A Layer 2 Encrypted Blockchain Network

By A. Phil Smith – TLC Secure, Inc.

Abstract – blockchains are the foundation of cryptocurrencies and the transformation of a vast number of business transaction systems. Security and privacy are not, however, integral to their architecture. The public blockchain implementations for popular cryptocurrencies (e.g., Bitcoin and Ethereum) lead to the misconception that they are secure by virtue of transparency and scale. With market caps of $42B and volumes over a trillion dollars, network vulnerability is a growing concern. This paper describes risk in the current implementations and proposes a network of layer 2 peer-to-peer encrypted nodes, cloaking the blockchain from visibility outside its community members.

Blockchain Key Features

Blockchain technology represents a revolutionary change in the way organizations conduct business transactions. It is, fundamentally, a *distributed ledger* and database. The key features are:

Redundancy – each node in the network communicates with peer nodes that maintain redundant copies of transactions.

Consensus - nodes synchronize to ensure they have the same, current information.

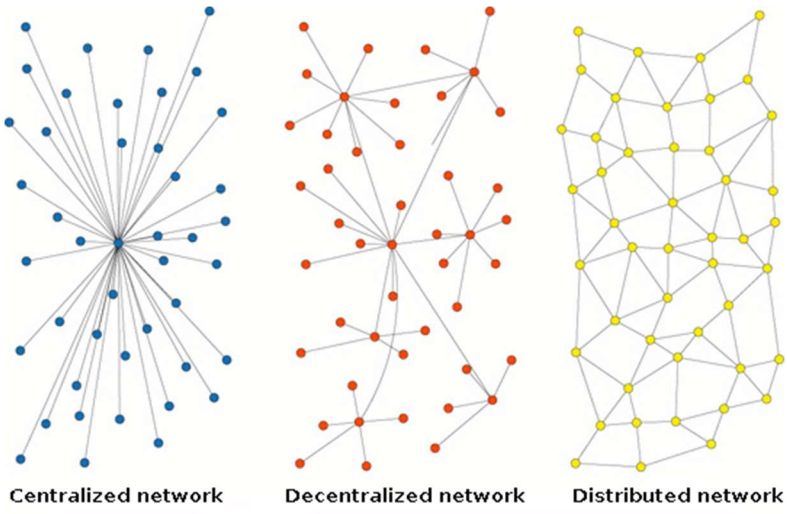
Immutability – the transactions cannot be modified. This is achieved by methods of verifying integrity of the chain with each transaction.

Disintermediation – because transaction integrity is synonymous with blockchain integrity, there is no need to have special trust relationships with 3rd parties.

Blockchain Topology

Blockchains are predominantly **distributed** networks. Data networks were historically either centralized, or decentralized (see figure 1). Blockchains have no central administration and is a network of peers.

Figure 1 – network topologies



Vulnerabilities

The problem is, despite the blockchain scale, nodes are individually subject to Denial of Service attacks that can take down strategically significant nodes and risk overwhelming other nodes as transactions are processed sub-optimally. Blockchain.info reports over 23,000 Bitcoin nodes since the network went operational, but a scan of current status reveals only a few hundred are active at any given time. An example of the vulnerability was March 2017 when the Bitcoin Unlimited network suffered a shutdown of 500 of its 800 nodes by exploits of its protocols. Bitcoin Classic experienced a similar cyberattack shortly after.

Port vulnerability remains a major weakness in TCP/IP networks. Any given host can have up to 65,535 TCP and UDP ports. There are 1024 commonly used for well-known services, such as FTP, SSH, HTTP, SMTP, DNS, etc. The vulnerabilities include penetration and protocol exploits. Open ports are actively used by port listeners. Ports that are closed, but not secured can be used by malicious software as backdoors. A list of many of the trojans using ports is given in ref 4. A current database of these is available from many penetration testing tools, such as Nessus by Tenable.

If TCP ports are like Swiss cheese for network nodes, it would seem the solution would be to have an alternative to TCP/IP networks or at the very least, to **plug the holes**. The Internet is founded on TCP/IP, and the vast body of network implementations and applications make it infeasible to use other protocols. Because of the diversity of hosts and network configurations, each blockchain node is managed by different individuals and organizations that have wide variance in the level of sophistication of administrators with respect to network security

Proposed Solution

The solution we propose is to have a blockchain with integrated peer-to-peer layer 2 encryption between nodes. The implementation will be a layer 2 over layer 3 VPN so from the inner perspective of the node, all ports are available. From the outer perspective of the node (the Internet side), all TCP ports are closed and filtered by iptables, except for the port used as a funnel for communication with a *named community of peers*.

The benefits of this architecture include:

- Reducing the outside attack surface
- Cloaking inter-node communication
- Normal intra-node communication
- Sealing all unused ports
- Eliminating threat of external packet-injection

The secure community can be limited to stakeholders and participants, while retaining the key benefits of the blockchain – redundancy, consensus and immutability between peers.

The TLC Secure Blockchain will produce Ethereum Secure Coin (ESC) cryptocurrency. A test network consists of a fork from Ethereum (ETH) open source adding integral peer-to-peer encryption while preserving the Dagger-Hashimoto algorithm to facilitate modified **ethminer** software for ASIC resistant Proof-of-Work mining in addition to Proof-of-Stake. Similarly, a security enhanced fork of the **open-ethereum-pool** will be a representative service for pool operators. Bootstrap nodes will follow the Kademlia protocol to publish active neighbor secure nodes in the community for new nodes.

ICO

An Initial Coin Offering (ICO) will be used to promote support and expansion of the Secure Blockchain network and Ethereum Secure Coin (**ESC**), with a planned supply of 10 billion tokens.
http://tlcsecure.com/tlc-ico

Coin Distribution

The ICO will involve 25 Million ESC tokens, plus an extra 5 million if fully reserved. If ICO is not fully reserved, 1,000,000 ESC are locked up as an incentive and released for development crew after 1,250 000 blocks (1 year) from genesis. If ICO is fully reserved, a minimum of 500,000 ESC will be purchased for the development crew from market by the ICO BTC funds after ICO closure. If all 25 Million tokens are reserved prior to ICO end date, an additional stack of up to 5 Million ESC can be released at the ESC Team's discretion at various outlets, for a price of approx. 0.0004 BTC each. A pre-ICO for select OpenLedger users sold 330,000 tokens about 1.3% of the ESC ICO supply.

Rate

The ICO itself involves ESC credits, not final ESC tokens these will be issued on PROOF (http://proofsuite.com). Ultimately, the 25 million ESC tokens will be distributed pro-rata to those who hold ESC credits.

The rate varies by currency and has several tiers, given by the table below.

Note that no PROOF holder can invest more than 15 million PROOF (333k ESC or 1.3% of the ICO supply at the average PROOF price).

Table 1 – ESC Credit Price Levels

- TBD --

About TLC Secure, Inc.

TLC Secure, Inc. is a network security products and consultancy startup in Northern California. It began with acquisition of WirelessWall, a multi-platform FIPS certified layer 2 encryption technology used by government and large enterprises to secure wireless campus' and communications with sensor networks.

References

Ref 1 – IBM Blockchain basics: Introduction to distributed ledgers, Brakeville, Perepa, et al
https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Ref 2 – Common (Bitcoin) Vulnerabilities and Exposures
https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

Ref 3 – Bitcoin Unlimited cyberattack
https://dcebrief.com/attackers-exploit-bitcoin-unlimited-vulnerability/

Ref 4 – SANS Which backdoors live on which ports?
https://www.sans.org/security-resources/idfaq/which-backdoors-live-on-which-ports/8/4

Ref 5 – N2N A Layer Two Peer-to-Peer VPN
http://luca.ntop.org/n2n.pdf

Ref 6 – Kademlia: A peer-to-peer Information System Based on the XOR Metric
https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf