SAPOTACOIN

A Peer-to-Peer Electronic Currency

Email : info@sapotacoin.com
Web : https://sapotacoin.com

Sapotacoin is also a peer-to-peer web currency that grants prompt, near-zero value payments to anyone within the world. Sapotacoin is an open, supply, the world payment system that's perfectly decentralized without any central influences. Mathematics secures the network and grant individuals to manage their own finances. Sapotacoin features faster trade approval times and appreciates storage capability than the leading math-based currency. With valuable industry supporter, trading volume and liquidity, Sapotacoin are explaining the medium of commerce complementary to Bitcoin.

Decentralization is the means of distributing, powers, people or things away from a central location or authority. We want no central management and no central point of failure. Systems run by specific people, in specific locations, with specific computer systems, are susceptible to government interference, coercion, legal issues and more. This document describes how SAPOTACOIN can operate as a self-sustaining entity. Open source code, freely distributed, with systems in place that reward and facilitate trust. Users will be free to use and operate the network in the way they think best.

The Sapotacoin Project was conceived and created by SAPOTA TECHNOLOGY. It was pre-announced and was launched on March 31, 2018. Based on Bitcoin's peer-to- peer protocol, Sapotacoin brings a number of features viewed by its development team as improvements over other coin implementation.

The main feature is the use of scrypt as its proof-of-work algorithm. A proof-of-work algorithm creates a computational challenge to be solved by the network of computers in order to "certify" a "block" of transactions. This change reduces the efficiency gain an economic incentive to develop custom hardware such as Application Specific Integrated Circuits (ASIC). While ASICs can be adapted for any purpose and are likely to be introduced for Sapotacoin, the use of the script should delay this change, and preserve the decentralization in mining that brings a decentralized currency so much of its value and resiliency.

The second important feature is a reduced transaction confirmation time targeted at 2.5 minutes on average.Sapotacoin’s faster confirmations provide end-users with faster access to their finances, especially in time-sensitive situations.

Other parameters have remained unchanged, such as the number of blocks between difficulty changes, and the number of years between block reward halving events. This means Sapotacoin has a difficulty change about every 3.5 days and will produce a total of 210 million Sapotacoin—four times the number of Bitcoin currency units.

This math-based currency is seeing an increase in its adoption. A recent announcement by the world's leading sapotacoin exchange. stated that it is integrating Litecoin in its portfolio. This news ignited a lot of speculation over Sapotacoin and ultimately led to a substantial rise in value.Sapotacoin's first reward halving will occur around October 2018 at which time 42 million Sapotacoin will be in circulation.

PROBLEM DEFINITION

The SAPOTA TECHNOLOGY system employs the best features of decentralized technology with some extra safety and privacy-centric network design features. The dual blockchain system, as outlined in the sapota technology Whitepaper, acts as the data backbone and does not rely on any centralized systems like databases to operate. Although the dual blockchains are decentralized, the scripts which process transactions have to be run on a public facing web server. This is a single network point referenced by an IP address. The processing scripts of the sapota technology system are managed and maintained by a DevelopmentTeam. Despite the reliance of the SAPOTACOIN Development Team, we designed the old system to be extremely hard to shut down. We run the system on multiple servers using different service providers based in various countries.

We store the processing scripts on GitHub and have backup copies scattered around the world. We store backups of the subchain and processing servers wallet files. Everything needed to restore the system has multiple backups stored on multiple continents. If a malicious actor tried to take down the sapota technology system, we could have new servers up and run in a matter of hours with minimal losses. However, this still relies on the Sapotacoin Development Team being available to set up the new servers. Until now, this has meant we are the single point of failure in the sapota technology system.

HIGH-LEVEL SOLUTION

At a high level, the solution to the issue of the Sapotacoin Development Team being the single point of failure for the sapota technology system is simple. We decentralize the administration of the sapota technology network by making the subchain and processing scripts publicly available and operational. In creating a viable solution, there are of course many security concerns which need to be addressed before independent operators can run their own sapota technology systems. These will be outlined in the Solutions Detail chapter of this document.

The primary technique for resolving most of the security concerns is to limit interactions between servers to within trusted clusters. This way, we are able to have multiple public or private clusters setup and users can choose which entities they interact with.

HIGH-LEVEL SOLUTION

Users will have the option to use official Sapotacoin sapota technology Servers, switch completely to a 3rd party service or use a mixture of servers. In the latter case, the software will randomly pick which network the transaction goes through. Each cluster will have a public rating; users can upvote/downvote the cluster as well as leave feedback. This feedback and rating system will alert other users to possible scams, long wait times, high fees or hopefully the reliable service they received.

HIGH-LEVEL SOLUTION

When designing solutions we weren't looking to redesign the wheel. We looked at how existing technologies have overcome similar problems and implemented familiar solutions eg. When using Tor, users are able to specify which nodes they use. In turn, the nodes are able to restrict themselves to operate in clusters. This eliminates the risk of using unknown Tor nodes who might be and often are logging data or performing other malicious behaviors. This was our major inspiration to opt for a cluster system over an open mesh. MD5 hashes are used by Bitcoin and many other software providers to validate file integrity. This is the method which we have implemented to assure users that the software a cluster is using hasn't been modified. Public voting mechanisms and lists are often used to host important public information and it is entirely possible to duplicate this information anywhere on the web.

SOLUTION DETAILS

One thing to note is that checking the hash isn't foolproof. It would be possible for a malicious actor to modify the code to simply return a hardcoded copy of the correct hash whenever a request was made. The hash should not be used as an absolute proof the source is genuine.

PUBLIC LISTING AND VOTING ON CLUSTERS

Allowing public methods for network operators to list their servers is essential. The Sapotacoin Team cannot be responsible for curating the list if we are to remove ourselves as a single point of failure. Currently, the server listings will be hosted through the Sapota technology Only posts containing server addresses, fees and hashes will be allowed. Users can use voting and be commenting to alert people to the quality of the service they received from particular providers.

PUBLIC SOURCE CODE

When the system is decentralized, the source code for both the Sapota Technology processing scripts and the Subchain will be available to the public from our Sapotacoin GitHub account: This allows people to inspect the code we have written, set up their own servers, fork their own versions, contribute to the code base or whatever else can be imagined.

Sapotacoin is frequently compared to othercoin , which functions almost exactly the same, aside for the cost of transactions, which are around 1/50th of the size. For many cryptocurrency traders and users, Litecoin pricing acts more rationally than Bitcoin, and with a more sustainable future.

In addition to trading and purchasing sapotacoin, it is possible to mine it, though this is a very technical activity and requires a decent amount of computer knowledge. A good computer is enough to mine coins very slowly, but a serious miner would use processing units that rapidly solve mathematical equations that support the blockchain.

Algorithm

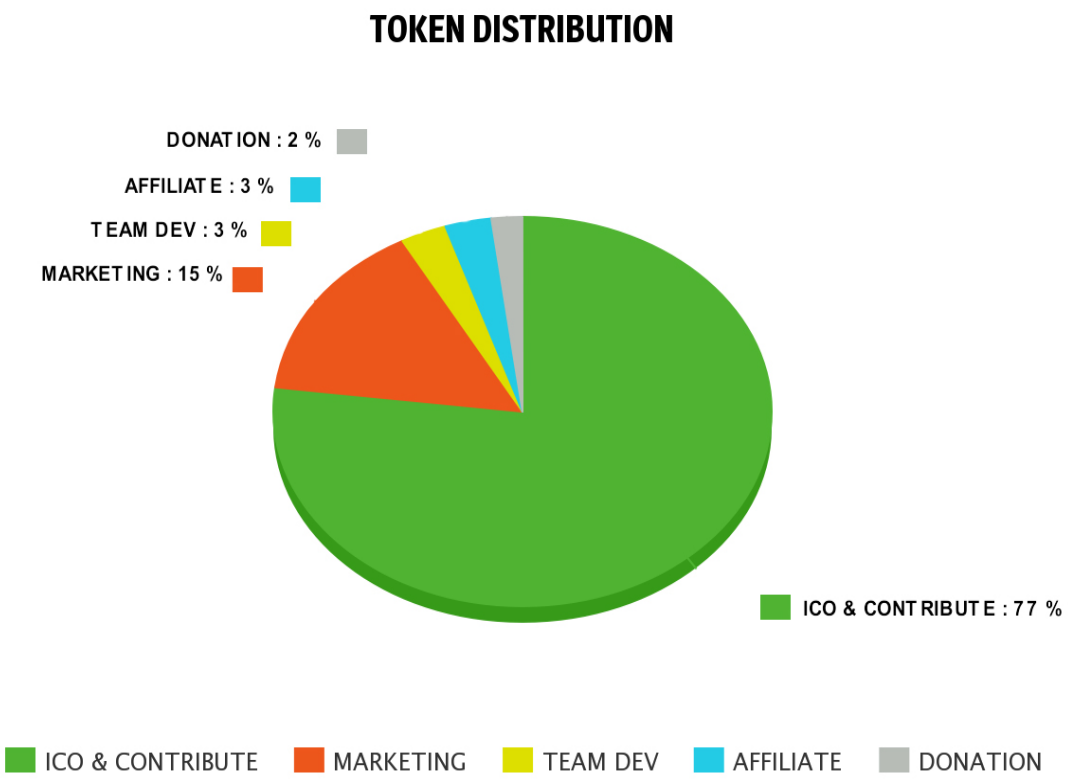
The algorithm includes the following parameters:

- Passphrase - The string of characters to be hashed.
- Salt - A string of characters that modifies the hash to protect against Rainbow table attacks
- N - CPU/memory cost parameter.
- p - Parallelization parameter; a positive integer satisfying $p \leq (232- 1) * hLen / MFLen$.
- dkLen - Intended output length in octets of the derived key; a positive integer satisfying $dkLen \leq (232- 1) * hLen$.
- r - The blocksize parameter, which fine-tunes sequential memory read size and performance. 8 is commonly used.
- hLen - The length in octets of the hash function (32 for SHA256).
- MFlen - The length in octets of the output of the mixing function (SMix below). Defined as r * 128 in RFC7914.

```
Function scrypt
   Inputs:
      Passphrase:                Bytes    string of characters to be
hashed
      Salt:                      Bytes    random salt
      CostFactor (N):            Integer  CPU/memory cost parameter
      BlockSizeFactor (r):       Integer  blocksize parameter (8 is
commonly used)
      ParallelizationFactor (p): Integer  Parallelization parameter.
(1..2^32-1 * hLen/MFlen)
      DesiredKeyLen:             Integer  Desired key length in bytes
   Output:
      DerivedKey:                Bytes    array of bytes, DesiredKeyLen
long

   Step 1. Generate expensive salt
   blockSize ← 128*BlockSizeFactor  //Length (in bytes) of the SMix
mixing function output (e.g. 128*8 = 1024 bytes)

   Use PBKDF2 to generate initial 128*BlockSizeFactor*p bytes of data
(e.g. 128*8*3 = 3072 bytes)
   Treat the result as an array of p elements, each entry being
blocksize bytes (e.g. 3 elements, each 1024 bytes)
   [B0...Bp−1] ← PBKDF2HMAC-SHA256(Passphrase, Salt, 1,
blockSize*ParallelizationFactor)

   Mix each block in B 2^CostFactor times using ROMix function (each block
can be mixed in parallel)
   for i ← 0 to p-1 do
      Bi ← ROMix(Bi, 2^CostFactor)

   All the elements of B is our new "expensive" salt
   expensiveSalt ← B0//B1//B2// ... //Bp-1  //where // is concatenation

   Step 2. Use PBKDF2 to generate the desired number of bytes, but using
the expensive salt we just generated
   return PBKDF2HMAC-SHA256(Passphrase, expensiveSalt, 1, DesiredKeyLen);


Function ROMix(Block, Iterations)

   Create Iterations copies of X
   X ← Block
   for i ← 0 to Iterations−1 do
      Vi ← X
      X ← BlockMix(X)


   for i ← 0 to Iterations−1 do
      //Convert first 8-bytes of the last 64-byte block of X to a
UInt64, assuming little endian (Intel) format
      j ← Integerify(X) mod N
      X ← BlockMix(X xor Vj)

return X
```

```
Function BlockMix(B):

    The block B is r 128-byte chunks (which is equivalent of 2r 64-byte
chunks)
    r ← Length(B) / 128;

    Treat B as an array of 2r 64-byte chucks
    [B0...B2r-1] ← B

    X ← B2r−1
    for i ← 0 to 2r−1 do
        X ← Salsa20/8(X xor Bi)  //Salsa20/8 hashes from 64-bytes to 64-
bytes
        Yi ← X

    return ← Y0‖Y2‖...‖Y2r−2 ‖ Y1‖Y3‖...‖Y2r−1
```

GRAPH



TECHNICAL BENEFITS

The solution details outlined provide a very high level of security to the sapota Technology system as well as the confidence to the end user. Due to the fact that servers operate in private clusters, there is virtually no point for a malicious actor to attempt to extract sapota from the Sapota technology

network. If the network operated as one large mesh with no boundaries, it is impossible for a user to have confidence their sapota will make it out the other end because they would have no control of who was processing their coins. The largest attack vector for sending subchain transactions to an outgoing server in an attempt to extract sapota from their pre-loaded pool has been patched. With the user input server addresses and MD5 hashing, users can be confident they know the servers they are transacting with and have some assurances about the software running on those servers.The community server lists and the public GitHub source gives the guardianship of the system over to the public and truly decentralizes the sapota technology system. As with any system, there is some trust involved in using our Official sapota technology servers or any of the 3rd party listings. The beauty of open source software is that it provides tiers of trust which users can subscribe to. Easy to use options often entail more trust, but low-level solutions are also provided for the paranoid.If you trust our servers and the highest rated 3rd party servers, then you can add them all to your wallet config and your wallet will randomly choose which provider to use. If you only trust the Official sapota technology servers then you can continue to use only those servers which we guarantee will be running the exact source available on our GitHub account. If you don't trust the Official sapota technology servers (or any 3rd party servers), you can download our sapota technology and Subchain source, set up your own sapota technology servers and list only them in your wallet config file.If you don't trust our source, you can fork it or write your own source and process payments, however, you like using our subchain. These layers of control truly allow the end user to be the master of their own fate when it comes to protecting their financial privacy.

BUSINESS BENEFITS AND FUTURE GROWTH

Any server operators who set up a sapota technology cluster are going to be ready to specify the percentage fee that is charged once a user makes a dealing through their network. This provides a revenue stream for the operator and can support cover the charges of maintaining their network. The operator will also the most worth value a user can send in a single transaction and how many servers they run in their group.This allows for a good scope of systems to perform. From a high-end result with hundreds of servers and high transaction limits to a single server pair designed for private use to private clusters that only accept coins from whitelisted addresses. The possibilities are unlimited. We will still give the Official sapota technology servers for as long as we are able, yet we will also actively encourage and interaction with competitors and different operators. We also hope that open sourcing the project will encourage other others to contribute to the project and that we are excited to see how the technology is used and applied in the anticipation.

KEY BENEFITS

Using these security actions, operators will safely run their Sapota technology servers without worry of having their pre-filled pool of sapota stolen by a malicious performer.Users will positively choose which operators they execute with. The sapota Coin Development team removes themselves because of the single point of the loser.

RISKS

If you're using 3rd party servers there will continuously be the danger of malicious server operators. It's one thing that can't be avoided. But we have a trend to hope that with the habit we have performed,the community can weed them out quickly and therefore the problem outweigh any small gains that they might make.

CONCLUSION

Conclusion Upon validation of our design within the Market, we suppose to proof-of- stake designs to become a potentially more competing style of peer-to- peer crypto-currency to proof-of- work designs due to the rejection of dependency on energy expenditure, thereby achieving lower inflation/lower transaction fees at comparable network security levels.

ACKNOWLEDGEMENT

Many thanks to SAPOTA TECHNOLOGY for serving to out with testing and different network/fork connected work. We prefer to thank Development and Marketing Teams whose great pioneering work opened our minds and create a project like this potential Used perfectly, the Sapota technology System should be very safe to use and offer an unparalleled level of financial secrecy. We have mastered all the core technical difficulties which have arisen when presented with the challenge to decentralize the system. Once resolving challenges we have implemented solutions that have been tried and tested in parallel fields of interest instead of trying to attempt to redesign the wheel. We are positive that the Sapota technology Anon System can be decentralized in a way that is harmless, secure and accessible.

VISIT MORE DETAILS ON

https://sapotacoin.org
https://twitter.com/sapotacoin
https://facebook.com/sapotacoin
https://reddit.com/sapotacoin
https://reddit.com/sapotatechnology