Compute; the Last Blockchain: Software as a Service Cryptocurrency

Sever Neacsu compute@provgn.com
www.putez.org

Abstract: *Compute aims to solve geological problems and benefit from the demand for cloud resources by offering a universal platform for dAPPS by utilizing Citrix (Hypervisor) and Docker (Virtualization). A centralized BaaS (Bitcoin-as-a-Service) that isolates processor resources paired with a decentralized storage platform will save on environmental pollution. The Compute blockchain will be used for further development of DDoS and 51% based blockchain attack mitigations to the Bitcoin protocols by further expanding on endpoint detection through AI NAT traversal detected packet loss and De-Centralized DDoS Scrubbing Master nodes.*

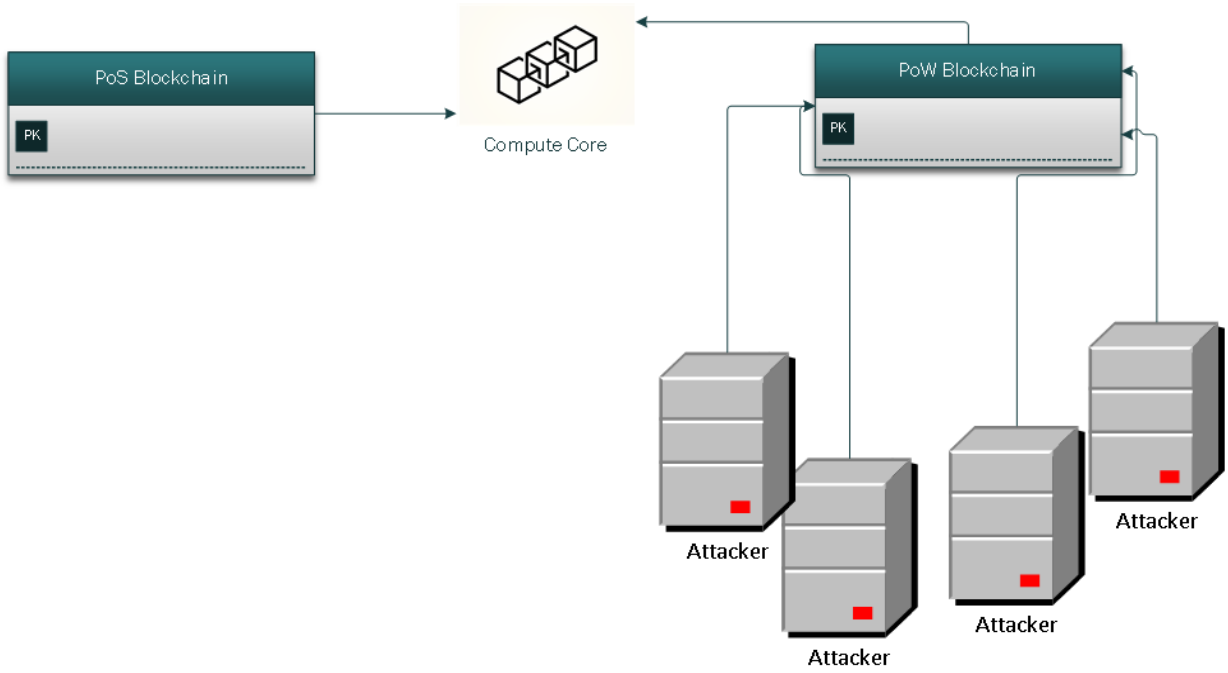
Executive Summary

There have been numerous and variable attacks on PoW based blockchains such as the $18 Million Bitcoin Gold heist in 2018[1] There are several reasons to run a PoW based blockchain such as secured block generation from a trusted source and not insta-mined. However the amount of power required just to mine[2], not even including the power draw that a 51% attack puts on the powergrid[3] and on the responses to them is enough light up small Cities. And with the demand for Cloud Services increasing exponentially [4], the future demand for dAPPS will naturally increase along with it. The solution to this was to create an Aux based chain which still was not enough to stop attackers from circumventing it. We propose an auto switching Aux chain that can detect sudden increases in hash rates and respond accordingly based on previous attack data on other crypto-currencies. Compute aims to stream real C++ and C# directly to your Compute Core. Compute will use the latest blockchain technologies to provide a simple solution to blockchain-based network attacks and software engineering.

Problems with PoW Blockchains

In a Typical Auxiliary based chain, the attacker targets the PoW chain as seen in Illustration 1.

Illustration 1.



A subsidiary of Provigen Networks, Compute Core was released to provide a geologically friendly solution to Cryptocurrency network attacks while paving the way for future blockchain development and blockchain DDoS mitigation developments. Compute Core will a layer of Super Nodes, above the Master Nodes layer. Super Nodes will be incorporated as mini-OSes with pfSense routers attached. They will form a bridge to all continents and will effectively switch their gateways amongst themselves to create packet loss so substantial that it will mitigate the 51% attack. Since Super Nodes are purchasable for 10,000 PuteZ, they are hard to attain and even harder to setup. Compared to Master Nodes, Super Nodes require a substantial expertise in VPN routing to configure properly and constitutes a high PuteZ requirement for support. Super

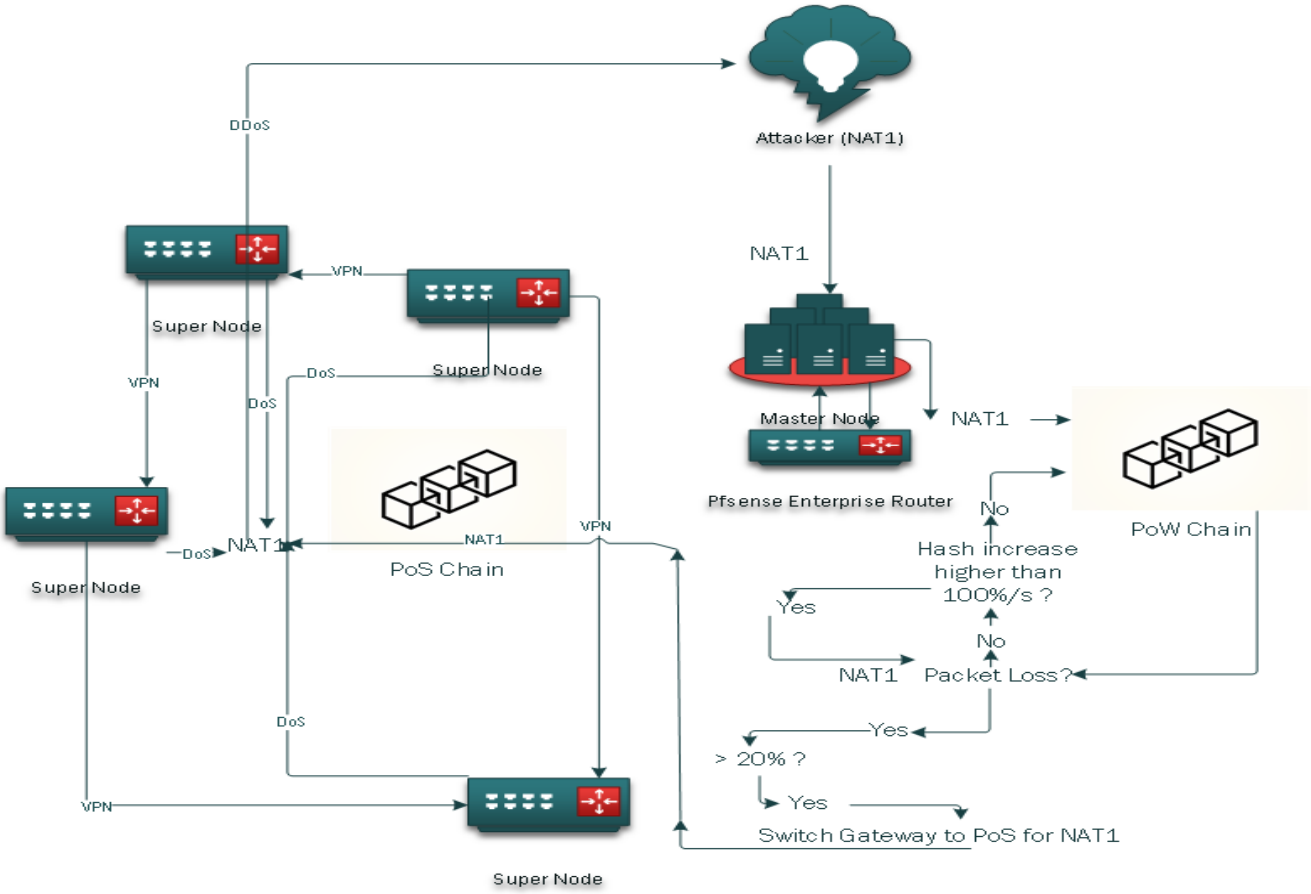
Nodes will monitor and traffic shape packet channel width as well as flow to deter any sudden spikes in activity that would otherwise be considered a 51% attack (Higher growth than 100% within a short period of time) to seek out the geographical source and type of 51% attacks. The Super Nodes will base their educated guess on the source of the 51% attack. Their decision will be based on Poisson distribution and complex Quantitative Methods, subnet ban and flood their routers with millions of packets since attackers simultaneously 51% multiple coins. Therefore the DDoS will slow down their attacks on other coins. Since many times an ISP can be unaware or negligible that their clients are performing a 51%, DNS, or NTP attacks, the DDoS attack could spread to them and alert them to take action.

Super Nodes and Xen Hypervisor

Within each Compute Core will be a portal to all of your software you use most, heavily encrypted and remotely hosted to save on resources locally. Hosted by decentralized Super Node servers, they will be powered by virtual resources that are provided by the users in that geographical area. Super Nodes will host Virtualized Software by making use of numerous decentralized blockchains. To provide storage, IPFS will be used. For processing power, either GPU or resources can be drawn upon for less PUTEz than during heavy demand such as when there are minimal transactions or during 51% attacks. By offering a centralized solution to decentralized 51% attacks, new blockchains can focus on developing instead of attack mitigation.

Drawing on years of experience with the Xen Hypervisor, our team is able to offer custom Bitcoin XenApps that will be a super layer to the Computechain. The Super Nodes will be at a

higher level of permission than Master Nodes and are purchasable at a premium for 10,000 PuteZ's compared to 1000 PuteZ's for Master Nodes. The Increased costs are justifiable since they need to be trusted and therefore owners must be fully invested. Super Nodes run on the XCP-NG Xen Hypervisor and along with a pfSense Enterprise Router, include XenApps that will host Bitcoin Clients. The owners need not manage them as they will be deployed using Swarm technologies and with Kerberos, managed solely by Super Node team. They will be strategically connected to each other with Virtual Private Networks. Using AI technologies, they will be able to determine the source of the 51% attack due to an extra layer in Computechain that will interpret the NAT of packets and DDoS accordingly. Regions split arbitrarily providing load balancing and switching gateways. Once a gateway has been switched for an area, all packets are directed to the PoS chain. Super Nodes that handle the PoS chain will simultaneously DDoS the target and cause packet loss effectively neutralizing the threat.



Wallet Security

There have been numerous breaches to different wallet stores. For instance Ethereum's chain was attacked targeting their wallet system which led them to switch to a storefront app that would manage their private keys and public keys. Numerous file-reading viruses and Trojans spread targeting wallet.dat files, as well as carelessness has lead wallets being corrupted, or even worse taken over. A simple backup of the wallet.dat could fix all problems people are experiencing. With the blockchain technology being so fragile in its current state, and the amount of encryption to a wallet.dat being so multilayered, it is almost impossible to figure out how to repair the wallet without reading memory and making sense of large amounts of encrypted characters. It is almost impossible to restore a wallet back to use if it has become corrupted. Corruption can occur in many ways such as the user moving it when the Compute Core has not

been fully shut down. Compute plans to utilize the IPFS filesystem to ensure redundancy to the Computechain and encapsulate Bitcoin and other Altcoins within a single Compute Core Client. Merging clients offers many benefits. Namely: ease of automating backup system that will switch off memory use to the wallet.dat temporarily while a backup is taken.

Software as a Service

Numerous blockchains have attempted Apps on the blockchain however, had numerous syncing issues where the developers of the blockchain were clueless. Hypervisors have numerous forms and their benefits are vast. Software based virtualization solutions can be applied directly to a bare-metal install or on-top of an already virtualized Hypervisors container (Suse, Xen, Hyper-V, or KVM), making Docker and LXC's functions extremely accessible. Their ease of use has dramatically dropped since very little Linux knowledge is needed to setup since Xen supports not only Unix, and Linux OSes, but also Windows in Para virtualized driver Mode. This allows the Xen hypervisor to ration CPU and I/O directly. Virtualization application can be seen everywhere from Datacenters to households in a wide range of usage such as Development and Research. A lot of the times resources are wide ranging from SANs to single thread CPU applications. By using Citrix XenApp, Storefront, Windows Server iSCSI Initiators and Samba servers, Compute believes it can bridge the gap between Idle resources and On-Demand-Power from anywhere in the world for any project.

Bibliography

1. https://www.investopedia.com/terms/1/51-attack.asp
2. https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one/

3. https://www.huffingtonpost.ca/salman-sakir/can-cryptocurrencies-become-viable-currencies_a_23558850/
4. https://www.provgn.com/knowledgebase/9/About-Us.html