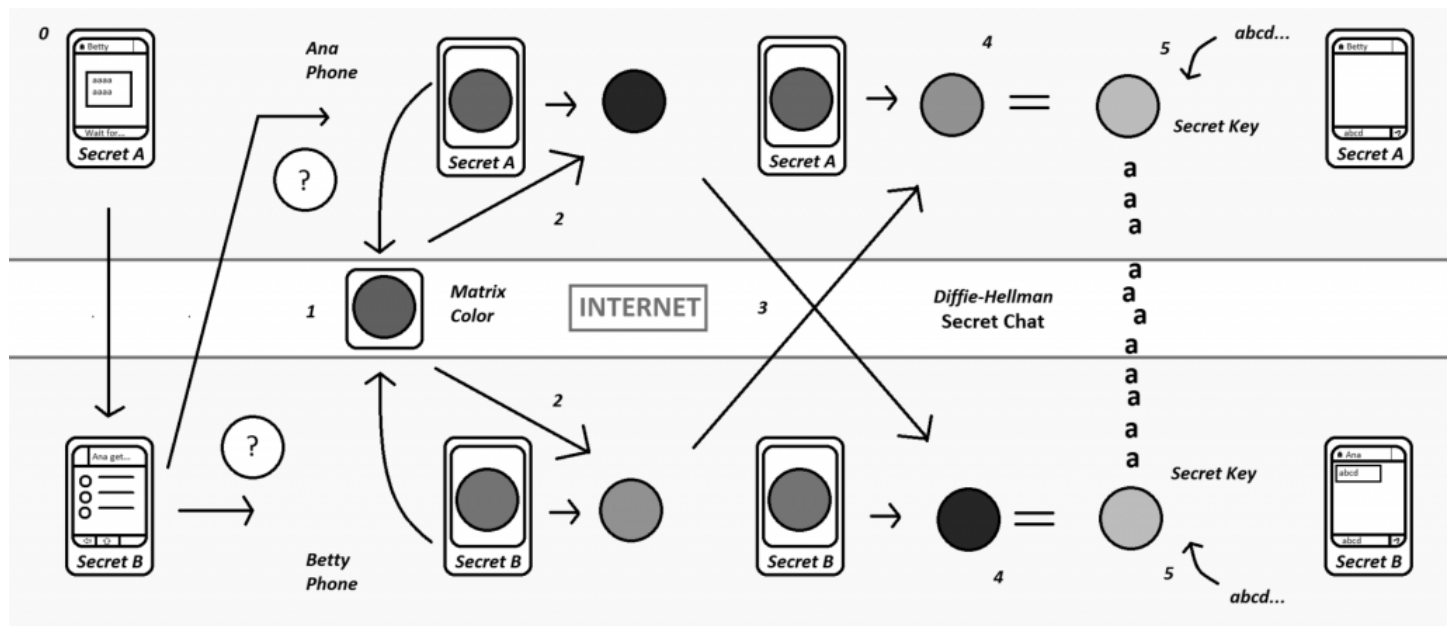


WarRin Protocol-A peer to peer anonymous and private communication system



New York, Airmont, Feb 2, 2021 ([Issuewire.com](https://www.issuewire.com)) - With the rapid development of the Internet, everyone inevitably needs to use communication tools to communicate with the outside world or relatives and friends. However, the traditional centralized communication system (WeChat, WhatsApp, Facebook) monitoring, privacy leakage, insufficient security and other problems frequently occur, which can no longer meet the increased privacy and security needs of users. The emergence of the WarRin Protocol makes people communicate anonymously and privately become possible.

WarRin Protocol

The WarRin Protocol is a peer-to-peer anonymous private communication system. It uses the characteristics of blockchain decentralization and non-tamperability, combined with innovative technologies such as elliptic curve encryption algorithm, pre-key and extended X3DH handshake, which perfectly solves traditional centralized communication. The system faces a series of problems such as the monopoly of the head company, personal privacy security, data leakage, communication security, etc., which truly protects the privacy and security of every user, and returns the ownership, control and income rights of personal communication data to the user. Any individual in the world can use this communication system to achieve peer-to-peer private communication.

The following is an excerpt from the WarRin Protocol white paper:

Two types of communication

I General Chat mode: Using point-to-point encrypted communication, the service side has access to the key and can log in via multiple devices.

I Secret Chat mode: Encrypted communication using point-to-point can only be accessed through two specific devices.

The design combines some of the advantages of RaiBlocks multi-chain construction with IOTA/Byteball DAG, which we call the Waring protocol. With improvements, we have given the WarRin protocol greater throughput and faster processing power while ensuring the security of the ledger, and network nodes can store the ledger in less space and search their communications accounts quickly in the ledger. When two users communicate, third parties contain content that neither manager can access. When a user is chatting in secret, the message contains multimedia that can be designated as a self-destruct message, and when the message is read by the user, the message is automatically destroyed within the specified time. Once the message expires, it disappears on the user's device

How chat history is encrypted?

The WarRin communication system draws on RaiBlocks' multi-chain structure for point-to-point communication. Each account has its own chain that records the sending and receiving behavior of the account. For example, in Figure 1, there are 7 accounts, each with 7 chain records of the account sending and receiving communications. On the graph, horizontal coordinates represent the timeline, and portrait coordinates represent the index of the account.

Transferring information from one account to another requires two transactions: one to send a communication from the sender's transfer content, and one to receive information to add that content to the content of the receiving account. Whether in a send-side account or a receiving account, a PoW proof of work with the previous communication content Hash is required to add new communications to the account. In the account chain, poWwork proves to be an anti-spam communication tool that can be done in seconds. In a single account chain, the Hash field of the previous block is known to pre-generate the PoW required for subsequent blocks. Therefore, as long as the time between the two communications is greater than the time required to generate the PoW, the user's transaction will be completed instantaneously.

The WarRin protocol uses triangular shrapned storage technology to crack impossible triangles in the blockchain through the shrapghine technology, with extensive node engagement and decontalination while maintaining high throughput and security:

I Complete shraping of blockchain status;

I Secure and low-cost cross-synth trading;

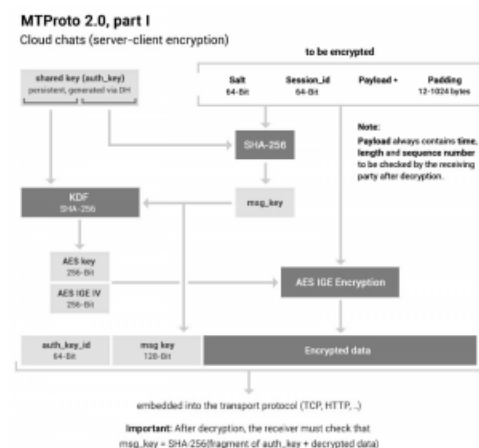
I Completely random witness selection;

I Flexible and efficient configuration

Complete decentralization ensures absolute security and scalability of the standard chain.

Incentives

On the basis of the WarRin agreement, by adding the incentive layer, we can effectively avoid the whole network being attacked and eliminate spam. As long as honest nodes control most of the calculations, for an attacker, the network is robust because of its simplicity of structure, and nodes need little coordination to work at the same time. They do not need to be authenticated because the information is not sent to a location.



Media Contact

WarRin Protocol

service@WarRin.com

Source : WarRin Protocol

[See on IssueWire](#)