the genesis block, which is 50,000,000 ATB.

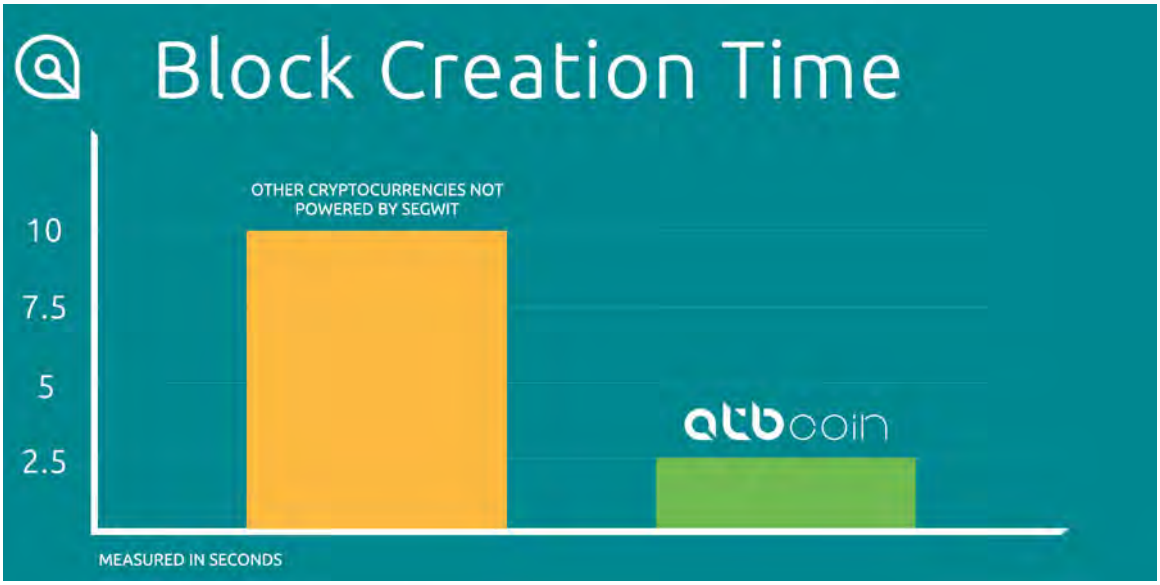
2.1.5. Nodes

Due to the properties of the POS algorithm—which doesn't require massive amounts of electricity to be spent on hashing blocks where a large amount of data is stored—as well as to the recent launch of the cryptocurrency, the node in ATB Coin are lightweight and use an SPV, standing for simplified payment verification mode, that allow the users to download only a part of the blockchain relevant to their node instead of downloading the whole copy of blockchain.

2.1.6. Transactions: fees and processing time

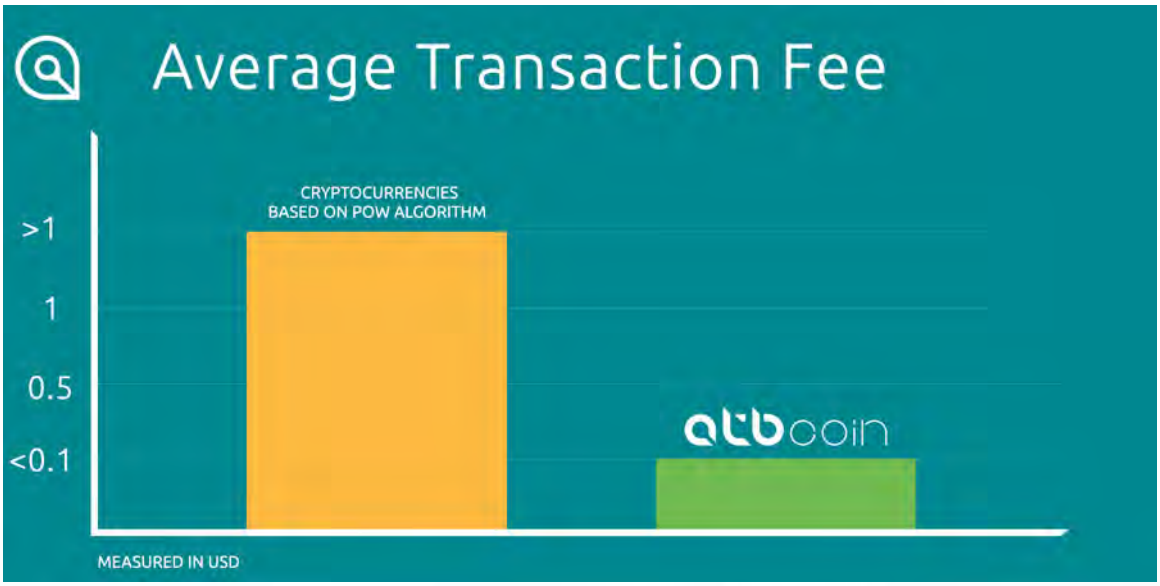
If we take the average transaction processing time in a large POW based cryptocurrency and compare it with the same value in POS based cryptocurrencies, we will see that in POS algorithm the transactions are processed at least twice faster.

However, thanks to the usage of SegWit that implements a 4 time increase in the block size, every block in ATB Coin will be generated in 2.5 minutes against 10 minutes in POW based cryptocurrencies.



Apart from this, the network throughput in ATB Coin, which equals the transaction processing time, will be unlimited following the launch of Lightning Network sidechain solution on top of ATB Coin blockchain.

When it comes to the transaction fees, they are estimated to be at least 10 times lower than those in cryptocurrencies powered by POW algorithm. Such a significant decrease in the transaction fees is possible thanks to a lack of physical mining of coins in POS algorithm and inclusive distributions of coins among all active members of the network.



2.2. Segwit

Segregated Witness, which is most often called SegWit, is a proposed update to Bitcoin that was officially released 6n October 2016 in v0.13.1 of the cryptocurrency core. All though, it was originally proposed for Bitcoin network, it can be implemented in any other cryptocurrency.

SegWit is aimed to improve the network scaling by increasing the block size limit and decreasing the transaction processing time and fees, enhancing P2SH security to 256 bits, fixing transaction malleability enabling an array of smart contracts as well as sidechain solutions like the Lightning Network, and so on.

ATB Coin will be initially powered by SegWit in the very first place—and Lightning Network in the near future—avoiding the process of its adoption by 95% of the active nodes in the network, which is unnecessary for an emergent cryptocurrency.

2.2.1. Overview

The key aim of SegWit soft fork is to scale the network of a cryptocurrency and improve its performance and efficiency. Since more and more people are currently using cryptocurrencies for their everyday financial needs, the overall number of transactions processed by a blockchain grows very rapidly.

Due to the blockchain properties, a txid of a transaction also features information on the previous inputs and outputs of the coins and wallets associated with this transaction, this way occupying to about 60% of the transaction size. Hence, the increasing numbers and size of transactions slow down and overload the network, leading to slower processing times and higher fees.

SegWit solves this problem by increasing the block limit size from 1MB up to 4MB. Such a marked increase in the block size was possible thanks to fixing transaction malleability by moving scriptSig data out of the transactions and off the blockchain, both enhancing the network performance and preventing any possibility of malleability attacks.

At the same time, increased block size allows implementation of a wide array of smart contracts—digital signatures included in the transactions that serve as the evidence of the right of someone over something—as well as many other sidechain solutions like Lightning Network that will make it possible to process all transactions literally instantly and for free despite of their number.

Apart from this, SegWit provides an wide range of other important features like increased P2SH security, linear scaling of sighash operations, reducing UTXO growth, overall efficiency gains, and so on.

2.2.2. Security

All blockchain networks let their users perform a kind of escrow transactions—called multisig or multisignature—that require up to five signatures from different parties in order to sign a transaction.

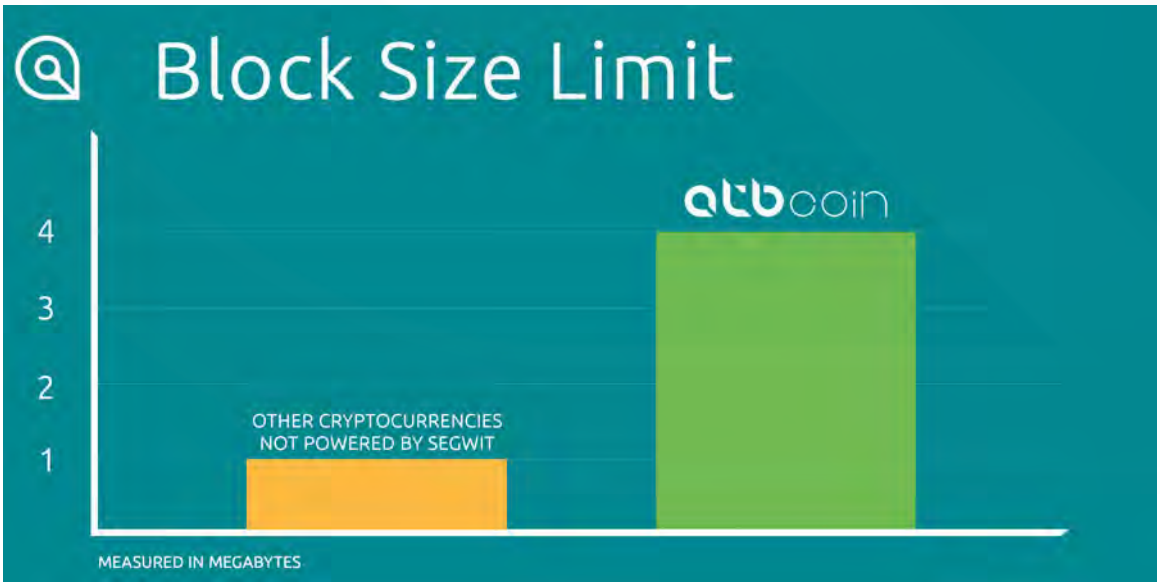
Currently the majority of cryptocurrencies use pay-to-script-hash (P2SH) protected by 160-bit HASH160 algorithm that has its loopholes, letting a corrupt multisig transaction member steal money. In SegWit this roadblock will be fixed by using HASH160 only for single public key transactions, whilst all multisig transactions will be using 256-bit SHA256 algorithm.

Also, an increased block limit size that is proposed in SegWit improves the overall security of the network and therefore allows for a seamless and safe implementation of smart contracts and second layer solutions on top of the network.

2.2.3. Block size and network capacity

Initially, the block limit size of 1MB was set by Satoshi Nakomoto in 2010 in Bitcoin for purposes of protecting the network from DoS and spam attacks, but since then it became the default value used by the majority of world's cryptocurrencies.

Since this limit leads to slower transaction approval time and higher transaction fees within a busy blockchain network, leading to lower overall performance, SegWit increases this limit to up to 4MB per block by excluding witness data, scriptSig and scriptPubKey fields with the signature data that occupies 60% of the transaction size, out of the transaction.



With the new block weigh algorithm that SegWit proposes, all non-witness data in a block will amount to 4 weight units per byte and the witness data will amount to 1 weight unit per byte in the same block. This constitutes a 4x increase in the network capacity and performance as well as allows for implementation and utilization of smart contracts and sidechain features—which occupy a certain amount of the transaction size—that was impossible to carry out earlier because of low block size and network throughput.

2.2.4. Malleability and smart contracts

By taking the witness data out of the transaction and increasing the block size, SegWit solves another important problem that cryptocurrency blockchains were dogged by in the past couple of years.

When a transaction is sent to the blockchain network, any node that processes it can possibly make minor changes to the signature data in the txid of this transaction. And though this minor changes cannot influence the input and output transaction information—meaning that it still will be sent and received by the right people—it can make the txid information unreliable, making it more difficult to trace it within the blockchain.

However, such malleability of the transaction txid may also lead to safe but rather pestering attacks[4] within the network.

By storing witness data outside of the transaction under SegWit, no node will be able to alter it. This, in turn, makes the transaction fit more non-witness information and increases both the block size and network capacity, leading to the possibility to create smart contracts that require a certain amount of space within the transaction for their successful implementation.

Smart contracts are small parts of code that are included in a transaction—marking and coloring it—that serve as an evidence of possession of a certain right over something by someone (e.g. tangible/intangible funds and resources as well as intellectual or any other property) and turn a common transaction into a powerful tool for documenting purposes.

[4] https://cointelegraph.com/news/the-ongoing-bitcoin-malleability-attack

2.2.5. Lightning Network

Since SegWit fixes transaction malleability, the whole cryptocurrency blockchain network become more secure. This allows for creation of sidechain solutions like Lightning Network.

Lightning Network is a solution that allows for sending literally instant and free transactions to one or more users of the network thanks to the usage of multisig payments and smart contracts.

The idea behind Lightning Network is to create micropayment channels off the blockchain so that the users can send an unlimited amount of payments between each other by either securing them with only one ledger entry in the blockchain and using the blockchain as the arbiter through smart contracts or by applying to a trusted third party for escrow purposes.

ATB Coin is planning to launch Lightning Network solution in about three months after its release for purposes of improved scaling of the network as well as cutting the transaction processing times and fees down to the minimum.

3. Key features

Apart from the features intrinsic to the Proof-of-stake algorithm, Segwit update, and Lightning Network solution that ATB Coin is powered by, it also has a wide array of proprietary characteristics—a user-friendly and lightweight wallet, cloud mining options, forging incentives, and others — that are meant to make its daily usage convenient for everyone irrespective of their financial needs.

3.1. Wallet

ATB Coin cryptocurrency comes with an array of lightweight and user-friendly wallets—for desktop, iOS, Android, and web that will be released one month after the cryptocurrency launch—that provide all necessary features for convenient daily use of the cryptocurrency for your financial needs and do not require much space on your PC or smartphone.

The most important advantage of the ATB Coin wallet is that it requires a very small amount of space for its installation and therefore can be used by anyone, anywhere, and anytime. This became possible thanks to the system ATB Coin is built on, Proof-of-stake, which makes using full node wallets an almost completely redundant thing.

Since there's no physical mining of coins involved—and the distributed consensus is achieved via a proof of possession of coins in one's wallet—you will not need to download the full copy of the blockchain to use ATB Coin, resulting in usage of less space and bandwidth as compared to the full node wallet.

Apart from the basic functionality that lets the users perform operations associated with receiving, sending, and exchanging their ATB Coins between the world's most widely-used currencies, the wallet will also have at array of additional features that will ensure the ultimate user experience.

3.2. Cloud mining

As it has been mentioned above, users in ATB Coin do not need to constantly hash data using costly equipment that consumes a lot of electricity. However, in order to enter the coin forging pool and be able to earn with ATB Coin, you will need to keep your PC and wallet online to be considered an active blockchain node.

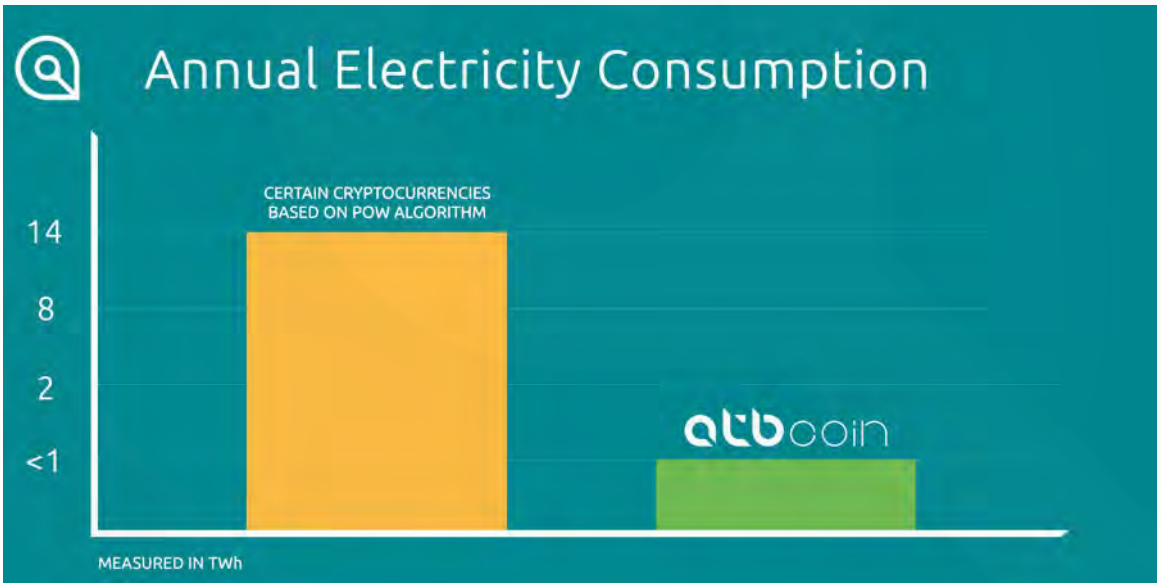
Though this is definitely a better and more eco-friendly way of maintaining the blockchain security, it will still lead to often unnecessary power spending. This is exactly why ATB Coin offers a special service of cloud mining for all of its users irrespective of whether they are just regular users or investors.

There will be three deposit maturity options—90, 180, and 360 days—available as part of the cloud mining service. During these time periods the user will not need to keep their PC and wallet open, therefore decreasing their electricity consumption, whilst the daily ROI as well as the monthly and yearly bonuses will be credited to their wallet on the same day.

The cloud mining services will be provided both by ATB Coin and several other trusted third-party companies so that the cryptocurrency members can enjoy a wide selection of payment options and service conditions tailored especially to their needs.

3.3. Low energy consumption

According to the publicly available statistics[5], currently some of those cryptocurrencies based on POW algorithm use up to 14.18 TWh of electricity yearly, which is comparable to the total consumption of power in entire country like Slovenia.



A rapid growth of any POW based cryptocurrency will undoubtedly lead to sustainable increase of electricity consumption.

[5] https://digiconomist.net/bitcoin-energy-consumption

Since ATB Coin is based on Proof-of-stake algorithm, which was developed to make cryptocurrencies more resource efficient and eco-friendly, its users don't need to buy expensive equipment known as ASICs—which most often get obsolete as early as one year after their purchase and eventually end up at landfills—and waste massive amounts of electricity on performing unnecessary calculations.

Everything that a user needs to do to start creating coins in ATB Coin and earn is to sign up, download a lightweight desktop wallet, and keep their device online or use a special cloud mining service in order to cut the energy consumption associated with forging ATB Coins to the minimum.

3.4. Agility and cost-efficiency

Featuring the most fundamental characteristics of Proof-of-stake algorithm—eco-friendliness, ease of use, and lightweight wallet—as well as the most up-to-date technologies—Segwit that provides a 4x increase of the network capacity and bandwidth, Lightning Network that allows for unlimited throughput of off-blockchain transactions, and cloud mining—ATB Coin is set to become the world's most agile, cost-efficient, and user-friendly cryptocurrency.

4. Risks and risk management

Cryptocurrencies offer a whole range of tools and measures that are meant to contribute to the development of a more transparent, just, and open global financial market and ensure the security and growth of one's funds.

But just like any other complex and elaborate systems, cryptocurrencies present certain flaws and risks associated with financial instruments. In the sections below we will explain such risks and talk about the ways of managing them and cutting their impact down to the minimum.

4.1. Security: attacks and hard forks

There are various kinds of attacks and vulnerabilities that the cryptocurrencies may be exposed to but the two most important of them are a majority attack, or 51% attack that has to do with monopoly problems, and double spending attacks.

The most harmful attack that may be performed within a blockchain network is known as a 51% or majority attack. It may happen when one node of the blockchain possesses 51% of it or more and therefore gains complete control over it.

However such attack may theoretically take place in POW based cryptocurrencies—in case of which the evildoer will need to purchase mining equipment in the amount of over $15 mln—it won't be feasible to perform it in ATB Coin for two reasons.

Firstly, since ATB Coin is a POS based cryptocurrency, the attacker will then need to get hold of at least 51% of all network resources. Even if we consider the possibility of this attack straight after the launch of ATB Coin when there will be still a small number of coins forged, the evildoer will need to purchase at least 25.5 mln of ATB Coins, which is 51% of the genesis block.

Secondly, even if such attack happens, it won't be beneficial for the attacker. Since spreading of the news about the attack will likely influence the market rate of the cryptocurrency in a negative way, the evildoer will be attacking himself selves and will suffer from losses.

When it comes to double-spending attacks, in ATB Coin they will be prevented by means of cementing every transaction that is included in a certain block. This way, in order to be confirmed and considered as valid by the blockchain, the transaction will need to receive at least 6 confirmations.

4.2. Inflation

Due to the fundamentals of POS algorithm that proposes a daily reward in exchange of the user's help in achieving the distributed consensus, all cryptocurrencies based on this system usually face inflation issues.

Inflation concerns in ATB Coin will be tackled thanks to including a relatively small amount of coins in the ICO—only 50 mln of ATB—decreasing the daily reward rate twofold every two years, and following an effective and intensive marketing campaign that will ensure a stable influx of new users for the cryptocurrency for years to come.

4.3. Centralization

Yet another pressing issue for all cryptocurrencies irrespective of whether they are based on POW, POS, or DPOS algorithms another pressing issue is centralisation concern.

Since it's both illogical and too costly to perform a 51% attack within a POS based cryptocurrency, appearance of the general tendency towards centralization of the network in ATB Coin is very unlikely.

As an additional measure against centralization, the creator of the next valid block in the ATB Coin blockchain will be selected using deterministic randomization formulas—based on the stake size and the lowest hash values—that will limit wealth accumulation possibilities and ensure that the cryptocurrency doesn't get centralized.

5. Conclusion

This whitepaper has been prepared for purposes of offering the most detailed information about the cryptocurrency—concerning its key characteristics and features, the most important technologies used in its development, and risks associated with it as well as all measures that will be used to manage such risks—that will be understable by and helpful to both a beginner user and an IT and cryptocurrency specialist.

We have succeeded in finding out and establishing that Proof-of-stake system ATB Coin is based on proves to be a more secure, just, and eco-friendly as well as less corrupt and less difficult to use alternative to Proof-of-work algorithm.

At the same time, the latest technologies that ATB Coin is powered on—SegWit and Lightning Network—and the proprietary features like cloud mining, lightweight wallet, and forging incentives make it a truly agile, cost-efficient, and user-friendly tool that can answer and satisfy the needs for financial freedom of any person irrespective of their place of birth, technical competence, or social status.

www.atbcoin.com

Good for Business
Good for You