Applicability of Red Belly Blockchains in the Air Force

Kelly Fam and Claudia Richoux
Information Assurance Interns, AFRL Information Directorate

6 July 2017

This report describes Red Belly blockchains and explores their potential in the Air Force.

1 Introduction

The growth of blockchain revealed multiple scaling problems in current implementations. Both Bitcoin and Ethereum lack the ability to resolve issues that may arise in the communications between the nodes during node consensus. Specifically, for Bitcoin, network delays and long mining times increase the number of blocks that are not agreed upon by the entire network, which leaves some transactions un-validated for up to hours. Ethereum attempts to address this with an algorithm called GHOST that uses "sibling" blocks that link back to a common ancestor and lower the probability that an attacker's block will be chosen next, but fails to address the uncertainty in message delays to alter previous transactions. [3] Blockchains, using the Red Belly consensus protocol, avoid these problems thanks to the asynchronous, reliable, point-to-point communication and multi-valued Byzantine consensus. Red Belly claims to have resolved the scalability, double-spending, and latency issues that come with more popular blockchain implementations.

Since this paper is so recent, there is no formal analysis of Red Belly. However, in our research, we discovered a forum post that was highly critical of this protocol, saying that they had essentially implemented a simplified version of another blockchain protocol, with a lot of assumptions and a lack of rigor. [2] The forum members commenting here seem to be experienced with blockchain technology, and their skepticism should be taken seriously with respect to this technology.

2 Red Belly Blockchain Overview

Red Belly addresses the balance attack, where attackers can transiently disrupt communications between subgroups of a blockchain network. [4] By communicating over an asynchronous, reliable, point-to-point network, Red Belly assures finite delays in message transfer, the inability for the network to alter and remove messages, and the ability to identify a sender of a message. Red Belly uses a multi-valued Byzantine consensus algorithm, also used by consortium blockchains, where the system is traditionally centralized through cryptographic means. [5]

This algorithm has no elected leader, safety during delays, and restrictions in consensus participation. An elected leader favors a certain hash, instead of allowing all nodes to play an equal part in mining it. Equality makes it so a node of a consortium cannot favor another node during consensus. The system is resilient against double spending or compromised information because it is unavailable during delays. Lastly, a consortium blockchain reduces

the chances of a Sybil attack, where a peer-to-peer identity may be forged to access the system because all members of the consortium are known. [4]

3 Applications in the Air Force

Blockchain technology can be very useful to the Air Force in order to build secure systems, made up of components that may or may not trust each other. Red Belly's fast and decentralized consensus protocol will allow so many transactions per second that it will become feasible to instantaneously log many processes that occur often and produce a lot of data.

For example, this blockchain is fast enough to record all the server logs in a small network every few seconds, to check for events like new USB devices or root logins, and ensure that no data is leaving the system through unintended means. This could help the Air Force to identify hackers or leakers trying to exfill data from sensitive systems.

Alternatively, Red Belly could enable autonomous distributed systems to communicate and reach a consensus about their actions, without adding a significant delay onto normal networked communications. This would be applicable if unmanned systems needed to coordinate their positions and actions without access to a trusted authority.

Essentially, Red Belly is capable of any application of any other blockchain, but new transactions become trusted at a much faster rate than with other Proof-of-Work blockchains like Bitcoin or Ethereum. This technology is quite new, and there does not seem to be much cryptanalysis of the protocol, with the exception of one highly critical forum post. If it turns out to actually deliver what it is promising, Red Belly will securely make blockchains useful for a wide range of real-time applications.

References

[1] McLean, A. (2017, July 03). University of Sydney builds new Red Belly Blockchain technology. Retrieved July 06, 2017.

[2] Pucksterpete, Tulo, Tommytrain, JoelKatz, Nikb, FMGC, Creddit_ecksarepee, Alluvial, and Cmbartley (04 July 2017). So I Emailed Vincent Gramoli (Red Belly). Alt-coins Forum. Xrp Chat. Retrieved July 6, 2017.

[3] Natoli, C., & Gramoli, V. (2016, December 30). The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example. Retrieved July 6, 2017.

[4] Crain, T., Gramoli, V., Larrea, M., & Raynal, M. (2017, May 5). (Leader/ Randomization/ Signature)-free Byzantine Consensus for Consortium Blockchains. Retrieved July 6, 2017.

[5] Thompson, C. (2016, October 26). The difference between a Private, Public & Consortium Blockchain. Retrieved July 06, 2017.