**AtlasCoin : Community Backed Cryptocurrency for a micropayments platform .**

AtlasCoin Team
https://atlascoinpro.com

## *Abstract*

*A peer-to-peer crypto-currency design derived from Bitcoin where Proof-of-Stake replaces Proof-of-Work to provide most of the network security.*
*Under this hybrid design proof-of-work mainly provides initial minting and is largely non-essential in the long run. The energy consumption doesn't affect the security and integrity of the chain thus providing a clean and efficient system .*
*Proof-of-Stake is based on coin age and generated by each node via a hashing scheme similar to Bitcoin but on a smaller search space . The integrity of the blockchain history and transactions is guaranteed by a broadcasted checkpoint mechanism .*

## History and Future Vision

AtlasCoin started as a simple idea building a cryptocurrency around an active community,according to a recent poll on one of the many Facebook cryptocurrency group in Africa more than 200,000$ is being traded daily on exchanges it's 100 the GDP Per Capita in Morocco in 2015 AtlasCoin isn't just a cryptocurrency it's a complete platform that aims to provide an Exchange,a Micropayements API and Blockchain technology powered by and for the North African community and soon to expand on the whole continent considering the idea of a crypto currency powered by active tourism .

African countries mainly Nigeria,Kenya,Morocco become leaders in bitcoin adoption mainly because of the

exorbitant fees that the banking system asks for and especially how hard is it to transfer wealth outside ,Bitcoin adoption was predictable africans became able to send money to their relatives easily and the many exchangers made it possible to convert it to cash faster than a Bank Transfer and a lot less expensive than traditional money transfer service ,thus the AtlasCoin team saw an opportunity to build a native currency  for this group the goal set was to provide a Blockchain complete platform leveraging strong cryptography and Bitcoin primitives to create a scalable platform targeting mainly the African continent .

The choice of the underlying primitives is justified by the goal of AtlasCoin to simply provide an efficient implementation that doesn’t require exorbitant fees like Bitcoin currently and even if the energy consumption approaches zero the network still uses Proof of Stake making AtlasCoin a long term energy efficient implementation .

## Coin Age

The concept of coin age was known to Satoshi Nakamoto at least as early as 2010 and was discussed in during 2011 by the early circles  and was mainly used in Bitcoin to help prioritize transactions, for example,although it didn’t play much of an critical role in Bitcoin’s security model. Coin age is simply defined as currency amount times  holding period. For example, if Bob received 20 coins from Alice and held it

for 60 days, we say that Bob has accumulated 1200 coin-days of coin age.
Additionally, when Bob spent the 20 coins he received from Alice, we say the coin age Bob accumulated with these 20 coins had been consumed or destroyed). Block timestamp and transaction timestamp related protocols are strengthened to secure the computation of coin age.

## Proof-of-Stake

The Proof Of Stake algorithm aims to achieve distributed consensus unlike Proof of Work where the algorithm rewards the nodes who solves cryptographical puzzles thus rewarding the nodes with the highest computing power ,PoS rewards the creator of the next block in a deterministic manner and the odds of being choosen depends on the stake (wealth) .
Initially Proof-of-work helped to give birth to Nakamoto's major breakthrough, on the other hand it makes it dependent on computing power thus energy consumption.
Introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees making it hard to adopt .
As the mint rate slows in Bitcoin network, eventually it could put pressure on raising transaction fees to sustain a preferred level of security. One naturally asks whether we must maintain energy consumption in order to have a decentralized crypto-currency?
Thus it is an important milestone both theoretically and technologically, to demonstrate

that the security of peer-to-peer crypto-currencies does not have to depend on energy consumption.
The end goal of AtlasCoin is affordability and mass scale adoption and we think that a PoS scheme makes our odds higher for mass adoption .

In the case of AtlasCoin we choose a stake age between 15 days and 30 days with 7% annual stake reward

## Main Chain Protocol

The protocol for determining which competing block chain wins as main chain has been switched over to use consumed coin age. Here every transaction in a block contributes its consumed coin age to the score of the block.
The block chain with highest total consumed coin age is chosen as main chain.
This is in contrast to the use of proof-of-work in Bitcoin's main chain protocol, whereas the total work of the block chain is used to determine main chain.
This design alleviates some of the concerns of Bitcoin's
51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities.
Also attacker's coin age is consumed during the attack, which may render it unusable for an

attacker since it will become harder to prevent transactions from being written on the main chain .

## Checkpoint: Protection of History

One of the disadvantages of using total consumed coin age to determine main chain is that it lowers the cost of attack on the entire block chain of history. Bitcoin has proven a it's strong protection over the history Checkpoints were introduced in a later update in 2010 the goal was to add an extra layer tos strenghten the blockchain, preventing any possible changes to the part of blockchain earlier than the checkpoint. Another concern is that the cost of double-spending attack may have been lowered as well, as attacker may just need to accumulate certain amount of coin age and force reorganization of the block chain.

## Block Signatures and Duplicate Stake Protocol

Each block must be signed by its owner to prevent the same proof-of-stake from being copied and used by attackers the signature renders each block unique to the next one and so on .

A duplicate-stake protocol is designed to defend against an attacker using a single proof-of-stake to generate a multitude of blocks as a denial-of-service attack. Each node collects the (kernel, timestamp) pair of all coin stake transactions it has seen. If a received block contains a duplicate pair as another previously received block, we ignore such duplicate-stake block until a successor block is received as an orphan block.

## Implementation:

The Current implementation of AtlasCoin have been battle tested to run as core nodes of the network providing cross platform wallets ,the next steps on ward are aimed to facilitate the access to the blockchain making it easy to build applications on top of AtlasCoin blockchain .
Our goal is not to build a new innovation but rather to simplify and make accessible a current technology to a mature and very active group that has been ignored for a long time .

## Acknowledgement:

We would like to thank the whole collective of crypto community the researchers,the pionneers ,the developers who made AtlasCoin a reality and of course our work is just a result of standing on the shoulders of the giants like Sir Isaac Newton said .

## References:

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): Decentralised currencies are probably impossible (but let’s at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)
Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.(http://www.bitcoin.org/bitcoin.pdf)