A BLOCKCHAIN-BASED MARKETPLACE FOR COMPUTER AND INTERNET NETWORK HARDWARE, SOFTWARE AND SERVICES

A DECENTRALIZED CYBER-DEFENSE PLATFORM FOR BITCOIN, ETHEREUM AND OTHER PUBLIC CRYPTOCURRENCY NETWORK NODES
“If you can keep a node running that accepts incoming connections, you’ll really be helping the network a lot.”

Satoshi Nakamoto
Inventor of Bitcoin
Friday 9th January 2009
ABSTRACT

The Internet is the global communication platform that enables all humans to connect, share and transact freely across the world.

In the simplest of terms, the Internet is the ‘thing’ that connects us to everything and everybody, everywhere.

The Internet comprises of software-driven networked switches, routers, firewalls, servers and storage hardware that switch, route, protect and store all our voice, video, text and blockchain data from our smartphones, tablets and computers intelligently across the world.

The Internet is also the infrastructure that connects all blockchain nodes, and upon which all blockchain traffic traverses. Accordingly, its availability, reliability and security to all cryptocurrencies and decentralised applications cannot be over-emphasised.

Therefore, it can be concluded that:

1. Without the Internet, there is no Blockchain;
2. Without Internet-connected computers called "Nodes", that relay, validate and irrevocably record transactions on memory blocks that are chained together cryptographically, there will be no cryptocurrencies like Bitcoin;
3. As the de-facto reserve currency for the broader cryptocurrency economy, without Bitcoin, all other cryptocurrencies will lose credibility and drop in value.

As evidenced, by the growing hostility from some powerful governments and financial corporations towards the increasing popularity of decentralized and 'un-regulatable' public cryptocurrencies such as Bitcoins, it is increasingly likely that one of such adversarial actors, will sooner or later launch a systematic cyberattack to silently choke "offshore" Bitcoin nodes, and thereby force the centralization of the remaining active nodes ("centralization attack") within the jurisdiction of a single entity (or union of nations) that is malicious to cryptocurrencies, who may then essentially "seize control of", and/or attempt to regulate or worse yet, fatally undermine the Bitcoin network.

Below are the options available to adversaries that consider the threat posed by Bitcoins (and other public cryptocurrencies, hereinafter collectively referred to as "Bitcoins") to be existential:

1. Discredit Bitcoins by alleging that they are tools for illicit trade, and hope this would roll-back their popularity and adoption. Too late, already tried and did not work.
2. Shut down the Internet. Impossible…. at least not the entire Internet. However, since only three Internet Service Providers ("ISP") intercept 60% of Bitcoin traffic¹, it is possible to temporarily ‘Blackhole’ Bitcoin traffic via Border Gateway Protocol ("BGP") Hijacking and dent its reliability.
3. Launch a systematic ‘centralization attack’ on Bitcoin nodes that will place all or majority of the active nodes under the control of a single actor – THIS IS POSSIBLE.

As the world’s first and only, apolitical and independent provider of decentralized software integrity maintenance and cyber-defense services for all Internet networks, irrespective of the underlying hardware and software, Multiven is firmly aligned with the freedom, transparency and socio-economic empowerment that Bitcoin and other public cryptocurrencies, represent to mankind and is hereby taking steps to secure their future by fostering further decentralization of full Nodes into space, while hardening all Earth-based Nodes from cyberattacks.

This white paper explores:

I. How Multiven intends to disrupt the entire $3 Trillion per annum worldwide Information Technology market, starting with the $600 Billion per year computer networking equipment market by creating the Multiven Open Marketplace (MOM), the world’s first blockchain-based, peer-to-peer marketplace for new, pre-owned and re-cycled computer and Internet network hardware, software and services. The secondary goal of this marketplace is to make Bitcoin node hardware more affordable for less affluent people in emerging markets which will lead to further decentralization;

II. How Multiven intends to use some of the MOM transaction fees to cyber-defend and help secure the future of Bitcoin and other public cryptocurrencies by ensuring that “centralization attacks”, malicious BGP Hijacking² and other forms of network and non-network-based cyberattacks will less likely succeed;

III. How Multiven intends to Map-the-Internet via the MOM and transparently back-it-up onto the blockchain so that it can be restored should any portion/s of it be taken offline due to malicious attacks;

IV. How Multiven intends to create the world’s first immutable Proof-of-Ownership record for all IT products;

V. How Multiven intends to further the decentralization of Bitcoin nodes into space, by designing, manufacturing and launching multiple open source autonomous full nodes, into Earth’s low-orbit, pre-configured with Delay-Tolerant Networking architecture and Inter-planetary Internet³ protocols;

VI. Why Multiven is the only company in the world today, capable of achieving all the aforementioned.

MULTIVEN’S GOALS; VISUALIZED

Transaction fees from the marketplace will help compensate the engineer community actively cyber-defending public blockchain nodes

Public Blockchain Nodes on earth and in space will keep recording full Dapps transactions

Engineer Community will monitor and protect public Blockchain nodes

³https://en.wikipedia.org/wiki/Interplanetary_Internet
“Hardware vendors (and their Governments) have significant control over Bitcoin. A competent backdoor could be extremely difficult to detect and [could] act as a kill switch for hashing power, allowing the network to be killed outright or putting Bitcoin under the control of a single actor.”

Peter Todd
a Bitcoin core developer
1. INTRODUCTION

Founded in 2005 by Peter Alfred-Adekeye (Cisco Systems’ former Technical Leader for IOS, the software that runs 75% of the Internet infrastructure), Multiven is today, the world’s first and only, apolitical provider of decentralized software integrity maintenance and cyber-defense services for all the Internet Protocol-enabled devices (routers, servers, switches, firewalls etc.) that make up the global Internet network infrastructure.

The Company’s services are powered by a combination of its global community of an elite team of 1200 Internet network experts, security researchers, cryptographers and distinguished engineers in 55 countries, called “Pingsta” (www.pingsta.com - a Multiven subsidiary) and its proprietary Artificial-Intelligence engine called mySolvr.

Realising that the most efficient and scalable way to heal the Internet was through Artificial Intelligence, Multiven invented its AI, mySolvr in 2007 and then invited an elite team of 1200 from the world’s leading Internet experts, security researchers and cryptographers to join its Pingsta community that mySolvr learned from. Multiven’s goal is to, some day in the near future, have mySolvr self-heal 99% of all Internet software, technology and security issues without human involvement.

Multiven aims to:

A. Harness and deploy decentralized human-powered artificial intelligence towards defending Bitcoin, Ethereum and other public cryptocurrency network nodes from centralization cyberattacks. This will be a free service for all Bitcoin, Ethereum and other public cryptocurrency nodes;

B. Maintain the integrity of the software that runs all other non-Blockchain Internet networks globally. This will be a for-fee service, payable in Multiven Coins (“MultiCoins”);

C. Document and map every device (type, geo-location, owner etc.) on the Internet (hardware and software) and make them globally available on the blockchain.

D. Launch the Multiven Open Marketplace (“MOM”), the world’s first blockchain-based marketplace that will simplify and lower the cost of buying, selling, and sharing of computer and network hardware, software and services between businesses and consumers using Multiven Coins, on a peer-to-peer basis, without intermediaries.

E. Design, launch and maintain active Bitcoin full Nodes-in-Orbit (“NiO”) to serve as a spatial extension of the global node network that will be out of reach of earthly adversaries.

Multiven is disrupting the $600 Billion-a-year centralized computer networking equipment industry by creating the world’s first Blockchain-based marketplace, with the Multiven Coin (“MultiCoin”) as its sole crypto-currency, powered by smart contracts for new, pre-owned and recycled IT and network hardware, software, and services.

The reduced cost of purchasing computer and networking equipment via the marketplace, will hopefully help to make node and mining equipment more affordable and therefore incentivize more people to operate full nodes, leading to further decentralization of nodes across all geographies.

On the Cyber-defense side, Multiven aims to:

- Maintain the integrity of Bitcoin and Ethereum network nodes by limiting the attack surface of their directly connected Internet Gateways ("IG" or "NADs") via live monitoring and proactive security patches, updates and bug fixes. This will be a free service for all Bitcoin, Ethereum and other public cryptocurrencies nodes and their IGs.

- Limit the attack surface of all Internet networking equipment. This is a for-fee service, that is payable in “MultiCoin”. The solutions, knowledge, and best practices gleaned from this service will be “pushed” to Bitcoin nodes and their IGs, so they may benefit from them proactively.

*Node-Attached-Devices: Switch, router, server etc.*
In order to simplify and eliminate costly intermediaries in the centralised, monopolised and silo-ed telecommunications equipment global marketplace ecosystem, Multiven is creating the world’s first Blockchain-based open marketplace, powered by smart contracts, that enables the world to buy and sell new, pre-owned and re-cycled computing and Internet network hardware, software and services, directly on a peer-to-peer basis.

The /bitnodes.21.co map shown below confirms that there are only a handful of active Bitcoin nodes in Africa, Latin America and South East Asia. This is no doubt due to the high cost of acquiring and operating computers in emerging economies. Our hope is that the vastly reduced cost of purchasing node hardware, amongst other types of computing equipment, via the Multiven marketplace will lead to greater decentralisation.

II. INTERNET & BLOCKCHAIN

The Internet is a global system of interconnected computer networks that use the Internet protocol suite (called TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.

The Internet carries a vast range of information resources and services, such as the interlinked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

The Internet is the infrastructure upon which all Blockchain traffic traverses. Accordingly, its availability, reliability and security to all cryptocurrencies and decentralized applications cannot be over-emphasized.

THE OSI MODEL – ISO/IEC 7498-1

Governing computer communications interoperability
According to Gartner, there are 8.4 Billion devices connected to the Internet today, of which, less than 12,000 nodes make up the Bitcoin network and about 23,000 nodes make up the Ethereum Network.

A Blockchain is a continuously growing list of records stored in computer memory blocks, that are chained and secured together, using cryptography.

Each block contains a cryptographic hash pointer as a link to a previous block, a timestamp and transaction data.

For use as a distributed ledger, a Blockchain is typically managed by a peer-to-peer network of computers called Nodes, that relay, validate and record transactions onto memory blocks. Specifically, mining nodes validate transactions, add them to the block they are building, and then broadcast the completed block to all other nodes. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchain was invented by Satoshi Nakamoto in 2008 as the public transaction ledger for Bitcoin.

Alarming fact: 70% of the routers and switches that make up the world’s Internet network infrastructure today are made by Cisco Systems, an American company headquartered in San Jose, California. Cisco’s routers and switches are run by Cisco IOS software.

Accordingly, 7 out of every 10 Bitcoin nodes globally connect to the Internet and other nodes, via a Cisco device. With the current concentration of Bitcoin nodes in North America and the EU, it is estimated by Multiven that in fact, about 90% of all nodes today, connect to the Internet via Cisco equipment.

There are volumes of critical security defects and backdoors in all networking equipment software, some of which allow remote cyber-attackers to gain full access to these devices, and their attached networks, without authentication and take full control of them and all the data that pass through them.

The recent public release of multiple exploits, implants and tools developed by the US National Security Agency (NSA) and leaked by a group called Shadowbrokers have made all Internet networks and their attached Blockchain node computers and servers, vulnerable to advanced nation-state type attacks.

The probability of a cyberattack corrupting the data structures of Bitcoins’ Blockchain-ed memory blocks diminishes with every passing day because of the growing size of the Blockchain, all of which are secured cryptographically, with each block containing a hash pointer linking it to the previous block.

However, with the growing angst towards the rapid rise of Bitcoin and other cryptocurrencies, it is highly likely that, sooner or later, an adversarial actor (or union of nation states) that is hostile to cryptocurrencies will launch a cyberattack that exploits a new, or one of the several now publicly available vulnerabilities, to systematically

---

2. https://github.com/misterch0c/shadowbroker
4. https://blog.comae.io/shadow-brokers-nsa-exploits-of-the-week-3f7e17bd216
centralize Bitcoin nodes within their country/countries/area of jurisdiction, so they could seize control of it and regulate or discredit it, or worse yet, shut it down.

In order to maintain the decentralized nature of Bitcoin, Ethereum and other public Blockchain cryptocurrency networks, it is imperative to proactively monitor and defend all participating nodes and their connected Internet gateways from cyberattacks that could either knock them and/or their directly connected next-hop Internet gateway Customer Premise Equipment ("CPE") e.g. a switch or router, offline or overwhelm them with high interrupt level activity that leads to resource starvation and incapacitates them from processing Blockchain traffic or respond to inter-node messages in a timely manner.

In the interest of security, we will not be detailing further, all the possible network-based centralisation attack options that hostile adversaries could deploy against Bitcoin nodes in this whitepaper.

III. DECENTRALISING PUBLIC BLOCKCHAIN NODES INTO SPACE

As the threat from Earthly adversaries continue to grow, Multiven is taking the unprecedented step of expanding the Bitcoin node network into space by using some of the proceeds of this token sale, to fund the research, development, design, launch, monitoring and maintenance of low-Earth orbiting space-based nodes.

The initial concept will have the orbiting full nodes running atop solar-powered open-source white-boxes configured with Delay/Disruption Tolerant Networking - Key Protocol Components - RFC 4838 for space-based communication and low-latency TCP/IP for shorter distance communication.

To achieve its mission for NiOs, Multiven will collaborate with, amongst others, the InterPlanetary Networking Special Interest Group (IPNSIG), which is tasked with developing new InterPlanetary Networking communications protocols to handle signal delay and connectivity disruption; aerospace engineering to create space-borne networking platforms, and cognitive sciences research to create platforms smart enough to protect themselves against natural and human threats.
“Internet routing has become far too centralized. Not just a reliability problem; it is a security vulnerability”

Nick Szabo
inventor of Smart Contracts and BitGold
https://twitter.com/NickSzabo4/status/928025799646519296
Nov 7, 2017
3.1 TECHNOLOGY APPROACH

3.1.1 CONTACT BETWEEN NODES

Delay/Disruption Tolerant Networking (“DTN”) is an end-to-end architecture and an evolution of the architecture originally designed for the Interplanetary Internet, a communication system envisioned to provide Internet-like services across interplanetary distances in support of deep space exploration.

A DTN node is an engine for sending and receiving bundles – an implementation of the bundle layer. Applications utilize DTN nodes to send or receive ADUs carried in bundles (applications also use DTN nodes when acting as report-to destinations for diagnostic information carried in bundles). Nodes may be members of groups called “DTN endpoints”. A DTN endpoint is therefore a set of DTN nodes. A bundle is considered to have been successfully delivered to a DTN endpoint when some minimum subset of the nodes in the endpoint has received the bundle without error. This subset is called the “minimum reception group” (MRG) of the endpoint. The MRG of an endpoint may refer to one node (unicast), one of a group of nodes (anycast), or all of a group of nodes (multicast and broadcast). A single node may be in the MRG of multiple endpoints.

Contacts between nodes fall into the following categories:

1. **Persistent Contacts** i.e. always available i.e., no connection-initiation action is required to instantiate a persistent contact;
2. **On-demand Contacts** i.e. require some action to instantiate but then function as persistent until terminated;
3. **Intermittent or Scheduled Contacts** i.e. an agreement to establish a contact at a particular time, for a specified duration e.g. a link with a low-earth orbiting satellite.
4. **Intermittent – Opportunistic Contacts** i.e. unscheduled contacts that present themselves unexpectedly e.g. an unscheduled aircraft flying overhead and beaconing its availability for communication.
5. **Intermittent – Predicted Contacts** i.e. based on no fixed schedule but rather are precisions of likely contact times and durations based on historical data.

The DTN architecture provides a framework for routing and forwarding at the bundle layer for unicast, anycast, and multicast messages.

Because nodes in a DTN network might be interconnected using more than one type of underlying network technology, a DTN network is best described abstractly using a *multigraph* (a graph where vertices may be interconnected with more than one edge). Edges in this graph are, in general, time-varying with respect to their delay and capacity and directional because of the possibility of one-way connectivity. When an edge has zero capacity, it is considered to not be connected.

Because edges in a DTN graph may have significant delay, it is important to distinguish where time is measured when expressing an edge’s capacity or delay. We adopt the convention of expressing capacity and delay as functions of time where time is measured at the point where data is inserted into a network edge.

For example, consider an edge having capacity $C(t)$ and delay $D(t)$ at time $t$. If $B$ bits are placed in this edge at time $t$, they completely arrive by time $t + D(t) + (1/C(t))*B$. We assume $C(t)$ and $D(t)$ do not change significantly during the interval $[t, t+D(t)+(1/C(t))*B]$.

DTN fragmentation and reassembly are designed to improve the efficiency of bundle transfers by ensuring that contact volumes are fully utilized and by avoiding retransmission of partially-forwarded bundles. There are two forms of DTN fragmentation/reassembly:

A DTN node may divide a block of application data into multiple smaller blocks and
transmit each such block as an independent bundle. In this case, the final destination(s) are responsible for extracting the smaller blocks from incoming bundles and reassembling them into the original larger bundle and, ultimately ADU. This approach is called proactive fragmentation because it is used primarily when contact volumes are known (or predicted) in advance.

DTN nodes sharing an edge in the DTN graph may fragment a bundle cooperatively when a bundle is only partially transferred. In this case, the receiving bundle layer modifies the incoming bundle to indicate it is a fragment, and forwards it normally. The previous-hop sender may learn (via convergence-layer protocols,) that only a portion of the bundle was delivered to the next hop, and send the remaining portion(s) when subsequent contacts become available (possibly to different next-hops if routing changes). This is called reactive fragmentation because the fragmentation process occurs after an attempted transmission has taken place.

As an example, consider a ground station G, and two store-and-forward satellites S1 and S2, in opposite low-earth orbit. While G is transmitting a large bundle to S1, a reliable transport layer protocol below the bundle layer indicates the transmission has terminated, but that half the transfer has completed successfully. In this case, G can form a smaller bundle fragment consisting of the second half of the original bundle and forward it to S2 when available. In addition, S1 (now out of range of G) can form a new bundle consisting of the first half of the original bundle and forward it to whatever next hop(s) it deems appropriate.

The possibility of severe resource scarcity in some delay-tolerant networks dictates that some form of authentication and access control to the network itself is required in many circumstances.

Many existing authentication and access control protocols designed for operation in low-delay, connected environments may not perform well in DTNs. In particular, updating access control lists and revoking (“blacklisting”) credentials may be especially difficult.

Also, approaches that require frequent access to centralized servers to complete an authentication or authorization transaction are not attractive.

To help satisfy these security requirements in light of the challenges, the DTN architecture adopts a standard but optionally deployed security architecture that utilizes hop-by-hop and end-to-end authentication and integrity mechanisms. The purpose of using both approaches is to be able to handle access control for data forwarding and storage separately from application-layer data integrity.

While the end-to-end mechanism provides authentication for a principal such as a user (of which there may be many), the hop-by-hop mechanism is intended to authenticate DTN nodes as legitimate transceivers of bundles to each other.

In accordance with the goals listed above, DTN nodes discard traffic as early as possible if authentication or access control checks fail. This approach meets the goals of removing unwanted traffic from being forwarded over specific high-value links, but also has the associated benefit of making denial-of-service attacks considerably harder to mount more generally, as compared with conventional Internet routers.

**Multiven's goal is to launch the first set of nine NiOs into Earth's orbit by 2022.**

Nodes in Orbit will permanently eliminate the risk of Bitcoin centralization beyond the reach of Earthly adversaries, leading to geo-spatial decentralization and thus, further ensuring the longevity of Bitcoin and all other public Blockchain-based cryptocurrencies and the decentralized applications they support.
AN EXAMPLE OF A LIVE BITCOIN NODE IN GERMANY THAT IS TARGETABLE

Source: https://bitnodes.21.co

BITCOIN NODES AS OF FEB 5, 2018 - 11,717 NODES

On Nov 23, 2017 there were only 5,129 Nodes online as a result of US Thanksgiving Holidays

Source: https://bitnodes.21.co
“Attack target: Bitcoin Core powers the Bitcoin peer-to-peer network, so people who want to disrupt the network may attack Bitcoin Core users in ways that will affect other things you do with your computer, such as an attack that limits your available download bandwidth.”

https://bitcoin.org/en/full-node#what-is-a-full-node
IV. MULTIVEN GROUP

Founded in 2005, Multiven is the world's only independent and apolitical provider of
decentralized software integrity maintenance and cyber-defense services for all Internet
Protocol enabled devices.

Multiven is 100% employee-owned with no institutional investors, zero bank debt, millions
in revenue and a 9-figure active service sales pipeline.

In that respect, Multiven is not only hardware, software and politically neutral, but is also,
financially - independent and thus free from influence from fiat banking institutions and
venture capital firms.

Over the past 12 years, Multiven's team have committed their time, intellectual capital
and financial resources and have endured tremendous persecution\(^1\) in order to break
the Internet's centralization from the grips of the most dominant Network Equipment
Manufacturer ("OEMs") Cisco.

Prior to entering the market in 2005, it became clear that the software that ran majority
of the Internet infrastructure was manufactured and controlled by Cisco, the dominant
Internet equipment manufacturer. Cisco monopolized this market by tying its software and
security updates to its maintenance services and denied customers that have purchased
its software licenses, access to software updates that correct Cisco-made defects in
the software, majority of which were exploitable for cyber-attack purposes, unless such
customers purchased, at additional costs, its supra-competitive maintenance service.

Despite a relentless smear campaign\(^1\), Multiven's 9-year advocacy for consumers right to
free software and security updates successfully ended the monopolies of all networking
equipment manufacturers in 2010.

On July 19, 2010, Cisco settled\(^2\) Multiven's antitrust lawsuit - Multiven vs. Cisco - which
along with the favorable 2014 ruling by the Swiss Competition Commission\(^3\) - www.
weko.admin.ch - pursuant to a Multiven complaint in 2012, effectively made Multiven the
world's first, and thus far, only manufacturer-independent provider of software integrity
maintenance and cyber-defense services that is able to provide owners and operators of
Internet networks worldwide with technology, tools and expertise to identify, isolate and
correct software defects for the life of the network install-base.

As of today, Multiven is fully operational with over 1.5 million mapped Internet network
devices (routers, switches, firewalls, servers etc.) all fully geo-located, and profiled
(hostnames, geo-coordinates, serial numbers, part numbers, manufacturer, IP address
etc) in its network asset management repository.

The Multiven "Map-the-Internet" initiative detailed in prior sections of this white paper will
ultimately transfer all these, and more mapped devices, onto the Ethereum blockchain
and will serve as a live backup copy of the global Internet install-base, from where,
portions of it that suffer outages, could be restored in future. Multiven's long term goal is
to "Map-the-(entire)-Internet", as a by-product of MOM transactions handling, and make
it available as an Oracle to other decentralised applications to enable businesses of all
sizes that previously struggled to track and visualise their network install-base. All such
read requests will be payable in MultiCoin.

DEMO SCREENSHOT OF A MULTIVEN MAPPED INTERNET DEVICE

---

\(^1\)https://en.wikipedia.org/wiki/Cisco_Systems#Antitrust_lawsuit
\(^3\)https://www.multiven.com/%2525252523/advocacy/07192010
\(^4\)http://bit.ly/2yJoiG
As of February 2018, Multiven maintains access, edge and core Internet networking platforms for large, medium and small customers across all vertical markets (e.g. Telecommunications, Aviation, Manufacturing etc.), on all continents.

In 2016, Multiven opened its first direct-sales office in Paris, France and within the first nine months, the sales pipeline grew from zero to $200 million with just three sales executives. This shows the strong customer appetite for the independence, innovation and cost-effectiveness that Multiven services represents.

Prior to the launch of the Blockchain-based Multiven Open Marketplace ("MOM"), Multiven has traditionally sold its services via reseller to owners and operators of Internet networks and today maintains devices on all continents for Telecom operators, Fortune 500 corporations, SMEs and Academia worldwide.

THE CURRENT LIVE MULTIVEN PLATFORM DASHBOARD
Multiven service pricing ranges from $20 per device per month for a wireless access point (wifi router) to $50,000 per device per month for a core telecom Internet router. Customers pay via credit cards for small recurring purchases and issue purchase orders for large purchases.

For perspective, Tier-1 telecommunications companies like Telefonica in Spain or Orange in France, each spend an average of $500 Million annually on maintaining the software and hardware that make up their Internet networks.

Multiven has traditionally sold its services via reseller partners, most of whom private-label brand Multiven services. The solutions and expertise that powers Multiven services are innovatively crowdsourced from a fully decentralized and vetted global pool of 1,200, (i.e the top 0.1%) Internet network experts, security researchers, cryptographers, inventors and technical leaders on-demand in 55 countries, that are compensated per-task, with the resulting knowledge, archived for proactive future re-use by an artificial intelligence engine, without human intervention.

- **Multiven Pearl**: a multivendor network hardware and software maintenance service for all Internet enabled devices e.g. routers, switches, firewalls, servers etc.
- **Multiven Pearl Guard**: a network-based cyber-defense product that neutralizes cyberattacks and restores affected services within 24 hours.
- **Multiven Open Marketplace**: the world’s first Blockchain-based open marketplace for new, used and decommissioned computer network hardware, software and services powered by MultiCoin tokens.
- **Multiven Oyster**: a Multiven proprietary computer and network hardware and software asset management, collaboration and mapping application.

Multiven’s current deal flow sales pipeline is in the 9 figures and is estimated to exceed $500,000,000 in 2018 and $1 Billion in 2019.

**V. SATOSHI NAKAMOTO?**

The late renowned cryptographer and early developer of PGP, Hal Finney, who, some believed was Satoshi Nakamoto, the creator of Bitcoin, and who was the very first engineer to code-review and fix bugs in Satoshi Nakamoto’s original Bitcoin code, and who was also the first recipient of Bitcoins from Satoshi Nakamoto, was an early member of Multiven’s decentralised community of Internet experts - Pingsta.

Hal joined the Pingsta as member number 62 in 2007.

Source: Pingsta.com, a Multiven Company
Other distinguished members of Multiven’s decentralized Pingsta community include:

- Dr Lawrence Roberts, the designer of the ARPANet, the precursor to the Internet, in 1967, [https://www.linkedin.com/in/lgroberts](https://www.linkedin.com/in/lgroberts)

- Tony Li, Fellow and co-inventor of BGP-4, the routing protocol that powers the Internet, [https://www.linkedin.com/in/tonyl2/](https://www.linkedin.com/in/tonyl2/)

- Harald Alvertrand, The former chairman of the Internet Engineering Task Force - IETF, the body that develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP), and many more, all of whom see the Internet as their ‘baby’ and a key tool for empowering mankind.

### VI. HARDWARE, SOFTWARE AND SERVICES MARKET SIZE

According to Statista, the worldwide revenue from hardware and software maintenance support services is currently at $105 Billion per year.

According to Gartner and Forrester Research, the worldwide Information Technology product and services market, which includes, network and IT infrastructure, data center, mobility and cloud will exceed $3 Trillion in 2018[^15].

By 2019, the annual sales of new telecommunications equipment is expected to exceed $500 Billion[^16].

Multiven conservatively estimates that the secondary market for pre-owned, decommissioned and otherwise unwanted and un-monetized computer networking equipment software to be worth about $100 Billion per year.

---

“Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai’s case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai). Only Finney (RPOW) and Nakamoto were motivated enough to actually implement such a scheme.”

Nick Szabo
Inventor of Smart Contracts and BitGold
http://unenumerated.blogspot.fr/2011/05/bitcoin-what-took-ye-so-long.html
May 28, 2011
As owners and operators of Internet networks seek new ways to lower their capital and operational expenditure, they are beginning to replace their expensive legacy proprietary ‘blackboxes’ from Cisco, HP, Huawei etc. that performed routing, switching, security etc. in hardware, with ultra-low cost Network Functions Virtualization (NFV)-enabled Commercial-Off-The-Shelf (COTS) x86 commodity ‘whiteboxes’, that host multiple Virtualised Network Functions (VNF) atop an open source operating system and a hypervisor.

Hence rather than buying routers, switches and firewalls normally sold as three separate devices, operators can now buy a single commodity whitebox with routing, switching and security ‘apps’ running in it. This consolidation translates into huge CapEx and OpEx savings in hardware, software, space, maintenance, energy and cooling costs.

This fast emerging market for x86 COTS whitebox-based Network Functions Virtualization (NFV) and Software Defined Networking (SDN) is growing fast and exceeded $5 Billion in 2017 with an annual growth rate of 50%.

Multiven intends to be the leader at providing software integrity maintenance and cyber-defense solutions for these multi-vendor Virtual Network Functions (VNF) devices. Multiven is currently rolling out these services for one of the world’s largest telecommunications firms that is replacing hundreds of thousands of proprietary hardware-based routers and switches with virtualized routers and switches sitting atop hypervisors running linux on bare-metal “Whiteboxes”.

6.2 ADDRESSABLE MARKET

From this perspective and global market size, Multiven aims to capture between at least 3% (i.e. $90 Billion) market share in transactions via its new Blockchain-based open marketplace by 2023.

Additionally, as Internet Service Providers globally rip out and replace their “Blackbox” hardware based CPEs (from manufacturers like HP, Huawei, Juniper networks etc.) with low-cost, low energy multi-VNF COTS whiteboxes, the Multiven Marketplace is positioned to be the platform of choice for trading these devices.

6.3 MARKET EVOLUTION TO COMMODITY WHITEBOXES

[17]https://www.theregister.co.uk/2017/11/21/at_and_t_calls_for_disaggregated_network_operating_system/
VII. MULTIVEN BUSINESS MODEL TRANSITION POST ICO

THE INTERNET, THE BLOCKCHAIN ECOSYSTEM AND MULTIVEN

The lack of a hardware, software and politically-neutral provider of services to maintain the integrity, security and reliability of the software that runs the world’s current Internet infrastructure and the fast emerging Internet-of-Things, led to the founding of Multiven in 2005. **Multiven’s secondary mission is to simplify the way the world buys, maintains and sells their computer and network equipment install-base.**

MULTIVEN CLIENTS POST ICO

Multiven Corporation and Multiven Marketplace will provide services to three end-user category clients:

1. Nodes from Public Blockchains will be allowed to register on the marketplace and subscribe freely to Multiven cyber defense service via an API library.

Node Registration will enable Multiven to map every device and push proactive security best practices and verified security updates, transparently to node Internet Gateways and significantly reduces their attack surfaces.
Private Blockchain Nodes and Non-Blockchain clients will be able to access Multiven marketplace to register freely and transact with manufacturers, resellers, and consumers to post their offers to the public. Multiven software maintenance service and decentralised expert community will also be available on the marketplace, at very competitive pricing, payable only in Multicoins.

As already mentioned, all nodes are either directly connected to their Internet Gateway router or connected to a switch and then a router i.e. Node-Attached-Devices (NAD). If we assume a ‘worse case’ scenario that all nodes are attached to both a switch and a router, then:

- The Bitcoin Network has: $11760 \times 2 = 23,520$ NADs
- The Ethereum Network has $24,514 \times 2 = 49,028$ NADs

Thus, there are a total of 72,548 node-attached routers and switches in the Bitcoin and Ethereum networks today.

In order to maintain and foster the decentralized nature of public Blockchain node networks, Multiven is deploying Node-and-Neighbour cyber-defense service, that will limit the attack surface of Bitcoin nodes by proactively pushing verified solutions and security patches and bug fixes to NADs, and thus creates a protective buffer zone for the node, which in turn ensures non-stop connectivity to all other nodes.

The network engineers, security researchers and cryptographers providing cyberdefense for the Bitcoin node network will be compensated from a portion of the transaction fees generated in the Multiven Open Marketplace.

Node cyberdefense is free for Bitcoin and Ethereum nodes. All others blockchain nodes will pay in MTCN.
Multiven’s marketplace will be situated on top of the Ethereum Blockchain and will be ERC-20 compliant. It will be at the center of a new-ecosystem, bringing every active entity from the hardware, software and maintenance services industry in one platform in order to transact and share knowledge in a decentralized peer-to-peer manner.

The Multiven marketplace will also allow private clients to register current and old devices from their infrastructure. Registering all devices will improve transparency and security while creating a liquid second hand market with the intention of driving prices significantly lower and breaking all existing monopolies while promoting innovative new ways of peer-to-peer consumption.

### MarketPlace Powered by Blockchain

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>multiven</th>
<th>Amazon</th>
<th>Alibaba.com</th>
<th>eBay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Globally accessible</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Blockchain-based</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Peer-to-peer</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Dramatically lower costs</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Decentralized procurement</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Immutable proof-of-ownership record</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>0% commission</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Anonymous transactions</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>One single global medium-of-exchange, the Multicoín</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>One-stop-shop for IT hardware, software and services</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Global free trade</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>
“Most full nodes also serve lightweight clients by allowing them to transmit their transactions to the network and by notifying them when a transaction affects their wallet. If not enough nodes perform this function, clients won’t be able to connect through the peer-to-peer network—they’ll have to use centralized services instead.”

https://bitcoin.org/en/full-node#what-is-a-full-node
Through its marketplace, Multiven is targeting two types of markets:

- **First hand/Brand new market**: is currently centralized around a handful of equipment manufacturers (Hardware and Software) selling hardware and software licenses, at dictated prices, only via a handpicked selection of channel “distributors” who sell to “authorized resellers and partners” who in turn sell to corporate, retail, government and Telecom companies.

- **Second hand market**: is on the other hand disorganized, passing through a very large number of independent resellers and brokers. The market has in fact remained untapped due to the absence of an innovative sales channel, connecting parties to buy and sell equipment. Additionally, most medium to large corporate firms and Telecom companies have a high inventory of decommissioned, unused/like-new or unwanted hardware (router, switch, server, processor etc) and software, all available to be monetized.

**THE MULTIVEN OPEN MARKETPLACE - MOM ECOSYSTEM**

MOM transaction records on the blockchain will contain a cryptographic pointer to the product’s constant data stored off-chain, linking it to the variable transaction data stored on-chain and a timestamp.

MOM transaction fees is calculated as follows:
Gas price of writing transactions onto the Ethereum blockchain + (2x of gas (half for MOM and the other half reserved for node cyber defence)).

**One-time “buy/sell”:** Basic transaction where two parties agree to exchange hardware and software, with physical shipment cost.

**Example:** Company A is looking to deploy its own internal network. Company A will login into the Multiven marketplace and trigger a peer-to-peer transaction, to buy computers, servers, routers, software licenses etc. from a pool of sellers.
Scenario 1: User A (Corporate or Individual) is looking for a Server (or any other equipment)

In order to avoid fake dishonest transactions, a Proof-of-Stake protocol will be included in the smart-contract so buyer and seller have more to lose should they engage in unethical behavior rather than honoring transactions.

Recurring transaction: transaction including recurring variables such as contract maturity date, automatic periodic payment (monthly, quarterly, annually) etc.

Example: A company is looking to purchase software maintenance service on a quarterly basis for an equipment. The company will select the appropriate service, append it to the equipment and authorise quarterly recurring payments in MultiCoins to be deducted from its corporate MOM wallet. All of this will be executed via smart contracts.

Scenario 2: User A (Corporate or Individual) is looking to subscribe to a service and make recurring payments.
A portion of the minimal transaction fees earned from the marketplace will be used to compensate the engineers providing active cyber-defense and monitoring of Bitcoin, Ethereum and other public Blockchain nodes.

Once the marketplace goes live, all Multiven services will be transferred to it via smart contracts and the MultiCoin will be the sole means of trade.

Once Multiven’s Blockchain-based marketplace goes live by Q1 2019, we anticipate that transactions volume may exceed $300 Million or 0.01% of market, within the first year and $30 Billion or 1% of market, by 2021 and $90 Billion or 3% of market by 2023.

Note: Multiven is not bound by these targets as they are given for information only

VIII. MULTIVEN TOKEN: MULTICOIN

To achieve the aforementioned objectives, Multiven is creating Multiven COIN tokens shortened to MultiCoin. Its designated ticker symbol will be "MTCN".

KEY FUNCTIONALITIES: MULTICOIN TOKEN

2,000,000,000 MultiCoin Tokens will be created by Mutiven, representing 100% of the MultiCoin token supply. No more tokens will ever be created.
MULTICOIN SUPPLY WILL BE RELEASED IN 4 DIFFERENT PHASES:

1. **ICO**: 5% of the MultiCoin token supply = 100m Multicoins will be sold during the ICO and the proceeds will be injected in Multiven Corporation in order to pilot the blockchain marketplace development.

2. **Incentive/referral program**: 10% allocated to the “Incentive program”

3. **Team, Advisors, Grants & Awards**: 19.5% split into the following:
   - 15% to Multiven Team, advisors, and evangelists – vesting equally over 24 months
   - 1% allocated to the Hal Finney Family – for contributions made to Bitcoins Technology - vesting monthly, over 24 months post-ICO
   - 1% allocated to Mr Wei Dai – for contributions made to B-money - vesting monthly, over 24 months post-ICO
   - 1% allocated to Mr Nick Szabo – for contributions made to Smart Contracts - vesting monthly, over 24 months post-ICO
   - 1.5% - Miscellaneous Reserve – For Bounty Program et al - No lock up period

4. **Foundation**: 60.5% split into the following:
   - 55.5% in the Multicoins reserve. (Half of the reserve will be sold 3 months after the “MOM” goes live through smart-contract)
   - 5% for the “Node-in-Orbit Program”.

The Internet network is the sole connection between us and all of our personal (e.g. photos, videos, social networks etc.) and corporate data (e.g. emails, legal, finance, engineering and other forms of corporate data) online. Hence its availability and integrity is of utmost importance to every man, woman and child, a fact that is further underscored by the United nations’ recent announcement that Internet access is now a fundamental human right.

As a 12-year old startup that’s been bootstrapped and funded solely by its founder, in order to remain financially independent and maintain its neutrality, Multiven has decided to re-create a new ecosystem with a token sale by:

1. Developing its blockchain technology rollout;
2. Strengthening the cyber-defenses of all the global nodes that make up the peer network for Bitcoin, Ethereum and other public block-chain based cryptocurrencies;
3. Developing and deploying the Multiven Open Marketplace Blockchain implementation, acquire users, buyers and sellers and expand brand awareness.
4. Generating the MultiCoin token, as the sole means of payment within the Multiven Blockchain-based Open Marketplace;
5. Funding the research and development, launch, monitoring and maintainance of open-source Delay Tolerant Network-enabled Bitcoin Nodes-in-Orbit (NiO). The first set of nodes is estimated to be in orbit in 2023.
6. Making its best efforts to maintain robust liquidity (subject to the liquidity risks detailed hereunder) and remain financially independent from fiat banks and venture capitalist;
The Multiven MultiCoin is ERC-20 compliant and will be available for purchase with Bitcoin, Ether, Litecoin and other leading cryptocurrencies. It will be tradable on all major cryptocurrency exchanges.

The MultiCoin will be the sole cryptocurrency for the Multiven blockchain-based marketplace for new, used, decommissioned and recycled computing and Internet network hardware, software and services, and the payment mechanism for compensating Multiven’s Pingsta community of Internet network experts, security researchers, cryptographers, technical leaders and bug bounty programs.

Multiven will dedicate its team and ICO proceeds towards the development of the marketplace, and structuring of Multiven Foundation. Token sold during ICO will be spendable on the marketplace, once such marketplace is fully implemented and opened to the public (subject to the risks detailed hereunder). As a result, the Company failing to develop the platform, or the platform failing to be widely used, could affect the usefulness and value of MultiCoin.

### POST ICO: MULTIVEN ORGANISATION

1. **ICO**: 5% of the MultiCoin token supply = 100m Multicoins will be sold during the ICO and the proceeds will be injected in Multiven Corporation in order to pilot the blockchain marketplace development.

2. **Incentive program**: 10% of the Multicoins allocated to the “Incentive program” will be located into the Foundation and then used upon MOM opening in order to power its adoption.

3. **Foundation**: this ICO is been conducted by Multiven Group, the parent company of Multiven Corporation, Pingsta and mySolvr, (“Multiven Group”). Upon completion of this ICO, Multiven Foundation will be incorporated, ideally as a DAO, multi-anchored in several crypto-friendly jurisdictions such as Zug, Singapore, Estonia etc.

   Upon incorporation of Multiven Foundation, it will take ownership of the 60.5% MultiCoin reserve (as well as the 10% allocated to the Incentive Program) and use some of the MTCN reserve, to buyout the assets of Multiven Group and essentially open-source them on the blockchain.

   Multiven Foundation will release MultiCoin token into the marketplace in two ways:

   - The “Incentive program” will be released via a reward smart-contract.
   - The “Foundation reserve” will release 50% of its Tokens to ensure liquidity within three months of the Marketplace going live via a reverse auction to ensure a fair distribution without giving unfair advantages to large buyers using a strict protocol powered by smart-contract.
All tokens allocated to Multiven Team, Advisors and evangelists will vest equally on a monthly basis over 24 months after the ICO. For example, an employee is granted 2,400 MultiCoins during the ICO. The full 2,400 MultiCoins will be held in escrow via a smart contract and 100 MultiCoins will be unlocked and credited to the employee’s wallet every month over the next 24 months.

Unsold tokens in the ICO will be burned.

To fund the aforementioned, Multiven is looking to generate a minimum target of €10m, a soft cap of €25M and a maximum hard cap of €50M from its Token Sales.

The 200M or 10% MultiCoin - ERC-20 Tokens will be sold in the following manner:

<table>
<thead>
<tr>
<th>Bonus scheme</th>
<th>#Token sold at ICO</th>
<th>%Total ICO</th>
<th>%Total Supply</th>
<th>% Bonus Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tranche 1</td>
<td>30 000 000</td>
<td>15%</td>
<td>1,5%</td>
<td>25%</td>
</tr>
<tr>
<td>Tranche 2</td>
<td>40 000 000</td>
<td>20%</td>
<td>2%</td>
<td>20%</td>
</tr>
<tr>
<td>Tranche 3</td>
<td>60 000 000</td>
<td>30%</td>
<td>3%</td>
<td>15%</td>
</tr>
<tr>
<td>Tranche 4</td>
<td>70 000 000</td>
<td>35%</td>
<td>3,5%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>200 000 000</strong></td>
<td><strong>100%</strong></td>
<td><strong>10%</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bounty Program</strong></td>
<td>2 000 000</td>
<td>1%</td>
<td>0,1%</td>
<td></td>
</tr>
</tbody>
</table>

When the tranche 1 has reached its target, it passes automatically to the next tranche and applies the next Bonus. As an example: If Tranche 1’s target is reached in 2 days, then it switches to tranche 2. Every tranche will run until, either the deadline date in the calendar above or when target is reached.

A Bonus scheme will be applied within every tranche period as stated in the table above.
MultiCoin will be available for purchase during the pre-sale, pre-ICO and ICO period only at the following address: WWW.MULTIVEN.IO

Following the ICO, MultiCoin is expected to be listed in some of the major crypto-exchanges globally (subject to the liquidity risks detailed hereunder).

MultiCoin will be sold during the ICO presale at a fixed price of 0.5€/coin

**SOURCES & USES**

The incentive program will be powered by a smart-contract, located in Multiven foundation.

Multiven “Incentive program” will be activated at the same time the marketplace goes live. The program will incentivize entities that register their IT and network hardware and software (“device”) in the Multiven Open Marketplace with MultiCoins, once the registered item is purchased.

Users registering devices on the marketplace will help to create a dynamic map of the Internet.

All device profiles will be saved on the Blockchain (specifically, the constant data e.g. device part number, serial number etc. will be hashed and saved off-chain and linked to the variable data e.g. geo-location, ownership, etc. which will be saved on-chain) creating a Back-up of the Internet infrastructure global install-base.

Multiven will allocate 200M MultiCoins (10% of the MultiCoin Supply) to the incentive program which will be released in the following manner:
As mentioned before, according to Gartner, 8.40 Billion devices are now connected to the Internet. From that perspective, the incentive reward will be set as follows:

- First 5m devices registered: 2 Multicoins per device
- Next 10m devices registered: 1 Multicoin per device
- Next 50m devices registered: 0.5 Multicoin per device

Thereafter 155M / 8.335Bn = 0.01859 MultiCoins for every device registered on the marketplace.

Additionally, an escrow system, a "Proof-of-Existence" protocol, will be put in place to validate the true-identity of every device registered in the Marketplace. Furthermore, security layers will be created to avoid faulty devices or fake transactions to un-escrow Multicoins.

Multiven will introduce a referral feature on the back of the incentive program to further enhance marketplace adoption.

8.4 PHASE 3: MULTICOIN RESERVE

MultiCoin token reserve placed in Multiven foundation will be 60.5% of total supply i.e. 1.21 Billion MultiCoins.

Multiven Foundation will use its MultiCoin reserve to achieve three key objectives:

A. Successfully acquire intellectual property and other assets from Multiven Corporation and fully merged Multiven into a foundation structure.

B. Ensure Multicoin supply liquidity as the marketplace grows in volume of transaction.

C. The Released/sold token will follow a strict automated protocol powered by a smart-contract.

The following are some of the reasons why the MultiCoin (MTCN) should appreciate in value:

1. Permanently capped maximum supply - there will only ever be 2 Billion MTCN in circulation, addressing a $3 Trillion market. Thus at maximum market penetration, 1 MTCN could be worth as much as $1,500.

2. The fact that both buyers and sellers on the MOM are required to stake MTCN, will drive demand up;

3. DApps that access the MOM for Proof-of-Ownership records will pay in MTCN. One of the major headaches in today’s world is been able to prove that you are the rightful owner of a product in order to be able to access post-sales warranty, especially for equipment that have changed ownership at least once. Since all products bought and sold over the MOM are immutably documented on the Ethereum blockchain with timestamped ownership records, the MOM Proof-of-Ownership (PoO) record will serve as an Oracle to other DApps, that require this data. Use cases include but not limited to, an OEM polling MOM PoO records to verify that a customer that purchased an equipment second hand, is indeed the lawful owner of it and thus entitled to post-sales warranty support. Another use case is an insurance service provider validating ownership before approving a claim for the replacement of a stolen product.

4. DApps that access the MOM for Map-the-Internet install-base record will pay in MTCN. The Map-the-Internet feature of the MOM dynamically backs up the world’s Internet network install-base onto the Ethereum blockchain. This means that medium to large businesses, telecommunications firms and government agencies that previously struggled to track and visualise their network and relied on inefficient excel spreadsheets for network map data, can now simply probe the MOM as an Oracle for real-time data on what is installed where and when. All such read requests will be payable in MultiCoin.
5. As each NiO have the capacity to accommodate multiple Blockchain cores, other projects other than Bitcoin and Ethereum that want to reside on our NiOs will pay in MTCN;

Use Cases of MOM Map-the-Internet and Proof-of-Ownership features

Map-the-Internet - Use case and Multicoin-ization
The Map-the-Internet feature of the MOM dynamically backs up the world’s Internet network install-base onto the Ethereum blockchain. This means that medium to large businesses, telecommunications firms and government agencies that previously struggled to track and visualise their network and relied on inefficient Excel spreadsheets for network map data, can now simply probe the MOM as an Oracle for real-time data on what is installed where and when. All such read requests will be payable in MultiCoin.

Proof-of-Ownership records - Use case and Multicoin-ization

OEMs have no visibility into products once it is re-sold by the original purchaser. One of the major headaches in today’s world is been able to prove that you are the rightful owner of an IT product in order to be able to access post-sales warranty support, especially for equipment that has changed ownership at least once. Since all devices bought and sold over the MOM are immutably documented on the Ethereum blockchain with timestamped ownership records, the MOM Proof-of-Ownership (PoO) record will serve as an Oracle to other Dapps, that require this data. Use cases include but not limited to, an OEM polling MOM PoO records to verify that a customer that purchased an equipment second hand, is indeed the lawful owner of it and thus entitled to post-sales warranty support. Another use case is an insurance service provider validating ownership before approving a claim for a replacement of stolen equipment for instance.

The “Incentive Program” will help the market to adopt the MOM from the supply side because as shown above, the first 65 million device profiles created on the MOM will ‘mine’ MTCN for their owners. The demand side will be driven by (1) a strong marketing campaign to businesses of all sizes educating them on the vastly lower cost benefits of decentralised sourcing and procurement on the MOM and; (b) MTCN miners looking to spend it.
### IX. ROAD MAP POST ICO

**MOM, Bitcoin Cyber-defense & NiO Roadmap**

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2005</td>
<td>Launch of Multiven Platform</td>
</tr>
<tr>
<td>Q3 2007</td>
<td>First Large Customer - Lucent Technologies</td>
</tr>
<tr>
<td>Q4 2008</td>
<td>Multiven sues Cisco to end its Monopoly of the Internet</td>
</tr>
<tr>
<td>Q3 2010</td>
<td>Cisco settles lawsuit by providing Multiven with software and security updates</td>
</tr>
<tr>
<td>Q2 2012</td>
<td>Multiven files new complaint against Cisco with Swiss competition commission</td>
</tr>
<tr>
<td>Q3 2014</td>
<td>Swiss competition commission grants Multiven wishes making all Cisco software transferable</td>
</tr>
<tr>
<td>Q4 2015</td>
<td>Multiven re-locates headquarters to Netherlands</td>
</tr>
<tr>
<td>Q1 2016</td>
<td>First direct Sales office opens in Paris, France</td>
</tr>
<tr>
<td>Q1 2017</td>
<td>Marketplace Development Commences</td>
</tr>
<tr>
<td>Q1 2018</td>
<td>ICO Public Sale</td>
</tr>
<tr>
<td>Q2 2018</td>
<td>Live Monitoring &amp; CyberDefense of Bitcoin et al Nodes Commences</td>
</tr>
<tr>
<td>Q2 2018</td>
<td>Nodes-in-Orbit (NiO) R&amp;D Commences</td>
</tr>
<tr>
<td>Q3 2018</td>
<td>MOM QA Testing and Security Audit</td>
</tr>
<tr>
<td>Q4 2018</td>
<td>Launch of MOM MVP in Alpha</td>
</tr>
<tr>
<td>Q1 2019</td>
<td>Deployment of Stable version of MOM with ongoing QA Testing</td>
</tr>
<tr>
<td>Q1 2019</td>
<td>Launch of the MOM Wallet</td>
</tr>
<tr>
<td>Q2 2019</td>
<td>Official Launch of MOM Platform and Trading</td>
</tr>
<tr>
<td>Q2 2019</td>
<td>Map-the-Internet Commences</td>
</tr>
<tr>
<td>Q3 2022</td>
<td>Launch of first 9 Bitcoin Nodes-in-Orbit (NiO)</td>
</tr>
</tbody>
</table>
MULTIVEN FINAL ORGANIZATION STRUCTURE

1. Multiven Corporation will merge into Multiven Foundation to become a unique entity within five years of MTCN going live.

2. To ensure lifetime continuity on the Blockchain, all of Multiven Corporation’s tangible and intangible assets e.g. proprietary technology, applications, services, APIs, mySolvr, Pingsta community etc. will ultimately be acquired by Multiven Foundation using its reserve tokens and made openly available on the Blockchain marketplace.

X. CORE TEAM

PETER ALFRED-ADEKEYE

CEO & Chief Technology Architect

Peter is a technology entrepreneur & consumer advocate. Prior to founding Multiven, Peter was the Technical Leader at Cisco Systems in Silicon Valley responsible for maintaining the integrity of Cisco IOS, the software that ran 70% of the Internet.

Peter led the team responsible for all critical source-code level software issues in Cisco IOS. Before Cisco, he was a multi protocol escalation engineer at IBM Global Network Services in England.

Peter holds a BSc in engineering from University of Ife, and has completed executive education in leadership from Stanford University. Peter is a member of ENISA, the EU organisation tasked with formulating policies to secure EU’s cyberspace.

Linkedin

HUGUES CHRISTOPHE-REMY

Blockchain Business Development

Hugues runs business development for Multiven worldwide. Prior to Multiven, he spent 8 years at Evernex, a Carlyle portfolio Company in the computer networking hardware lifecycle industry based in France. An avid traveler, Hugues has been to over 30 countries on all continent and earned his bachelors degree in Australia.

Linkedin
ROMAIN GILGER

MOM Business Development

Romain runs sales for Multiven in Spain and Latin America. Romain ran Evernex in Spain, Portugal and LATAM for eight years. He holds a bachelors degree from the University of Pau in southwest France and is an avid skier.

PAUL LITTRE

Blockchain Partnerships

Successfully managed multi-million Euro sales in retail commerce; knowledge that will be tapped as we develop the Multiven Open Marketplace.

TOUAIBA HOUMIRAT

Off-Chain Operations

Seasoned operations expert that oversees quoting, invoicing, payments, customer on-boarding and logistics. These pre-blockchain experiences that will come in handy as we code and automate the entire process into MOM smart contracts.

SEBASTIAN SCHWARZ

Products and Public Relations

Sebastian has a bachelors of Science degree in applied mathematics from Université Paris I – Panthéon-Sorbonne and is pursuing a joint Msc in Data Science at École Polytechnique and HEC. He is fluent in German, English, French and Python. In his downtime, he plays the guitar and enjoys fine wine.

MAXIME JEANTET

Project Team Leader

BELISARIO ALFONSO

Technical Leader, MOM

Belisario is the technical leader for MOM development. He is an expert in solidity, ethereum/smart contracts development and big data. He holds an MSc in information systems from Stanford University school of engineering in Palo Alto California.

Linkedin

REGIS MILLET

Technical Leader, B-Fence

Regis is the technical leader for Multiven B-fence. He is a very senior full stack engineer with a strong background in cybersecurity. He holds a degree from the institut national des telecom in France.

Linkedin

PABLO CHAVIDA

Head of Product Design

Pablo is MOM’s head of design. He is a brilliant UI/UX designer and holds a degree in graphic design and multimedia communications from Escuela Superior de Publicidad (ESP), Spain.

Linkedin

OUR ADVISORS

JILLIAN GODSIL

Advisor & Evangelist

Blockchain Advocate, Journalist, Keynote Speaker, Named one of the 50 Most Influential Women In Blockchain
Trinity College Dublin, BA, MA (Hons)

Linkedin

FERNANDO SANCHEZ

Communications Specialist

Senior writer, storyteller, and digital content provider, now focussed on crafting Multiven’s communications strategy through articles, blog posts, and other written material. Cryptojournalist and blockchain enthusiast Limerick Institute of Technology, Aerospace Science & Technology

Linkedin
XI. CONCLUSION

There is no Bitcoin without a strong decentralized network of active nodes that relay, validate and irrevocably record transactions.

Support Multiven in its goal of keeping the Bitcoin, Ethereum and all public Blockchain cryptocurrency node networks secure, available and reliable around the clock.

Blockchain is bringing to life, new possibilities in technology that will have a lasting positive impact on mankind. Multiven is helping to ensure this future becomes a reality.

Miscellaneous Facts on the Global Bitcoin Network:

1. 80% of all bitcoin nodes are currently 'centralised' in 10 countries; (i.e. US, Germany, France, China, NL, Canada, UK, Russia, Singapore and Hong Kong);

2. Hong Kong with a population of 7 million people has 170 nodes (1.44%) while India with a population of 1.30 Billion people has only 52 nodes;

3. The US accounts for almost 30% of all Bitcoin nodes;

4. Approximately 40% of all bitcoin nodes reside within the European Union;

5. Africa with a population of 1.22 Billion people has only 32 Bitcoin Nodes;

6. There are only 110 bitcoin nodes in South America, a sub-continent with 420 million people;

7. As of December 12, 2017, in a world with a global population of 7.6 Billion people, there entire bitcoin network consist of 11,784 nodes.

In conclusion, it is clear from the aforementioned data that Bitcoin and other cryptocurrencies are not deployed in emerging countries very likely because of the prohibitive cost of acquiring and operating computers and servers.

The Multiven marketplace will dramatically lower this cost of acquisition and lead to a true decentralisation of the global bitcoin network.
“Decentralization is, I would argue, the most important property of the bitcoin network. Without it, many of bitcoin’s other properties, such as its ability to facilitate transactions without a third party or provide a permissionless platform for innovation, would be compromised”.

Jameson Lopp,
creator of Statoshi.info

XII. LEGAL DISCLAIMER

Any buyer purchasing the Company’s products or services expressly acknowledges technical and market uncertainties which are inherent in any business development project as presented in this White Paper (see below for risk factors) and that this project may therefore never come to fruition or may have to be abandoned, without the MultiCoin being used. In such a case, the buyer expressly acknowledges and accepts that it will not be entitled to sue or bring any direct or indirect legal action before the courts, the arbitration bodies or any alternative dispute settlement body, either in France or abroad, against the Company, its directors, shareholders, employees or subcontractors in the event of the non-performance, non-deployment or non-implementation of the project, even in cases where its MultiCoin have lost some or all of their value.

In addition, the Company may not be held liable for any of the following:

I. use of services that are not compliant with the applicable terms;
II. non-performance, failure, malfunction or unavailability of the services due to a third party, the buyer, a third-party product, or the buyer’s breach of its obligations;
III. indirect damages such as business loss or disturbance, loss of orders, operating loss, infringement of the trade mark, loss of profits or clients (e.g. improper disclosure of confidential information concerning said clients due to failure or piracy of the platform, third-party proceedings against the client, etc.);
IV. loss, disclosure or unlawful or fraudulent use of user sign ons by the buyers or third parties;
V. suspension of access or temporary or permanent suspension of services (in particular, arising from a request issued by an appropriate administrative or judicial authority, or notification received from a third party);
VI. loss, alteration or destruction of all or part of the content (information, data, applications, files or other items) hosted on the infrastructure, insofar as the Company is not responsible for managing the continuity of buyers activities, and data backups in particular;
VII. mismatch between the services and the buyer’s needs (in particular, with regard to the sensitivity of the relevant data);
VIII. security incidents relating to use of the Internet, concerning in particular the loss, alteration, destruction, disclosure or unauthorized access to the buyer’s data or details on or via the Internet; and
IX. damages to systems, applications and other items installed by the buyer on the infrastructure.
This White Paper does not constitute an offer or an invitation to sell shares, securities or rights belonging to the Company or any related or associated company.

None of the information or analyses in this White Paper is intended to provide a basis for an investment decision, and no specific investment recommendation is made. Accordingly, this White Paper does not constitute investment advice or an invitation to invest in any security or financial instrument of any nature whatsoever.

This White Paper does not constitute or form part of, and should not be construed as, an offer for a sale or subscription, or an invitation to buy or subscribe securities or financial instruments. This White Paper, or any of its component parts, does not constitute the basis for, or should not be used as a basis for, or in connection with, a contract for the sale of securities or financial instruments or a commitment to sell securities or financial instruments of any kind.

The Company expressly disclaims any liability for any direct or indirect loss or damage of any kind arising directly or indirectly from:

I. any reliance on the information contained in this White Paper;

II. any error, omission or inaccuracy in said information; or

III. any resulting action that may be brought.

This White Paper has been constructed in accordance with the applicable EU regulations.

In a security or a financial instrument within the meaning of EU Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 relating to markets in financial instruments: MultiCoin confer no direct or indirect right to the Company's capital or income, nor does it confer any governance right within the Company;

Control over a MultiCoin does not grant the controlling individual any asset or share in the Company, or in the Platform. A MultiCoin does not grant any right to participate in control over the Company's management or decision-making set-up, or over Platform.

Within the meaning of EU Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 relating to access to and pursuit of the business of electronic currency institutions: MultiCoin are not accepted outside the platform and do not have a fixed exchange value equal to the amount delivered at the time of their issue;

Within the meaning of EU Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 relating to payment services in the internal market, nor within the meaning of EU Directive N° 2015/2366 of the European Parliament and of the Council of 25 November 2015 relating to payment service 2 (DSP 2): the ICO does not involve the purchase and/or sale of MultiCoin and the Company's business does not consist in receiving currencies against the delivery of MultiCoin; as such, a MultiCoin is not a means of payment either.

A MultiCoin is a crypto-currency, i.e. an unregulated digital asset issued and controlled by its developers and used and accepted by the members of a given community.
XIII. SALES RESTRICTIONS

Participation in the ICO is restricted to natural or legal persons acting within the scope of their professional activities. Any private individual acting on a non-professional basis as a simple consumer, within the meaning of EU Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, is excluded from the ICO.

Documents linked to the ICO may not be transmitted or distributed to a "U.S. citizen" or to mail or email addresses in the United States of America. It is prohibited to transmit, distribute or reproduce documents linked to the ICO to or for a "U.S. citizen" or within the territories of the United States of America, in whole or in part.

To ensure their eligibility for the purchase of MultiCoin, buyers expressly declare that they are not a "U.S. citizen" (within the meaning of "Regulation S" of the Securities Act 1933 under U.S. law), i.e.:

I. any private individual resident in the United States of America;
II. any partnership or business organized or established under U.S. law;
III. any property of which the executor or administrator is a U.S. citizen;
IV. any trust of which a proxy is an American citizen;
V. any agency or branch of a foreign entity located in the United States of America;
VI. any non-discretionary account or similar account (other than a trust or property) held by a trader or other trustee for the benefit of or on behalf of a U.S. citizen;
VII. any discretionary account or similar account (other than a trust or trust) held by a trader or other trustee, that is organized, established or (if a private individual) resident in the United States of America; and
VIII. any partnership or company if:
   1. it is organized or established under the law of a foreign jurisdiction; and
   2. it is formed by a U.S. citizen primarily for the purpose of investing in securities not listed under the U.S. Securities Act, unless it is organized or established, and owned, by accredited investors who are not private individuals, trusts or properties.

More detailed sales restrictions are provided for in the Multiven Terms of Token Sale to be entered into by any MultiCoin purchaser.

XIV. WARNINGS ON THE RISKS INHERENT TO THE ICO

RISK OF LOSS OF ACCESS TO A MULTICOIN DUE TO LOSS OF CREDENTIALS

Until it is distributed to the buyer, the said buyer’s MultiCoin may be linked to a Company account. You can only access the Company account using the credentials selected by the buyer. The loss of these credentials will result in the loss of the MultiCoin. Good practices advise buyers to store their credentials securely in one or more backup locations that are geographically separated from the work location.

RISKS ASSOCIATED WITH THE ETHEREUM PROTOCOL

Both MultiCoin and the Platform are based on the Ethereum protocol. Therefore, any malfunction, unplanned function or unexpected operation of the Ethereum protocol may cause the Platform or MultiCoin to malfunction or operate in a way that is not expected. Ether, the native Ethereum Protocol account unit, may itself lose value in a similar way to MultiCoin, and also in other ways.

For more information on the Ethereum protocol, see > http://www.ethereum.org/
RISKS ASSOCIATED WITH THE BUYER’S CREDENTIALS

Any third party that obtains access to the buyer’s credentials or private keys may be able to use the buyer’s MultiCoin. To minimize this risk, buyers must protect themselves against people gaining unauthorized access to their electronic devices.

LEGAL RISK AND RISK OF ADVERSE REGULATORY INTERVENTION IN ONE OR MORE JURISDICTIONS

Blockchain technologies have been reviewed by various regulatory bodies around the world, including within the European Union. The ICO has been structured to comply with EU law applicable at the time of the offer.

The operation of the platform and of MultiCoin may be impacted by the passing of restrictive laws, the publication of restrictive or negative opinions, the issuing of injunctions by national regulators, the initiation of regulatory actions or investigations, including but not limited to restrictions on the use or ownership of digital tokens such as MultiCoin, which may prevent or limit development of the platform.

Given the lack of crypto-currency qualifications in most countries, each buyer is strongly advised to carry out a legal and tax analysis concerning the purchase and ownership of MultiCoin according to their nationality and place of residence.

RISK OF AN ALTERNATIVE, UNOFFICIAL PLATFORM

Following presales and development of the original version of the platform, there is a possibility that alternative platforms may have been established using the same open-source code and open source protocol that underlies the platform. The official platform may find itself in competition with these alternatives, unofficial platforms based on MultiCoin, which could potentially adversely impact the platform and MultiCoin.

RISK OF A LACK OF INTEREST IN THE PLATFORM OR DISTRIBUTED APPLICATIONS

There is a possibility that the platform may not be used by a large number of companies, individuals and other organizations, and that there may be limited public interest in the creation and development of distributed applications. Such a lack of interest could impact on the development of the platform and, therefore, on the uses or potential value of MultiCoin.

RISK THAT THE PLATFORM IS NOT DEVELOPED

The main right associated with MultiCoin is the right access the marketplace on the platform. The value of the MultiCoin is therefore heavily correlated with the existence of such platform and network, which has not yet been implemented. MultiCoin may lose part or all of their value if the platform and/or marketplace is never fully developed.

RISK THAT THE PLATFORM, AS DEVELOPED, DOES NOT MEET BUYER EXPECTATIONS

The platform is currently under development and may undergo significant redesign prior to its launch. For a number of reasons, not all buyer expectations concerning the platform or MultiCoin form and function may be met on the launch date, including changes in design, implementation and execution of the platform.

RISK OF THEFT AND PIRACY

Hackers or other malicious or criminal groups or organizations may attempt to interfere with the platform or the availability of MultiCoin in several ways including, but not limited to, denial of service attacks, Sybil attacks, mystification, surfing, malware attacks, or consensus-based attacks.
RISK OF SECURITY WEAKNESSES IN THE PLATFORM’S CORE INFRASTRUCTURE SOFTWARE

The platform’s core software is based on open source software. There is a risk that the Company team, or other third parties, may intentionally or unintentionally introduce weaknesses or bugs into the core infrastructure elements of the platform, by interfering with the use of, or causing loss of, MultiCoin.

RISK OF WEAKNESS OR EXPLOITABLE BREAKTHROUGH IN THE FIELD OF CRYPTOGRAPHY

Advances in cryptography, or technical advances such as the development of quantum computers, may present risks for crypto-currencies and the platform, which could result in the theft or loss of MultiCoin.

RISK OF A MULTICOIN MINING ATTACK

As with other decentralized cryptographic tokens and crypto-currencies, the blockchain used for the platform is vulnerable to mining attacks, including but not limited to, dual-expense attacks, powerful mining attacks, selfish mining attacks, and critical competition attacks. Any successful attack poses a risk to the platform, the expected performance and sequencing of the Company’s markets, and the expected performance and sequencing of Ethereum contract calculations. Despite the best efforts of the Company’s team, the risk of known or new mining attacks exists.

RISK OF THE PLATFORM FAILING TO BE USED OR ADOPTED

While MultiCoin should not be considered an investment, their value is bound to change over time. This value may be limited if the platform is not sufficiently used and adopted. In such a case, there could be few or no markets at the platform launch, which would limit the value of MultiCoin.

RISK OF A TIGHT MARKET FOR MULTICOIN

There are currently no exchanges or trading facilities on which MultiCoin can be traded. If such exchanges or trading facilities do develop, they will probably be relatively new and subject to poorly understood regulatory oversight. They may therefore be more vulnerable to fraud and default than the established and regulated exchanges that exist for other products. Should exchanges or trading facilities that represent a substantial part of the MultiCoin trading volume be involved in fraud, security failures or other operational problems, the failures of such exchanges or trading facilities may limit the MultiCoin value or liquidity.

RISK OF AN UNINSURED LOSS

Unlike bank accounts or accounts in other regulated financial institutions, funds held through the Company or Ethereum network are generally uninsured. At present, there are no public or private insurance agents providing buyers with coverage against a loss of MultiCoin or a loss of value.

RISK OF WINDING-UP OF THE COMPANY’S PROJECT

For a number of reasons including, but not limited to, an unfavorable fluctuation in Bitcoin value, an unfavorable fluctuation in MultiCoin value, the failure of business relationships or competing intellectual property claims, the Company project may no longer be a viable activity and may be dissolved or simply not launched.

RISK OF MALFUNCTION IN THE PLATFORM

The platform may be impacted by an adverse malfunction including, but not limited to, a malfunction that results in the loss of MultiCoin or market information.

UNFORESEEN RISKS
Crypto-currencies and cryptographic tokens are a new, untested technology. In addition to the risks stipulated above, there are other risks that the Company's team cannot predict. Risks may also occur as unanticipated combinations or as changes in the risks stipulated herein.

XV. RECENT REGULATORY ACTIONS

As mentioned above, operations of the platform and of MultiCoin may be impacted by future restrictive laws, regulations, opinions, decisions, injunctions, actions or investigations by national regulators and lawmakers.

Some regulators have already initiated formal or informal proceedings related to the regulation of ICOs and tokens, some of which are listed hereunder. This list is provided for information purpose only and do not constitute legal advice.

- **The United States Securities and Exchange Commission (SEC)** issued (i) a report dated July 25, 2017 stating that tokens offered by the company The DAO were securities within the meaning of the 1933 Securities Act, and (ii) an “investor bulletin” informing potential investors on ICOs.

- **The United Kingdom Financial Conduct Authority (FCA)** issued a statement on September 12th, 2017 warning potential investors about the risks associated with ICOs.

- **The Canadian Securities Administrators (CSA)** issued a “staff notice” dated August 24th, 2017 in which it states that ICOs might be governed by Canadian securities laws (knowing that tokens would, however, not always constitute securities for the purpose of such laws) or by Canadian derivative laws (if the products issued qualify as derivatives).

- **The Israel Securities Authority (ISA)** published a statement dated August 30th, 2017 announcing that it would organize a committee to study the applicability of securities law to ICOs.

- **The People’s Bank of China**, together with other Chinese regulators, issued a statement dated September 4th, 2017 prohibiting token fundraising transactions. Companies that have already launched an ICO are required to refund the tokens issued.

- **The Monetary Authority of Singapore (MAS)** released a statement dated August 1st, 2017 concluding that some tokens might be qualified as securities within the meaning of the Singaporean Securities and Futures Act.

- **The Securities and Futures Commission (SFC)** of Hong Kong made a declaration on September 5th, 2017 in which it stated that tokens may qualify as securities under the Securities and Futures Ordinance.

- **The Financial Supervisory Commission (FSC)** of South Korea declared, on September 3rd, 2017, that it established a “joint task force meeting” to discuss crypto-currencies regulatory framework.

- **The Financial Market Supervisory Authority (FINMA)** of Switzerland, in a press release dated September 29th, 2017, announced it was investigating various ICOs. The FINMA specified, in Guidance 04/2017 published on the same day, that ICOs are susceptible, depending on their structuring, to be governed by (i) AML/KYC regulations (ii) banking monopoly provisions (iii) securities and derivatives trading regulations and (iv) collective investment schemes regulations. As mentioned by the FINMA, “due to the close proximity in some areas of ICOs and token-generating events with transactions in conventional financial markets, the likelihood arises that the scope of the application of at least one of the financial market laws may encompass certain types of ICO model”.

- **The Australian Securities and Investments Commission (ASIC)** recently published
the Information Sheet 225 as guidance about the potential application of the 2001 Corporations Act to businesses conducting ICOs. According to this document, an ICO, depending on how it’s structured, could be qualified as a managed investment scheme, as a public offer and/or as an offer of derivatives.

- Abu Dhabi’s Financial Services Regulatory Authority (FSRA) released guidelines on crypto currencies and ICOs dated October 8th, 2017, in which it specified that (i) existing KYC would be applicable to ICOs and (ii) some tokens, on a case-by-case basis and depending on how they are structured, may be classified as securities while others may be classified as commodities.

- The French Financial Markets Authority (AMF) launched on October 26th, 2017, (i) an ICO assistance and research program dubbed “UNICORN” to provide issuers with a framework for their ICO and to explore potential future regulatory actions, and (ii) a public consultation on ICOs, in which three regulatory options are presented: issuing guidelines on ICOs without changing the existing regulations, placing ICOs under the regime applicable to public offers of securities, or enacting a new, specific regulation for ICOs. The Japanese Financial Services Agency (FSA)

- The Japanese Financial Services Agency (FSA) published an investor alert on October 27th, 2017 underlying the “high risks” associated with ICOs (i.e. token volatility and likelihood of fraud) and warning issuers and investors that ICOs, depending on how they are structured, may fall within the scope of the Japanese Payment Services Act and/or of the Japanese Financial Instruments and Exchange Act.

- New Zealand Financial Markets Authority (FMA) published a statement dated October 25th, 2017 on ICOs, explaining that the specific characteristics and economic substance of an ICO will determine if the token should be classified as a financial product. More importantly, the FMA specified that “all tokens or cryptocurrencies are securities under the FMC Act – even those that are not financial products”.

### XVI. KYC PROCESS

ICO KYC process will ensure full transparency and will be obligatory in order to acquire MultiCoin token during the ICO period.

**STEP 1:**
Upon receipt of the information, Chaineum will automatically trigger through verification

<table>
<thead>
<tr>
<th>INDIVIDUAL PROCESS</th>
<th>COMPANY PROCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Required:</strong></td>
<td><strong>Information Required:</strong></td>
</tr>
<tr>
<td>- First/Last name</td>
<td>- Company Name</td>
</tr>
<tr>
<td>- Date of Birth</td>
<td>- Date of Incorporation</td>
</tr>
<tr>
<td>- Email address</td>
<td>- Country of Incorporation</td>
</tr>
<tr>
<td>- Citizenship (US Persons are excluded from this ICO)</td>
<td>- First/Last name of contact</td>
</tr>
<tr>
<td></td>
<td>- Email address</td>
</tr>
</tbody>
</table>
in:
1. International sanctions list
2. Politically Exposed Person list

If the search returns null, then the investor will be cleared to complete the subscription process.
If the search returns a non-null value, then the investor will be denied access to the subscription.
For potential investors on Politically Exposed Person list, a case-by-case authorization access will be considered.

ALL US persons will be denied access to the subscription stage.

ACCEPTATION OF TERMS & CONDITIONS

YES - I confirm that I have read and understand the Terms and Conditions included in the Multiven Terms of Token Sale and that I expressly accept all the terms, conditions, obligations, affirmations, representations and warranties described in these Terms and agree to be bound by them.

YES - I hereby confirm that I am an “Eligible Purchaser” within the meaning of these same terms.

I declare and certify not to be a consumer within the meaning of the directive 2011/83/EU on consumer rights and equivalent texts in the jurisdiction I am in; I furthermore certify that I am acting in my professional capacity.

YES - I declare and certify carrying out the research or taking the relevant advice from specialized attorneys to ensure that no Legislation or regulation applicable to my situation

STEP 2:

**INDIVIDUAL PROCESS**

- ID or Passport of representative
- Registration number
- Legal Name
- Legal Address

**COMPANY PROCESS**

- ID or Passport of representative
- Registration number
- Legal Name
- Legal Address

Following the upload, control and access will be provided, except for US persons. **ID document will be used at the end of the ICO in order to proceed to:**

- Random verifications conducted by the Chaineum Compliance Officer
- Update internal verification files on « Politically Exposed Person » (or « PEP ») and their level of exposure:
  1. In case of serious PEP = ineligible and reimbursement of perceived funds;
  2. In case of ordinary PEP = pursue of the process;
More detailed background check for investors above 10,000€

- Manual verification or additional control by including proof of address process (Address, Postal Code, City, Country and Utility Bills).

APPLICABLE LAW AND JURISDICTION

This White Paper and any contractual relationship arising in relation with the products and services sold by the Company are governed exclusively by French law, the Company’s commitment being subject to this clause. The Parties agree to seek an amicable settlement prior to bringing any legal action. Failing this, any dispute, of any nature whatsoever, will be brought expressly before the [courts of Paris]/[International Chamber of Commerce], as no document can effect a novation or waiver of this jurisdiction clause.
REFERENCES

• https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html
• https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html
• https://www.mail-archive.com/cryptography@metzdowd.com/msg05000.html
• http://www.etsi.org/technologies-clusters/technologies/nfv
• InterPlanetary Networking Special Interest Group (IPNSIG). http://ipnsig.org
• https://www.exploit-db.com
• http://www.gartner.com/newsroom/id/3598917
• https://bitnodes.21.co
• https://www.ethernodes.org/network/1
• https://www.multiven.com/#/advocacy/
• https://en.wikipedia.org/wiki/The_Shadow_Brokers
• Multiven v. Cisco, Original Complaint, December 1, 2008
• Multiven v. Cisco, Settlement Agreement, July 19, 2010
• Justice Mckinnon Ruling, May 31, 2011
• Swiss Competition Commission Ruling, 2014
• https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
• 1https://btc-hijack.ethz.ch
• 3https://en.wikipedia.org/wiki/Interplanetary_Internet
• 4Node-Attached-Devices: Switch, router, server etc.
• 5https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html
• 6https://github.com/misterch0c/shadowbroker
• 7https://www.washingtonpost.com/world/national-security/poweful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-3753347913f5_story.html?utm_term=.f506f1100290
• 8https://blog.comae.io/shadow-brokers-nsa-exploits-of-the-week-3f7e17bdc216
• 10https://en.wikipedia.org/wiki/Cisco_Systems#Antitrust_lawsuit
• 12https://www.multiven.com/%2525252523/advocacy/07192010
• 13http://bit.ly/2yJsiIG
• 15https://www.gartner.com/technology/research/it-spending-forecast/
• 16https://www.theregister.co.uk/2017/11/21/at_and_t_calls_for_disaggregated_network_operating_system/
• 17http://www.etsi.org/technologies-clusters/technologies/nfv