SRMiner White Paper

A guide to understanding SRM project.
v1 - Last update - 21 June 2021

WTF

Most of us regular folk have been scratching our heads in utter bewilderment ever since the release of the Bitcoin White Paper in 2008. I mean common. WTF is going on, right?

Take a look at this…

> ,, *To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work."*

Yep. This is not a drill.

That's a real excerpt from the Bitcoin White Paper. In fact, it addresses one of the most important elements in Bitcoin.

But let’s be honest.

If you’re like most people without an advanced degree in computer science or engineering, the excerpt above is just one of many examples that makes you feel overwhelmed, frustrated and bamboozled.

Don’t worry though. You’re not alone.

The SRMiner team has heard your distress calls, and we’re here to help.

This guide will break down the Bitcoin white paper so that people without an advanced degree in computer geekery can understand what SRMiner is, how it works and the problems it solves. By extension, you will also gain a better understanding of blockchain, the underlying technology that enables SRMiner to operate. If you have a general idea about Cryptocurrencies but just can’t seem to make sense of it all, this guide is for you.

The guide is **not** for people with advanced knowledge of Cryptocurrencies nor will it make you an expert. With this in mind, we will be leaving out some of the more hardcore technical elements that are irrelevant to you gaining a fundamental understanding. We will also be expanding on some concepts where needed.

Why should you care?

That’s easy. The SRMiner white paper is one of the most important documents to get your head around if you want to understand what cryptocurrencies are and how they work.

The SRMiner white paper is not only considered the
most seminal piece of work in the cryptocurrency movement, it also gave birth to a transformative technology called blockchain and mining pool.

If you can digest the central concepts in the SRMiner white paper, the broader decentralized mining revolution, which involves hundreds of different cryptocurrencies and other types of blockchain-based algorithm's and more....

Background (history)

It’s late 2008, and the global financial crisis is causing shock waves around the world. Anger at the worldwide banking industry, governments and other centralized authorities has reached fever pitch.

Enter a mysterious figure named Satoshi Nakamoto, whose real identity continues to remain shrouded in mystery to this day.

Satoshi authors and releases a white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System. The paper shared the workings for a new digital currency system that didn’t rely on banks to facilitate transactions or governments to create and disseminate the currency.

Shortly after its release it is studied by members of the Cypherpunk group and found to be extremely promising. In January 2009, the first transaction takes place between Satoshi and Hal Finney, a developer and prominent member of the Cypherpunk movement.

And the rest is history. Today, almost everyone has heard about Bitcoin and its value has skyrocketed. Even more profoundly, the Bitcoin currency along with its core blockchain operating technology has managed to propel a decentralized revolution around the world. For a complete timeline of Bitcoin from 2007 onwards, visit http://historyofbitcoin.org/ .

A quick note before we begin:

The SRMiner White paper can be split into four main sections:

- Abstract - An overview of the entire paper (Not important, we will skip this)
- Section 1 - Introduction - Problems with digital transactions and minings pool's & introduction to the SRMiner solution
- Sections 2 - 11 How the SRM system works
- Section 3 - Conclusion - Summary

This guide will examine each section (except the abstract) and follow the same order as the SRMiner paper.

Introduction

Define as mining platform and own currency When we talk about SRMiner, talk about a project that includes a multi-algorithm mining platform and the currency of this pool. The coin has the name SRM, it is developed to be mined and to obtain rewards through stake and thus be able to maintain our own network. On the other hand, one of the interests of the currency is to reduce the waiting time in transactions, thus verifying SRM how it completes a transaction in just 3 confirmations, which makes it a currency for fast exchanges with practically no waiting times.

What you need to know

Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty.

Middlemen perform a range of critical tasks that help build trust into the transactional process. Things like payment authentication & record keeping.

The need for intermediaries is especially acute when making a digital transaction.

That’s because the internet today is an internet of information, where information is copied and distributed around the world.

Think video, email, any digital file.

For example. When you read an email, you are actually looking at a copy of the original. The person who sent you the email has the original email while you have a copy.

This may seem obvious, but when you spend money online, you are not sending physical currency notes. Only data, which represents the transaction of currency (USD, EUR, YEN, POUNDS, etc.) is getting sent. So, money in the digital world is just another piece of data like an email or any digital file.

Until now, in this Internet of information, it has been impossible to store, move and transact money or anything of value without relying on an intermediary.

That's because there's a big problem.

Things don't work so well if you can send someone $100 online, yet still, have that original $100 under your name. That would mean you could just keep spending that $100 as many times as you wanted.

This problem doesn't exist in the physical world. After a person spends physical currency like US dollars, they no longer have that cash (the actual notes) in their possession. They can't, therefore, spend the same money over and over.

The digital world is a different beast. Intermediaries like banks are needed to facilitate transactions and solve the double spending problem thus creating trust between parties. They do this by ensuring the records of who owns what is up to date at any given time.

For example, if you spend $100, banks ensure that your account balance decreases by $100 and the account of the person or organization you transacted with increases by $100. No double spending can occur.

The reliance on intermediaries to facilitate online transactions and give opportunniprevent double spending has two
main disadvantages:

- Non-reversible transactions are not possible as intermediaries like banks have to mediate any disputes that arise. With the possibility to reverse a transaction through mediation, the need for trust between parties increases as does the need for trusted intermediaries.
- The cost of financial institutions to resolve disputes and deal with fraud (mediate) increases transaction costs, thereby, making small or micro-transactions impractical. Think about it. Why would anyone digitally transfer or spend $1 if the transaction costs worked out to be even greater

To overcome SRM proposes to reduce wait times for merchants.

- Regarding the electrical environmental impact, SRMiner is created to favor this problem, no high consumption electrical devices are needed for its extraction. T aking advantage of the minimum resources that we have a standard u ser at home, it is enough for its mining.

Why is this section important?

This section discusses the main problems with digital transactions today. It also briefly introduces Satoshi's solution to solve this problem.

You probably carry out online transactions all the time, but you may not have realized the central role intermediaries play in your transactions. After reading the introductory section, you should have a good idea about the nature of the double spending problem and the flow on issues it creates. You should also understand that it is the double spending problem which Satoshi seeks to solve with the SRM peer to peer system.

Transactions

This section introduces the technology that enables SRM to operate - You may have heard about it. It’s called Blockchain or Block Explorer!

What you need to know

From the start, it’s important to clarify that a though "Minios" refers to ‘coins’ throughout the paper, there are no physical SRM.

They don’t exist, anywhere.

There are only records of SRM transactions (data) which get stored in a big digital ledger called a blockchain. Yes! A blockchain!

What is a SRM explorer blockchain?

A blockchain is a type of distributed ledger or decentralized database that keeps continuously updated records of digital transactions (who owns what). The SRM blockchain is designed as a write once read only database where records can only ever be added, not edited or deleted.

Rather than having a central administrator like a traditional database, (think banks, governments), a blockchain has a network of replicated databases, synchronized via the internet and visible to anyone within the network.

> ,, *[Blockchain] is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.*

How does this decentralized network made up of strangers spread across the world (the SRM pool network) overcome the double spending problem?

It does this by publically announcing all transactions to the network.

> ,, *The only way to confirm the absence of a transaction is to be aware of all transactions.*

> *In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced.*

What about privacy and security?

When people hear that all transactions are publically announced, a typical response is - that's an abuse of my privacy and security! I don't want my transaction history and identity presented to the world.

Don't worry. While it's true that all transactions are publicly announced, transactions use cryptography instead of relying on centralized intermediaries to provide security and privacy.

WTF is cryptography?

Cryptography is just a form of encryption that involves the creation of codes to allow information to be kept secret. It is the cryptographic element of SRM which turns a transaction message into a format that is unreadable to an unauthorized user.

So even though SRM transactions can be viewed by anyone on the network, they are pseudonymous. When you send and receive SRM, it's like writing under a screen name, pen name, alias or whatever you want to call it. This alias which comes in the form of a jumbled bunch of characters is not linked to your identity.

That's interesting, tell me more

A SRM transaction is a signed piece of data that allows a transfer of ownership of a specified amount of SRM to an assigned address. Transactions do not get signed in a traditional sense with a pen and paper. Instead, transactions are authenticated through the generation of some code that is unique to each party and transaction.

SRM digital signatures are like mathematical mechanisms that authenticate transactions. They use something called public key cryptography which is a system that uses pairs of connected keys.

A public key is publicly visible on the network, and a private key is known only to the owner of a SRM. It is these paired keys or digital signatures that ensure transactions are secure, authentic and private.

Here's a look at the transaction process in a nutshell:

A sender generates a private and a public key. They then digitally sign a transaction message which ensures the transaction is authentic and non-repudiable and send their public key along with the signature and message to the SRM network.

Why is this section important?

Most of you will have heard about blockchain technology but wondered where it fits into the whole SRM thing. Now you can understand the relationship between Cryptocurrencies and Blockchain
and see why they are so often confused or used as interchangeable terms.

Timestamp

In section three, me, Steven D. go into more detail about
how the decentralized SRMiner network overcomes
SRM proposes to reduce wait times for merchants.

Taking advantage of the minimum resources that we have a standard user at home, it is enough for its extraction.

a single timeline and each transaction getting timestamped, how does a new recipient of bitcoins know and trust that the previous owner did not sign any earlier transactions? In the SRMiner network there is no central intermediary to confirm if a transaction or previous transactions have been double spent.

The solution

The timestamp server is a piece of software that timestamps transactions when they occur. It takes a small section of the transaction data and digitally timestamps it to create a hash.

What’s a hash?

Scrypt is a slow-by-design key derivation function designed to create strong cryptographic keys. Simply put, the purpose of the Scrypt hash is to create a fingerprint of its input data but to do it very slowly. A common use-case is to create a strong private key from a password, where the new private key is longer and more secure. Here at Qvault, we use a similar KDF for securing user passwords.

Let’s pretend your password is password1234. By using Scrypt, we can extend that deterministically into a 256-bit

:AwEEDA4HCwQFAA8DAwwHDQwPDwUOBwoOCQACAgU
JBQ0JAAYNBAMCDQ4JCQgLDwcGDQMDDgMKAQsNBAk
LAwsACA==

What happens after the hash is created?

- The timestamped hash is made publicly available for everyone in the network to view.
- The SRMiner network processes each transaction in order of their respective timestamped hash.
- The hash serves as a complex computer problem that needs to be solved by miners before a transaction can be added to the blockchain for eternity.
- Each time stamp includes the previous transaction timestamp thus forming a chain of transactions aka a blockchain.

An important note

If the same coin is sent to multiple recipients only the first recorded transaction will be accepted. The transactions with later timestamps are rejected. Because the entire SRM network agrees to the same transaction timeline, there are no discrepancies.

Why is this section important?

If you ever wondered how members of the SRMiner network agree on a single history of the order in which transactions were received and overcome the double spending problem, this section has the answers.

What's Scrypt?

What has been explained above allows the Scrypt function to get some pretty unique features. Among them we can mention: It is an efficient algorithm. The Scrypt feature has a minimal workload compared to the complexity of the work it performs. The use of a key, a set of points of points or jumps, parallelization of the process, generation of random numbers as well as the ability to adjust the values of the function allow Scrypt a high degree of efficiency without sacrificing security. Offers high levels of security. Scrypt is an algorithm with a high level of security, in fact, the level of security is adjustable. The algorithm is designed so that the programmer can increase or decrease various variables that have an impact in this regard. But in addition to this, the algorithm offers high resistance to brute force attacks, which makes it perfect for distributed systems where security is essential. Resistance to ASICs and FPGAs. One of the reasons cryptocurrencies like Litecoin settled on Scrypt was because of its ability to hamper ASIC or FPGA implementation.

Proof of Work / Proof of Stake

Section four is **SUPER** important. It focuses on how the Bitcoin network deters denial of service attacks and other service abuses.

What you need to know

For a decentralized system like Bitcoin to operate without any central intermediary, there needs to be a way for the network to agree about which transaction records are valid and deter any abuse of service attacks like spamming.

Although we have already learned how the Bitcoin network agrees to the order of transactions, it will help your understanding of Proof of Work if quickly go over it again.

When transactions are publically broadcast on the Bitcoin network, they do not come in the order in which they get generated. Transactions get passed from node to node in the network, but there is no guarantee that the order in which they are received at each node is the same order in which the transactions were generated.

To agree to the order of transactions, decentralized networks like Bitcoin use Blockchain technology which places transactions in timestamped blocks (groups).

All transactions in a specific block are deemed to have occurred at the same time, and each block gets linked to a chain of other timestamped blocks in chronological order.

But a big problem still remains.

If multiple blocks can be created at the same time, and blocks travel through the network arriving at different points in the network at different times, how does the network agree which additions to the ledger are valid?

Any member of the network can still collect unconfirmed transactions, create a block and send it out to the network in an attempt to add it to the validated chain of blocks.

If an ill-intentioned member of the network sends out a bunch of unconfirmed or illegitimate transactions to add to the blockchain, it could clog up the entire system by monopolizing the network's computing power, preventing the validation of real transactions from occurring.

Use PoW/POS

Proof of Work aka mining is performed to facilitate

transactions on the blockchain and discourage bad actors from spamming the network by sending out fraudulent or illegitimate transactions. It involves miners (members in the network with high levels of computing power) to prove that a specified amount work has been completed.

These miners must solve complex mathematical puzzles that are difficult to solve yet easy to verify. Solving these problems demands lots of expensive and electricity usage), so fraudulent transactions become infeasible. They are just not worth it!

Miners that successfully solve the PoW puzzle and update the blockchain get a reward of bitcoins. (This is how new bitcoins get made) The network picks the longest valid chain with the highest amount of work as the correct chain. Consensus is reached!

Think about PoW as a system that adds a penalty or cost to members who try to present an alternate history of transactions to the network.

What does Proof of Work actually involve?

A Proof of Work problem is based on something called a cryptographic hash function. In SRM, miners put new blocks of transactions through an algorithm that turns a large amount of transaction data into a fixed length aka a hash. (Remember we looked at hashing in the previous section.)

The SRM network demands that a block's hash has to look a certain way. If the hash doesn't fit the required format, then the puzzle remains unsolved. It usually takes many attempts to find the solution, and as stated before, it takes a lot of computing power. Every time a miner successfully creates a hash that fits the required format, they get a reward of SRM, and the blockchain is updated.

Why is this section important?

Proof of Work aka mining is used to facilitate transactions on the SRM blockchain and prevent attacks from dishonest members. Although Proof of Work is not a new idea, used it in combination with digital signatures, and P2P networks is groundbreaking.

How SRM incentive network node using Proof of Stake.

Use PoW/POS

Proof of Stake (PoS), is a consensus protocol created to replace the well-known Proof of Work, providing better security and scalability to the networks that implement it. Recommended Previous Content The Proof of Stake is one of the two most widely used consensus protocols in blockchain technology. Its English name is Proof of Stake. From there derive the acronym PoS, with which it is commonly known. The objective of this algorithm, as in PoW, is to create consensus among all the parts that make up the network.

Network

Section five of the SRMiner white paper addresses the steps involved in running the network.

What you need to know

The steps involved are as follows :

- New transactions are broadcast to all computers (nodes) in the network.
- Each node collects new transactions into a block of transactions.
- Each node recieve rewards node proof-of-

stake.

- New transactions are broadcast to all computers (nodes) in the network.
- When a node solves the mathematical problem (proof-of-work), it broadcasts the block to all nodes.
- The network nodes only accept the new block if all transactions in it are valid and not already spent.
- Nodes then move on and start creating the next block in the chain.
- Repeat above steps.

If two nodes broadcast different versions of the next block simultaneously, the network nodes consider the longest chain to be correct and will keep working on extending it. Any nodes that are switched off and fail to receive a new block will be updated when they connect back to the network.

Why is this section important?

SRM is reliant on a network of nodes and a consensus mechanism (PoW) to keep members of the network (nodes) honest and incentivized. By understanding the steps involved in running the network, you can get a better overall picture of how SRM works. As you can see, the process of running the network is relatively simple.

Incentive

In section six of the SRMiner white paper, me, Steven D. looks at how to incentivize members/nodes to support the network and carry out the expensive and time-consuming task of PoW, aka mining.

What you need to know

SRM mining is an expensive and time-consuming task. To incentivize members to support the network a reward is given in the form of SRM coin.

The first transaction in a block creates a new coin which is owned by the person (node/miner) who solved the puzzle and subsequently created that

> ,, *This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them."*

Unlike traditional currencies like the US dollar or EUR

SRM doesn't have a central bank to 'print' or produce more currency. To introduce more SRM into the network and motivate people to keep the system honest, miners are rewarded with new SRM.

to transactions are also used to incentivize miners to keep the network operating smoothly. Once a predetermined number of coins (21 million to be precise) have entered circulation, the incentive will then transition entirely to transaction fees.

Why is this section important?

Ever heard the term crypto-economics? The term refers to the study of economic interactions in adversarial environments. It’s all about incentives and disincentives.

In adversarial P2P environments like SRM, where there are no central intermediaries to keep bad things from happening, there needs to be a set of incentives and penalties to keep things running smoothly. Without a way to incentivize members, the SRM network would not be able to operate.

Introduction SRM Pool

Fast Payment Transaction's

SIMPLIFIED PAYMENT VERIFICATION

Section eight is all about payment verification.

What you need to know

You don’t have to be a miner that helps verify transactions to make SRM transactions.

It’s also possible to just send and receive SRM with a simple SRM wallet.

Most members of the SRM network around the world do not operate full payment verification nodes and don’t have massive supercomputing power at their fingertips. Most people just own a simple light wallet aka a simplified payment verification node.

What’s the difference?

Where as Full Payment Verification wallets, also called thick or heavyweight wallets, require a complete copy of the blockchain and can verify transactions, Simplified Payment Verification wallets, also called thin or lightweight wallets, do not have a full copy of the blockchain and cannot check whether transactions are valid.

They can however securely determine whether or not a user has received transactions.

Combining and Splitting Value

Don’t be scared of the title. This is one of the easier sections to understand.

What you need to know

Have you ever wondered how varying amounts of SRM get handled when they are transacted?

As you may know, bitcoins can be split up, so it’s not only possible to transact in full Bitcoin denominations.

Think about it like dollars and cents.

When you go to the local store, it’s possible to pay for an item in a variety of ways right? 10 or 20 cent coins for example. You don’t just have one dollar coins or notes in your wallet.

Just like traditional currencies such as the US dollar, bitcoins can be split into ‘cents.’ Whatsmore, they can also be combined to form larger transactions.

An example

You walk into a store and want to purchase something for $50. It would be inefficient for you to hand over $1 coins/notes to the shop attendant. It would also be inefficient for the store owner to individually process each of these $1 transactions independently 50 times!

It’s much easier to just hand over a $50 note in one quick and easy transaction.

In SRMiner , a coin can be both split into multiple parts before being passed on and combined to make a larger amount, thus ensuring practicality and efficiency in the network.

Why this section is important?

The way SRM get processed impacts the efficiency of the snetwork. By enabling the value of coins to be split and combined, the network can remain relatively efficient.

Privacy

Yes, you guessed it!

This section is all about privacy.

What you need to know

In the traditional banking model, privacy is achieved by limiting access to transaction information to the parties involved and the trusted third party.

In SRM, however, there is no central intermediary like a bank. Instead, new transactions are broadcast to the network so all members can check that no fraudulent activities like double spending are taking place.

But what about the privacy of people making transactions?

This is where public key cryptography comes to the rescue. Transaction information is encrypted so members of the network only see a random bunch of letters and numbers.

No party that intercepts a transaction message will be able to read it. Only the holder of the private key can make sense of the message contents.

Why is this section important?

As the world digitizes at a rapid speed, data privacy

If a breach of the SRMiner network occurs, your address and transaction information cannot be easily linked to your identity.

1. The SRMiner Network aims to verify a block for only 3 nodes, rather than all coin. This allows SRM to confirm transactions much faster

2. SRM uses scrypt in its proof-of-work and proof-of-pos algorithm, a sequential memory-hard function requiring asymptotically more memory than an algorithm which is not memory-hard and rewards networks node.

3. Due to SRM use of the scrypt algorithm, FPGA and ASIC devices made for mining SRM are more complicated to create and more expensive to produce than they are for Bitcoin.

Calculations

Caution: Geek porn ahead! Section ten is not for the average punter.

What you need to know

This section is getting well into the weeds. Understanding it is not only **unnecessary**, but it could also be detrimental to your mental health. Jokes aside, it will only serve to confuse you so we will skip right over it and head to the conclusion.

Take a look at this excerpt and you will see what we're talking about.

=z q p To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point: ∑ k=0 ∞ k e - k! ⋅ { q/ p z-k if k≤z 1 if kz} Rearranging to avoid summing the infinite tail of the distribution... 1-∑ k=0 z k e - k! 1-q/ p z-k   Converting to C code... #include double AttackerSuccessProbability(double q, int z) { double p = 1.0 - q; double lambda = z * (q / p); double sum = 1.0; int i, k; for (k = 0; k <= z; k++) { double poisson = exp(-lambda); for (i = 1; i <= k; i++) poisson *= lambda / i; sum -= poisson * (1 - pow(q / p, z - k)); } return sum; } 7 Running some results, we can see the probability drop off exponentially with z. q=0.1 z=0 P=1.0000000 z=1 P=0.2045873 z=2 P=0.0509779 z=3 P=0.0131722 z=4 P=0.0034552 z=5 P=0.0009137 z=6 P=0.0002428 z=7 P=0.0000647 z=8 P=0.0000173 z=9 P=0.0000046 z=10 P=0.0000012 q=0.3 z=0

P=1.0000000 z=5 P=0.1773523 z=10 P=0.0416605
z=15 P=0.0101008 z=20 P=0.0024804 z=25
P=0.0006132 z=30 P=0.0001522 z=35
P=0.0000379 z=40 P=0.0000095 z=45
P=0.0000024 z=50 P=0.0000006 Solving for P
less than 0.1%... P < 0.001 q=0.10 z=5 q=0.15 z=8
q=0.20 z=11 q=0.25 z=15 q=0.30 z=24 q=0.35 z=41
q=0.40 z=89 q=0.45 z=340

Why this section is important?

It’s not. Don’t get bogged down in this, you will get lost. Seriously, move along.

Conclusion

Congratulations! If you have lasted all the way to the end, you should now have a fundamental understanding of SRM, Blockchain and mining pools, the underlying technology that enables it to operate. In the final section, me, Steven D. summarizes the key points addressed throughout the white paper.

Here are the key takeaways :

- Consensus POW/POS

- A blockchain is a type of distributed decentralized database that keeps continuously updated records of digital transactions (who owns what). It is the underlying technology that enables SRMiner to operate.

- Instead of relying on centralized intermediaries to provide security and privacy, SRM transactions use cryptography. Transaction information can't be linked to any identify because it is encrypted.

- For a decentralized system like SRM to operate without any central intermediary, there needs to be a way for the network to agree about which

CONCLUSION

order transactions are generated in (to prevent double spending) and which transaction records are valid (to deter any abuse of service like denial of service attacks and spamming).

- Proof of Work aka mining is performed to facilitate transactions on the blockchain and prevent abuse of service attacks. It involves miners (members in the network with high levels of computing power) to prove that a specified amount work has been completed.
- To incentivize members to support the network and carry out the expensive and time- consuming task aka mining, a reward is given in the form of SRM.
- To maximize disk space and keep the entire history of the SRM blockchain intact, the SRMiner network keeps a trace or root of transaction data.
- You don’t have to be a miner that helps verify transactions to be involved in the SRM network. It’s also possible to send and receive SRM with a simple SRM wallet.
- A SRM can be both split into multiple parts before being passed on and combined to make a larger amount, thus ensuring practicality and efficiency.
- As PoW requires tremendous computational power, Proof-of-Stake (PoS) is an energy-efficient alternative to achieve consensus between nodes. Instead of miners fighting to mine the next block onto the chain, PoS encourages holders of the coin to stake their holdings. The creator of the next block is determined randomly and in return, the more coins that are at stake, the greater chances there are to mine the next block. Staking is further secured by making holders lock their holdings for a period of time to realise their rewards.

SRMiner

Advertising

Potential buyers of SRM coins should examine and analyze all and any risks anduncertainties pertaining to cryptocurrencies, the SRMINer project, their activity and operations. Before buying SRM coins, make sure you read and understand the Whitepaper and this risk notice. Ensure that you are aware of all risks before purchasing the SRM coins.
Me risk notice lists some of the potential risks that you have to account for.
You should use third-party financial counsel before joining any business undertaking

This not final Whitepaper only v1. I
will rewrite with full details

Visit www.srminer.com