TLC Secure Network

A Community of Blockchains

WHITE PAPER

Revision 1.7

2017 October

Table of Contents

Executive Summary

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.

The TLC Secure Network is a ***Community of Blockchains***, with member nodes securely connected within their community. This network is extensible and could potentially secure and enjoin the host nodes of *ANY* private blockchain (institutional or enterprise) or public blockchain (i.e., Bitcoin, Ethereum, Litecoin, Ripple, Dash, Zcash, Monero, etc.). Nodes are rendered *invisible* to hackers, thieves or snooping from the public Internet, thereby reducing risk from exploits, denial-of-service downtime of strategically critical blockchain nodes that can impact cryptocurrency market operations and disrupt transactions.

Our open-source leveraged technology represents an opportunity to invest in a unique security blanket that could literally cloak every blockchain node in existence, and what's to come.

The 3EMU Token

There is Ethereum (ETH) and Ethereum Classic (ETC). Now there is a third choice – 3EMU.

3EMU offers the same advantages of PoW, PoS and Solidity Smart Contracts but as part of the TLC Secure Network, adds encryption and cloaking to mitigate disruptions and hacks.

Our name 3EMU reflects our network – we build on Ethereum with TLC technology to produce the best and most secure blockchain system (3EMU is an anagram of Ethereum).

Commented [1]: ok

Commented [2]: Made a comment

Commented [3]: I changed this back to 3EMU from Three Emu because I think it will get confusing as to which name is which. 3EMU is fine. If you just read it, it comes out right, so I don't think we need to spell it out.

About TLC Secure, Inc.

TLC Secure, Inc. is a network security products and consultancy startup in Northern California. Among our products is WirelessWall, a proven, multi-platform FIPS certified layer 2 encryption technologies used by government and large enterprises to secure wireless campus and sensor networks. We also created SafeConnect, an award-winning fast, efficient layer 2 over layer 3 VPN with built-in firewall.

1. Overview

1.1. Mission Statement

“Our mission is to provide a secure, distributed and robust public/private network for blockchains”

1.1.1 Blockchain Key Features

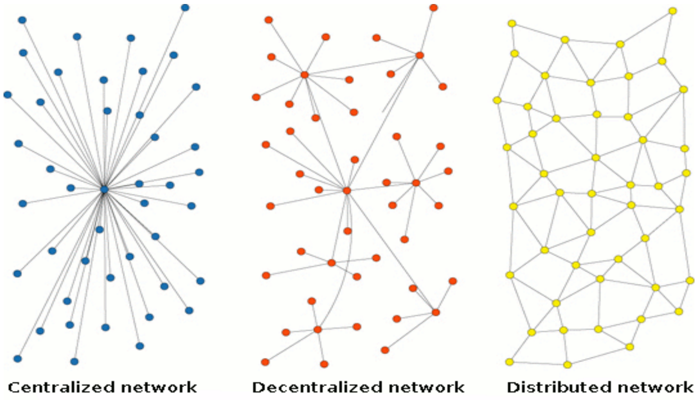
Blockchain technology represents a revolutionary change in the way organizations conduct business transactions. It is, fundamentally, a *distributed ledger* and database. The key features are:

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.



1.1.2 Blockchain Topology

Commented [4]: Do we need to use the name WirelessWall here? (maybe)
Also, should we talk here in the first page about the acquisition? I think there’s a good story there, but either tell it more fully, or just say “it was developed” and not use a product name.

Personally, I think here might be a good place to actually say more:

“Our special network technology was originally developed by a venture-backed company for government and military customers. When those VCs decided not to pursue the government sector, the code was sold to key engineers, and TLC was founded. Those developers also created an award-winning fast, efficient Layer 2-over-Layer 3 VPN with built-in firewall.”

We could use the product names here. Not sure if that’s good or not.

Commented [5]: I feel strongly that we need to keep mention of WirelessWall and SafeConnect in the About section. I agreed with you about dropping "acquired". No need to mention Cranite or VCs or anything more in this paper. All of that info is on the web site and the 1-page (conventional) investor document. I will be making all those documents visible.

Commented [6]: Department of Redundancy Department to say “our mission is” - it says “Mission Statement” right above.

Mission Statement:
“Provide the most secure communications possible between blockchain nodes and networks.”

(providing a secure and distributed VPN is how we accomplish our mission, it’s not the mission itself)

Another Mission Statement might be:
“Operate the world’s most unhackable network for blockchain communications”

Or:
“Keep blockchains safe from network attacks”

Commented [7]: Section heading is not part of the sentence. It’s grammatically incorrect to start the sentence with a verb. It’s important to say we secure both private blockchains and public/private blockchains. We cannot say its unhackable.

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

Figure 1 – network topologies

In distributed networks with peer-to-peer nodes, there is a need for peer-to-peer security. Because there can be many blockchains, there is also a need to have communities of blockchains to determine peer relationships.

1.2. Problem Statement

1.2.1 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.

Commented [8]: So what does this mean? Are we saying here that since there are relatively few nodes active at any one time that it is easier to disrupt them? (it's fine – I think we should spell it out)

Commented [9]: At the beginning of the paragraph it says attacks can "take down strategically significant nodes" and the next sentence states that Bitcoin Unlimited was shutdown this way. Seems like it's spelled out pretty clearly.

Commented [10]: Made a comment

Vulnerabilities in TCP/IP network services can be a major weakness in blockchain networks. Any given host can have up to 65,535 TCP and UDP ports. There are 1,024 commonly used ports for well-known services, such as FTP, SSH, HTTP, SMTP, DNS, etc. The services and applications communicating through open ports on hosts have vulnerabilities that attackers can exploit to cause damage to the hosts. For example, during the March 2017 Bitcoin Unlimited attacks discussed above, vulnerabilities in the bitcoin service running on TCP port 8333 were exploited to execute a denial of service (DoS) attack against the Bitcoin Unlimited nodes. Ports that are unused, but not secured, can also be used by malicious software as backdoors. Network vulnerability scanners, such as Nessus by Tenable, and online databases, including Common Vulnerabilities and Exposures (CVE) contain thousands of publicly known vulnerabilities, exploits, backdoors, and trojans in network services and applications. A list of many of the trojans using ports is given in ref 4.

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

Commented [11]: Layer 2 is what we use, and our solution uses private addressing, not a TCP/IP protocol solution.

Commented [12]: Made a comment

1.2.2 Market forces

More of our lives are transferred onto the Internet daily. This creates more opportunity for our data to be stolen, hacked, filtered or misused. Privacy has become almost impossible.

There is also increased data vulnerability. One of the main forces driving the market for privacy and security solutions is the vast market to collect or steal and sell personal information. Other forces include:

1) Remote workforceS need safe connection to corporate servers

Every year more work is done by freelancers. Having a safe connection to corporate servers becomes more urgent. Small businesses also require secure communications, but creating their own VPN can be a financial and technical challenge. This is a more conventional use for VPNs.

2) Growth of cyber threats

Every year the number of cyberattacks increases followed by a greater awareness of the need for countermeasures. Companies and individuals tend to change their online behavior in response to cyberattacks, resulting in rapid expansion of VPN market.

3) Explosive Growth of Blockchains and Cryptocurrencies

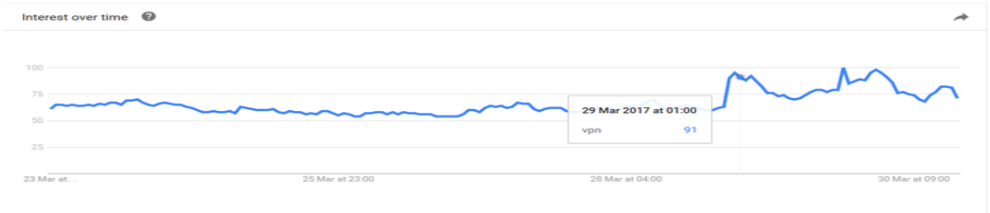
More blockchains for enterprises and institutions add cost and risk to provide security. Cryptocurrencies represent a unique risk due to the possibility of disruption of operations having a direct impact on transaction settlements and if the disruption or outage is large enough, can negatively affect the price of the currencies being traded.

4) Western countries become accustomed to VPN services

At present, the primary countries using VPN are in Asia. As governments around the world develop more sophisticated monitoring, the number of people looking for Internet privacy solutions worldwide is rapidly increasing. Both China and Russia recently announced they are banning VPNs, demonstrating that they are in fact monitoring network activity. In other words, no privacy in those countries.

5) Government legislation

Another tendency is for governments to exploit our connected world to intrude into our private lives, our finances and activities. The more we are on the Internet this intrusion will only increase.



Google trends graph for VPN days after USA Congress Overturned Internet Privacy Regulation.

Keeping the current world situation and visible trends in mind, increasingly people are growing concerned about their privacy. According to one study, the use of ad blockers has risen by more than **40%** (198 million monthly active users in total). After recent Federal Communications Commission (FCC) change of regulations, the search for privacy solution in USA has skyrocketed.

According to Market Research Future project report: “the global VPN market is expected to reach at USD **106 billion** by end of year **2022** with compound annual growth rate of **13%**.”

VPN can be used to provide a security layer to both private and public networks such as WiFi Hotspots and the Internet. Organizations operating in healthcare and telecommunication industry deal with sensitive information that needs to be protected constantly. Hackers are mostly targeting these industries due to very high price of data in black market. The same study shows that “*currently, the world is experiencing more than half million attacks every minute, which will rise due to high technology proliferation*”.

Keeping these trends in mind (increasing demand after privacy policy changes in multiple countries, increasing cybercrime, IoT and growing dependence on online services) the need to restore privacy on the Internet is becoming essential to counter the serious threat posed to both personal liberty and business security. Restoring privacy has become a salient global trend worldwide. Once launched, the TLC Secure Network will help users restore privacy, providing peace of mind while conducting personal and business life.

1.3. TLC Solution

1.3.1 Product

The solution we propose is to have a blockchain with integrated peer-to-peer Layer 2 encryption between nodes. Our product, SafeConnect L2P2P is a layer 2 over layer 3 VPN so from the inner perspective of the node, all ports are available.

Commented [13]: I think for consistency we should capitalize the word Layer. I know it’s written both ways, but in this paper, I think it lends credibility to use caps. In many places in this document Layer is already capitalized.

Commented [14]: OK

Commented [15]: Made a comment

1.3.2 Solution

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.*

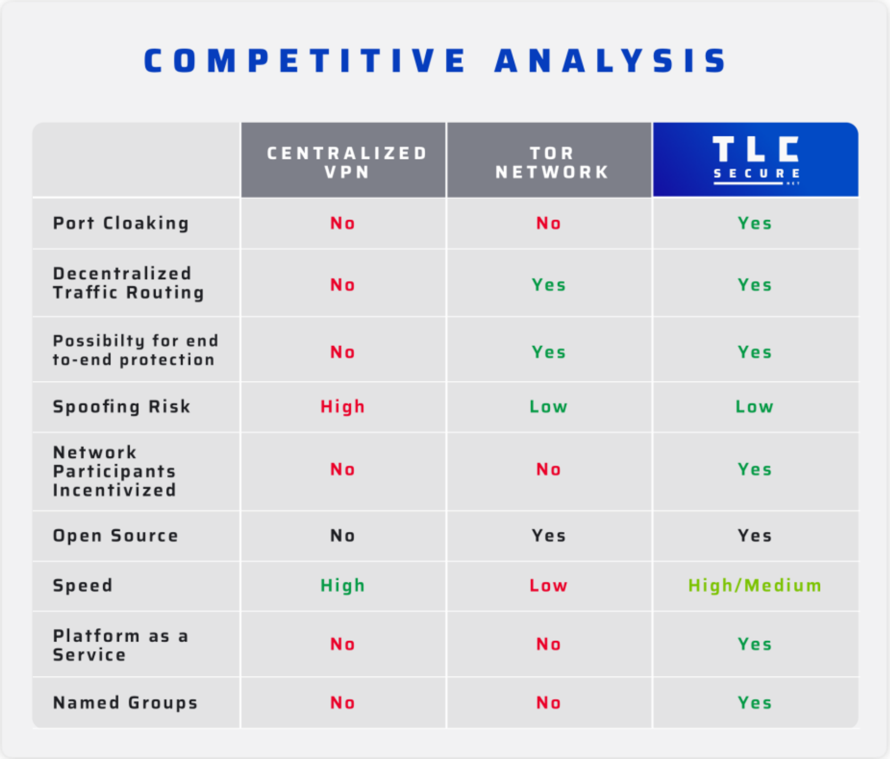
The benefits of this architecture include:

- Reducing the outside attack surface
- Cloaking inter-node communication
- Normal intra-node communication
- Sealing all unused ports
- Eliminating threat of external packet-injection
- Improves the uptime and performance of blockchain nodes

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

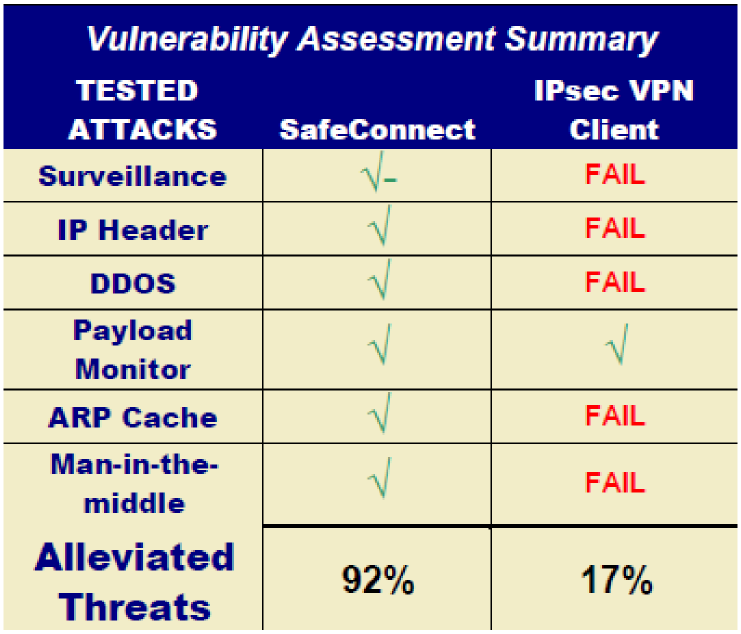
1.3.3. Competitive Analysis

The following tables compare typical VPN provider, TOR and the TLC Network.



COMPETITIVE ANALYSIS

	CENTRALIZED VPN	TOR NETWORK	TLC SECURE
Port Cloaking	No	No	Yes
Decentralized Traffic Routing	No	Yes	Yes
Possibilty for end to-end protection	No	Yes	Yes
Spoofing Risk	High	Low	Low
Network Participants Incentivized	No	No	Yes
Open Source	No	Yes	Yes
Speed	High	Low	High/Medium
Platform as a Service	No	No	Yes
Named Groups	No	No	Yes



Vulnerability Assessment Summary		
TESTED ATTACKS	SafeConnect	IPsec VPN Client
Surveillance	√-	FAIL
IP Header	√	FAIL
DDOS	√	FAIL
Payload Monitor	√	√
ARP Cache	√	FAIL
Man-in-the-middle	√	FAIL
Alleviated Threats	92%	17%

1.4. Approach

1.4.1 Phase I: Building a network of Layer 2 Peer-to-Peer VPN Nodes

Our first goal is to develop a decentralized node network, by using TLC Layer 2 Peer-to-Peer VPN technologies (L2P2P), Ethereum blockchain, smart contracts, state-channels, decentralized database solutions, privacy ensuring compatibility with coins based on existing Ethereum blockchain network.

This will be achieved throughout the development of Phase I, which is made up of 3 different stages (see section 3. Roadmap). At the end of the 3rd Stage of Phase I, a completely distributed and open source VPN network with all of its functions also decentralized will be released. No single point of failure will be possible from this time forward.

1.4.2 Phase II: TLC Secure Network Expansion

In this phase, TLC will promote and market TLC Secure Network to the overall blockchain community. Both public and fully private nodes (institutional and enterprise) will be solicited as well as engagement and incentives offered to independent node operators.

1.4.3 Phase III: L2P2P Protocol - as standard

In Phase III - our vision is to provide a keyed set of APIs for developers to plug into the L2P2P network. The TLC protocol will eventually become a combination of different elements united into a coherent system.

Once complete, this Protocol will ensure that node functionality and reporting be extended by third parties.

1.5 Tokens

The TLC Secure Blockchain will produce Three EMU Coin (**3EMU**) cryptocurrency. A test network consists of a fork from Ethereum (ETH) open source adding integral peer-to-peer encryption.

1.5.1 Token Use Model

The ecosystem for token use is:

- End Users Purchase Cloaking Services with 3EMU Coins for both access and support.
- Miners Earn 3EMU from PoW
- Node Operators will be given 3EMU incentives to add nodes/recruit other operators of other blockchains.

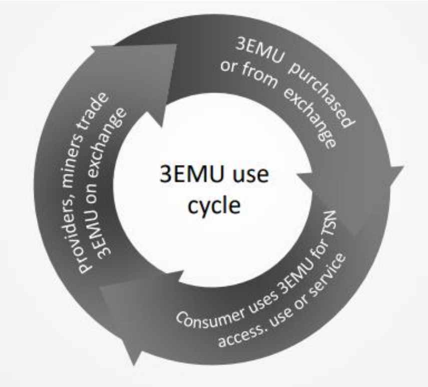
Commented [16]: For Access and Support

Commented [17]: Made a comment

Participants of the TLC Token Sale will gain access to tokens which will form the foundation for all transactions happening within the network.

Node owners who run their nodes will be incentivized for their support of the network. In such a way node owner will essentially act as a miner, with reward coming in 3EMU token form. This differs from the typical blockchains which typically don't reward node operators and miners are only rewarded either for their computing power (Proof of Work), or ownership of the currency (Proof of Stake). 3EMU tokens will also be awarded based on the monthly hours of operation.

NOTE: The incentives promote the expansion of the TLC Secure Network. TLC will consider the possibility of giving 3EMU node operators an added benefit of sharing in network services fee for each transaction in the TLC Secure Network with payments being conducted in currencies other than 3EMU. In this sense, node owners would be part of a "pool". The per-transaction fee would be miniscule


3EMU purchased or from exchange
3EMU use cycle
Consumer uses 3EMU for TSN access, use or service
Providers, miners trade 3EMU on exchange

Token Usage Model

1.5.2 Token Differentiation

The network we are building will have opportunities for various levels of development by entrepreneurs and communities after it has been deployed. The Network will also be open to applications to make censorship less effective, ways to make payments easier and more efficient and new networking related services to be made available by reusing infrastructure and protocols developed by TLC. See 1.3.3 Competitive Analysis for comparison to similar services.

VPN-like services on the TLC network will be available early into Phase I. VPN service provided by the Network in this stage will be comparable with and improve upon existing Virtual Private Networking services. TLC market model will result in creating a VPN service which is both competitive and almost infinitely scalable, giving other entities (e.g. other VPN providers or app developers) an option to buy VPN service from TLC, integrating it into their solutions. This competitiveness comes from the open nature of the network and the ease with which anyone can earn money by joining it as a VPN service provider. Further improvements and new applications will follow in later stages.

2. Token Mechanism

2.1 ICO Terms

The Initial Coin Offering (ICO) will be used to promote support and expansion of the Secure Blockchain network and generation of the Three Emu coins (**3EMU**).

ICO open date **Q4FY17**, and will close in 30 days.

Commented [18]: Subject to change to a pre-ICO sale

At ICO opening, TLC credit tokens will go on sale. Buyers who purchase credit tokens will be awarded 3EMU coins at genesis.

2.1.1 Rate

The ICO itself involves **TLC credits** (ECR20 standard tokens), not final 3EMU coins. These will be issued (tentatively) on **PROOF** (http://proofsuite.com). Ultimately, the 10 million 3EMU tokens will be distributed pro-rata to those who hold credits.

Commented [19]: Alternative launch sites under evaluation

The rate varies by currency and has several tiers, given in section 2.4.4.

Note that no PROOF holder can purchase more than 15 million PROOF (333,000 credits or 1.3% of the ICO supply at the average PROOF price).

2.1.2 Coin Distribution

The ICO will involve **25 Million TLC credit token**s, plus an extra 5 million if fully reserved. If ICO is not fully reserved, 1,000,000 TLC 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 tokens will be purchased for the development crew from market by the ICO BTC funds after ICO closure. If all 10 Million tokens are reserved prior to ICO end date, an additional stack of up to 5 Million tokens can be released at the TLC Team's discretion at various outlets, for a price of approx. 0.0004 BTC each. A pre-ICO for select users will sell 330,000 tokens about 1.3% of the ICO supply.

The post-ICO token issued during the Token Creation is known as the Three Emu Coins, or **3EMU**. This is the only time that these tokens can be created, and therefore the supply is fixed. The supply of 3EMU coins at genesis will be **10 billion total coins**.

3EMU will be an integral part of the TLC Network where VPN consumers will be charged fees for services. The biggest slice of those fees will go to the VPN node owner (service provider) the leftover will be dedicated to protocol development and support. These fees will initially be denominated in 3EMU, which is a subject to change in the future.

2.2. Token Creation Details

TLC Token Creation will commence on Q4FY17 .

Commented [20]: This date is un-achievable. We need more time to market the whole ICO.

Commented [21]: Must be this year

Commented [22]: Made a comment

1. The ICO launch will raise funding in Bitcoin (BTC) or Ethereum (ETH) from buyers. They purchase our credit tokens on the proofsuite.com website. The ICO will offer 10 million TLC credit tokens @ $1 (currently, .004 Bitcoins) each. Purchaser funds remain in an ICO escrow wallet.
2. If our funding target is met (roughly $10M = 4000 Bitcoin), we would close escrow for the ICO and transfer the earnings to a company wallet. From there, we distribute a portion of the BTC funds to our team (TLC stockholders, contributors and legal). The balance of the money would remain in the company escrow wallet for operations, The company would periodically draw from that wallet as needed for operations (converting the draw to US dollars via exchanges such as **Coinbase**, **Bittrex**, or **Poloniex**).
3. The 3EMU Blockchain is made live (**genesis**) within **30 days** of close of ICO. We issue one 3EMU for each TLC token purchased. These transactions will be on the permanent blockchain ledger. The 10 million 3EMU coins will then be in circulation.
4. Now that we have Bitcoin backed funding, we can list our 3EMU currency on the exchanges with a (Soft) market cap defined as $10M x coins in circulation. The number of coins available will be much larger (10,000,000,000 possible).

2.3 3EMU Creation Ratios

- Before Soft Cap is reached, 1 USD = 1.2 3EMU (ETH price per 3EMU will be determined 3 hours before Token Creation Event).
- After Soft Cap is reached (72 hours period), 1 USD = 1 3EMU.

2.4 Additional 3EMU

Additional 3EMU will be created, designating them for working capital for operations, a bounty program; compensation for employees, Advisory Board and Board of Directors; and finally, for seed investors.

2.4.1. Future Funding

Part of 3EMU supply will be reserved for future as an additional fundraising mechanism for the TLC Secure Network project to continue development of Phase II, but may never be issued, depending on circumstances in the future.

The amount reserved for future funding will be as following:

- If up to 2 million USD is collected, 50% of all tokens will be reserved for future funding.
- The percentage will decrease gradually to 15% with further funding until 6 million USD is reached.
- After 6 million USD, the number of tokens reserved for future funding will be fixed at 15%.

Tokens reserved for future funding will be locked for 12 months, after which they will be sent to a multisig wallet belonging to TLC Secure.

2.4.2. Founders, Foundation, Bounty program and Advisors

- TLC Secure, Bounty program and Advisors will receive 9% of all tokens. Tokens will be received by the TLC multisig wallet, and will be used to reward assistance from: early node operators (mining), bounty program participants, advisors and new employees via a Vesting program, etc.
- Founders will receive 10% of all tokens. Founder tokens will be locked for 12 months.

2.4.3. Seed Participants

Seed Participants will be rewarded with the following token multipliers for their early commitments with ETH/USD ratio calculated at the commencement of the Token Creation:

- 1x if 2 million USD (or less) is collected.
- 1x to 5x gradually increasing seed multiplier if more than 2 million USD and less than 6 million USD is collected.
- Multiplier will stay at 5x if 6 million USD (or more) is collected.

Seed Participant tokens will be separated in two parts: the 1x multiplier part will be released to Seed Participants right after the Token Creation ends. The second part will be locked for 12 months.

2.4.4. Example of Token Structure after Creation is over

As contribution is pegged to ETH value in USD, in this example we assume that 1 ETH value at the moment Token Creation will be dictated by current FMV.

Donation, in USD	**$2M**	**$3M**	**$4M**	**$5M**	**$6M**	**+$9m**
Tier 1: Token Creation Contributors (instant)	27.60%	34.10%	40.80%	47.70%	54.60%	57.50%
Tier 2: Foundation, Bounty, Advisors (instant)	9.00%	9.00%	9.00%	9.00%	9.00%	9.00%
Tier 3: Seed Participants (locked)	3.40%	5.70%	7.70%	9.50%	11.40%	8.50%
Tier 4: Phase 2 (locked)	50.00%	41.20%	32.50%	23.80%	15.00%	15.00%
Tier 5: Founders (locked)	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

3. Roadmap

3.1. Funding Breakdown

Funds raised during the Token Creation will be used solely for the refinement and expansion of the TLC Secure Network. The following distribution of funds is preliminary and can is subject to change.

3.1.1. Core Development – 40%

Core development will involve the development of the technology as described in this document. This includes: TLC node network, integration of VPN protocols, smart contract systems, supporting protocols and services, end user applications, etc.

Commented [23]: I have a concern here about making it sound like most of the TLC code is not ready. If we are to leverage the Cranite code, then we need to be careful here. If it sounds like too much is not done, then we may turn off potential investors.
It doesn't mean we embellish anything, but if we want to sell the story that this network was already built and with significant expense, then we don't want to imply that we have to start all over again.

Commented [24]: Nothing to do with Cranite code, which is our code, by agreement. Significant changes are still needed to the open-source per my email reply.

Commented [25]: Made a comment

***

3.1.2. Operational – 25%

This covers the necessary costs incurred for a functional system. This includes: hosting and infrastructure costs, staffing, outsourcing, management and other related expenses.

3.1.3. Marketing and Sales – 25%

Marketing costs will be used for partnerships development and direct consumer marketing. Sales costs will largely be incurred by direct B2B sales to businesses selling TLC as a platform solution.

3.1.4. Legal and Compliance – 10%

There are legal costs associated with privacy protection and fighting censorship. The legal costs might vary from region to region.

3.2. Development Roadmap

The whole development is spread out into distinct phases starting with Phase I and Phase II. Each phase is further divided into several internal stages.

3.2.1. Phase I

Goal of this Phase is to adapt our existing decentralized VPN technology for secure blockchain communications. .

Phase I components:

- Discovery mechanism - node and customer matchmaking smart contracts;
- Smart contract managing TLC Identity;
- Payment mechanism - a combination of state channels and smart contracts clearing payments;
- VPN Node protocol and libraries - the "*workhorse*" of the network, providing the actual VPN service to customers;
- Node applications - native node applications built for major operating systems, capable of running TLC protocol and providing VPN service to customers;
- Client applications - allowing end users to connect to the network as VPN customers;
- Interface into the Network for third party applications.

Achieving this will take 3 stages to complete.

Stage 1

Goal of this stage is to launch a Decentralized node network, leaving certain elements centralized for speed, security and learning purposes.

Development goals for Stage 1:

- Smart contract for clearing payments;
- TLC Client V1.0 - developed for 3 major operating systems, including Linux;
- TLC Wallet on 3 main operating systems / smartphones;

- TLC central server overseeing node Discovery, Identity management and Micro payment accounting processes;
- Node network deployment and initial testing.

Stage 2

Goal of this stage is to integrate additional VPN protocols into the node and work further towards decentralization

- TLC Node V2.0 & Client V2.0 - adding new protocols, developed for major operating systems, integrating with new smart contracts;
- Smart contracts for Discovery and Identity Management;
- Simplified Central server - down to oversight of Micro Payment accounting processes;
- Marketing.

Stage 3

Goal of this stage is complete decentralization, with removal of central server role as oversight and management position, moving to decentralized infrastructure.

- Removal of Central server;
- Smart contract performing Micro Payment accounting;
- TLC Node and Client V3.0 - State channel integration, removal of all ties to central server connection;
- Interface into the network for third party applications
- B2B Sales and Marketing;

Once initial technology is in place and a Decentralized node network is functional - TLC will open up for various third-party services to be built on top of this network.

According to our calculations, $6M is enough to develop a fully decentralized and open network, fully operational and without a single point of failure.

Commented [26]: Don't put comments like this in. It then starts the reader to ask "you mean you guys as a team could pose a risk??"
I realize you meant it to sound like a good level of stability, but I think it has the opposite effect.

Commented [27]: Agreed

Commented [28]: Made a comment

3.2.2. Phase II

Goal of Phase II is to develop TLC protocol as standard VPN API with user messaging APIs through the Network of TLC Nodes - providing complete end to end encryption, peer-to-peer. Additional plans for *XMSS Quantum Resistant Digital Signatures* in wallets is anticipated.

If we are able to raise at least $9M USD during this token creation, we will have enough funds to finish and refine the complete Phase I items. Once that is done, we will research, design, plan, start developing and implementing Phase II protocols.

3.2.3 Phase III

There are multiple streams of revenue planned for Phase III:

Software as a Service – TLC will charge a licensing fee for certain developer APIs and infrastructure.

Professional Services TLC will build custom projects for enterprise clients. Partnering possibilities include IBM, Deloitte, and Gem. Other services may include White Hat wallet security testing and cybersecurity audits.

Flat Fees & Transaction Fees – TLC can charge a subscription fee or a transaction fee on activity in the network, particularly if we host (see SLA).

Service Level Agreements - Some businesses build platforms and host infrastructure for enterprise customers. We may offer a SLA for uptime and maintenance.

Cryptocurrency market growth - The management holds a significant amount of the 3EMU cryptocurrency. As Market Cap increases, TLC may periodically sell from its supply of tokens to raise revenue.

4. TLC Secure Architecture

Although the code for TLC Secure is substantially developed, the architecture for the secure blockchain network will undergo changes and refinements as more nodes and blockchain communities are added. Therefore, we expect the architecture described in this section to change over time.

Commented [29]: Not true. It is not fully developed. It's proof-of-concept functionality. Essential features must be implemented. The smart phone apps are in development.

Commented [30]: Made a comment

Commented [31]: Made a comment

4.1. Operational Overview

VPN service consumer find and pay service providers in TLC Secure Network by using built-in smart contract based Identity, Service Discovery and Payment services. The network itself is cloaked, and nodes use the Ethereum blockchain for censorship resilient distributed storage and transactional processing needs. The TLC Secure Network will use Registered Identities to enable means of creating limited trust when engaging with services and account payments.

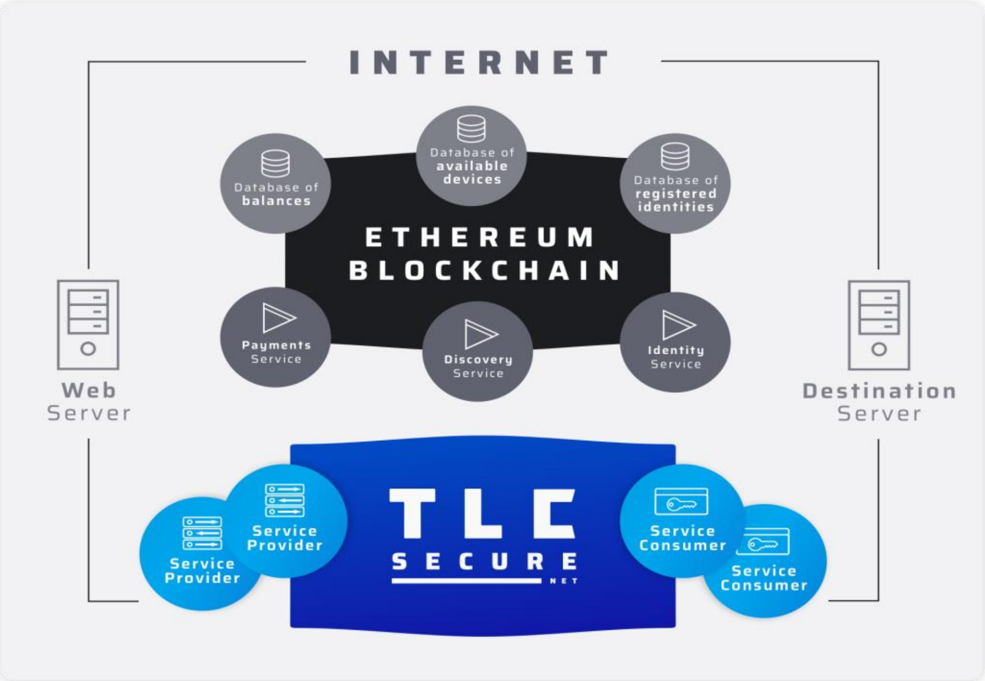


Illustration: Cloaked TLC Secure Network (contains many other blockchains)

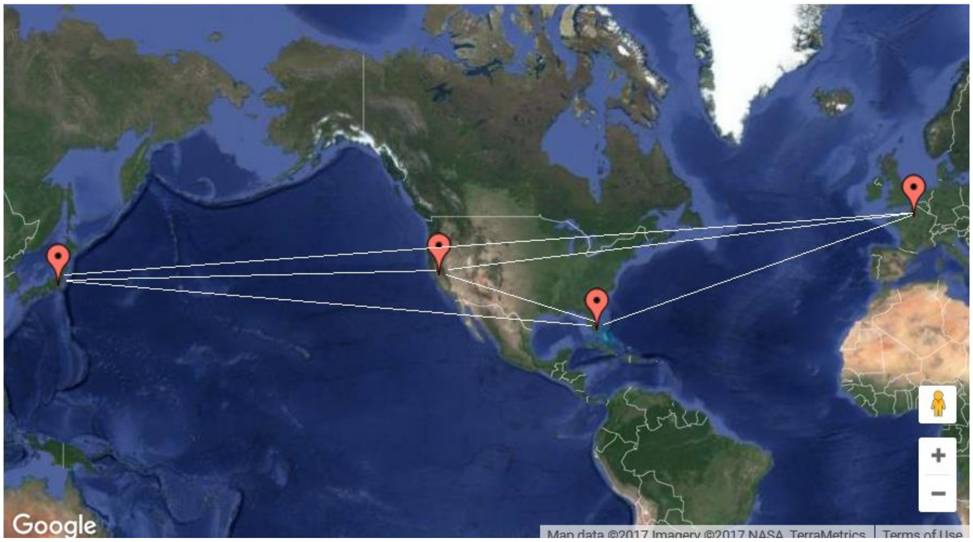
All parties who have their identity registered on The TLC Secure Network can announce VPN services (compatible with the network's VPN service protocols) along with the payment terms for these services. Other users of the network will be able to find services matching their specific needs (location, price, etc...) and use search results to establish a connection to selected VPN service providers and use the announced services. A consumer of VPN service and VPN service providers will exchange several messages to negotiate the payment terms (e.g. service metering granularity) and technical information necessary to establish the secured VPN session. During this negotiation, a consumer of the service will make a promise to pay for some amount for services to be received in advance and this promise will be updated by the consumer every time an extension of service is desired. The VPN service provider later will use this promise to clear payment via smart contracts on the Ethereum blockchain. If the consumer's balance held in the network's deposit account is sufficient then the promised amount of 3EMU tokens will be transferred from the consumer's deposit account to the service provider's account.

4.1.1. Core components

1. **Ethereum** allows the TLC Secure Network to run decentralized code with smart contracts, enabling reliable services and payment handling.
2. **Identity service and database of registered identities** will be added to ensure the proper identity acknowledgement between client and service provider.
3. **Discovery service and database of available services** will be created to announce VPN services availability.
4. **Payment service and database of balances** will be developed to secure promise-based micropayments for services.

4.2. Test Network

The current TLC Secure Network already in operation is a pilot program with “supernodes” in the **US** (California, Miami), **Japan** (Tokyo) and **France** (Paris). All communicate peer-to-peer with Layer 2 encryption (see screenshot below from Google Maps). These nodes are cloaked and inaccessible via public Internet.



Screenshot: Test Network Topology

The centers have the capacity to bootstrap thousands of edge nodes. Thereafter, the edge nodes communicate with each other autonomously.

4.2.1 Cryptographic Mechanisms

Because of computation costs and limitations of running long computations on Ethereum Virtual Machine, the cryptographic mechanisms backing the registered identities technically will use EVM's built-in implementations of keccak256 hashing, ECDSA signature verification and identifier recovery functions. A key pair and an identifier used behind the identity are technically identical to the cryptologic security artifacts behind Ethereum's external account. A TLC key pair should not be reused to hold value in Ethereum blockchain.

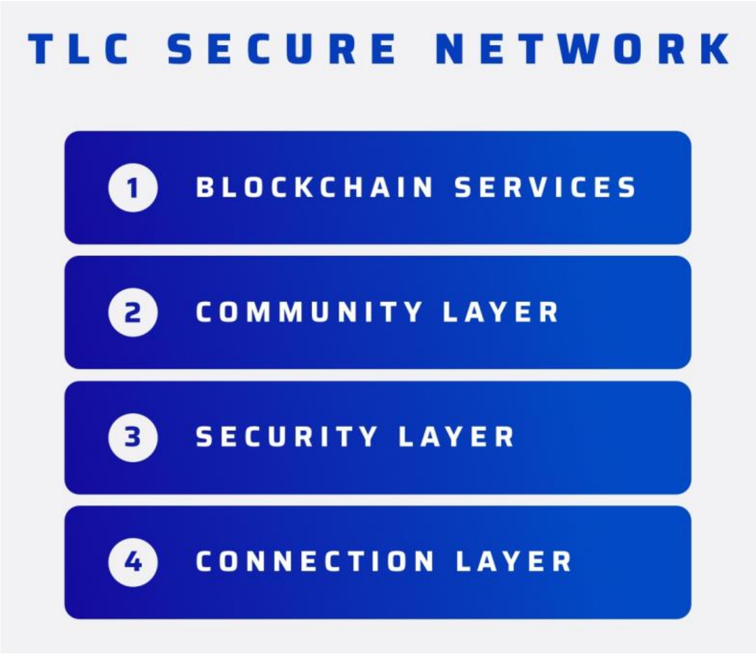
4.2.2 Types of Services

There will be one type of VPN service available on the TLC Secure Network, Layer 2 Peer-to-Peer (L2P2P). IP tunneling and Socks proxy style services have known vulnerabilities and will not be implemented. Other kinds of networking-related services such as VPN DHCP may follow. Node capabilities may be advertised as a separate service. Nodes durably store all proposals they announce and still regard as valid.

Nodes may support multiple types of VPN services. Every service type has to be valid. The valid proposal is a proposal of service the provider is willing to deliver on terms defined in the qualitative description.

4.3. Platform Layers

The TLC Secure Network will be composed of four primary layers (from bottom up): The Connection Layer, Security Layer, Community Layer and Blockchain Services.



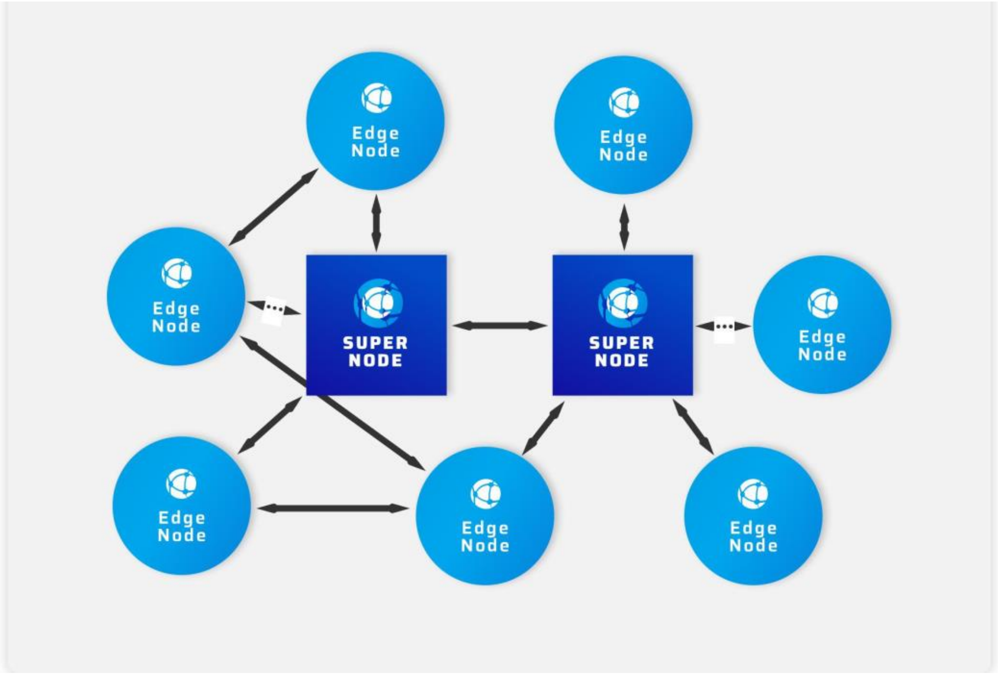
***

4.3.1 Connection Layer

This is based on Richard Andrews'[1] N2N VPN[2]. There are *supernodes*, and *edge nodes*, as depicted below:

[1] Advisor to TLC.

[2] (http://luca.ntop.org/n2n.pdf



The edge nodes send a request to the supernodes, which registers, their MAC address and sends an IP lease confirmation to set an IP on the edge. The process is similar to DHCP. Thereafter the edges have layer 2 peer-to-peer communications directly with other edge nodes

4.3.2 Security Layer

The Security Layer provides:

- Compression

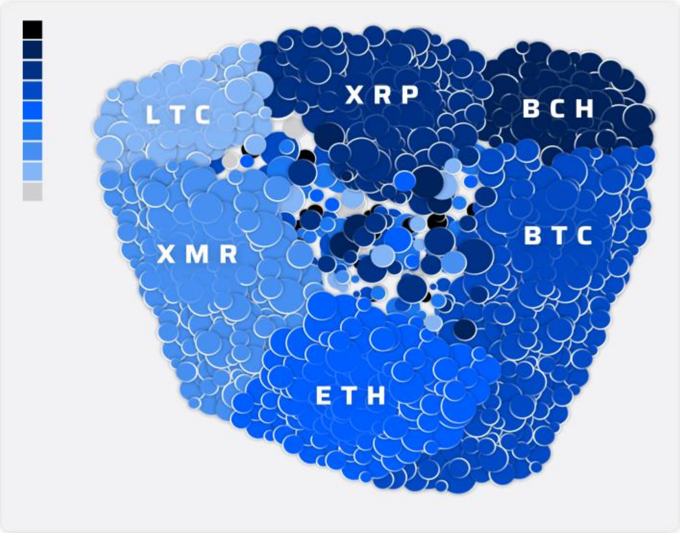
- Encryption w. Bruce Schneier's[3] Two-Fish 128-bit encryption, which is:
  - Fast, unbroken
  - Non-proprietary, royalty-free

Planned:

- Replace shared key model
- Propagate firewall rules from supernode to edge nodes
- Based on Tom Eastep's[4] Shorewall (https://en.wikipedia.org/wiki/Shorewall)
- Use 256-bit keys (faster than Rijndael)

4.3.3 Commmunity Layer

The Community Layer provide Namespaces for Blockchain identification or grouping. It avoids address collisions and provides additional node classification. For public-private nodes, community names can be made of acronyms derived from the cryptocurrency trading name, e.g. BTC, BCC, ETH, ETC, LTC, DASH, etc.



[3] Advisor to TLC.

[4] Advisor to TLC.

There are over 16 million potential cloaked edge nodes per supernode. If IPv6 addressing is used, there are 18,446,744,073,709,551,616 potential addresses. The VPN communities can cloak every blockchain node in existence.

Planned:

- Community / Blockchain Specific APIs
- IPv6 VPN node addressing.

4.3.4 Blockchain Services

This layer consists of blockchain applications and APIs, including:

- **Private Blockchain Cloaking**
- **Public-Private Gateways**, to allow nodes in larger blockchains like Bitcoin to be cloaked and joined to the TLC Secure Network
- **Cloud Sync** / **Backup** with third-party services, for blockchain storage and recovery, including:
  - Amazon Cloud Drive
  - Google Drive
- **Mining** Services / Pools
- **Wallet** Services (web, smartphone)

The 3EMU blockchain implementation preserves 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. Thereafter, each node will use a peer discovery sequence (such as **RLPx**) to find its neighbors.

5. Contact

To reach us visit our website at 3emu.info or http://tlcsecure.com

6. 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://www2.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

Reg 7 – RLPx: Cryptographic Network & Transport Protocol
https://github.com/ethereum/devp2p/blob/master/rlpx.md