ENTERSOFT

Technical White paper review

CREDITS.COM

Prepared for:
CREDITS.COM PTE. LTD.
Reg. No.: 201725929C

79 Ayer Rajah Crescent #05-08 Singapore 139955

1st December 2017

By:

Entersoft Security
Brisbane | Bangalore | Hyderabad
www.entersoftsecurity.com

Contents

Version Control

Version Date	Created/Modified by	Description/Pages Modified
28th November 2017	Sri Chakradhar	Author
1st December 2017	Mohan Gandhi	Editor

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to: (i) cybersecurity vulnerabilities and issues in the framework and algorithms based on white paper, the details of which are set out in this report, (White paper review). In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Entersoft Information Systems Pvt Ltd and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Entersoft) owe no duty of care towards you or any other person, nor does Entersoft make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Entersoft hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Entersoft hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Entersoft, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the white paper alone. No applications or operations were reviewed for security. No code has been reviewed.

Background

Entersoft was commissioned by Credits.com Pte Ltd to perform security review of their white paper. The review was conducted between 25th November 2017 and 3rd December 2017 .

More information on the whitepaper can be found *here*.

The report is organized into the following sections.

- Executive Summary: A high-level description of the findings of the review.
- Technical analysis: our detailed analysis of the white paper
- Conclusion: What is Entersoft's conclusion

The information in this report should be used to understand overall security posture of Credits.com. No Code review, Technology stack review were performed. The analysis is entirely limited to white paper.

Executive Summary

CREDITS is an open blockchain platform with autonomous smart contracts and an internal cryptocurrency. The platform is designed to create services for blockchain systems using self-executing smart contracts and public data registry.
The platform can handle more than 1,000,000 transactions per second for a low price and has a execution time from 0.01 seconds. CREDITS platform is the first completely autonomous system with a complete Turing system capable of creating services using cycles, schedules, a new extended API, and other improvements. Smart contracts working at a high speed are not yet offered on other platforms.

This is why CREDITS is fundamentally different from other projects. On the platform it will be possible to create completely autonomous and independent services that operate without the need of participation from other external systems.

We at Entersoft, believe that Blockchain is suitable for BFSI services, Trade, Healthcare, Identification, Exchanges, Internet of things services and many others. Blockchain offers a refreshed economy and a new life to services already estimated in trillions of dollars. Credits leverages Blockchain with autonomous smart contracts.

Overall security

	ITEM	RESULT
1	HASHING ALGORITHM & ITS TRUST FACTORS	✓
2	AVAILABILITY (MAIN NODE)	✓
3	LEDGER TRANSACTIONS SECURITY	✓
4	SCALABILITY & EFFICIENCY	✓
5	DDOS RESILIENCE	✓
6	DATA FRAUD DETECTION	✓
OVERALL SECURITY POSTURE		**SECURE**

Technical analysis

Credits platform consists of the following components which are essential to build applications, mainly for financial users

1. Network Node
2. Ledger
3. Transaction
4. Smart Contract
5. Contracting party or end user.

Entersoft has clearly distinguished what's technical and what's mathematical based on the technical inputs mentioned in the whitepaper.

Categorically each component has its own set of rules and execution flow. After thorough review of the Credits technical white paper, following is our analysis.

Component Analogy

Any new user who adopts the platform through a client will be considered as a common node. This particular user might not necessarily be a trusted user; he/she/it can be any organization as well.

This Common node will be allowed to transact only if it is verified by other nodes in the network. A common node can only become a trusted node, after it is approved by the other network nodes through a mathematical hashing computation by verifying this node in the distributed ledger to check whether this user is malformed or not. **We found the hashing algorithm mentioned in the paper strong enough to use as a trust factor.**

A common node can also become a Main node through an algorithmic approach by calculating the computational performance of the node and compares the hashing efficiency with respect to the other nodes in a decentralized network. The node with highest performance and availability will be considered as a main node since it is the first one which allows itself to compute the 1 or n hashes in a given time interval. Before it becomes a main node, depending upon its potency to compute, it has to be verified and accepted as a trusted node. This leads to racing for Main node and it is a good approach to bring efficiency in the network. It is also easy to switch the main nodes in case of targeted attacks. **We found the main node's philosophy strong with respect to security and efficiency.** The race for main node and the underlying technology of the credits platform can be highly scalable and can manage high volumes. With enough common nodes, managing 1 M transactions a second as mentioned in the white paper seems possible.

Efficiency

Credits have considered that their platform is capable of computing 1 million hashes per second but we believe this is entirely dependent on the number of common nodes, trusted nodes & main nodes. As per the white paper, the Main node is responsible for populating the ledger with all the recent transactions of other nodes which are under constant communication with the main node. In a failsafe mode, we are not sure about 1 Million hashes per second when there is a targeted attack on a main node. **The difference between next 10 prospective main nodes can be a key to scale.**

Credits uses only 50% of trusted nodes for the hashing and its computation. This makes them scalable and protected. Only downside to this approach would be during a targeted attack. What if the network is filled with 45% unvalidated or targeted attack nodes? This poses a challenge of trust but Credits leverages trust factor through its common nodes.

The below mentioned are the Entry points that have been identified during the white paper security review. The attacks on these Entry points are written with an assumption of minimum security, precisely threats that might affect the system.

Blockchain: trusted for correctness but not privacy. We assume that the blockchain will always correctly store data and perform computation, and will always remain available. However, the blockchain exposes all of its internal states to the public, and retains no private data.

Arbitrarily malicious contractual parties. We assume that contractual parties are mutually distrustful, and they act solely to maximize their own benefits. In particular, not only can they deviate arbitrarily from the prescribed protocol, they can also abort from the protocol prematurely.

Network influence of the adversary. We assume that messages in between the blockchain and parties are guaranteed to be delivered within bounded delay. However, an adversary can arbitrarily reorder these messages. We assume that communication channels in between the parties can be unreliable – and an adversary can drop or reorder messages between contractual parties.

All the above threats have been evaluated by Credits through trust network. All the applications built on Credits should have good enough application level support for privacy of the users, expecially Fintech users.

P2P network. P2P has an complex structure as it allows the unreliable nodes to frequently access or quit the system. Moreover, the decentralized property makes the traditional "smart server" security mechanism, such as, VPN cannot work in P2P environment. Therefore, the security issues in P2P networks are important and challenging.

The malicious activities that may happen on a P2P network are like Routing attacks, DoS and DDoS attacks, Query flooding attack, TCP syn flooding attack, index poisoning attack, routing table poisoning attack, sybil attack, eclipse attack. Credits should consider evaluating few home grown protocols for nodes.

The below mentioned issues and attack surfaces are some plausible scenarios which we want to address in the review.

Nodes infected with Network(Internet) Worms. There are a lot of network or internet worms which can create some possible chaos in the current set up.

Let’s assume any of these nodes (Common, Trusted, Main) which are part of the network gets infected before or after, there is a high chance for this machine to become a part of a large botnet. The botnet can be leveraged to launch large scale attacks.

Example: Storm Worm is a difficult worm to track down as the botnet would be decentralized and the nodes that are part of the botnet will be consistently updated with the fast flux DNS technique. Consequently, it would be difficult for infected machines to be isolated and cleaned. Also, it is very difficult to identify the nodes.

Impact on the platform: This won’t affect the platform as such, but it is always good to be proactive.

If the main node gets infected there is a strong possibility that the worm can propagate across the networks and perform similar attacks on the other connected nodes.

Sybil attack: An attacker can attempt to fill the network with nodes controlled by him, Credits would then be very likely to connect only to attacker nodes(50% is the criteria).

This state can be exploited in (at least) the following ways:

- The attacker can refuse to relay blocks and transactions from everyone, disconnecting you from the network.
- The attacker can relay only blocks that he creates, putting you on a separate network. You're then open to double-spending attacks.
- If you rely on transactions with 0 confirmations, the attacker can just filter out certain transactions to execute a double-spending attack.

These attacks will become more difficult by only making an outbound connection to one IP address per /16 (x.y.0.0).

Incoming connections are unlimited and unregulated, but this is generally only a problem in the anonymity case, where you're probably already unable to accept incoming connections.

Looking for suspiciously low network hash-rates may help prevent the second one.

Smart contract security

Credits.com does not use Merkle trees but uses custom and secure functions written in Java. Java's security features can be leveraged by Credits.com but have to continuously assess and fix Zero day vulnerabilities in Java.

Transaction Security

The transaction implementation of CREDITS platform as per the technical white paper is found to be secure and is according to the industries best practices.

Conclusion

We have thoroughly evaluated the transactions flow, block assignment, and all the different parameters (node identifier hash, timestamp, write-off units, etc) that are added to the distributed Ledger. **This platform looks secure** as it uses custom encryption for adding transactions to the ledger.

Also, the concept of synchronized Last Ledger(LR) eliminates the bandwidth consumption of the all the network nodes and increases transaction processing performance.

The race to become the Main Network Node, Consensus building and transaction processing seemed like idea to create a sense of competition which can help the overall ecosystems to be scalable.

When an application is written on top of CREDITS platform, CREDITS should start an evaluation process for secure applications. They can consider the following

1. Make sure all the below requests are authorized using anti-forgery tokens
    a. Requests which contains the variables (parameters) for triggering a smart contract method.
    b. Requests which trigger ledger changes.
    c. Requests which results in trusted transaction processing.
2. Validate user inputs thoroughly enough to filter out malicious codes in application level which may trigger transaction processing actions.

    Applications and application functionalities written on the CREDITS platform differ in many different ways and in turn have different types of data to process. Hence, while processing data make sure to filter malicious file content and types at the application level. This however doesn't directly affect CREDITS platform but affects the client applications