WHITEPAPER

New and Straightforward path towards cashless and electronic transactions based on blockchain technology

POOLCOIN

Smart Digital Money & Intelligent Blockchain

version 1.0

* Introduction to Blockchain Technology

Blockchain technology has been garnering great hype recently. It gained popularity after the introduction of Bitcoin in 2009 by the person or group of people by the pseudonym Satoshi Nakamoto. Many people confuse and believe blockchain to be bitcoin. But, bitcoin is one application of the blockchain technology. There are many other applications and use cases that can be solved using blockchain other than just payment systems.

What is a blockchain?

A blockchain is defined as a peer to peer distributed ledger forged by consensus, combined with a system for smart contracts.

-Hyperledger, Linux Foundation

Now, that definition might contain a lot of uncommon terms so lets start by breaking it into parts and understanding each term.

Peer to Peer Network
You must be aware of BitTorrent and Tor. Both of these are built on peer to peer network design. A peer to peer network is a distributed application architecture that consists of computing devices connected to each other, without a central server.

In centralised networks, the security is dependent on a single entity. If that central server is attacked, the security of the overall network is compromised. But a peer to peer network is more secure as there is no single point of failure.

* Introduction to Blockchain Technology

Distributed Ledger
A ledger is a system containing all the records of a input and output of a process. A distributed ledger is a data structure which is spread across different computing devices. DLT (Distributed Ledger Technology) is the technology that distribute records across all the users. DLT consists of 3 components – Data Model (current state of ledger), Language of transactions (which changes ledger state) and Protocol (used to build consensus). Blockchain is a type of DLT. This way the data is shared among all its users increasing transparency and avoiding corruption.

Consensus
Consensus is a process of ensuring that all the different users n a blockchain come to an agreement regarding the current state of blockchain. There are several consensus mechanisms that are used by different blockchains to achieve consensus. For example, Bitcoin uses Proof-of-Work while Ethereum is moving from Proof-of-Work to Proof-of-Stake algorithm.

Smart Contracts
Forget smart contract and blockchain for a moment. Think about contracts in general. These contain some conditions which need to be fulfilled in order for some transaction (eg; money exchange) to occur. For example, if you are selling me a laptop a contract will contain that I will be responsible to pay you only if the laptop works properly. Similarly, smart contracts are pre-requisite conditions which need to be fulfilled for transactions to happen in a blockchain.

* Introduction to Blockchain Technology

What is inside a blockchain?
A blockchain is a chain of blocks connected to each other. A block consists of four parts:
-> Previous Hash
-> The timestamp
-> Nonce
-> Merkle tree root
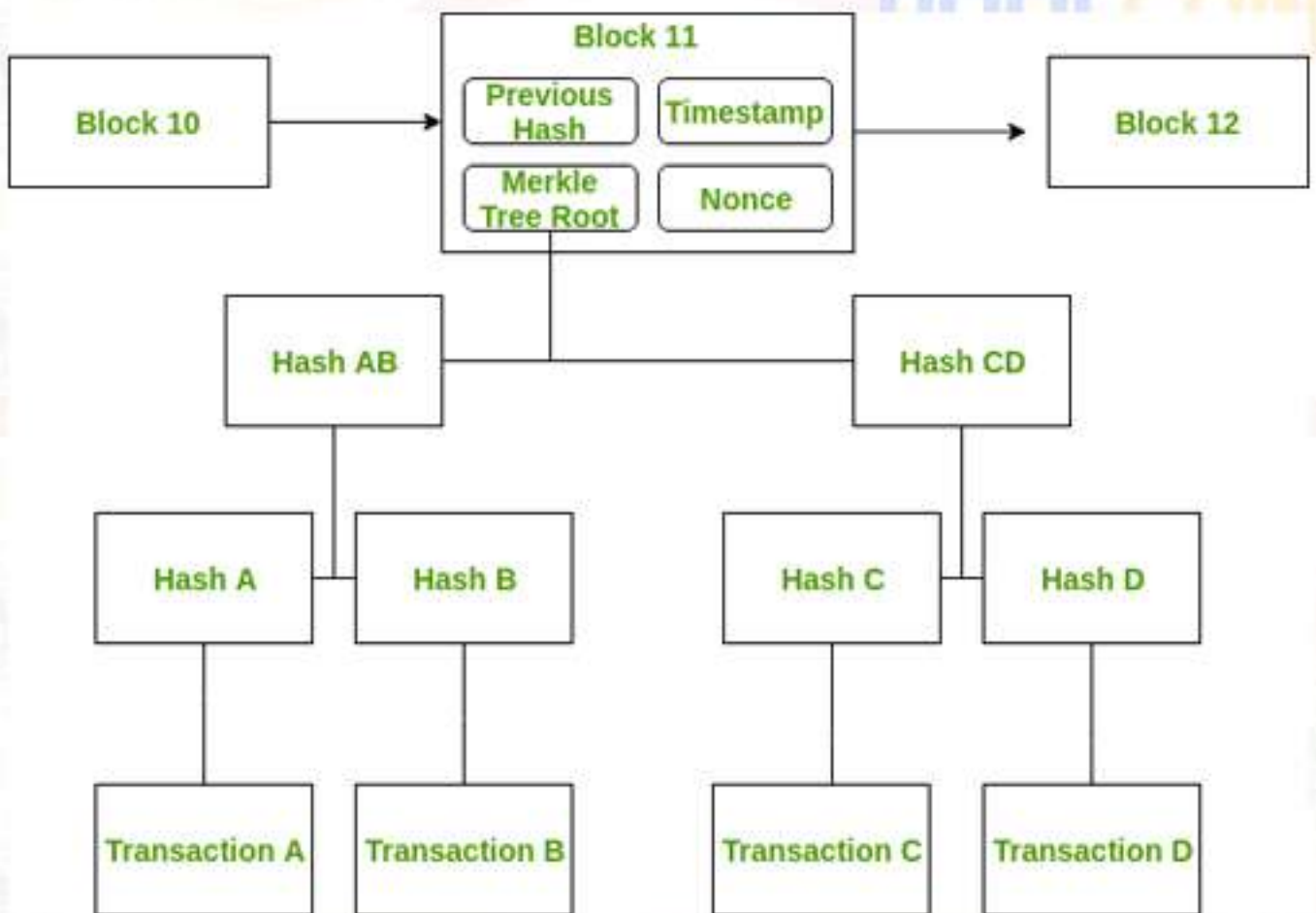
Each block contains a cryptographic hash of the data of the previous block. The nonce is calculated by the miners by solving a cryptographic puzzle to propose the next block in the chain. It is known as proof of work. The blockchain is said to be immutable because of its cryptographic properties. But this does not mean that changing the data is impossible. It means that it is extremely hard to change the data and any change can be easily detected. A merkle tree is a binary tree with hash pointers.

* About POOLCOIN

We at **POOLCOIN** are different between other cryptocurrencies. By different, we mean literally.

With POOLCOIN, our philosophy is *"START WITH SMALL, SURE BECOME LARGE"*.

POOLCOIN are created and developed by our experienced Programmer Teams. This to make sure all things goes right to avoid any miscalculation and problems ahead.

POOLCOIN are forked from Blackcoin based, but in additional to make sure **POOLCOIN** stay up to date, our Programmer Teams already make some modification to Blackcoin base and become **POOLCOIN**.
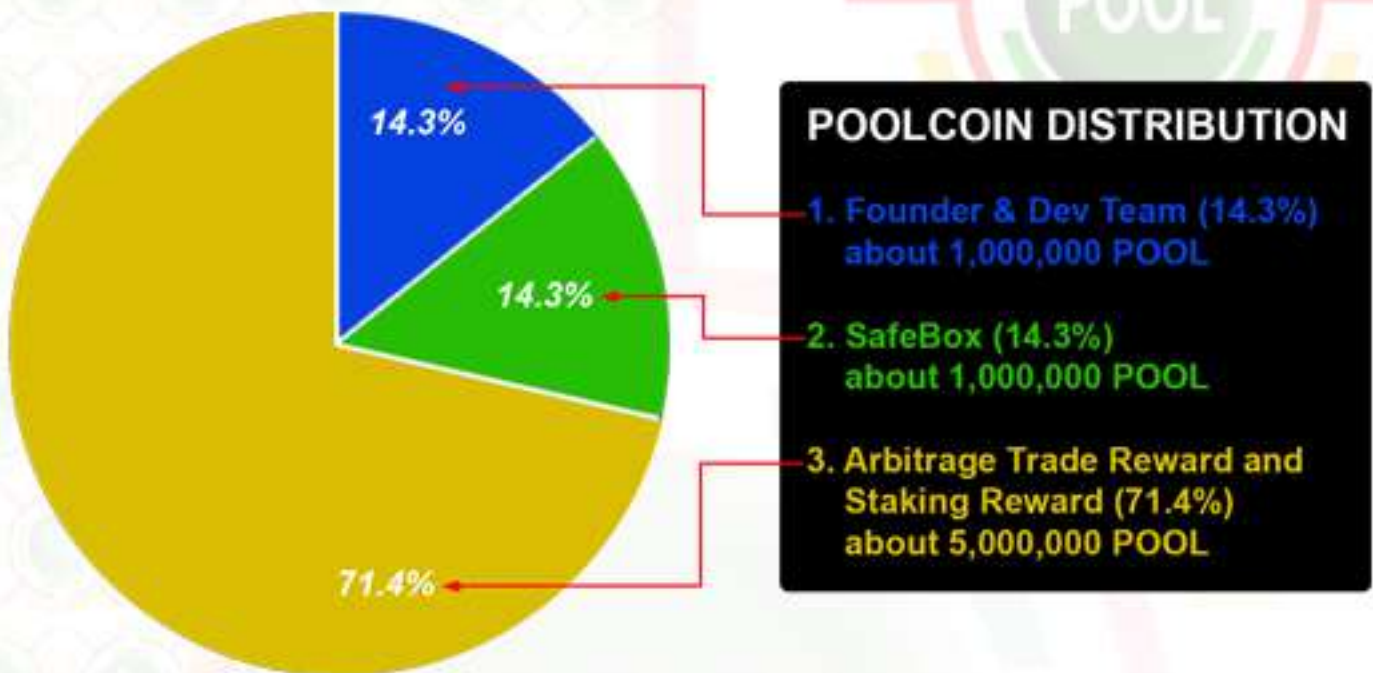
POOLCOIN Details as below:
1. Coin Name: *POOLCOIN*
2. Coin Ticker: *POOL*
3. Algorithm: *Bitcoin & Script (Proof of Work - POW + Proof of Stake - POS)*
4. Total Supply: *7,000,000 POOL*
5. Pre-Mined: *100% (7,000,000 POOL)*
6. Circulation Supply: *based on web https://poolcoin.world*
7. Mineable: *Yes (by staking your coin ballance in wallet)*
8. Staking Reward: *min 0.0002 POOL*
9. Block: *max every 4 minutes.*
10. Coin Logo:

* About POOLCOIN

POOLCOIN DISTRIBUTION

POOLCOIN DISTRIBUTION

1. Founder & Dev Team (14.3%)
   about 1,000,000 POOL

2. SafeBox (14.3%)
   about 1,000,000 POOL

3. Arbitrage Trade Reward and
   Staking Reward (71.4%)
   about 5,000,000 POOL

1. Founder and Development Team (14.3%)
This allocation about 1,000,000 POOL is for marketing,
reserch dan development progress and also to maintain
and support POOLCOIN Main Nodes

2. SafeBox (14.3%)
This allocation about 1,000,000 POOL act as insurance
for all of our users.

3. Arbitrage Trade Reward and Staking Reward (71.4%)
This allocation about 5,000,000 POOL
- *Arbitrage Trade Reward*: to make sure our users get fair and
  decent return, we give users rewards for Arbitrage Trade
  (https://poolcoin.world)
- *Staking Reward*: This reward can be gained when Staking
  happen in Hodl Wallet.

* How Transaction Been Verified

It is possible to verify transactions/payment without running full network nodes. It is very simple and easy for users. Because of **POOLCOIN** is *Proof Of Stake (POS)* coins, user not require to run any nodes and no need to copy of the block headers of the longest *Proof Of Work (POW)* chain. This is because our main system already have *Staking Pool* that do human works to queriying network nodes until convinienced has longest chain and obtained the Merkle branch linking the transaction to the block that timestamped in.
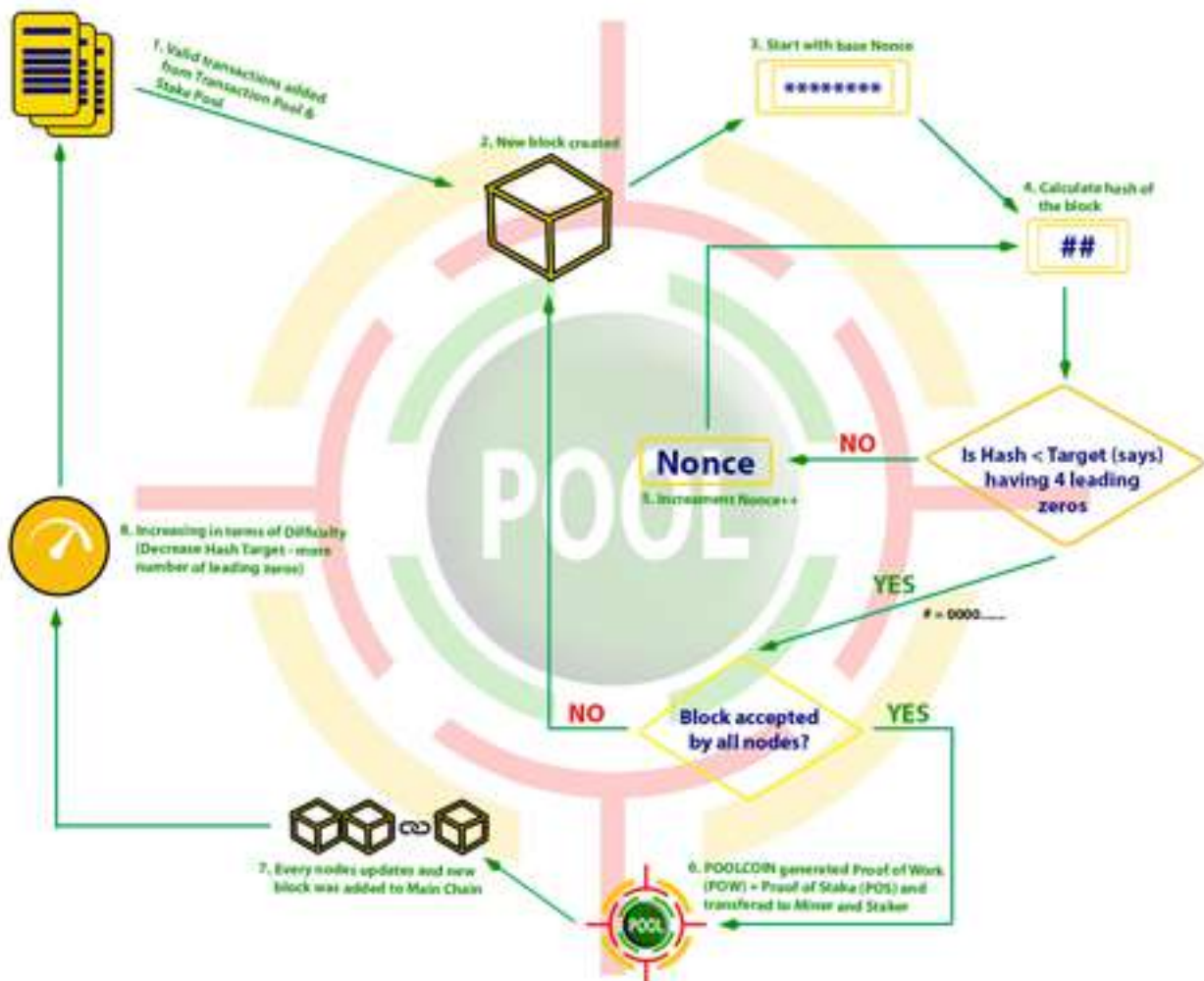
* Staking

Staking Definition

Staking is the process of holding funds in a cryptocurrency wallet to support the operations of a blockchain network. Essentially, it consists of locking cryptocurrencies to receive rewards. In most cases, the process relies on users participating in blockchain activities through a personal crypto wallet.

The concept of staking is closely related to the Proof of Stake (PoS) mechanism. It is used in many blockchains that are based on PoS or one of its many variants.

Who created Proof of Stake?

Sunny King and Scott Nadal were likely the first to introduce the ideas of Proof of Stake and staking, back in 2012. They described Peercoin as an innovative PoS cryptocurrency. It was initially based on a hybrid PoW/PoS mechanism but gradually phased out its emphasis on Proof of Work (PoW). This allowed users to mine and support the project in the early stages, without becoming fully reliant on a PoS system.

In 2014, Daniel Larimer developed the so-called Delegated Proof of Stake (DPoS) mechanism. It was first used as part of the Bitshares network, but other cryptocurrencies adopted the same model. Notably, Larimer also created Steem and EOS, which also adopt the DPoS model.

Staking POOLCOIN

In **POOLCOIN**, we have varient type of staking such as *QT Wallet Staking, Web Base Staking and Mobile Apps Staking*. User can choose what suitable to himself/herself to start **POOLCOIN Staking**.

* Blockchain Precomputation and Long Range Attacks

At the time of this writing, there is no known solution for secure timestamping in a largely distributed network. Rules of the current block timestamp give an attacker a degree of freedom in selecting the proof hash described in Eq. 1 and therefore increase the probability of a successful attempt to fork from several blocks in the past.

In addition, the current stake modifier does not obfuscate enough hash function to prevent the attacker from precomputing future proofs. Therefore, someone who attempts to attack the network in a malicious way will be able to calculate the future interval for future proof of completion, which allows the individual to produce several consecutive blocks and perform malicious attacks that may harm the network.

* POOLCOIN Platform

The **POOLCOIN** platform consists of components that provide the network and protocol for the use and construction of social security systems, including the Client, tools and frontend applications.

The purpose of the platform is to create an ecosystem in which social security systems can be developed, tested, simulated, managed and productively used as quickly as possible.

* POOLCOIN Targeted Market

Southeast Asia has a population of more than 600 million and a GDP of at least $2.31 trillion. The Association of Southeast Asian Nations is becoming a force of nature not to be trifled with. With China and India showing signs of slowing down and as the U.S. shifts its focus to the East, the region has become a hot spot for investment. ASEAN Economic Community also have plans to integrate regional economies to enable ASEAN countries to be more competitive with the rest of the world.

7 Recent research also shows the region receiving more foreign direct investment inflows than China. A recent example of a huge marketmoving IPO in 2013 would be the $2.1 billion listing for BTS Rail Mass Transit Growth Infrastructure Fund in Thailand.

* POOLCOIN Roadmap

April ~ July 2019
Research for POOLCOIN and Market Study

August 2019
Development for POOLCOIN started

September ~ October 2019
Testing and verify the POOLCOIN Nodes and started to link Our Wallet System to Arbitrage Trade

November 2019
Finalize POOLCOIN Nodes and Arbitrage Trade System (Confirm)

December 2019
Open https:/poolcoin.world for users to involved in Arbitrage Trade.
Starting to develop Web Based Wallet that link to the system

more features and technology in 2010