SCRIV NETWORK

WHITEPAPER

ABSTRACT

The Scriv Network is a unified blockchain technology that delivers state-of-the-art data assurance, verification, time-stamping and an IPFS (InterPlanetary File Sharing) network. The Network provides safety, impartiality, and cost-efficiency without the need for a third-party intermediary.

We are excited to present to you the SCRIV Data Verification and IPFS Network.

SCRIV NETWORK

Your Data Verified

TABLE OF CONTENTS

SCRIV WHITEPAPER

INTRODUCTION TO SCRIV

1.1 INTRODUCTION

The SCRIV network can verify the existence of digital data at any point in time. This data is linked with a publicly verifiable date and time (timestamp) to provide data assurance. This link can be verified without the need for a centralized service or third-party authority. The data assurance of the SCRIV Network allows users to verify data ownership and its originality.

1.2 TECHNOLOGIES INVOLVED

1.2.1 Hashing

Hashing is the process of submitting data to the input of a hashing algorithm which returns a short hash identifier (that allows for the data to be uniquely distinguished) as output. This output is called a "hash."

The hash is used to quickly distinguish datasets without having to compare the entire contents. This single process of comparison occurs only once and is much faster than comparing every bit of data. If the hashes are different, the data is not the same. If the hashes match, then, with a probability of 99.99%, the data is the same.

The hashing algorithm meets the following criteria:

> Matching data always returns the same unique hash.
> Non-matching data sets return a unique hash for each set. However, this condition is not always fulfilled completely. When a hash is assigned to non-matching data, it is 99.99999% unique.

1.2.1 Proof-of-work

Also referred to as POW, the proof-of-work system is very effective at protecting the network from abuse (i.e. DoS attack). With POW, complicated operations are solved on the client side, and then easily and quickly verified on the server side. The primary benefit of POW is the validation of the asymmetry of the time expenditure. "The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work." [1].

1.2.3 Masternodes

Typical blockchain nodes are servers which run on a decentralized P2P network. These nodes allow peers to send and receive updates across the network. The nodes require the ability to handle significant amounts of traffic and other resources and carry substantial cost with little reward. It is for this reason that the number of Bitcoin nodes has decreased continuously. "Much of the reason for the decrease of full nodes on the Bitcoin network, is the lack of incentive to run one. Over time the cost of running a full node increases as the network gets used more, creating more bandwidth and costing the operator more money." [2]

Masternodes solve this problem. "Masternodes are full nodes, just like in the Bitcoin network, except they must provide a level of service to the network and have a bond of collateral to participate. Collateral is never forfeit and is safe while the Masternode is operating. This allows investors to provide a service to the network, earn interest on their investment and reduce the volatility of the currency." [2]

1.2.4 IPFS Network

What is IPFS? IPFS is a distributed file system which synthesizes successful ideas from previous peer-to-peer systems, including DHTs, BitTorrent, Git, and SFS. The contribution of IPFS is simplifying, evolving, and connecting proven techniques into a single cohesive system, greater than the sum of its parts. IPFS presents a new platform for writing and deploying applications

and a new system for distributing and versioning large data. IPFS could even evolve the web itself.

IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high throughput content-addressed block storage model, with content-addressed hyperlinks. This forms a generalized Merkle DAG, a data structure upon which one can build versioned file systems, blockchains, and even a Permanent Web. IPFS combines a distributed hashtable, an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other. [3]

IPFS is an ambitious vision of new decentralized Internet infrastructure, upon which many different kinds of applications can be built. At the bare minimum, it can be used as a global, mounted, versioned filesystem and namespace, or as the next generation file sharing system. At its best, it could push the web to new horizons, where publishing valuable information does not impose hosting it on the publisher but upon those interested, where users can trust the content they receive without trusting the peers they receive it from, and where old but important files do not go missing. IPFS looks forward to bringing us toward the Permanent Web. [3]

1.3 NETWORK STRUCTURE AND OPERATION

The SCRIV Network's operation algorithm is as follows (See fig. 1)

1. User load data to be verified (PDF, JPEG, ZIP) in the wallet.
2. SHA3 Hash is generated.
3. Wallet checks the SCRIV blockchain to determine if this is new data or if has it already been established on the blockchain in the past.
    - New Data -> Launch Data Assurance Process
        1. User pays assurance fee [see Additional Rewards].
        2. Data is saved to IPFS network (generation of
           service data).
3. SCRIV EXPLAINED

5

SCRIV NETWORK

3. All required verification data is inserted into the
next block of the SCRIV blockchain.
- Previously Assured Data -> Launch Verification process
1. Search the SCRIV blockchain for the service data.
2. The algorithm returns IPFS address of the data.

Verified data can be accessed on the IPFS network through the SCRIV block explorer when the necessary conditions are satisfied [see "Privacy and anonymity"].
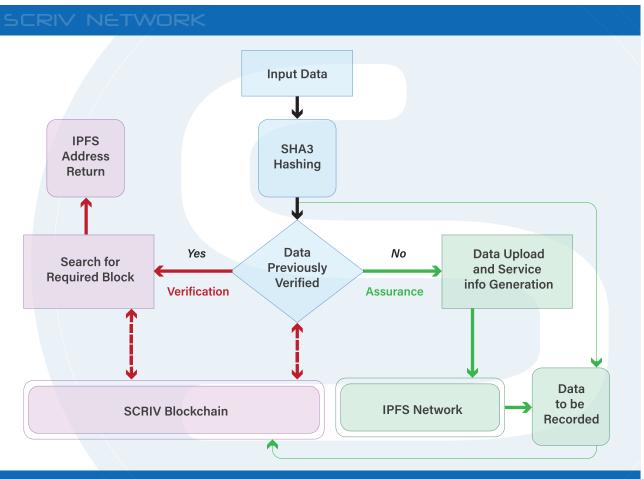

Fig.1 SCRIV network operation algorithm

1.4 ADDITIONAL REWARDS

In addition to the rewards paid for block generation, miners and masternode operators receive assurance fees. These fees are paid by the user. [see "Network structure and operation"]. The first part of this reward is included in the next block and paid to the miner who found it. The second part is distributed equally among all running masternodes.

This procedure greatly reduces inflation and ensures that the natural circulation of SCRIV will occur.

1.5 PRIVACY AND ANONYMITY

All user-dependent SCRIV operations are available within the wallet. The SCRIV network provides a fast and secure connection between the user, the blockchain, and the IPFS network.

Our blockchain is built upon the Dash source code, and all network transactions and file transfers are secured with high-level encryption.

By default, public keys are private. However, a user can request to link his identity to his public key. This requires that personal information is confirmed. Once this information has been verified, the users public key will then be appropriately labeled.

By default, all verified data is encrypted before it is saved to the IPFS network. However, it is also possible to save it as-is so that it will be publicly available.

2. USE CASES

The SCRIV network is open to everyone. From emergency operations to everyday use, from large companies to educational institutions. It can be used by lawyers, copywriters, artists, etc. Here are some potential use cases:

2.1. DEMONSTRATING DATA OWNERSHIP WITHOUT REVEALING ACTUAL DATA

This can be used to help protect content creators as well as retailers who sell digital goods. The content creator can protect his content by assigning a unique identifier (hash) on the SCRIV network which he can then give to authorized resellers. The customer can then be confident that the reseller owns the rights to sell the content by checking the assigned hash on the SCRIV network.

2.2 DOCUMENT TIMESTAMPING

This functionality can be used within the sphere of law where determining the originality of data plays a significant role. The SCRIV network can verify that digital data (documents, photos, videos, etc.) has not been altered or modified since being immutably registered and timestamped on the SCRIV blockchain.

2.3 VERIFYING DOCUMENT INTEGRITY

The SCRIV network can be used to ensure the integrity of business documents and contracts. When a document is registered on the SCRIV network it will be impossible for changes to be made without the knowledge of both parties. If changes are made, the document will fail validation.

2.4 PREVENTING UNWANTED DUPLICATION AND OVERWRITING

The usage of the SCRIV blockchain, in combination with the IPFS network, protects against unwanted storage duplication and the overwriting of documents.

8

3. SCRIV EXPLAINED

3.1 COMPARING SCRIV WITH OTHER DATA VERIFICATION SYSTEMS

Criteria	SCRIV	Stamp.io	Stampd.io	Poex.io
Blockchain	SCRIV	Bitcoin	Bitcoin, Bitcoin Cash Dash, Ethereum	Bitcoin
Average Confirmation Time	30 sec	10 min	5.5 min	10 min
Verification Fee	.01 USD	-	2 USD - average 0.25 USD min.	.01 USD
File Storage Integration	Yes	No	No	No
Instant File Access	Yes	No	No	No
IoT Integration	See Roadmap	-	-	-

3.2 GOALS

Quality Development

We are a team of perfectionists, who are passionate about making SCRIV a top-tier blockchain innovation. The SCRIV project has been divided into various stages, and upon the completion of each stage, the network will be put through rigorous tests before being released. We are highly committed to making the SCRIV network a highly efficient satisfying, and failure-free system to use.

Marketing

As you are well aware the cryptocurrency space has recently exploded and there are many new projects on the horizon. As a result, it is becoming increasingly difficult to stand out amongst the crowd. However, we intend to make the SCRIV network notable through better technology and more creative marketing. We are building strong relationships across the entire cryptocurrencies space, and leveraging the social media capabilities of the rapidly expanding cryptocurrency community.

3.3 SPECIFICATIONS

General Information

Algorithm	Tribus
Type	PoW / Masternodes
Maximum Coin Supply	~ 146 000 000 SCRIV
Block Time	30 sec
Premine	24 000 000
Masternode Collateral	100 000
RPC Port	7998
P2P Port	7979
Transaction Confirmations:	15
Block Max Size	4MB

Block Rewards

Approximate date,	Block interval,	Block reward (SCRIV)
Premine	1	24 000 000
Mar 2018	2 - 86500	9.6
Apr 2018	86501 - 100900	17.2
Apr 2018	100901 - 115300	24.8
Apr 2018	115301 - 129700	32.4
May 2018	127901 - 345700	40
Jul 2018	345701 - 691300	32
Nov 2018	691301 - 1036900	28.8

*Every 345600 block rewards will be decreased by 10%

Reward Distribution

Approximate date,	Block interval	PoW reward, ratio	MN reward, ratio
Mar 2018	1 - 86500	0.5	0.5
Apr 2018	86501 - 100900	0.55	0.45
Apr 2018	100901 - 115300	0.6	0.4
Apr 2018	115301 - 129700	0.65	0.3
May 2018	127901 - 345700	0.7	0.3

*Every 172800 blocks PoW/MN ratio will be moved towards MN by 5%

11

3.4 Marketing Plans

We understand that a quality product is only half the story of success. The other half of the story is marketing. Therefore, We have created a balanced marketing strategy to increase the interest in the SCRIV network. The marketing is divided into several steps.

All funds have been distributed in advance. We are leaving 10% of the premine for "Unexpected spends" to take care of new items of expenditures that will arise during future development.

Premine Usage

Item of expenditure	SCRIV coins	Premine percentage
Burned	4 000 000	16.7%
To be burned	8 000 000	33.3%
Premine left:		
Development expences	4 000 000	33.33%
Marketing expences	2 550 000	21.25%
Team payments	1 750 000	4.58%
Volunteer rewards	600 000	5.00%
Bug bounties	450 000	3.75%
Discord invitational comp	50 000	0.42%
Rewards to youtubers, etc	500 000	4.17%
Bounty campaigns	600 000	5.00%
Airdrop	300 000	2.50%
Reserve	1 200 000	10.00%

CONCLUSION

The SCRIV network provides a state-of-the-art solution to the problems of human error and the high-costs of data verification. It also provides a viable data verification process that spans across a plethora of industries and provides long-needed innovation in the data storage, real-time data verification, and protection of content authorship space.

The network is fast. It can process more than 100 data sets/second, extract their unique secure cryptographic identifiers, build a cryptographic tree with all this data in real-time, and publish the result to the SCRIV blockchain.

SCRIV also proves privacy. All the data sent to the network is encrypted with cryptographic identifiers (hashes) before hitting the SCRIV blockchain. Since hashes are oneway cryptographic algorithms, users can prove that a determinate hash relates to their data, but no one will ever be able to obtain that data by only having its hash.

SCRIV is an industry disrupting technology which eliminates the necessity of scriveners and lawyers. The SCRIV blockchain performs these jobs with greater speed safety and cost-efficiency.

What will you be able to do with SCRIV?

References

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2009.

2. E. Duffield, D. Diaz, "Dash: A Privacy-Centric Crypto-Currency", 2015.

3. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System", 2017.

4. P. Thevoz, "How can anyone check the authenticity of my University

Certificate on the Blockchain?", 2016.

5. S. Azmi, "A Blockchain based file verification system", 2016.

SCRIV WHITEPAPER

SCRIV NETWORK