*Astronomy & Astrophysics* manuscript no. output
December 21, 2019


# "SIRIN OS"- Blockchain Based Operating System

MD. Fahad Mojumder, ID : 1712145642

[1] North South University
e-mail: fahad.mojumder@northsouth.edu
[2] Plot-15,Block-B,Bashundhara R/A
Dhaka,Bangladesh

**ABSTRACT**

With the continuous development and application of blockchain technology, the academic and commercial circles are constantly exploring the research directions and practical application of blockchains. Today, in the financial, sales, medical and other fields, the blockchain has already played its advantages. In this paper, we focus on the SIRIN operating system and application of SIRIN in the field of blockchain technology. And try to provide a new feasible direction for the research and development of the blockchain in the next stage.

## 1. Introduction

The blockchain was produced in 2008 and was proposed by Nakamoto. It is a smart peer-to-peer network that uses distributed databases to identify, disseminate, and record information, also known as the value internet. Blockchain has develop rapidly in recent years and has become another technological innovation after cloud computing, big data, mobile internet and other new generation information technology. Blockchain technology enables distributed public ledgers that hold immutable data in a secure and encrypted way and ensure that transactions can never be altered. The information in a blockchain is recorded as blocks where a new transaction is chained to previous blocks in an append-only manner using cryptographic techniques which ensure that a transaction cannot be modified once it has been written to the ledger. SIRIN OS is an open source operating system which is developed by SIRIN LABS. The FINNEY Smartphone and FINNEY PC devices will use the SIRIN LABS open source SIRIN OS, an Android based operating system with an ultra-secure cryptography core. At the center of the SIRIN OS there is a distributed, scalable, light-weight, and ASIC-resistant ledger. SIRIN OS is designed and ready to run on millions of smart electronic devices around the globe. SIRIN OS implements an ultra-secure, peer-to-peer cryptocurrency transactions mechanism with a user-friendly, hassle-free interface. Those are the enablers: feeless  fast payments, resource sharing, and service offering. To ensure the integrity of the distributed leger transaction, SIRIN OS will offer multi-layered cyber protection. It makes use of innovative methods to secure the weakest link in cryptocurrency transactions, which is in the interface between the wallet, the internet connection, and the blockchain network.

## 2. SIRIN LABS SECURE BLOCKCHAIN TECNOLOGY

2.1 Overview and Requirements

SIRIN OS the basis for FINNEY devices, is a freely distributed open source operating system based on Android, designed to enable safe use of blockchain applications on mainstream devices. The SIRIN OS provides an enhanced blockchain features, decentralized resource sharing and a lightweight, feeless and quantum-proof transactions of cryptocurrencies.

2.1.1 Security Requirements

To enable mass market adoption of blockchain technologies, cryptographic tools should be a simple and foolproof. Experience with the first generations of connected payment systems shows that any Vulnerability that may exist between the moment a sensitive information is processed (on a network or storage) up to the moment it is displayed to end users (Such as on display) is eventually exploited, and at large scale. Complex procedures of maintaining key pairs, protecting private keys, planning one's recovery procedures and verifying transaction data are routine for today's blockchain users, but cannot be routine for all users.
The security scheme used in SIRIN OS must ensure that private keys are never exposed, and can only be accessed by a limited set of "secure mode" procedures, that are included in the OS, that authenticate the User and sign transactions or method calls with the keys. Keeping the secrets out of reach is the only way to ensure that it is impossible to steal them by using malware, by exploiting a bug in an app or even by cheating the user into sharing his secrets.
Additionally, users must have a simple and foolproof way of distinguishing fake from real payment interfaces, to protect them from phishing attempts. This requires a physical indicator on the device shell of when the device is in secure mode. Such indicator can be a unique LED, a physical switch, or even a separate Screen for secure mode operations. Users of the device only need to learn that the physical indicator must be set in order for them to make payments of Other secure operations.
While the above requirements are mandatory to prevent wallets being compromised by theft, phishing or keylogging, one must note that the advanced features enabled by FINNEY Create new opportunities for attackers. Specifically, we believe that resource sharing (and particularly sharing of CPU and network resources) could create a risk of eavesdropping and breach of access restrictions. To mitigate that risk, FINNEY will feature cybersecurity elements as a service by SIRIN LABS.

2.1.2 Blockchain Requirements

The blockchain operations provided natively by SIRIN OS can be used on any common blockchain technology. However, for common usages of payments and resource sharing, we find that none of the current standard blockchains is suitable for mainstream users. The native blockchain used for payments and resource sharing must provide fast transaction confirmation, ensure extremely low transaction costs to enable micropayments, and have light clients capable of operating nodes on devices with entry-level CPU and limited network connectivity. PoW design that enables a long-state equilibrium in which user devices do most of the validations in the network, rather than centralized mining pools, is also required to ensure the long-term independence of the network.

2.1.3 Hardware Adaptation Requirements

To comply with the private-key protection schemes and ant-phishing measures required by SIRIN OS, two security requirements must be aided by hardware elements: protection of private keys from application access, and user protection from phishing. Naturally, special hardware requirements may add a burden on manufacturers and designers, which we must ensure will not be a barrier to widespread adoption of SIRIN OS. To counter that, SIRIN LABS will provide a choice of hardware designs (and certify other designs if suggested by 3rd parties) that can satisfy these requirements, allowing OEMs to choose the design that can best fit their constraints.

2.1.4 Resource Sharing Requirements

Perhaps the most promising capability of a blockchain device is its ability to dynamically trade its resources with other devices, thus providing its users with better experience as they need it and better utilizing its resources when not in use.
Resource sharing must be seamless, secure and efficient for mass-market users to enjoy it. SIRIN OS introduces a virtualization layer between the OS interfaces and any of its shareable resources, making access to each of the resources virtualized both by the sharer and by the receiver. This ensures that partners to a shared resource (such as network or CPU) cannot undermine each other's security or privacy. The virtualized containers will also provide accurate metering of the shared resource, the sharer meters the amount of use of the shared resource at his sole discretion.
Two types of resource sharing protocols will be designed: Local Boost for sharing resources with directly- connected devices, and Cloud Boost for sharing resources over the network. SIRIN LABS will publish an RFC for both protocols. Being open protocols, any device- not just SIRIN OS devices-may contribute or use resources; this allows WIFI routers, cloud or edge-cloud computing services, public charging stations and many other devices to be also a part of the resource sharing network.

2.1.5 Development Methodology

SIRIN OS is developed in accordance with the SDLC (Security Development Lifecycle), and OWASP SCP including secure coding and penetration testing done by specialized 3rd parties and occasional hacker bounties.

2.2 Architecture

Adaptation Layer and HAL

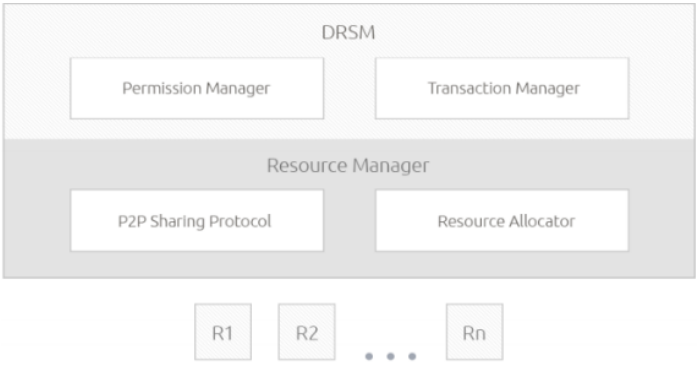

The adaptation layer and the hal defines a standard interface for OEMs to integrate SIRIN OS on top of their existing Software/Hardware platforms, in order to abstract resource access in a secured manner.

2.3 System Services and Core Libraries

System Services are modular components exposed by the SIRIN OS to the Application Framework and its APIs.


2.4 DRSM

The DRSM (Decentralized Resource Sharing Manager) is responsible to allocate, authorize and share resources over a decentralized network in a secure, trusted and private fashion. A background service operated by DRSM manages payments to resource sharers according to a dynamically calculated cost benefit protocol.




2.5 Block Shield

As SIRIN OS is designed as an inherently secure architecture, in addition to providing secure blockchain operations it can provide a toolkit of security and privacy related services. Parts of this toolkit are designed to provide security features to non-blockchain use are optional and OEM vendors may choose not to embed it in their products.


## 3. SIRIN LABS Token (SRN)

3.1 NUTSHELL

1. SIRIN LABS was founded in 2014 with the aim of development of mobile phone focusing on security and privacy.
2. They released a phone in 2016 called SOLARIN and are currently developing a second generation of the products the FINNEY smartphone and PC.
3. Both devices will use blockchain and will have a P2P resource sharing ecosystem for payment and apps, supported by the SRN token.
4. Company is based in Switzerland, they held ICO in Dec where they raised 158$M$.

3.2 USAGE

1. The smartphone and PC will both used the open source SIRIN OS which is an Android based operating system aiming to be light weight and ready to run on millions of smart electronic devices.
2. There is focus on security and privacy via cyber protection, BlockShield which is hiding IP addresses and MAC addresses, consensus module based on Tangle for free and fast transactions.
3. Decentralized app-store (dapps) will be available. Essentially Google Store for dapps.
4. There will also be P2P resource sharing market module where users can share digital resources.

3.2 TOKENS

1. The OS will implement peer-to-peer simple and user friendly cryptocurrency transaction mechanism.
2. The device will have hardware cold storage wallet built in that will hold all of the major cryptocurrencies and also SRN tokens.
3. The SRN tokens will be used to purchase device, apps, services and other products from SIRIN LABS. For example, special Cyber Security Suite.
4. Users will also be able to purchase warranty, repair and other services with the SRN tokens.

3.3 MY VERDICT

1. This is an interesting idea done by a reasonably large company that already has experience with phone production.
2. While I struggle to see the usage for PC (due to OS) I think the phone will gather a niche fan-base of users that will value security and identity protection above everything.
3. That being said I doubt the phone will go mainstream, too expensive for that. People will go for iPhones or flagship Androids instead.
4. The usage of crypto is forced in the ecosystem and the mcap is already really high. It might be good short term investment due to Liqui listing but long term I think there are better options.

## 4. Conclusions

The following are the risk factors in relation to SIRIN LABS business in general and SRN token sake event in particular:

1. SIRIN LABS is developing a complex hardware and software project and its launch may be delayed due to unforeseen development barriers.
2. The use of SRN tokens may come under the scrutiny of governmental institutions.
3. The ownership of SRN tokens may fall under new and unpredicted taxation laws that will erode SRN benefits.
4. The positions and plans outlined in this report may be altered as the project progresses.

## References

[1] Nakamoto SBitcoin: A peer-to-peer electronic cash system[J] Consulted (2008) Google scholar: https://bit.ly/2sQhw1E
[2] Blockchain Tecnology https://bit.ly/2Q5yzF8
[3] Prezi Inc. https://prezi.com/p/cyoargzghwn0/sirin-labs/
[4] SIRIN LABS white paper, page: 11-19 https://bit.ly/391iB7J