Ammbr

Ammbr

WHITEPAPER

15 August 2017

Updates in progress for Part F: Token Sale

Please note that certain details of the token sale outlined in Part F will be updated before a public token sale commences. As of 3 September 2017 the original public token sale has been put on hold and a new date has not yet been confirmed. Please ensure you subscribe to email updates to get any late breaking news.

Also, you should rely on the updated whitepaper that will be available at the time of the sale for updated details.

Caution

This white paper has been prepared in compliance with industry best practices and regulations as understood by the authors at this time. This white paper is not a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

A copy of this white paper has been delivered to the Monetary Authority of Singapore (MAS) for information purposes, although there are no pertinent regulations at this point that require approval or registration. Seeking approval, whether tacit or express, of this white paper by the MAS is not undertaken as an indication of the merits of the Ammbr Foundation or its cryptographic tokens. The cryptographic tokens offered in this white paper have not been approved or disapproved by the MAS or any other regulatory body in any jurisdiction.

Prospective contributors should carefully consider the matters set forth under the caption "Risk Factors" in Part F of this Whitepaper. If you are in doubt about the contents of this Whitepaper, you should consult your investment advisor, stockbroker, lawyer, banker, dealer or any other financial consultant.

Whitepaper in respect of a public offer of **AMMBR** cryptographic tokens of the proposed Ammbr Mesh Network at a starting price of **USD 0.10c per AMMBR,** representing, after their issue, **60%** of the total issued number of **AMMBR** to ever exist on the Ammbr Mesh Network.

Important notice

This Whitepaper is important and should be read in its entirety.

Prospective contributors, in particular, should read the whole text of this Whitepaper. Their attention is specifically drawn to the discussion of certain risks and other factors that should be considered in connection with a contribution into the offered tokens, as set out in the section titled "Risk factors" in Part F of this Whitepaper.

If you are in doubt about the contents of this Whitepaper or what action to take, you are advised to contact your investment advisor, financial advisor, banker or other relevant professional advisor who specialises in advising on the acquisition of cryptocurrency.

To the best knowledge of the authors, this Whitepaper contains information that is provided only in compliance with the requirements of applicable laws, rules and regulations of Singapore, including, but not limited to, the Companies Act, the Securities and Futures Act (SFA) and the Financial Advisers Act (FAA) insofar as they are pertinent, or can provide guidance.

This Whitepaper is issued by the Ammbr Foundation and has been prepared in respect of the issue of and subscription for the offer tokens and the subsequent listing of the tokens on various cryptocurrency exchanges. This follows approval of the offer by the Board and the existing shareholders of Ammbr Foundation through a resolution dated 1 July 2017.

All references in this document to times are to British Summer Time (BST).

The definitions provided under the "definitions and abbreviations" section of this Whitepaper apply throughout the document, unless indicated otherwise.

Directors' responsibility

The directors, whose profiles are provided in Part E of this document, have taken all reasonable care to ensure that the facts stated and the opinions expressed herein are true and accurate in all material aspects, and no other material facts have been omitted. The directors accept responsibility for the information contained in this Whitepaper in relation to Ammbr Foundation.

Legal uncertainty

Significant uncertainty reigns in the area of token offerings and cryptocurrency. We advise seeking legal advice before participating in this, or any other, Crowdsale.

Prospective contributors should read the whole of the text of this Whitepaper. Their attention is specifically drawn to the discussion of certain risks and other factors that should be considered in connection with a contribution into the offered tokens, as set out in the section titled "Risk Factors" in Part F of this Whitepaper.

Forward Looking Statements

This Whitepaper contains forward-looking statements with respect to:

- Ammbr's financial and technical viability
- Certain of the plans and objectives of Ammbr
- The effects of regulation on Ammbr's activities by the governments of countries in which it may wish to operate
- Ammbr Foundation's expectations regarding the launch and rollout dates for products, services or technologies
- Expectations regarding the operating environment and market conditions for the Ammbr Mesh Network
- Growth in terms of customers and usage, and the rate of exchange in the value of Ammbr cryptographic tokens

Forward-looking statements are sometimes, but not always, identified by their use of a date in the future or such words as "will", "anticipates", "aims", "could", "may", "should", "expects", "believes", "intends", "plans", or "targets".

By their nature, forward-looking statements are predictive, speculative and involve risk and uncertainty because they relate to events and depend on circumstances that will occur in the future, involve known and unknown risks, uncertainties and other facts or factors which may cause the actual results, performance or achievements of Ammbr Foundation, the Ammbr Mesh Network, or its industry to be materially different from any results, performance or achievement expressed or implied by such forward-looking statements. Forward-looking statements are not guarantees of future performance and are based on assumptions regarding present and future business strategies of Ammbr Foundation and the environments in which it operates now and in the future.

All subsequent forward-looking statements attributable to Ammbr Foundation, or any persons acting on its behalf, are expressly qualified in their entirety by the cautionary statements.

Ammbr Foundation expressly disclaims any liability in respect of the content of any forward-looking statement and also expressly disclaims any obligation or undertaking to disseminate any updates or revisions to any forward-looking statements contained herein or to reflect any change in their expectations with regard thereto or any change in events, conditions or circumstances on which any such forward-looking statement is based, after the date of this Whitepaper, except as may be required by law.

Diversity Statement

At Ammbr, we have created, and will maintain, an environment in which all of our people and partners can feel valued, included and empowered to fully contribute.

We recognise that each contributor's unique experiences, perspectives, and viewpoints across the Ammbr Foundation value chain are critical to creating and servicing products that engage and inspire stakeholders and participants. Therefore, our goal is to foster an environment that is an incubator for great ideas, is attractive to the best talent, and instills a profound sense of pride in the Ammbr Mesh Network.

Our diversity and inclusion efforts focus on:

- Inclusion of women at all business levels
- Leading and managing inclusivity – embracing different cultures, ethnicities, genders and sexual orientations
- Creating a work environment that fosters growth and advancement
- Engaging with our audiences in a way that reflects and respects their unique perspectives and experiences

Our diversity and inclusion objectives, and our progress towards achieving them, will be assessed annually to ensure they align with our business and talent objectives.

Directors' Declaration

We hereby declare that the Board has taken reasonable care to ensure that the information contained in this Whitepaper relating to Ammbr Foundation is in accordance with the Securities and Futures Act (Cap. 289) (SFA), applicable Money Laundering and Terrorist Finance regulations, and that the Directors take responsibility for the accuracy of such information.

We certify that to the best of our knowledge and belief, there are no other facts the omission of which would make any statement within this Whitepaper relating to Ammbr Foundation false or misleading and that we have made all reasonable enquiries to ascertain such facts and that this Whitepaper contains all the information required by law.

We confirm that none of the directors individually or with others, or in a company of which they were directors, has been involved in bankruptcy, liquidation or other regulatory prohibitions.

As directors, (being the persons set out in Part E of this Whitepaper under the heading "Team" "Directors"), we collectively and individually accept full responsibility for the accuracy of the information provided in this Whitepaper (but only insofar as it relates to Ammbr Foundation and only to the extent that the Board is required to accept such responsibility in terms of the Companies Act), and that all reasonable enquiries to ascertain such facts have been made and that this Whitepaper contains all information relating to Ammbr Foundation as required by law.

Benny Pang	**Derick Smith**	**Rakesh Rajagopal**	**James Lanshe**	**Kaustuv Ghosh**
Director & Chairman	Managing Director	Director	Director	Director
15 August 2017	15 August 2017	15 August 2017	15 August 2017	15 August 2017

Definitions and Abbreviations

3G	Third generation of wireless mobile telecommunications technology
4G	Fourth generation of wireless mobile telecommunications technology
5G	Fifth generation of wireless mobile telecommunications technology
Ammbr Foundation	The not-for-profit organisation formed to administer and govern the Ammbr Network and its assets
AML/CFT	Anti-money laundering/countering the financing of terrorism
Ammbr	The Brand of the Ammbr Foundation Pte Ltd
Ammbr Network	The mesh network built on the technology of Ammbr proposed and described in this document
AMMBR	The cryptographic token that enables micro-payments and the monetisation of the Ammbr Network
Applicant	A person who applies for offer tokens pursuant to the offer
Application form	The application form presented on the Ammbr website at www.Ammbr.com
API	Application Programming Interface
AQM	Active Queue Management
Backhaul	The backhaul portion of the network comprises the intermediate links between the core network, or backbone network and the small subnetworks at the "edge" of the entire hierarchical network.
Board	The Board of directors of the Ammbr Foundation
Closing date	The date of closing of the offer, which is on Saturday 30 September 2017 upon the mining of the 112,888th block of the Ethereum Blockchain after the start of the Crowdsale.
Companies Act	Companies Act (Chapter 50) (Original Enactment: «Act 42 Of 1967) Revised Edition 2006 (31st October 2006), as amended from time to time
Contribution	The amount paid in ETH or BTC to the receiving smart contract by an applicant in consideration for the issue and allotment of the offer tokens, which is the offer price multiplied by the number of offer tokens issued pursuant to the offer
Crowdsale	Unlike traditional crowdfunding, a Crowdsale doesn't pre-sell a widget, or promise to put your name in the credits of a movie. Instead, it sells you something that you might not know what to do with, unless you are clued in: a token. A token is an intrinsic component in a next-generation cryptocurrency 2.0 application.
Directors	The directors of the Ammbr Foundation, collectively the Board
Document	This public offer document and accompanying appendices
ETH	The cryptocurrency token of the Ethereum blockchain, called "ether", traded under the ETH acronym,
Financial Advisers Act (FAA)	Financial Advisers Act (Chapter 110) (Original Enactment: Act 43 Of 2001) Revised Edition 2007 (31st March 2007), as amended from time to time
Gb/s	Gigabit per second
GSM	Global system for mobile communications
GSMA	GSM Association – representing the interests of mobile operators globally, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem

Hashing	Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
ICT	Information and communications technology
IP	Internet protocol
IoT	"Internet of Things" or IoT is a term applied to devices, able to perform computation, and connected to each other and the Internet, allowing them to send and receive data.
ITU	International Telecommunication Union
KYC / AML	"Know Your Customer" or "Know Your Client" is the process of a business identifying and verifying the identity of its clients. The term is also used to refer to the bank and anti-money laundering (AML) regulations which governs these activities.
Licensed Spectrum	Broadly speaking, radio spectrum is divided into two types: licensed and unlicensed. Licensed spectrum includes frequencies that can be reserved for a specific use, and may be allocated, under license, by governing bodies in specific jurisdictions.
Listing date	Friday 1 September 2017, the date on which the offer tokens will be made available by the smart contract
LTE	Long-term evolution
M2M	Machine-to-machine
MAS	Monetary Authority of Singapore, the regulator of the currency and capital markets in Singapore.
Mesh Network	Mesh network is a network topology in which each node is capable of relaying data for others
Minor	A person who has not attained the age of 18 years
Non-executive director	A director who is not involved in the administrative, managerial or day-to-day operations of Ammbr Foundation
Number of tokens offered	Tokens shall be issued by Ammbr Foundation on demand for the entire duration of the offer period pursuant to the offer, where after no further tokens shall be issued, save for those expressly accounted for in this document, in perpetuity.
Offer	A public offer of the offer tokens by Ammbr Foundation as described in this document
Offer period	The period required for the completion of the mining of 112,888 blocks on the Ethereum Blockchain, during which the offer will be open for acceptance; the period opens at 12:00 pm on Friday 1 September 2017 and will close at approximately 12:00 pm on Saturday 30 September 2017.
Offer price	The price of ETH equivalent to USD 0.10 (ten cent) per offer token, set according to the quoted price of ETH on Coinmarketcap (https://coinmarketcap.com/) at 12:00pm on Friday 1 September 2017.
R&D	Research and development
QoS	Quality of Service

Securities and Futures Act (SFA)	Securities and Futures Act (Chapter 289) (Original Enactment: Act 42 Of 2001) Revised Edition 2006 (1st April 2006), as amended from time to time
Smart Contract	Smart contracts are computer protocols intended to facilitate, verify, or enforce the negotiation or performance of a contract.
SiGE Semi-conductor	SiGe, or silicon-germanium, is an alloy with any molar ratio of silicon and germanium, i.e. with a molecular formula of the form Si1−xGex.
SoHo	Small office-home office
Spoofing	Where one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.
Tbps	Terabytes per second
TEE	The Trusted Execution Environment (TEE) is a secure area of the main processor that is meant to guarantee code and data loaded inside to be protected with respect to confidentiality and integrity.
Token Offering	A formal sale of cryptographic tokens structured and executed through the use of so called “smart contracts” rather than conventional market intermediaries.
USD	United States Dollar
VoIP	Voice over Internet protocol
VPN	Virtual private network

Trademarks

Wi-Fi® Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®

Chairperson's Statement

On behalf of the Board it is my pleasure to present this White Paper in respect of Ammbr Foundation's public offer of AMMBR cryptographic tokens, the utility currency for a new, highly innovative mesh network technology.

The offer is intended to be in line with the global best practices for tokenized Crowdsales, as those standards continue to evolve at the present time. As integral parts of the overall structure described herein, we are striving to achieve sound corporate governance practices, high-level competency that enables significant enhancements to the Ammbr Mesh Network infrastructure and technology, and the ability to effectively and efficiently execute the strategic and operational imperatives described herein.

Ammbr Foundation's capital raising initiative through this Crowdsale is commensurate with the Foundation's core mission to further develop and strengthen the global telecommunications sector by enabling enhanced access to connectivity for virtually all citizens, recognizing that access plays a key role in driving of economic growth and socio- economic development.

Our approach is also designed to broaden financial inclusion among the less privileged segments of society, and to economically empower the many people currently constrained by the so-called "digital divide".

Efficient and reliable internet access has become critical to supporting the growth and development of any country. We believe that, upon introduction of the Ammbr Mesh Network, it will play a significant role in uplifting underserved communities and significantly increasing the overall quality of internet service to all.

Through our ongoing investment into both blockchain technology and mesh networking, we are committed to being a key contributor to the objectives of the United Nations Sustainable Development Goals (SDGs) to 2030.

The selection of Singapore as our jurisdiction of operations is made in recognition of the country's long-term growth potential.

This White Paper provides a significant amount of pertinent information on the offer, and I therefore urge you to read it carefully, including particularly the risk factors described herein, before participating.

On behalf of the Board I look forward to welcoming you as a potential user of the Ammbr Mesh Network.

Yours faithfully

Benny Pang
15 August 2017

Managing Director's Statement

On behalf of the management and the team members of Ammbr Foundation, I welcome you as a potential participant in the Ammbr Foundation's token sale. We are delighted that you are considering a contribution to the future of the Ammbr Mesh Network.

Ammbr Foundation is a not for profit organization headquartered in Singapore, which was established to manage and govern the development and implementation of the vision of a global mesh network that delivers fast internet connectivity efficiently, to a much wider population than currently enjoy the privilege of digital access. Ammbr Foundation is supported by a growing community of people and enterprises from around the world.

Ammbr Foundation follows policies for best practices and knowledge transfer, leveraging the global expertise of its team and supporters. Ammbr Foundation is well positioned to design, develop, manufacture and support innovative and affordable products and services to the highest standards of corporate governance. Extensive research underpins our work, and we see opportunity in the confluence of technologies and enormous market need.

Ammbr Foundation's vision is to fully democratize telecommunications and change lives through technology.

Ammbr Foundation is the culmination of years of leading edge development across different platforms, products, services and sectors, that has resulted in the formulation of the distinct and revolutionary solution presented in this Whitepaper.

The time has now come for Ammbr Foundation to move to public participation. This public token sale will bring essential capital infusion and broader engagement in the process of building out a global, distributed, and community owned telecommunications network.

The values and principles of egalitarianism and excellence that define the Ammbr Network bode well for a future where individual rights are unassailable.

Derick Smith
15 August 2017

Corporate information

Ammbr Foundation Pte. Ltd.

Registration number
201718209E

Postal address
Ammbr Foundation Pte. Ltd.
140 Robinson Road
#04-01
Singapore 051531

Registered office
531A Upper Cross Street
#04-95
Hong Lim Complex
Singapore 051531

Company secretary
Darren Ku Zhi You
531A Upper Cross Street
#04-95
Hong Lim Complex
Singapore 051531

Auditors
Pending

Financial year ends
31 December

Main bankers
United Overseas Bank Ltd.
396A Alexandra Road 17-00
Singapore 119954

Board of Directors

Director	Position
Mr Benny Pang	Non-Executive Chairperson
Mr Derick Smith	Managing Director
Mr Rakesh Rajagopal	Director
Mr James Lanshe	Director
Mr Kaustuv Ghosh	Director

Table of Contents

PART A

EXECUTIVE SUMMARY

Ammbr's vision is to build the world's largest fully decentralised, self-sustainable, wireless mesh telecommunications network using blockchain technology. Using this network, Ammbr will compete with centralised legacy telecommunications distribution models to provide universal fast Internet access. Backed by a multinational team with deep expertise in both wireless and blockchain technologies, Ammbr combines wireless advances with the emerging technology of blockchain to bridge the last-mile gap that traditional cable and telecom wireless systems handle poorly.

Each Ammbr unit (or node) consists of a core router capable of communicating across a mixed spectrum of wireless TCP/IP, Bluetooth, and IoT spectra - a first for router devices. Additionally, each unit has a built-in functional web server and data store that can host edge computing applications and support backless server support. This turns a network of Ammbr servers into a dedicated peer network that can connect to the Internet, making a mesh of Internet servers possible.

The global Ammbr network will be owned and operated by the owners of Ammbr wireless routers, offering users high-speed, low-cost internet access wherever they are within range of any Ammbr router. Each Ammbr mesh network node supports a firmware-based blockchain infrastructure, and will communicate with other Ammbr nodes to maintain the integrity of that blockchain. With this capability, an Ammbr network can be used to support wallet-oriented micropayment systems, secure contracts, and securely manage transactions. The broader the Ammbr network, the more robust these abilities.

Each Ammbr node operates autonomously in the order-driven market, which determines packet transit pricing in real time based on local network conditions. Internet access is billed and paid for in the native cryptocurrency of the Ammbr network, AMMBR. Node owners earn AMMBR tokens by providing wireless broadband connectivity to neighbouring nodes or roaming mobile users. The interconnected Ammbr routers also negotiate with, and pay each other for connectivity, in AMMBR.

Ammbr routers are autonomous, with only the router owners setting certain key operational parameters. A high level of security is provided to routers, their owners and their AMMBR wallets through a sophisticated digital identity layer, combined with the blockchain technology built into each router.

This public offer of the AMMBR cryptocurrency will raise funding for the ongoing development of the Ammbr network, manufacture of the Ammbr routers, and to support realistic deployment efforts for rapid global growth. The Ammbr Foundation will ensure all funds raised are used effectively to further the growth and the health of the network and its constituent parts globally.

PART B

THE RATIONALE FOR AMMBR

Introduction

Today, the Internet is a critical infrastructure that enables the digital economy, including remote healthcare, education, employment, e-governance, social networks, and more. As such, Internet access should be considered a universal utility[1] that is available to all. Although this vision is shared among major stakeholders, the reality of today's Internet and its level of digital inclusion is plagued by a persistent digital divide. Increasing geographic and socioeconomic challenges separate those with sufficient access to the Internet and those who do not have access. The reasons for this are diverse.

The Internet started off as a decentralised network, but has become increasingly centralised, with the vast majority of communications flowing through access and service infrastructures controlled by a relatively small set of corporations. The other estimated 3.9 billion[2] excluded individuals are dependent on these few providers to bridge the gap. Decentralisation of access capability is a form of empowerment, allowing for fairer participation. Decentralisation permits smaller players (e.g. local stakeholders) to offer wider inclusive access. It is widely acknowledged that decentralised telecom infrastructures could serve to connect the remaining 3.9 billion who are poorly served now.

At Ammbr, we are taking up the challenge of **enabling universal access to high-speed broadband for all**. To achieve this, we have an ambitious, yet realistic, vision of building the **world's largest decentralised, community-distributed, telecommunications network based on blockchain technology**.

Blockchain-controlled micropayments will incentivise and drive supply and demand.

The Ammbr Mesh Network Strategy

Mesh networking has long been imagined as a key ingredient in the future of a fully integrated world. However, the technology has not yet lived up to this expectation. **Open source mesh packet routing protocols** have made tremendous strides, with the Internet Engineering Task Force (IETF) spearheading several standardisations in this space. Additional improvements in various hardware technologies promise lower costs as well. Several additional frequency spectra are also now under consideration for unlicensed radio use.

Despite these advances, mesh network deployments have mostly been limited to free Wi-Fi initiatives to bring Internet connectivity to impoverished communities or remote areas with limited infrastructure[3]. Numerous successful community network initiatives across the world, such as the Guifi.net[4] in Catalunya Spain - which is currently the largest community network in the world.

Considering the massive potential of untapped users, mesh network technology could solve the accessibility problem. However, the **missing ingredient for widespread adoption has always been the issue of economic sustainability.**

---

[1] https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/%24file/15-1063-1619173.pdf

[2] Working Group Report 1: Enabling the Use of ICTs and Broadband: Understanding What Works to Stimulate ICT Adoption (November 2016) ~ Broadband Commission Working Group on Demand, with contributions from the ITU and telecoms industry players

[3] J. Saldana et al, Alternative Network Deployments: Taxonomy, Characterization, Technologies, and Architectures, IRTF GAIA RFC 7962, August 2016.

[4] Guifi.net, http://guifi.net/

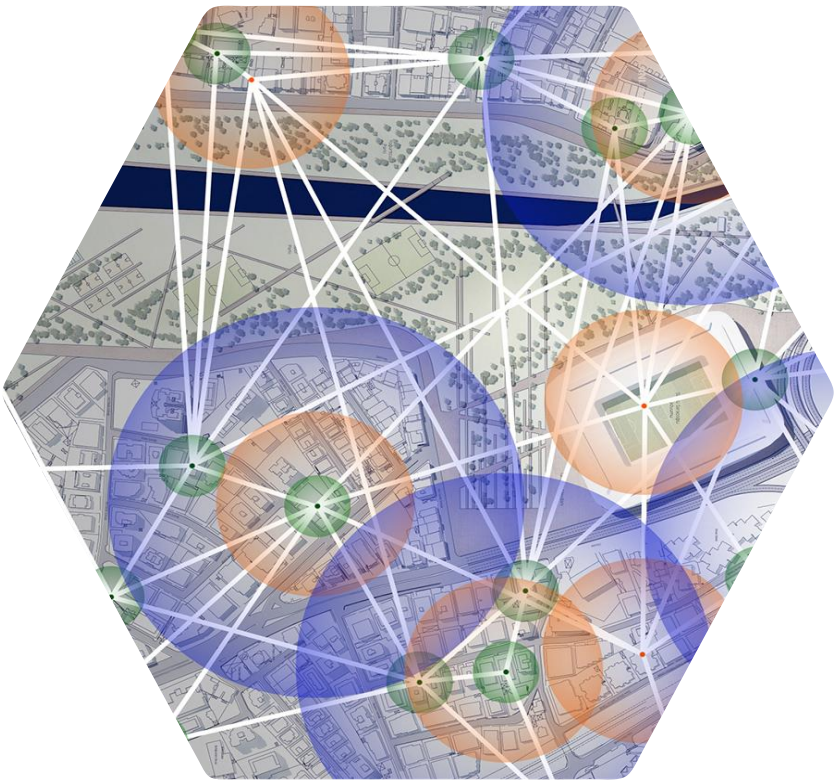
Ammbr **directly addresses this by adopting the sharing economy model for network access**, providing an economic incentive that allows users to share their unused bandwidth for profit. Monetising the free exchange of bandwidth, via a secondary market, allows for free market forces to drive network growth where it is most needed.

Why Mesh Networking?

A mesh network is a network topology in which each node is capable of relaying data for others. All mesh network nodes cooperate, and with each participating node, the reach, throughput and resilience of the network expand. When powered on, the mesh network node scans the radio spectrum to identify other nodes it can connect to. With sufficient incentives to participation, Ammbr can quickly grow to provide shared connectivity on a global scale. Considering the network effect of user-driven deployment, there are many reasons to suggest[5,6,7] this will transpire at a lower cost and higher rate than the current business models of centralized telecommunication providers allow.

Benefits of Ammbr mesh network:

- Low-cost: inexpensive Internet access
- Extremely flexible: multiple protocols and spectrum bands
- Resilient: self-healing and adapting
- More efficient: superior distribution for last mile connectivity and increased coverage



[5] Taknet: Community networking Thailand: https://blog.apnic.net/2017/02/17/taknet-community-networking-thailand/

[6] Zenzeleni: http://zenzeleni.net/

[7] Supporting the Creation and Scalability of Affordable Access Solutions: Understanding Community Networks in Africa, https://www.internetsociety.org/doc/cnafrica

Ammbr Mesh Technology

With the benefits and challenges of mesh networking in mind, we set out to develop a low-cost mesh networking appliance that elegantly addresses the requirements. The Ammbr wireless mesh device (an Ammbr node) behaves like a consumer-friendly Wi-Fi® router. However, under its skin, the device is effectively a multi-band heterogeneous mesh hub device extending connectivity well beyond the common Wi-Fi® range of 150 feet. Due to the variable and automatically selectable basket of radio spectrum bands and communications protocols, an Ammbr node can work efficiently over several kilometres, subject to regulations and local conditions.

Additionally, optional hardware modules can be mixed and matched to support a multitude of frequency ranges and protocols, dependent upon its operational circumstances.

Envisaged Series 1 Ammbr Modules

Base Wi-Fi® module

- Includes basic license-free Wi-Fi® support compliant with full suite IEEE 802.11 standards operating on the 2.4GHz ISM band including channel 12 &13 for Australia / Europe as well as through channel 14 for Japan. Wi-Fi® support at the 5GHz
- U-NII band is also provided
- Display indicating:
    - Network status
    - Number of users
    - Ammbr token balance
- Blockchain consensus protocol chip
- Internal antenna, GPS receiver & Full Suite Bluetooth
- Modular connectivity bus, external antenna jacks, RJ45 connector & USB C
- Power supply

Low-frequency module(s)

Support for sub 1 GHz IoT and obstacle penetrating spectrum with long range capability. Future support for the following:

- White Space spectrum support, from 470 MHz to 790 MHz with support for spectrum aggregation
- 902 MHz to 926 MHz
- Zigbee protocol @ 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA & Australia
- Dash7 protocol @ 433 MHz, 868 MHz and 915 MHz unlicensed ISM band/SRD band[8]
- LoRa license-free 169 MHz, 433 MHz, 868 MHz in Europe and 915 MHz in North America
- Sigfox ISM band at 902MHz in the US and 868MHz in Europe

3.5 GHz range module

Citizens Broadband Radio Service (CBRS) (currently only expected to be available in the US, although others are watching this shared-spectrum approach closely, and may adopt broadly-similar models in future)

5.5-6 GHz module

Shorter range, higher throughput LTE-U (unlicensed)

Commercial LTE module operating on licensed spectrum

Blockchain computing resource module

Processor, Memory & Hard Drive for smart contracts, cloud storage and network cache scheme

Mobility module

Lithium-ion battery, solar panel, all-weather enclosure for mobile usage or installation where power supply fluctuates

[8] 433 and 868 are not restricted to a particular protocol, they might have restrictions in terms of maximum duty cycle, and lower transmission power than in higher bands.

Mobility Considerations

Mobility is inherently supported by Ammbr's routing protocols - abstracting the Ammbr network into a single layer 2 collision domain. Thus, from the user perspective the entire mesh will look like a single LAN. The Ammbr network allows a device to quickly identify nearby Ammbr routers that are available for roaming, assuming there are no coverage gaps between Ammbr routers. When the signal strength of the current Ammbr router weakens and the device needs to roam to a new Ammbr router, it will already know the best candidate Ammbr router to connect to. Ammbr routers will also support several advanced mobility features including Client tracking, PMKSa caching, Opportunistic Key Caching (OKC) as well as supporting 802.11e, 802.11k, 802.11v and 802.11r.

Antenna Considerations

The Ammbr device is not limited to the physical constraints of a mobile phone, a single antenna per frequency channel can be used. This simplifies the antenna development process, as multi-band antennas are challenging and often not as efficient. The Ammbr router includes Omni-Directional and possibly Uni-Directional antennas.

- Helica, an external antenna, will be used for point-to-point links to enhance stability and provide higher throughput, as Signal-to-Noise ratio may significantly increase.
- Signal polarization with the goal of improving spectral efficiency.
- MIMO-OFDM designs are also being considered, although mechanically it can be more challenging due to the array of antennas needed.
- Multi point Beam forming antenna design which allows available radio energy to be directed towards a particular direction at the expense of omnidirectional coverage. This allows for better connections to a primary point of contact available to the node.

The Helica External Antenna

Routing

Ammbr is developing a unique routing protocol that will extend the BMX7[9] - a routing protocol which offers very advanced features (with security routing extensions) and a small network overhead calculating routes that fulfil following constraints.

- transit pricing optimisation
- maximum number of hops
- maximum end-to-end delay requirements

Ammbr will also support Better Approach to Mobile Ad Hoc Networking (B.A.T.M.A.N.) Advanced[10] (as default) - a Layer 2 routing protocol, which creates a bridged network and allows for seamless roaming of clients between wireless nodes.

In addition, Ammbr routers will also support several other traditional routing protocols as well as the multi-path routing protocols mentioned below

- Border Gateway Protocol (BGP)[11] with its well-studied behavior and scalability
- Open Shortest Path First (OSPF)[12] protocol
- Optimised Link State Routing (OLSR) Protocol v2[13]
- BatMan-eXperimental Version 6 (BMX6) protocol[14], which is based on IPv6 and tries to exploit the social structure of Community Networks
- Babel[15] is a Layer 3 loop-avoiding distance-vector routing protocol that is robust and efficient in wireless mesh networks
- Multipath OLSR[16]: Modifies OLSR to support multipathing
- Joint Multi-channel Multipath (JMM)[17]: Splits traffic among different channels at different times over multiple paths

[9] http://bmx6.net/projects/bmx6

[10] D. Seither et al, "Routing performance of Wireless Mesh Networks: A practical evaluation of BATMAN advanced", LCN, October 2011.

[11] Y. Rekhter, et al., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[12] J. Moy, "OSPF Version 2",RFC2328, April 1998.

[13] T. Clausen et al, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

[14] A. Neumann, A. et al, "An evaluation of BMX6 for community wireless networks", WiMob, 2012.

[15] J. Chroboczek, "The Babel Routing Protocol", RFC 6126, April 2011.

[16] M. Kun et al, “The research and simulation of multipath-OLSR for mobile ad hoc network, ISCIT 2005.

[17] W.-H. Tam and Y.-C. Tseng, “Joint multi-channel link layer and multipath routing design for wireless mesh networks.” IEEE INFOCOM 2007.

The Ammbr Blockchain Strategy

Introducing a blockchain for easy and trusted peer-to-peer management

Management: a use case for blockchain

Ammbr provides a very interesting use case for blockchain; decentralized and trusted management of added resources (bandwidth of WIFI) for large communities. The efficient use of the state-of-the-art cryptography ensures security of this management system. There are two levels of secure cryptography. First, Ammbr employs cryptographic primitives for hash functions and digital signatures, in order to both uniquely identify documents and authenticate these documents as coming from the known originator. Beyond this, secure timestamping identifies when the transaction occurs; one of the central roles of the blockchain. These employ Merkle-tree Blocks to aggregate streams of data.

Blockchain: the basis for strong security

Blockchain is a cryptographic tool and has to be considered as a utility. Blockchain was first designed for timestamping digital documents, i.e., adding a true secure and trusted timestamp to a document. Time is not an easy variable to be registered digitally and the best way to do it is to include each event in a chain of events in a public way. In 1990, Haber and Stornetta[18] did that with a trusted-third-party while publishing the results (the hashes of the documents) in a journal (NY Times). Soon it was proposed by Josh Benaloh[19] for use in a voting system. Haber proposed and patented a version of his blockchain using decentralized system (peer-to-peer), and a first experimental version was implemented in Belgium in 1997 (project TIMESEC). A notable research report from the bank of Japan in 2001 [20] highlighted the importance of decentralized timestamping and it is nearly sure that report was the trigger for the proposal of bitcoin: the report was challenging the establishment with the idea of decentralized systems for financial management. These were in turn cited by the inventor of blockchains and Bitcoin, who used these to build a secure distributed ledger system.

Securely adding (or removing) members in a blockchain community is very important: the goal is to avoid fake identities or multiple identities in such a peer-to-peer network (known as a “sybil attack”).[21,22] An elegant solution to this form of attack is handled by the blockchain part of bitcoin in the form of a lottery (cf. Consensus, below). A decentralized lottery with only peer-to-peer interaction was not easy to implement. One solution to this, the “Chinese Lotto”, made each chip a participant. Ammbr makes use of a variant of this approach.

The Ammbr proposal follows best possible practices and standards for the security of the cryptographic algorithms, keys, generators, and distribution processes. Additionally, Ammbr makes provisions for extended life cycles, with surety of unique keys now viable on a scale of centuries. Quantum computing may present a challenge to such systems, though it is also likely that, should that happen, quantum encryption itself will also evolve to provide a solution. Ammbr will continue monitoring research in this area.

Finally, the security of our hardware for protecting the secret keys and the computations, when needed, will

---

[18] S. Haber, Stornetta: “How to timestamp a digital document”, Journal of Cryptology, January 1991, Vol. 3, Issue 2, pp 99–111 (first presented at CRYPTO ’90). (see also patent US 5136647 A)

[19] J. Benaloh, M. de Mare: “Efficient Broadcast Time-Stamping”, TR from Clarkson University, 1991/1992 https://www.microsoft.com/en-us/research/wp-content/uploads/1991/01/tss.pdf

[20] M. Une: “The Security Evaluation of Time Stamping Schemes: The Present Situation and Studies”, Discussion Paper No. 2001-E-18, Institute for Monetary and Economic Studies, Bank of Japan, Tokyo

[21] https://en.wikipedia.org/wiki/Sybil_attack

[22] John R. Douceur. 2002. The Sybil Attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems* (IPTPS '01), Peter Druschel, M. Frans Kaashoek, and Antony I. T. Rowstron (Eds.). Springer-Verlag, London, UK, UK, 251-260

take into account the state-of-the-art evaluations including all side-channel attacks when needed.

Consensus

Consensus protocols are the defining quality of any blockchain platform. An effective consensus protocol should ensure the fair distribution of block leadership authority across a large number of qualifying node participants. The most proven consensus protocol is called *Proof of Work* (PoW), which is used in the two largest blockchains to date, Bitcoin and Ethereum. PoW requires participants to spend significant computational resources in order to earn a chance to be named the leader of a block.

PoW is effective and ensures that network authority is only exercised by participants that have expended an effort which cannot be faked or duplicated. To overcome the network, an attacker must do more than 50% of the work done by the entire network to have any effect. The difficulty of this feat provides the underlying security for a PoW blockchain model.

However, PoW has several undesirable traits.

- The computationally intensive process precludes use in mobile, edge or IoT computing applications.
- The large-scale resource (electricity) inefficiency of Proof of Work is often decried as socially irresponsible.
- The high cost of acquiring useful PoW hardware limits adoption.
- Successful PoW mining depends on efficiencies of scale. This ultimately incentivizes consolidation of nodes into a small number of very large institutional miners using proprietary data center designs, exotic hardware & government subsidized power. This centralization of majority block authority into such a small group - less than 50 in the case of bitcoin - is a growing security risk of colossal scale.
- PoW consensus generally requires longer block times as compared to other methods that don't require the processing time needed to find the result of a proof of work operation. Longer block times make it more difficult to improve transactional throughput in a blockchain design.

Although there are several other consensus models to consider, *Proof of Stake* (PoS) is particularly useful to review because it's been a popular proposed alternative to PoW due to it not requiring costly computational resources.

PoS instead establishes consensus by choosing a member of the blockchain to be the block leader based on their possession of tokens. However, PoS also has several undesirable traits. The arguments against PoS are:

- The 'apathy' problem where participants have to endure no ongoing burden in order to vote. In the case of a consensus failure for example, they have nothing to lose by voting for multiple blockchain forks which prevents the consensus problem from ever resolving.
- PoS consensus rewards those with big wallets by giving them a proportionally improved voting power. This process acts to not only enrich those with more capital, but in doing so it continues to increase their voting power in a trend that ultimately works counter to the objectives of a distributed security model.
- PoS schemas have a built-in attack vulnerability whereby an abandoned wallet from an early block, which previously had a large quantity of tokens, can be used to craft a 51% attack by reconstructing the blocks from that point up to the current block and forcing a takeover of the target blockchain with ongoing 51% authority.
- Since the token holdings (stakes) are publicly known, each node can predict with some accuracy which token account is likely to win the right to be selected as a leader, and forge the next block.

A final consensus method to consider is Proof of Elapsed Time (PoET) model developed by Intel's Sawtooth Lake blockchain research project, which has merged with the Hyperledger platform. PoET works by using the TEE portion of common SGX enabled Intel processors to establish a trusted entity from which to interact with the blockchain. Timestamps are used to determine a block leader while maintaining reasonable expectations of security. PoET consensus is very light on computing resources as compared to PoW and it's more fairly distributed a selection system as compared to PoS.

- Although PoET has been well received by the blockchain community, some criticisms remain. Since the security depends on the integrity of the TEE, the commonality of the TEE hardware used is a security risk. SGX based TEE's are built into virtually every new Intel processor made today. Should an exploit be found, an attacker could simply employ an infected botnet - with standard Intel processors - and overwhelm blockchain consensus with a 51% attack.
- PoET depends on TEE - Trusted Execution Environment - security which has been compromised in ways that are publicly known and, of more concern, perhaps in ways not yet known. For example, TEE security used by the entertainment industry was compromised by hackers through DMA exploitation which resulted in billions of dollars in loss and the end of the global DRM standard. TEE is not immune to back doors built into processors. An example of this is the undocumented backdoor in the Microsemi ProASIC3 which was only discovered through complex pipeline emission analysis. Intel itself recently announced a flaw in its processors that has allowed undetected remote access for the past 7 years via Active Management Technology.

PoET/PoV (Proof of Elapsed Time / Proof of Velocity)

PoET/PoV is a hybrid evolution of Intel's sawtooth lake consensus model and a Proof of Work variant called *Proof of Velocity (PoV)*, which together can be used to establish blockchain consensus.

PoV is a method of proving node authenticity with a speed-based Proof of Work challenge where a qualifying response can only come from a custom high-speed silicon-germanium semiconductor designed specifically for this purpose. Ammbr is using this for its Blockchain consensus manager to calculate the result. Our >300 Ghz F_{max} node chip can respond within *micro*-seconds to calculate results, compared to an Intel i7 processor which might take 12 hours to do the same. In order to prevent spoofing, it's PoV algorithm is memory sequential so that it cannot be broken down and parallelized by multiple computers, who might attempt to achieve the required speed by clustering. Failure to respond in the allotted time and with the correct answer invalidates the node keys, and prevents a hacker from affecting the network. This PoV method sets a very high bar for node security.

Ammbr's consensus model combines both PoET and PoV into its custom semi-conductor along with internal PKI capability which is used to enroll itself in PoET consensus work.

- The public key is presented to the Ammbr blockchain for node identification.
- The blockchain attempts to validate the node by sending a time stamped and encrypted PoV challenge to the node's private key.
- The node processor responds with a signed, encrypted and time stamped PoV answer.
- The blockchain accepts the node validity and lodges it's public key in the blockchain

Workflow

The workflow begins with a purpose built SiGe semiconductor present at each node. It cryptographically signs a time elapsed proof that is verified by the central authority and cannot be faked or counterfeited. The block creator is authorized to create the next block in the chain. Through the PoET mechanism, each node is randomly selected by determining who has the shortest wait time to create the block.

Wait times are determined randomly and distributed to all participating nodes. Upon receiving their wait time, each node goes into an idle condition for the predetermined amount of time, periodically with the node querying the server (or vice versa), in order to determine if it is ready for a new block to be created. This happens when the current leader submits a valid block.

If it is time for a new block to be created, each node declares how much wait time they have been allocated. The node with the shortest wait time remaining is declared the new leader. That leader will then be tasked with generating the next block, and the cycle repeats.

Cheating is prevented through cryptographic messages passed between the server and the node, verified through a trusted computing portion of the cryptographic hashing chip. As an added security measure, the server can request a proof of speed validation from any given node. The node is given a complex mathematical problem that is specifically designed for the custom silicon on the chip, at which time the chip should be able to rapidly produce a result that would take a general-purpose CPU or GPU orders of magnitude longer to calculate. The node will respond in a given time frame with the correct answer or it will be marked as a counterfeit node and future work rejected.

Why is the PoET / PoV hybrid effective?

PoET is a power efficient and fair solution to consensus. However, its reliance on common Intel processors and the presumed safety of Trusted Execution Environments, is a risk that cannot be reduced to zero. In case another flaw would be detected, it would be trivial to mount a 51% attack using a botnet of common Intel computers as security would then be reduced to an exposed secret.

In cases where security is based on secrets, for example in the context of encryption keys or a TEE environment, the exposure of the secrets would result in no recourse. On the contrary, with a proof of work element that cannot be copied or simulated, security would in principle never be lost. Hence the reason for its importance as a consensus mechanism. Proof of Velocity (PoV) provides such proof of work element for Ammbr. It does so without the wasteful resource, e.g. electricity expenditure, which prevents PoW from being used in mobile, edge and IoT computing. Instead, PoV only runs when validation is requested as opposed to in perpetuity.

PoET / PoV pseudocode walk-through

```
// We need to have a Pair of Public-Private key generated in advance.
Byte[] OurOwnPublicKey;
Byte[] OurOwnPrivateKey;

// We also need to remember servers PublicKey, generated specifically for us
// and may only be valid during this session
Byte[] ServerPublicKey;

// We need to know the server-address(s) for DAO. This is the server for PoET
// (proof-of-elapsed-time) communication. At first step, we need to obtain
// a dedicated public key which can be used to encrypt communication between DAO
// and Node (which helps prevent various types of attacks as well)
String ServerAddress = "192.168.0.1";

// Request a Proof-Of-Velocity from DAO Server. Our request is sent as Plain-Text, but the servers
// response will be encrypted using our public-key which we provided here. This ensures that only
// no one will be able to understand the response (as it will contain a key that we'll be using to
// encrypt our communication from this point on with the server).
var encryptedChallengeRequestResponse = RequestProofOfVelocityChallenge(ipAddress,
OurOwnPublicKey);

// First decrypt the response
var decryptedChallengeRequestResponse = RSA_Decrypt(encryptedChallengeRequestResponse,
OurOwnPrivateKey);

// Server responds with a Proof-Of-Velocity challenge, plus a public key we'll be
// using to encrypt our messages sent to DAO. We need to remember this key...
ServerPublicKey = decryptedChallengeRequestResponse.ServerPublicKey;

// Send the challenge to our ASIC
Byte[] solvedChallengeResponse =
ASIC_SolveChallenge(decryptedChallengeRequestResponse.ChallengeByteStream);

// Encrypt the challenge-solution and send to server. If server accepts, we can officially start
// our operation...
Byte[] encryptedAuthRequest = RSA_Encrypt(solvedChallengeResponse, ServerPublicKey);
var authRequestResponse_Encrypted = SendChallengeResposne(ipAddress,
encryptedAuthenticationRequest);

// Decrypt response first (server will encrypt it using the key we provided earlier)
var authRequestResponse_Decrypted = RSA_Decrypt(authRequestResponse_Encrypted,
OurOwnPrivateKey);

// If everything is OK, Server has responded back with Success, and will respond to our
// PoET requests from now on.
If (authRequestResponse_Decrypted.Status != SUCCESS)
{
   // Server rejected our request. Something must have gone wrong.
   // We need to abort at this point.
   Abort();
}
// We enter the program loop (repeatedly asking for PoET). Whenever chosen as leader,
// we will attempt to sign the given block and commit it to the network.
while (application_is_running)
{
   // Note, our request will be encrypted using the PubKey given by the server prior
   // to dispatch. What server returns will also be encrypted and needs decryption
   var requestPoET_encrypted = RequestPoET(ipAddress, ServerPublicKey);
```

PoET / PoV pseudocode walk-through cont.

```
// Decrypt response
    var serverPoET_Decrypted = RSA_Decrypt(requestPoET_encrypted, OurOwnPrivateKey);

    // We now need to wait for as long as the server has asked us to

    Delay(serverPoET_Decrypted.WaitTime);

    // Check if we are the leader

    // ...

    // ...

    // ...

    if (we_are_the_leader == false)

    {

        // Simply repeat the loop

        continue;

    }
    else

    {

        // We now sign the latest block and dispatch it to the network block

        // ...

        // ...

        // ...

    }
```

Ammbr Node ASIC

ASIC functions:

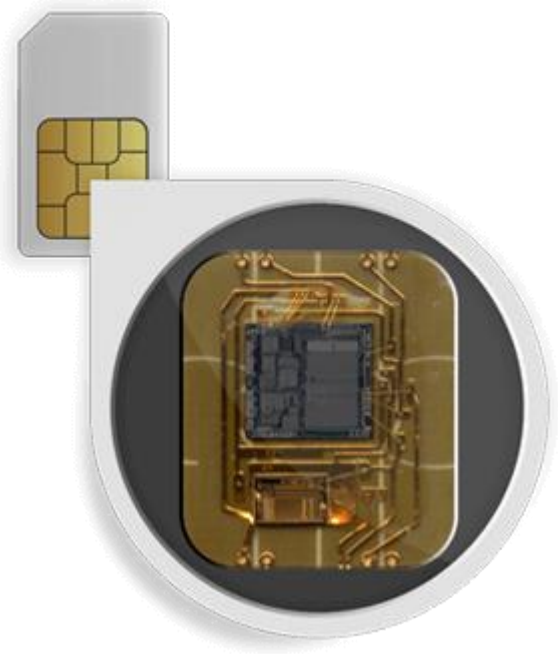
- PKI (Public Key Infrastructure)
- PoET (Proof of Elapsed Time)
- PoV (Proof of Velocity)

The SiGe chip will contain a very high-speed SHA2 (256Bit) digest function, operating at >20GHz F_{max} and one-hundred million rounds (approx. 5ms) vs. a computer CPU which would take approximately 1,000ms minimum to perform the operation.

As the digest function cannot be parallelized, the high frequency of the chip, combined with the high number of rounds, validates the authenticity of the client that is able to solve the challenge in the limited timespan allowed (e.g. 10ms).

This operation will be extremely time-consuming when executed on general-purpose CPUs, GPUs, FPGAs or even Silicon-based ASICs, as they are unable to match the SiGe clock-frequency.
Form factors:

- SIM Card
- MicroSD
- QFN surface mount 'chip' for general electronics SMT
- USB



Technology development

Low cost mesh hardware is the key to universal market adoption. Accordingly, the Ammbr hardware development team has clearly mapped a development path that commences with off the shelf transceiver protocol stacks, before ultimately migrating to its own proprietary multi-frequency / multi-protocol full spectrum chip. Although development of the full spectrum chip is expensive, once complete it will be possible to produce devices at a very low cost.

First generation

Ammbr's first generation mesh networking device will compete on cost and features with common state-of-the-art Wi-Fi® routers. Current off-the-shelf transceiver chips supporting the required basic protocols allow us to design and manufacture a low-cost product at a target price of $79 US. However, this is for a base Wi-Fi® module alone. Add on modules supporting additional frequency ranges require chipsets that are typically more expensive than commodity Wi-Fi® solutions.

Second generation

Ammbr's 2nd generation product will be based on a newly developed chipset of our own design, supporting a full collection of spectrum bands and protocols in a single CMOS design. Once complete, it will be possible to construct a highly purpose specific and capable mesh router at a considerable low cost. As a result, instead of users collecting several Ammbr node platters with each supporting a different protocol or frequency, a single base station would then cover all, at an estimated cost of no more than $50 US.

Ammbr's Security Strategy

A variety of security considerations and defences are built around different aspects surrounding mesh network, blockchain and relevant economic components. Most are resolved through the application of self-sovereign digital identity, a topic beyond the scope of this document. We encourage readers to familiarize themselves with the topic by reading the excellent work being performed by several organizations[23]. And individuals[24] [25].

On the Ammbr Network, participants, the owners of Ammbr mesh routers, as well as users, would use digital identities which they themselves create and exercise full control over, in order to gain access to network resources or interact with digital identities of others. This decentralized schema would provide extensive opportunities to lock down most of the vulnerabilities that we face online.

As a result, the ability to access and set parameters of any Ammbr mesh router will only be under the control of its owner. Without access to the private key used by its owner, it would be impossible to compromise or hack a specific router. Private keys are also intrinsic to the inclusion of particular devices that participate in the global consensus model of the Ammbr blockchain.

The distribution mechanism for firmware updates, distributed to Ammbr mesh routers, is also closely tied to the digital identities of the originating developers and the Ammbr Foundation. Any attempt to inject false firmware updates would therefore be rejected.

Such would be of particular importance considering attacks such as IMSI interception, tracking and using exploitations such as Karma[26] and Lure10[27]. To further mitigate against attacks aimed at mobile devices, the Ammbr client application would rely on the pseudonymous identification of users and their devices, removing potentially damaging information from the connection and handover protocols.

Another threat that is of great concern is the distributed denial of service (DDOS) attack. As a distributed network, Ammbr has the potential, if compromised, to be a potent tool in the hands of would-be attackers using this methodology. Conversely, Ammbr would be a powerful tool that can be utilized in order to identify and isolate sources of DDOS attacks.

Ongoing work in this area will allows us to state with confidence that the Ammbr Network will establish itself as a platform for safe and secure online interactions.

Marketplace Economics

Blockchain

Blockchain has been widely touted as a panacea for many ills. Despite the fact that the technology is considered as complex, its suitability has become apparent for following reasons.

- A means to agree on a singular version of a fact that many unrelated parties subscribe to
- An extremely high resiliency to untraceable changes, creating effectively immutable data

[23] www.sovrin.org
[24] http://www.windley.com/
[25] https://www.coindesk.com/path-self-sovereign-identity
[26] https://repo.zenk-security.com/Protocoles_reseaux_securisation/Attacking%20Automatic%20Wireless%20Network%20Selection.pdf
[27] https://conference.hitb.org/hitbsecconf2017ams/materials/D1T4%20-%20George%20Chatzisofroniou%20-%20Exploiting%20Windows%20Automatic%20Wireless%20Association%20Algorithm.pdf

This capability underpins a growing range of use cases that are being proposed and tested in the market by the industry.

The first and most thoroughly tested use case has been Bitcoin as a double-spend resistant currency of exchange.

Cryptographic Exchange of Value

The means of value store and exchange on the Ammbr Network is AMMBR, a cryptographically derived token, that prevents double spending. A number of these AMMBR tokens will be created and distributed to a broad audience during the Ammbr Crowdsale. AMMBR tokens will be purely for the purposes of payment for internet connectivity and associated services on the Ammbr Network and do not confer rights or privileges beyond this function.

Ownership and management of the AMMBR tokens will be through the use of secure digital wallets.

Value Creation

Mesh Scalability

Mesh networks have many advantages, with lack of scalability so far being a limiting factor in applicability. With the increase of the number of nodes with the growth of a mesh network, functionality of the network is often compromised. This drag occurs because of both protocol overhead and the inability to offload packet congestion. In some circumstances protocol overhead disproportionately grows relative to the overhead of carrying the data itself. Collisions, timeouts and a full halt to all packet routing can occur. These scaling problems are almost impossible to overcome in a standard mesh network because there are no alternate pathways or protocols to relieve the congestion. In particular, a regular stand-alone mesh network operating with a single protocol over a single spot on the radio spectrum will simply not scale well.

On the contrary, the Ammbr mesh network was conceived as a robust global network without these traditional mesh technology limitations. In this respect, Ammbr network displays following features.

Multipath

Ammbr operates simultaneously across multiple protocols and frequency bands of the radio spectrum. It supports path as well as link diversity. Multiple paths can potentially be resource pooled to route and forward packets. It can also be used either simultaneously or in a backup configuration, for increased reliability, end-to-end throughput, network efficiency and fault tolerance[28].

Backhaul

Ammbr is designed to reduce the required number of hops to as low a number as possible. Such is best achieved by providing a direct high-speed route to the backbone from as many points in the network as possible, which would represent the network's backhaul. The network's backhaul would predominantly be supported by its users connecting, or bridging, their Ammbr routers to existing home and SoHo broadband routers. Alternatively, in the case of for larger Ammbr networks, through interconnecting, or peering, to exchange points. It is also envisioned that several Ammbr networks would be peering with each other directly, thus localising network traffic.

Flexible bandwidth support

Ammbr will pioneer the notion of flexible bandwidth in cases where Ammbr users, by means of additional AMMBR token micropayments, would acquire higher bandwidth for a specific period of time, when required.

[28] J. Qadir et al, **Resource Pooling for Wireless Networks: Solutions for the Developing World,** ACM SIGCOMM CCR, November 2016.

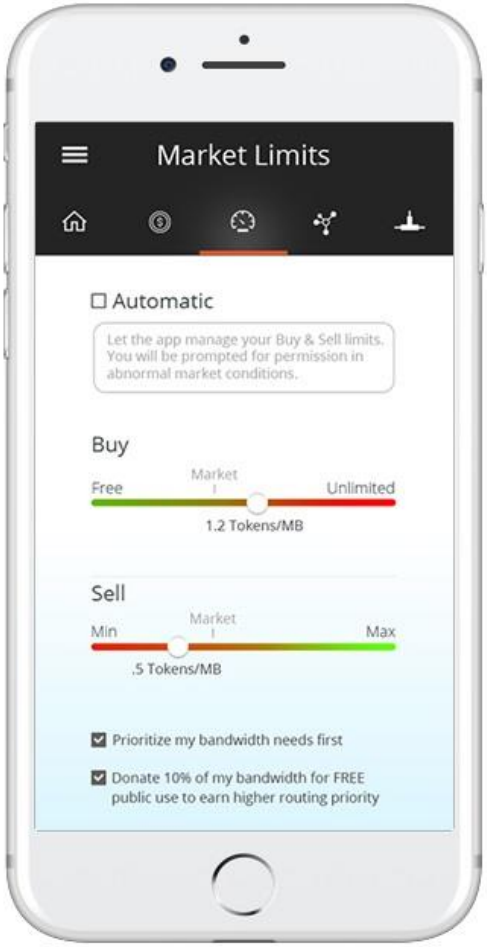
Market forces

The Ammbr bandwidth market would solve congestion problems by means of the automated setting of higher prices resulting from high demand. High prices in a particular zone would attract node operators seeking higher returns. Analytics will be provided to indicate where infrastructure can be added, as well as the type of infrastructure likely to earn most traffic. As a result, market forces attracting infrastructure deployments where needed would then realise the exponential scaling of the network. (Note. Over time a variety of pricing models are likely to emerge from the infrastructure operators themselves, and a variety of subscription and other packaged forms will offer more choice. This is beyond the scope of this document.)

Sustainable Usage Model and Incentives

Bandwidth market exchange

The Ammbr bandwidth marketplace is designed as an open and autonomous exchange for trading Internet connectivity using AMMBR as intra network micropayment medium of exchange.



Ammbr app showing market settings configuration

Participants, owners of the Ammbr routers, may opt to allow their routers to adjust the purchase and sell pricing automatically. Equally, through advanced settings, a direct control can be achieved for the execution of a preferred strategy.

Mining revenue

Each Ammbr wireless node is a fully operational node in the Ammbr (blockchain) network. Nodes are authorised to participate in blockchain consensus processes via their PoET/PoV semiconductors. Occasionally, nodes are identified as block leaders and are rewarded in AMMBR, which are funded by a portion of market transaction fees.

Governance

The Ammbr Foundation is tasked with the governance aspects of the Ammbr network. This covers a relatively broad range of particularities and can be defined by the ensuring of a fair and open participation by participants, infrastructure owners, and users in a secure and sustainable marketplace economy. The Foundation will decide, through consultation with all stakeholders and experts in the field on the rules set and delegation of tasks, in alignment with the stated goal of growing the world's largest and most inclusive wireless mesh network.

The Ammbr Foundation will reward its directors according to market related compensation standards.

In the long term, the Foundation would strive to achieve a broader and more direct participation of stakeholders through a possible related tokenisation and automation. The mechanisms of a proposed Distributed Autonomous Organization (DAO) could be a likely method of achieving such. However, this technology should first mature sufficiently before being initiated.

Trends Analysis

Cyclical Economic Model

The economic viability of the introduction of the Ammbr network proposition is based on a purposed early market seeding and targeted geographical expansion model. It is of necessity a project that has to scale up fast in terms of geographic space occupied. Based on trends from a number of sources, Ammbr has identified 23 high-potential markets suitable for early adoption. These collectively have close to 763 million Internet users. The identified markets are respectively Argentina, Australia, Bangladesh, Canada, Chile, Colombia, Costa Rica, Denmark, Finland, Ghana, India, Indonesia, Ireland, Latvia, Lithuania, Norway, Philippines, Singapore, South Africa and Sweden. Russia and China are left out for obvious reasons. The USA and UK are considered to be somewhat more difficult to enter. The markets chosen stand out for following reasons.

a) Basic Internet availability
b) Countries with high numbers of mobile subscribers and mobile broadband subscribers
c) Internet penetration percentage points to a lot of room for growth
d) Some of these markets have relative high levels of economic prosperity (Scandinavia, Australia, Singapore and the Baltics), a history of cutting edge consumer-centric innovation (Scandinavia, Finland, Baltics), size (India, Brazil Indonesia) and representative of moderate all-round success (Argentina, Colombia, South Africa, Ghana)
e) These are also countries that have at least one globally recognised megalopolis or well-regarded metropolis

We regard Japan, Kenya, Uganda, South Korea, Kuwait and Nigeria as the most difficult to enter, due to systemic issues or historical difficulties in market-entry.

Comparative Analysis

Recent years have witnessed several initiatives across the globe on enabling Internet access[29]. There are several successful alternative network[30] initiatives across the globe that have emerged in the last decade with the aim of bringing Internet connectivity to people or providing a local communication infrastructure to serve various complementary needs and objectives[31].

The problem of expanding Internet access has also received significant attention from the industry, especially organisations such as the Google, Facebook and Microsoft all touting novel solutions in this space[32]. Facebook has been spearheading innovations in open source cellular networks focused on addressing the rural, small cell markets via the Telecom Infra Project, while also looking at airborne solutions such as using drones for providing Internet access in hard to reach areas. Recently Facebook have started Express Wi-Fi® projects, mostly collaborating with existing Wireless Internet Service Providers (e.g. AirJaldi in India). Google has also been exploring airborne solutions such as the Google Balloons while Microsoft is pushing TV White Space (TVWS) based Internet access in rural areas.

Kenyan startup BRCK has built a waterproof, solar-powered Wi-Fi® box supporting several backhaul technologies as well as providing localised content. There are also initiatives such as the FON which uses the concept of crowdsharing Internet access that has been extremely successful with more than 20 million hotspots across the globe.

Solving the problem of universal Internet access requires a multitude of solutions and Ammbr intends to be a major player in this space with the ambitious goal of building the **world's largest decentralised, community-distributed, telecommunications network based on blockchain technology** -a first of its kind in the telecommunications industry. The unique selling points of Ammbr bringing together multiband meshing capabilities with novel blockchain technologies for solving the economic sustainability challenge will ensure Ammbr is well positioned to be a major player in the game of universal service provisioning.

[29] Closing the Access Gap: Innovation to Accelerate Universal Internet, https://www.usaid.gov/sites/default/files/documents/15396/Closing-the-Access-Gap.pdf

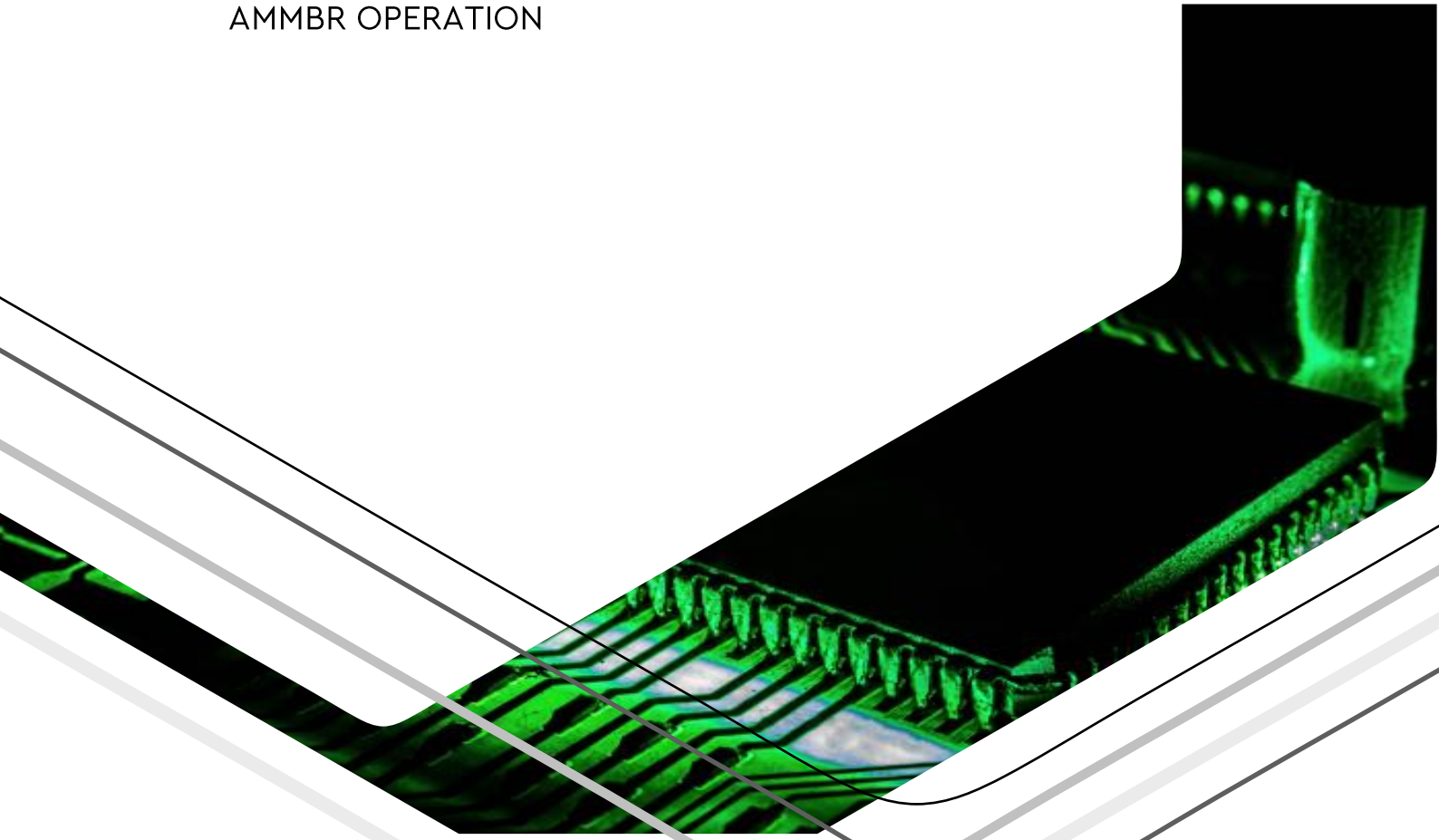
[30] J. Saldana et al, Alternative Network Deployments: Taxonomy, Characterization, Technologies, and Architectures, IRTF GAIA RFC 7962, August 2016.

[31] For case studies refer http://1worldconnected.org/case-studies/

[32] Satellites, Balloons, Solar Planes & Phones: Innovations in Emerging Market Internet Access? An Industry Overview, DIAL, January 2016.

PART C

AMMBR OPERATION



The Lifecycle of AMMBR

Commercial Rules

A limited number of AMMBR tokens will be created during the public Crowdsale. Thereafter, no further AMMBR tokens will be created, except through the splitting mechanism described below.

Users of the Ammbr network will require AMMBR to pay for access. Users will therefore require digital wallets to hold, manage and transact. These wallets will be tied to the users' digital identities.

Interactions on the Ammbr network will involve following marketplace dynamics.

- Pricing of services
- Rating of the potentially disparate presented pricing from alternative routes or services, and uptake of the selected routes or services

The exchange of routes and services for payment of AMMBR are carried out through transactions that are facilitated by the underlying blockchain technology of the Ammbr network.

AMMBR transactions will consist of:

- Offered and purchased services
- Portions of subsequent payments paid to providers by users
- Mining transaction fees paid to the infrastructure owners

Governance Layer

Ammbr mesh devices will include significant logic and capability. However, governance needs to be agreed and applied across the entire global community, with specific regional, national and local variants possibly applied in time. For example, local regulations may require formal identification of individuals using the service, alternatively provisioning of limited free connectivity for regulatory, social, economic or technical reasons may be imposed.

A governance layer of the Ammbr network would therefore offer a key component in building a scalable and sustainable ecosystem.

Definition of Rules

The Ammbr Foundation will consult regularly with Ammbr participants and users for the identification of governance issues. The Board bears ultimate responsibility for the definition and articulation of any new rules.

Impact of Rules

Advanced analytics and user experience measurement will measure the efficiency of the network and overall user experience. This feedback will then be used to refine or change rule sets.

Risk Management

Network rules will be reviewed by legal and industry specialists in order to identify any risks inherent in rules and, where required, make recommendations.

Acquisition

Creation and Token Sale

During September 2017, the Ammbr Foundation will sell AMMBR tokens in a public Crowdsale.

The tokens created during this process will be the only tokens created, except by the possible splitting mechanism described below.

Participants will have the opportunity to procure AMMBR in exchange for ETH and BTC.

Following the Crowdsale, the AMMBR token will be added for sale on a number of exchanges and trade platforms, where participants and users of the Ammbr network will be able to purchase AMMBR tokens.

Pricing

The pricing and bonus structure are dealt with in PART F of this document.

Value Determination

There will be two linked but separate valuation dynamics at play with regards to AMMBR.

- Exchange Rates
- Service Value

Initially, the exchange rate of AMMBR relative to other cryptographic assets will be the largest determining factor in the valuation of AMMBR.

However, as the Ammbr network grows and the volume of activity on the Ammbr network increases, the underlying value of the services on offer, i.e. Internet connectivity, will drive the value of AMMBR.

Arbitrage between these two valuations will be discouraged by both the time and effort required to bridge AMMBR from one environment to the other, as well as by the distributed nature of the Ammbr network. It will be difficult to circulate value fast enough to overcome the risks associated with valuation corrections and fluctuations, and arbitrage attacks would therefore not be realistic. Further study will be conducted in this regard and appropriate steps will be taken to guard against it, if and when required.

Economic Model and Sustainability

Ammbr Communities

To date, mesh networks have been successfully deployed within relatively small communities where social cohesion has driven the model. By adding robust monetisation and trading, it would become possible to motivate wider cooperation beyond the smaller community model.

Allowing for discounted or free access allocated to specific groups, small community cohesion can still be enabled and encouraged alongside wider commercial vigour. AMMBR would act as the micropayment medium exchange enabling participating communities across the Ammbr network.

Ongoing Valuation

- Growth: Demand for connectivity services offered would increase with the growth of the network, which in return would drive demand for AMMBR
- Devaluation: Less demand for Internet connectivity through the Ammbr network may have a deflationary effect on AMMBR

Liquidity

AMMBR will be listed on several exchanges initially, and more as time progresses. The objective is to make AMMBR available as widely and conveniently as possible to anyone who wishes to participate on the Ammbr network.

Addressing Scalability

With 16 decimal places, the AMMBR in circulation is highly divisible to support very high transaction volumes. If this proves insufficient, the splitting mechanism can increase the AMMBR in circulation.

Addressing Security

The Ammbr consensus mechanisms provide the highest security levels (see Part B for more on the consensus methodology). Ammbr wallets, underpinned by the robust self-sovereign digital identity schema, would ensure the security of AMMBR in user wallets.

Splitting

AMMBR is designed to accommodate extensive scaling of the Ammbr network, with the commensurate growth in both participants, users and micropayment transactions. The AMMBR token can be divided into 16 decimal places, and therefore it is not envisaged that more AMMBR tokens will be required anywhere in the foreseeable future.

However, should there be a need for more AMMBR tokens in future to meet the volume requirements of the network, the facility to split tokens is in the design of the tokens. The Ammbr Foundation is responsible for the governance of such an event. Should a split be decided on, all AMMBR tokens can be split into two tokens. This would effectively mean that any AMMBR residing at any address (for example in a user's Ammbr Wallet) would double. Such a split would occur at the same time globally.

A token split is not intended to raise the overall value of AMMBR holdings, but simply as a mechanism to increase the available number of AMMBR tokens in circulation.

Destruction of AMMBR

No AMMBR will be destroyed following the Crowdsale. Theoretically it may be desirable to contract the available AMMBR tokens through a halving action, similar to the splitting mechanism described above, but no such action is envisaged or specifically mandated.

Ammbr Device Lifecycle

Device Acquisition

Intended Rules / Terms and Conditions of Purchase of the Device

The owners of infrastructure, the participants, and the users of the Ammbr network interact in a marketplace where pricing and access are determined largely organically. To facilitate such flexibility, it would be necessary to give both participants and users the ability to segment traffic and access.

Participation on the Ammbr network requires the installation of an Ammbr client, software application, on a given hardware device used to connect to the Internet. This client application would require initialisation with the digital identity of the user.

The user will have a digital wallet associated with the digital identity used. The AMMBR balance of this wallet would determine if the user is able to pay for access to the Ammbr network.

The user would also be able to obtain attestations associated with the digital identity, which can then be used to categorise the digital identity.

Public Participants

Infrastructure owners, the participants, can allow or disallow public participation. Any device with a suitably loaded Ammbr client, initialised by a digital identity, is allowed access for payment. In this case, the attestations associated with the digital identity are irrelevant.

Closed Group Participants

The infrastructure owner, the participant, can also require specific attestations of any digital identity that accesses his or her part of the network. The pricing of access can also be varied according to the attestations presented.

For example, the owner of an Ammbr router, with an ISP connection to the Internet, may decide to charge his family members zero, friends a nominal fee, and the regular market price for strangers. To do this the owner could provide a family attestation to the digital identity of his family members, and a friend attestation to friends. The attestation is, in effect, a digital signature from the owner's own digital identity.

Attestations can be revoked if necessary, so a temporary preferential rate can be ended by revoking an attestation. In a commercial setting, this will be enormously helpful in administering access to employees and partners.

Device Pricing Model

The Ammbr Foundation is a not-for-profit organisation, and the Ammbr Mesh Router will be priced at levels designed purely to drive distribution.

End User Pricing Target

- Ammbr Series 1 Mesh Router: US$79, plus delivery
- Ammbr Series 2 Mesh Router: US$50, plus delivery

Depending on the amount of funds raised in the AMMBR token sale, the Ammbr Foundation will establish a finance vehicle to optimally drive the manufacturing, distribution, and uptake of Ammbr technology globally. This finance vehicle will put in place subsidies, financing and incentives aimed at wide proliferation of the Ammbr network.

Financial Model

The Ammbr Foundation will license manufacturers with its core technology to innovate, design and produce products that would add diversity within the Ammbr network.

The first such instance is the licensing of Spectramesh, Inc. Spectramesh will manufacture the Series 1 & 2 Ammbr Mesh Routers under license. The Ammbr Foundation will stipulate modest resale margins and certain other parameters that optimise the uptake and interoperability of these and other products introduced to the Ammbr network. A small royalty to be paid to the Ammbr Foundation will sustainably fund the ongoing research and the governance performed by the Foundation.

Retention

Maintenance

Maintenance services for hardware components such as the Ammbr mesh router will be put in place by the manufacturing partners. Such service points will include the manufacturer's own service points, partner service points, and entrepreneurs (possibly encouraged by free training and modest seed financing in under-serviced areas).

Support

The manufacturing partners will be required to put in place online and telephone support infrastructure to assist participants and users of the Ammbr network. Social media channels will also be used.

Return

Policy

Defective units will be covered by the usual manufacturer warranties.

Destruction

Any units returned under warranty will either be refurbished or scrapped in accordance with the sustainability directives below.

AMMBR hardware, when it reaches its end of lifecycle, or early scrapping, faces two possible scenarios.

- Scrapping
- Salvage, repair and re-deployment

If the hardware is found to be beyond salvage, the constituent parts will be disposed of in an environmentally sound manner. If the unit is deemed salvageable, then it can be repaired or refurbished, and re-deployed either in the primary market as a refurbished unit, or in alternative locations, for example, as part of charitable gratuities.

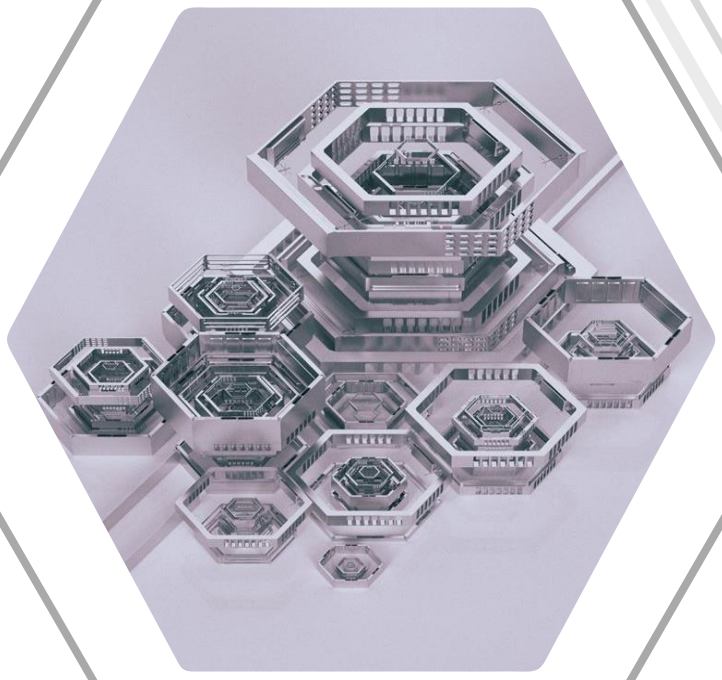
Local repair facilities will be made available through partner distribution networks, or small business owners.

Tradeability

Transfer of ownership
Ammbr devices are designed to be owned and operated through a digital identity. When a unit is freshly deployed it is initialised by its owner, and the owner's digital identity is injected into the unit. Should a unit be sold or transferred to another owner, the original owner must authorise the transfer, and the new owner's digital identity can then be injected to affect the transfer.

PART D

AMMBR ASSETS



Patents

Ammbr Foundation is in the process of drafting and filing for a number of patents, and will continue do so in future. Further details will be continuously disclosed as soon as possible for all proposed patent activity.

Hardware

Status

A number of designs and early Ammbr mesh router prototypes have been developed in order to test connectivity and certain protocols to be used by the proposed technological solutions. Major components that require further development are the following.

- PoeT/PoV Mining Chips
- Multi-band Wireless Chips
- Certain customised protocols for monetisation of the network
- Overall router management systems

Production Plan

The funds received in the Crowdsale would be allocated to the outstanding developments, with a view to achieving the first production units of the Series 2 Ammbr mesh routers by Q4 of 2018. Earlier trials would be conducted using interim Series 1 hardware built from off-the-shelf components and FPGA processors to simulate blockchain consensus protocols.

Intellectual Property

Capture

Usually, more than 80% of an organisation's value lies in its intellectual property (IP)[33], which renders it important in order to capture, catalogue, qualify and protect the creation of real enterprise value. Implementation of effective operational processes, in order to continuously capture new IP and identifying best innovations for obtaining legal protection, is an important strategic step to fully harness the value of our team project efforts.

The need for an effective IP capture

Considerable and continuous investment is required in order to support R&D. It is important to make sure that the goals and output of the Ammbr team are aligned with the needs of the relevant markets, whereby an effective innovation management and IP capture process will be executed. The Ammbr Foundation is working with experienced patent attorneys in order to attain such process.

Educate R&D team about IP

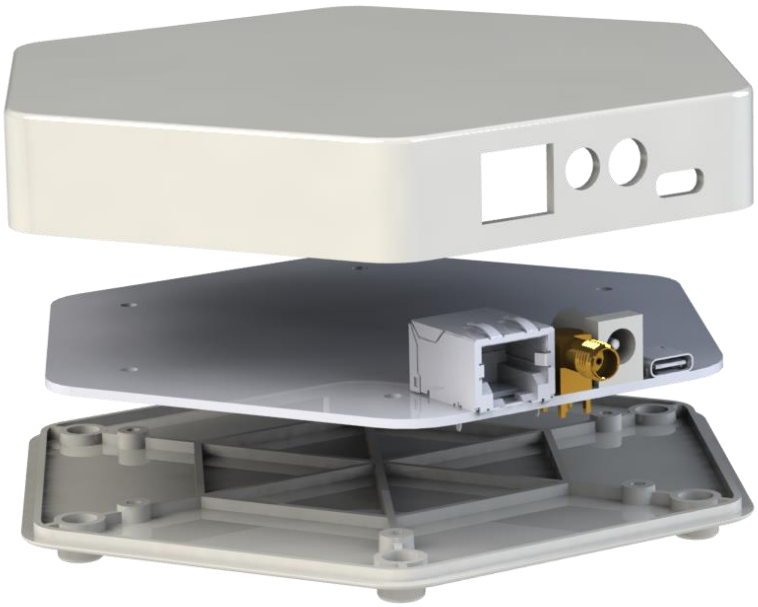
Problem solving is the source of most patentable inventions. IP education for inventors is an important step in the innovation management process. The aim should be to cover the basics of understanding of what may be protectable, keeping good notes and records, and strong internal communications. A basic process can yield tremendous benefits.

- Initial Record of Idea – inventions are added to the invention tracking system
- Initial Invention Capture – a short meeting with the inventor(s) generates sufficient information for a quick assessment of likely novelty, to determine business value and capture the key aspects of the invention

[33] http://www.lexology.com/library/detail.aspx?g=6f7dd161-e101-4809-9cb6-af37b853aae8

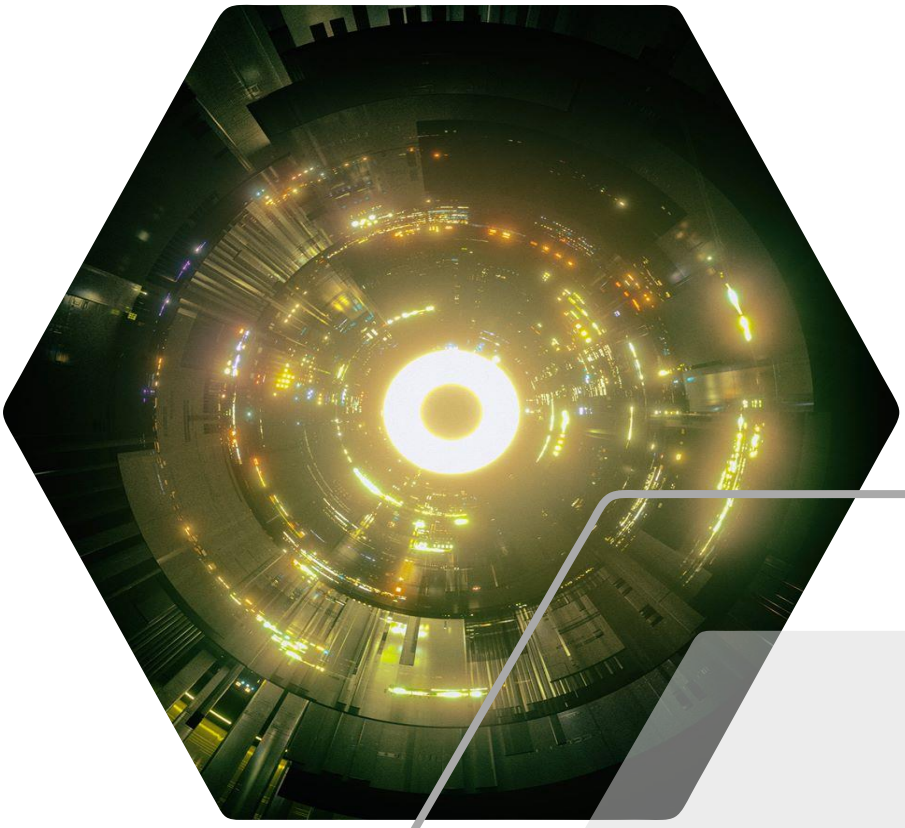
- Novelty search – assesses the prior art position and provides information for a patent attorney to position the state of the art in the patent application, the invention is also ranked for various technical and business attributes
- Invention decision form – documents the discussions with inventor(s) to further confirm the novelty position, which allows management and patent attorney to make a decision to proceed with patent filing, or not
- Full invention disclosure – an outsourced specialist captures the full details of the invention, including implementations, by having further in-depth discussions with the inventor(s), this ensures an efficient filing process, with less patent attorney resource time required

Between each main step, if the invention is not deemed novel, inventive or protective of the business, the invention can be archived in an invention database. This effectively acts as a comprehensive trade secret database. Alternatively, defensive publication is another option for these inventions and prevents competitors filing for patents.



PART E

ABOUT AMMBR



The Ammbr Foundation

The Ammbr Foundation Pte. Ltd. is a not-for-profit foundation formed in Singapore in 2017 to oversee the development and implementation of a fully decentralised, global telecommunications network, the Ammbr Network. The network will be powered by innovative technology being developed by a team of technology, business and legal experts.

The Ammbr Foundation's vision is that the Ammbr Network will be communally and jointly owned by the infrastructure owners, and not a centralised entity. The Ammbr Foundation will ensure the administration and governance of the network, as the network itself is unable to self-fulfil these functions.

The initial constituent parts of the Ammbr Network, described in this document, have been developed by the founders and form a part of the intellectual property portfolio of the Ammbr Foundation. Other vendors, services and solution providers will be able to develop and introduce further hardware and software, enhancing the functionality and features of the network under licensing by the Ammbr Foundation.

Structure

The Ammbr Foundation is managed by a Board of Directors. Each member of the Board subscribes to governance best practices that include the Director's Declaration in the preamble of this document.

Development

The Ammbr Foundation outsources all development of technology and products to external parties. The founders of the Ammbr Foundation are also the first vendor partners. As such, they will continue to develop, manufacture and implement network infrastructure and services under license to the Ammbr Foundation.

Spectramesh, Inc. (USA)

The developer and manufacturer of the Ammbr Series 1 & 2 Mesh Network Router.

Ipso Microelectronics SARL (Switzerland)

The developer and manufacturer of the digital identity management and hard wallet terminal to be used in conjunction with the Ammbr router.

Interested developers are welcome

Operational

The Ammbr Foundation outsources the distribution and support functions of the Ammbr Network technology to specific market channels. These will include direct to market, as well as value-added vendor channels.

Early implementations of the Ammbr Network will require a customised project approach, or may be conducted in association with existing community mesh networking projects. In either case, subcontractors to the Ammbr Foundation will ensure that network design principles are applied to ensure optimised coverage for the end users of the Ammbr Network. Local licensing and community participation are key to the success of the network, and experts in the process of implementation will be deployed as subcontractors.

Interested distributors | service providers welcome

The Team

The Directors

Benny Pang

Benny Pang practices corporate finance and securities law in Hong Kong, focusing on equity capital markets and mergers and acquisitions. Mr. Pang has worked on a broad range of corporate transactions with private and public companies. In addition, he has substantial experience representing issuers and underwriters in equity fundraising transactions, including share placements, rights issues and open offers, and he has completed over 100 and participated in more than 120 Hong Kong initial public offerings, including global offerings of SOEs and POEs. He has represented clients in Europe, Russia, Central Asia, North Asia and South-East Asia, the Middle East, the United States, Canada, South Africa, India and Australia.

Mr. Benny Pang was previously the Head of Hong Kong Office and Partner at Loeb & Loeb LLP. Mr. Pang served as Partner of Salans LLP until 2012 and at Paul, Hastings, Janofsky & Walker LLP. He is a Member of the Corporate and Global Real Estate Practice Groups. He has LL.M from The University of New South Wales, LL.B (Hons) from Bond University, and Bar Admission in New South Wales, Australia.

James Lanshe

Jim Lanshe has been actively involved in law and investment management for over twenty-five years, most recently as president and general counsel of a venture between a multi-line domestic insurance holding company and a major, international reinsurer. He had previously served as the chief executive of a fund services company administering over six billion dollars in fund assets. Currently, he also serves as the non-executive Chairman of Oppenheimer Resources SA, a Luxembourg based SICAV-SIF.

Mr. Lanshe has also been an assistant dean and faculty member at Seton Hall University School of Law, on the faculty at the University of Louisville's Brandeis School of Law where he taught mergers and acquisitions, as well as an adjunct at University’s School of Business. He has acted as a consultant to the United Nations Development Program for Europe and the Commonwealth of Independent States (UNDP CIS Program), where he advised on legislative reform within the CIS to facilitate the flow of private capital into that region. Currently, he holds an honorary research associateship at Oxford Brookes University School of Social Sciences and Law, Oxford, England, where he has lectured on transnational business issues.

Mr. Lanshe is a graduate of Georgetown University (B.A), Cornell University School of Law (JD), Harvard University (MPA), University of Hawaii (MBA), and Cardiff University (MPhil). He is admitted to practice law in the states of Arizona, New York, Pennsylvania, Texas and the District of Columbia, as well as various federal courts including the Supreme Court of the United States. Mr. Lanshe previously served as a captain in the United States Marine Corps Office of the Staff Judge Advocate during which time he held a State Department appointment as a United States representative to the courts of Japan.

Rakesh Rajagopal

After completing his BA in English and Economics at Kerala University, Raj moved to the UK where he joined Alexis Group, a precious metals trader, in a sales role. He was promoted to Business Development Manager in early 2001 and then grew his sales team to nine across Europe. After this he joined Bridgewater, a Hong Kong financial firm. His remit here was building a portfolio of clients in the commodities and energy sector.

Raj went on to fill operational roles at Sacvinam Global and Poly Resources (part of the Chinese conglomerate) before joining Upbest Precious Metals. At this listed company he managed two teams, one operational in the bullion supply chain, and the other in developing structured investment vehicles.

In 2011 Raj was invited to join the Canadian Imperial Bank of Commerce in the role of director of private banking. After having collaborated successfully in earlier startups with Derick Smith over the preceding fifteen years, he has been fully vested in the blockchain and digital identity companies they founded together since 2012.

Derick Smith

Derick's first startup was a computer memory chip import & distribution company he started with his brother at age 19 in 1984. He went on to work, first as a software developer on Unisys mainframes, then mini, UNIX and PC platforms. His early entry into Smart Card programming led him into EMV and payment systems in the late 1990's.
He co-founded the M.POS Group in 1998 as one of the first companies to design and manufacture a cellular Point of Sale terminal. The company also developed a high-throughput transactional switch, and was the first foreign POS provider to pass the China Unionpay type approval process. Derick exited M.POS in 2002.

Derick started a number of small to medium sized companies, predominantly in the telecoms space, in the following years. During this time, he became familiar with not only the technology, but the business models of the telecommunications sector. The value chain, starting at spectrum allocation, investment in infrastructure, and the subsequent division of the services into distinct business units, presented an opportunity for him to analyse and determine commercial opportunities in the market to participate in the gradual deregulation of the industry.

In 2012, he started becoming increasingly interested in the burgeoning world of Bitcoin and Distributed Ledger Technology. He co-founded Blockchain Labs and Ethereum Lab, and then moved on to create the Chainreactor group of companies, together with Rakesh Rajagopal, with a primary focus on blockchain. They also founded Ipso Microelectronics as a specialist electronics firm, working in self-sovereign digital identity.

The founding of the Ammbr Foundation is the culmination of extensive research and consultation in finding the optimum business use for blockchain technology outside of financial services.

Kaustuv Ghosh

Kaustuv began his startup career straight out of graduate school in 1996 by setting up a sales office for NDTV in Mumbai, India. He went on to design, manage and successfully sell NDTV Online, the world's first mobile news-on-demand service. Over almost a decade, he built the digital business for NDTV, now one of Asia's leading news broadcasters, in mobile, Internet advertising, e-commerce and video streaming.

He then repeated this act with Mobile 365(later acquired by Sybase, Inc) by starting their India office and operations, putting together a team and creating a strong revenue base. Sybase moved him to Singapore where he took over their natural language business and enabled its first ever sales outside USA - to some of the largest financial institutions in Asia.

Kaustuv worked for NETS, the Singapore payment processor, in 2009-10. He then went on to head mobile commerce for a leading Indonesian telecoms player owned by the Sinar Mas Group. He turned around their loss-making airtime top-up business by overseeing a complex payments platform replacement, re-design and launch. This included integration with all the bank switches in Indonesia in record time and on-boarding a new operator which was acquired along the way. Out of the 36-member team that he led and nurtured, came some of the finest young leaders of Indonesia's fintech revolution.

Thereafter, over a two-year period, he ran the business development and strategy portfolio for Orga Systems (later acquired by RedKnee) in the areas of prepaid, smart metering, IoT and real-time tolling. This was a global role which led to a strong partner ecosystem and revenue pipeline across Asia and Europe. Exiting Orga Systems, Kaustuv returned to the world of payments through SimplyTapp, the creators of Host Card Emulation. Along with the founders and co-creators of HCE, he went on to launch the first pilots of HCE outside North America, built the partnerships necessary for future growth and executed critical treaties for revenue growth.

Kaustuv was SVP at Matchmove, a leading fintech company. There, he launched mobile remittances, redesigned the mobile wallet, put in place product processes and created a very high-quality product management team from scratch. He initiated and oversaw successful early work on blockchain. He decided to leave to pursue his interests in cryptography, blockchain and the philosophy of consensus.

Kaustuv, a naturalized Singaporean, has degrees in accountancy and environmental management and a post-graduate diploma in communications.

Other Team Members

Jason Aspinall

Jason has an extensive background as a Systems Administrator, Project Manager and Electro-Mechanical Design Engineer. His skills in building requirements specifications, overseeing development, applying Agile methodologies, and delivering fully documented specifications and a meticulously validated and tested product is of immense value to the team.

Jason's proficiency with a wide range of tools makes him an indispensable backup, in addition to his strengths in design and project management.

Dr. Michelle Booysen

Dr Michélle Booysen is an economist with 30 + years' experience in business development and management. As a management consultant on business structure, systems, processes and market positioning for start-up, small and second stage businesses, as well as corporates, her focus is on making difficult concepts and complicated business matters easy to understand for all role players in enterprises. She focuses on process as key element in business performance, and links people to strategy in order for organisations to achieve their results. She has garnered numerous recognitions for her role in business development, including global awards for innovative business management methodologies and resultant impact on business efficiency.

●2008: finalist in the entrepreneur category of the BWA Regional Business Achievers Awards ●2009: finalist in the Technology Women in Business Award. ●2009 Petanque is Silver Award Winner for innovative BPM, Middle East and Africa Region, Top five Globally ● Top 10 Global Winner for application of Adaptive Case Management in a Case Study ● 2011 Winner Technology Women in Business, Small Companies Category, Award ● 2012 Winner, SME Sector; CEO Most influential Women in Business and Government ●2012 Finalist IWEC 2012 ● Finalist Sanlam Business Partners' Entrepreneur of the Year 2012●Finalist TOPCO Most Women Empowered Enterprise SME 2012 ● Winner Most Influential Women in Business and Government, SME sector, 2012. ●Awardee WVEFII, Mexico, 2012 ●Winner of 2013 International Enterprising Women, Small and Medium Business● Finalist Sanlam Business Partners' Entrepreneur of the Year 2014 ● 2014 Standard Bank Top Women Award – Small Medium Enterprises ● 2014 WfMC Global Winner for Excellence in Business Process Management – Case Study outcomes, ROI and approach winner. ● 2016 Pétanque became a Certificated Women Owned Business (WBENC) in the USA.

She holds a PhD Commerce degree, is a Project Management Institute (USA) certified Project Management Professional, holds a CPP Champion® qualification from the BPM Group (UK) and is the founder and President of the Petanque Group of Companies.

Membership: Project Management Institute, UnitedSuccess, Women's Presidents Organisation, WeConnect, Institute of Directors.

Dr. Wim Booyse

Wim has 26 years of experience on a corporate and consultative executive level, with a strong corporate strategy, governance, fiduciary, negotiation and business development focus. He has a significant knowledge of the ITC and healthcare sectors in Developing Markets, with particular reference to Southern Africa and the ASEAN Countries. He understands the intricate business practices and business cultures in these geographical areas. He has more than 20 years of experience in managing the inter-relationship between the public and private sectors in Developing Countries and their regulatory environments.

Wim holds a D. Phil in International Relations with a major in Strategy and Negotiations. He is a Research Associate at the Gordon Institute for Business Science [GIBS] at the University of Pretoria, and also functions as a mentor and supervisor to students completing their PhD's in Business Administration. He has published more than 150 articles on various topics. He also has a powerful advocacy for data privacy.

Dean Bubley

Dean Bubley (@disruptivedean) is the founder of Disruptive Analysis, an independent technology industry analyst and consulting firm. An analyst and futurist with over 25 years' experience, he specialises in wireless, mobile, and telecoms fields. He is one of the leading market observers covering network infrastructure & software, service provider business models, voice/video communications and telecoms policy.

He is known as a contrarian, often with challenging opinions that go against industry consensus. His present focus is on 4G/5G/ Wi-Fi® network technology, NFV/SDN, the "future of voice and video" & the roles of Blockchain, AI and other innovations within telecoms.

Mr Bubley was formerly an equity analyst, covering communications stocks with Granville Baird, the UK arm of US-based investment bank Robert W. Baird. Prior to that, he spent eight years at UK research firm Datamonitor, where he co-founded the company's Technology business, managed the Internet & Networking area and custom consulting operations, with roles of Chief Analyst & Director of Consulting.

He holds a BA in Physics from Keble College, Oxford University.

Kurt Cagle

Kurt Cagle is an author and industry analyst focusing on Fourth Industrial Era technologies - blockchain, artificial intelligence, data analytics, syncretic energy systems, distributed computing and environmental hacking. He is the author or co-author of twenty-one books on the Internet, future trends and data standards, and writes regularly for Linked-In, Data Science Central and IDG. He has also been an information architect with thirty years of experience in building enterprise scope data interchange systems and metadata hubs, with clients including The Walt Disney Company, The Data Services Hub for the Affordable Care Act, Warner Brothers Studios, the Library of Congress, the US National Archives, United Health Group and others. From 2005 to 2013, he was an Invited Expert to the W3C, working to design, develop and promote web specifications including HTML5, CSS, SVG, XForms, SHACL, Web Components and other standards.

Manoj Cherooparambil

Manoj graduated from the University of Manchester with a degree in Economics, Accounting and Finance and is a CAIASM charter holder. He has 16 years of experience in the finance sector, predominantly in Asia. Starting his career in Alternative Investments at a boutique investment firm in Hong Kong, he subsequently shifted his focus to Private Banking culminating in a position as VP of EFG Bank (HK) within that sector. Thereafter he was C.F.O of Once China Capital and CIO of an Asian Family Office.

In the recent past, his focus has been on India. He is a shareholder of a midsize brokerage in India having successfully helped it turn around after joining as MD, and executing multiple roles including that of CFO in that position. He has set up and run his own consultancy firm, worked as Director of Finance for a well-known Real Estate developer, and is also a partner and shareholder in a boutique investment bank, specialising in the IT/ITES space. His deep connect and convictions in where he chooses to work means that he often continues to fill advisory roles, even after leaving firms. Manoj brings not only the network he has created through his varied roles in Asia, but also a strong knowledge of regulatory, statutory and accounting standards as well as his astute business acumen.

Matthew Dooley

Matt is a founding board member of the FinTech Association of Hong Kong, and was previously the global head of Internet strategy at HSBC Group. Matt consults with banking and insurance clients to help them define cutting-edge strategies and implement engaging customer solutions that transform and disrupt the financial services industry. He is a respected thought leader, speaker and leading industry futurist. He shares emerging marketing trends, insights and strategies to his network of more than 14,600 Twitter followers. Matt features in the FinTech Asia 100, Top 20 Influencers in FinTech, and made the list of FinTech Influencers to follow in 2017.

Fon Allan Duke

Fon Duke is an executive government contractor with a long career focused on program management and government support. Fon brings new technologies to government at local, state and federal levels. His involvement in blockchain technology started in 2009 and has been involved in introducing blockchain to the Department of Defence.

Fon has an M.B.A from the University of La Verne and a Bachelor of Science from CSUSB.

Fon's contacts throughout the government of the United States are deep, at both the Federal and State levels. He brings his contacts and skills to Ammbr with an interest in providing the technical solutions to meet the needs of government as it works to bring community based connectivity to underserved communities, the military, and disaster zones to name a few.

MJ Fick

MJ has 25+ years of experience as project -, program - and PMO manager in the information technology field. She has delivered several successful ERP implementation programs, mainly in the oil industry and managed teams spanning several continents. Her passion is to work with clients to optimize processes for project management offices and to teach and coach project managers.

MJ holds the PMP® credential from the Project Management Institute in the US. MJ believes that project success is greatly enhanced by integrating project management with change management. She is also a PROSCI accredited change manager.

MJ is an entrepreneur and shareholder in Pétanque International. and TenStep ZA, which is the South African franchise of the international TenStep, Inc. group.

John Hooks

John Hooks began his 20+ year career in the Microelectronics Industry as a Financial Analyst at IBM Labs in Austin, TX. He was part of the executive team which guided the development of IBM's line of RISC chip sets (later Power PC). He also worked as a technical liaison between IBM Watson Labs and licensees to commercialize their Mobile Intellectual Property. He later joined Accenture, LLP (formerly Andersen Consulting) as a senior executive in their Mobile Commerce Lab. There he managed teams that did leading-edge engagements with multiple vendors in a variety of industry segments including Technology, Healthcare/Life Sciences, Consumer Products, Financial Services, and Manufacturing across existing and emerging markets. He was also an Expert-In Residence, Microelectronics in the Accenture Labs and an advisor on several acquisitions of Mobile Computing ventures for Accenture Ventures.

Today, he is head of the Blockchain (Distributed Ledger) practice at a boutique Management Consulting firm he founded, focused on the application of commercial off-the-shelf technology and proprietary algorithms across a variety of industry sectors. He is also an advisor and consultant to private equity and venture capital firms in areas of technology and telecommunications. He has written SBIR proposals for high performance computing platforms for the USAF, negotiated CRADAs with US Government Labs, and performed technology due diligence that has led to the establishment of over two dozen startup ventures. These include Goliath Technologies (Computer HW Distributor), Gargantuan Storage Devices (HD Multi-layer DASD), and XBrilliant (GaN semiconductor research and LED Design).

John Hooks holds a certificate in Private Equity and Corporate Governance from the Harvard Graduate School of Business, and an MBA, Financial Management degree from the Lubin School of Business, Pace University. He was also a Doctoral Candidate at New York University and held concurrent appointments to the faculty of the University of Bridgeport and Pace University.

John Hooks has held several securities licenses including Series 7, 63, 65, and 66 while an advisor with UBS Private Wealth.

Kyong Pak

Kyong Pak is a senior electrical engineer with deep experience in wireless communications hardware development. His career includes the design of several generations of multi-frequency products sold by Motorola and Uniden among others. Kyong is also an expert in radio frequency antenna design, testing and verification procedures. Kyong specializes in power systems optimization for low power consumer electronics.

Kyong's skills include microcontroller, electronic timing devices, switching and linear power supplies & Xeon illumination. His product design knowledge includes consumer products, industrial products, radio communication products, critical safety products and automotive related products.

His software knowledge includes Altium Designer CAD, Freescale Codewarrior (assembly language) & AS400 environments.

Ankur Patel

Ankur has a Marketing Degree from Depaul University, but his fascination with electronics has led him into the world of Printed Circuit Boards (PCB) and Assembly. With more than ten years in various roles in the industry, Ankur has strong skills in managing Bills of Material, cost reduction, logistics and procurement. He has also developed particular insights and expertise into thermal conductivity of materials.

Ankur is primarily responsible for logistics and procurement management.

Jurie Pieterse

Jurie Pieterse is digital marketing and brand strategy expert. He has 20 years of client and agency-side experience leading significant business and brand growth initiatives particularly where digital marketing has been a critical success factor. Jurie has worked with startups to multinational power brands in a wide range of industries including financial services, telecommunications and blockchain ecosystems, in addition to consumer packaging goods, e-commerce, manufacturing, non-profits, associations and technology.

In his early career, he established three digital marketing firms including for the major advertising agencies Leo Burnett and FCB. From 2001-2012 he created the customer acquisition engine for ING Direct, the leading online savings bank, building the brand and digital channels to fuel the bank's dramatic growth to 7 million customers and $80 billion in assets in the US. Since leaving his role as Chief Marketing Officer at Nationstar Mortgage, he has been consulting for a variety of clients including in the e-commerce, artificial intelligence, management consulting, B2B, non-profit and bitcoin industries.

Originally from South Africa, Jurie has won awards including Young Direct Marketing of the Year, People's Choice Webby Award and AdTech Winner of Show. He is most happy when he can roll up his sleeves and work in partnership with a talented team to solve complex business challenges and execute the best in digital solutions to deliver results.

Professor Jean-Jacques Quisquater

Jean-Jacques Quisquater is an emeritus professor of cryptography, multimedia security and secure circuits at the Ecole Polytechnique de Louvain, Catholic University of Louvain (UCL), Louvain-la-Neuve, Belgium, where he was responsible (at least at the scientific level) of many projects related to smart cards, to secure protocols for communications, digital signatures, payTV, protection of copyrights and security tools for electronic commerce. He was founder and responsible for the well-known group "UCL Crypto Group" (composed of 8 PhD students and 8 postdocs in 2011, and 2 professors). He is now scientific advisor for this group. His research group included people from (applied) mathematics, computer science, telecommunications and microelectronics: this diversity is the main strong point of the group able to study many views of the same problem.

From September 2001 till September 2003, he was the head of the Microelectronics Laboratory at UCL, Louvain-la-Neuve. From October 1st 2003 till September 2004, and from October 2007 till September 2008, he was on sabbatical leave at MIT, UCL London and ENS (rue d'Ulm, Paris). He is now research affiliate at MIT (jjq@mit.edu) from 2004.

Jean-Jacques has achieved qualifications as Engineer in Applied Mathematics (UCL, Belgium, June 1970), PhD in Computer Science (Doctorat d'Etat au LRI, Orsay, France, July 1987).

1970-1991: Scientist at the research laboratory of Philips (Brussels, and next to Louvain-la-Neuve). Head of their cryptologic research group (7 persons) for the whole company.

Consulting activities: He did a lot of consulting from 1985 while working for Philips, either as an independent, or as professor at UCL. The companies include: SWIFT, IBM, Microsoft, Philips, NXP, Isabel, Proton, Gemplus, Europay, Japanese government, Mitsubishi, SGS Thomson, Morpho-Safran, etc., with projects ranging across protecting a complete network by cryptography (SWIFT for 17 years), to many audits of security.

Invitations: Twice 6 months at the University of Lille for teaching and research, 3 months at the University of Orsay for research, two months at the University of Nice for research, one year part-time at FUNDP (Namur, Belgium) to teach security.
Short stays at the Universities of Stanford, MIT, Berkeley, Florida, Royal Holloway (London), Michigan (Ann Harbor) and Wisconsin (Milwaukee). Many invitations for workshops (Oberwolfach, CIRM, Dagstuhl, Harvard, etc.). Research affiliate at MIT-CSAIL from 2004.

Other interests: With Prof. Gary Urton (Harvard), and Eric and Martin Demaine (MIT), he has been working since 2004 towards a better understanding of the Inca khipus, some kind of old blockchains (2 invited talks at the National museum of Archeology in Lima, Peru, January 2009).

Member: IACR, IEEE, ACM, AMS (till 2010).

Awards: "Chaire Francqui au titre belge" for 2000-2001,
- Montefiore prize 2000 (given only every 5 years to an international scientist),
- Doctorate honoris causa (2003) at the University of Limoges, France,
- Listed in the "Who's Who in the World" (Marquis, 2002-...),
- IFIP Kristian Beckman award (2004, IFIP-TC11),
- Doctorate honoris causa (2010) at the University of Toulouse, France,
- Full member of the Club of Rome (EU chapter) from 2011 till 2014,
- IACR fellow (International Association for Cryptologic Research, 2010),

- Corresponding member of Académie des Sciences de Toulouse (2011-),
- Invited professor (2010-2017) at Collège de Belgique,
- ARCSI (France) : honor member from 2010,
- Associated member of the Royal Belgian Academy from 2012,
- 2013 RSA Award Excellence in field of Mathematics.

Scientific steering committees:

- STIC for the minister for research Claude Allegre (1997-2000), France,
- ANR-STIC (2009-2011), France,
- EQUIPEX-ANR (2010), France,
- Paris-Telecom (2008-2011), France,
- Company Intrinsic-Id (from the beginning),
- Company Intopix (from 2002).

Jean-Jacques was teaching *cryptography* at ENS (Ulm-Paris) from 1991 till 2002 and often gives talks at the universities of Namur and Limoges. He is a member of the steering committee of ESORICS (international conference about security), CARDIS (the main research conference about smart cards) and CHES (main scientific conference about secure hardware). Recently he was general chair of CHES 2010 in Santa Barbara (secure circuits, Ca., 2010), program chair of EVT/WOTE 2010 (electronic voting, Washington D.C.), general chair of IWONT 2011 (graph theory, Brussels) and program chair of cataCRYPT (2012-2017).

He was the main designer of several coprocessors for powerful smart cards, including CORSAIR (Philips) and FAME (Philips, now NXP). From 1986 till 1996 he improved the speed of execution of cryptographic algorithms inside smart cards by a factor of 250,000; going from a slow experiment in a laboratory into a faster product, still in use (at least four billion smart cards from NXP are used globally by the likes of Visa and Mastercard - thanks to his invention and design of accelerators of cryptographic algorithms for identity cards, passports, etc.) 85 % of the secure passports in the world are using his coprocessor for secure identification and signatures.

Author or co-author of about 250 papers including 200 in main conferences and international journals. He holds 17 patents in the field of smart cards and security.

He was involved in the process of standardization of secure cryptographic tools:

- digital timestamping (ISO and IETF):
- digital signatures (ISO): he is the co-inventor of the main schemes in use based on factorization and RSA.

Jean-Jacques is co-inventor of a very well used cryptographic scheme, the zero-knowledge GQ scheme, with Louis Guillou, used by about 100 million client systems in Novell (NDS, Netware) and 3 million servers. He improved the GQ protocol into the so-called GQ2 protocol (1999, again with Louis Guillou) and into a new version of the cryptographic GPS identification protocol (2001, with Marc Girault).

He has been working on blockchains for a long time, including a Belgian project TIMESEC, from around 1997, and the results are used and cited by the founder of bitcoin, Satoshi Nakamoto, in his seminal paper (2008).

Kirem Rahmani

Kirem has an extensive background in especially RF and mobile device electronics, most notably as the Leader of Development on the Smartphone Platform at Sendo, arguably the first smart phone development, ahead of Apple iPhone.

Kirem has a M.Sc. Electronic Product Design from the University of Glamorgan, and a B.Eng. Hons. (2.2) Electronics from the University of Cardiff. Kirem holds three patents.

Kirem has worked for LG and Nextwave, with deep understanding of Embedded software development including driver development on numerous platforms, PCB layout, component schematics, design validation, mechanical integration, production test, documentation and component sourcing. He is also adept at software development using database technologies, Java, C++ and other tools.

Dr. Arjuna Sathiaseelan

Dr Arjuna Sathiaseelan is a Senior Research Associate at the Computer Laboratory, University of Cambridge. He directs the Networking for Development (N4D Lab). This research group conducts research on novel Internet architectures for improving and reducing the cost of Internet access.

Arjuna has been involved in several Internet access projects across the globe deploying wireless and cellular networks as well as spearheading deployment of new Internet architectures for enabling flexible low-cost Internet access. He has brought together and led successful consortia related to universal Internet access projects in EPSRC, EU FP7 and EU H2020. He also founded the Internet Research Task Force's (IRTF) "Global Access to the Internet for All (GAIA)" research group. This group brings together some of the major players (industry, academia and NGO) in networking and ICT for development, under one common umbrella. IRTF aims to understand and scope out the challenges in providing universal access and to influence standardisation efforts that could potentially change the Internet landscape to be more inclusive. He is currently the Chair of the IRTF GAIA research group and a member of the Internet Research Steering Group (IRSG). Arjuna has been an advisor to the United Nations Foundation's $75 million Digital Impact Alliance (funded by the Melinda and Gates Foundation, USAID and SIDA). He is also in the advisory board of

- Ubuntu Power - a social enterprise focused on providing affordable, off grid energy and Internet to underserved communities.
- Ensemble Pour la Difference - a social business incubator in Democratic Republic of Congo.
- EU NETCOMMONS project.

Arjuna has co-authored and contributed to several Internet standards and drafts (IETF) and contributed to the DVB-RCS2 standardization at the ETSI TM-RCS. He has published more than 80+ peer reviewed papers in leading international conferences, journals and workshops, including best paper awards in leading conferences. He has given 25 invited talks including several distinguished lectures.

In the past, he was a Research Fellow (Connected Digital Economy - Rural Digital Economy Hub and Networking - School of Engineering) at the University of Aberdeen. He was also an Associate with the Center for Sustainable International Development (CSID) at Aberdeen, where he founded and convened the ICT4D group.

Arjuna Sathiaseelan has a PhD in Networking from King's College London (2005), MSc in Computing and Internet Systems from King's College London (2001) and Bachelors in Computer Science and Engineering from NIT, Trichy, India (2000). He was awarded the Young Alumni Achiever Award from NIT Trichy (2016).

David Stempels

David is passionate about people and the relationships that bind us. He has built up a considerable network throughout Asia and Europe through his career in finance, retail, and distribution. His ability to connect needs with abilities, resources with production, defines his philosophy of inclusiveness. David has a Degree in Economics, which adds insights to his natural abilities with people and marketplace dynamics.

David studied at the Business School of Economics in Amsterdam, and the University of Nyenrode before moving to Hong Kong.

Pieter van Ysseldijk

Pieter van Ysseldijk was trained as a EU lawyer in Brussels and London, where he qualified as a SFA corporate finance and banking representative.
In 1995 Pieter took over and headed his family group of shellfish farming and processing companies in the Netherlands, with subsidiaries in Belgium, Germany, Turkey, China, Ireland and Northern Ireland, which investment in farming and processing was based on a socio-economic development programme for local fishing communities in conjunction with an ethical bank. During his career Pieter has invested in and co-developed different technologies, ranging from different patented offshore shellfish farming technologies, a closed greenhouse technology using solar energy for self-sufficient aquaponics in remote arid geographical areas to a modular prefabricated light weight steel construction building technology, which eventually was sold to a Swedish multinational. Pieter has served as a director on the board of asset management funds, family offices in Luxembourg and a state privatisation programme in Greece. He has recently also acted as a management consultant for Belgium's largest food retailer. He holds a BSc in Law from Erasmus University in Rotterdam, an LL.M from the University of London and an MSc in Investment Analysis from Stirling University.

Location

Singapore HQ

Ammbr Foundation operates from the heart of Singapore, and has access to tremendous resources and people as a result.

Global Presence Through Partnership

The Ammbr Foundation is building a strong network of international corporate and organizational partnerships to ensure it is able to deliver and roll out network coverage, user and community development, and support across as broad a geography as possible.

PART F

THE AMMBR TOKEN SALE

Updates in progress for Part F: Token Sale

Please note that certain details of the token sale outlined in Part F will be updated before a public token sale commences. As of 3 September 2017 the original public token sale has been put on hold and a new date has not yet been confirmed. Please ensure you subscribe to email updates to get any late breaking news.

Also, you should rely on the updated whitepaper that will be available at the time of the sale for updated details.

There has been a significant increase in the use of Token Sales to raise funds for projects, especially blockchain technology projects, in recent months. The benefit of this mechanism is that project creators are able to access funding directly from funders without the intermediaries often associated with other fundraising mechanisms. The drawbacks include a lack of consistent or relevant legal frameworks and definitive guidelines from jurisdictional authorities. Additionally, there are often questions posed about the ethics and effectiveness of raising large sums from token sales, without the necessary alignment of proposed outcomes and rewards.

The Ammbr Foundation has gone to great lengths to research, and seek legal advice, on its offering. Funding obtained through the token sale will be administered and governed by the Ammbr Foundation according to the Use of Funds section below.

Objectives of the Ammbr Token Sale

The Ammbr Token Sale has as its primary objective the raising of funding for the Ammbr Foundation. The remit of the Ammbr Foundation is the development and implementation of the Ammbr Network, and its sustainable governance and growth.

The second objective of the Crowdsale is the wide propagation of AMMBR tokens into the global marketplace. The Crowdsale is expected to see thousands of participants taking up ownership of AMMBR. Thereafter the tokens will circulate freely, ultimately as the means of exchange in the Ammbr ecosystem, spreading through marketplace dynamics to the providers of connectivity on the Ammbr Network (i.e. owners of Ammbr infrastructure) and the users of the Ammbr Network.

AMMBR Tokens

AMMBR tokens are ECR20[34] compliant, and are issued on the Ethereum blockchain. Significant work has been conducted by the many participants in the Ethereum project to ensure the integrity of the platform and the actual ECR20 tokens.

Public Solicitation

The Ammbr Token Sale is being published exclusively on the website www.Ammbr.com. There will be numerous communications to inform our target audience about the sale. As such, this is a public solicitation. However, no targeted solicitation of individuals explicitly excluded by virtue of their jurisdiction, e.g. non-accredited citizens of the USA, will take place.

On-Boarding of Contributors

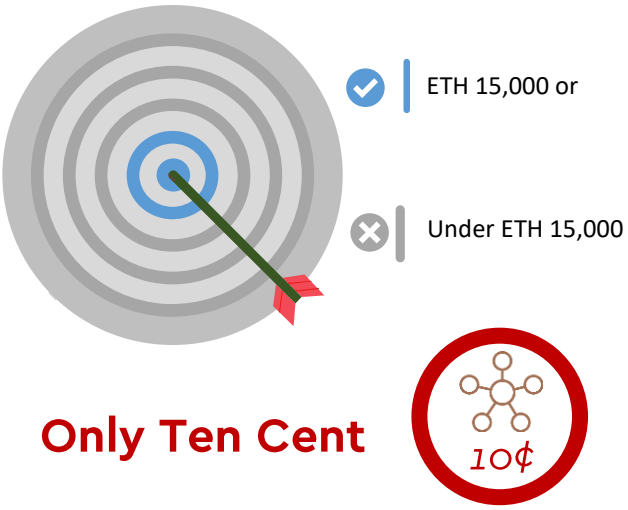
The nature of cryptographic token sales makes commonly adopted on-boarding processes difficult to apply. There must be a general reliance on controls, e.g. KYC/AML, as applied by cryptographic currency exchanges, to compensate for the largely anonymous nature of transacting in cryptographic currency.

[34] https://theethereum.wiki/w/index.php/ERC20_Token_Standard

Terms and Conditions

Minimum Raise

The AMMBR token sale is setting a total of **ETH 15,000** as its minimum target raise. Should the Crowdsale fail to raise at least this amount, the Crowdsale will be declared a failure and all contributions returned to their originating contributors.



Pricing

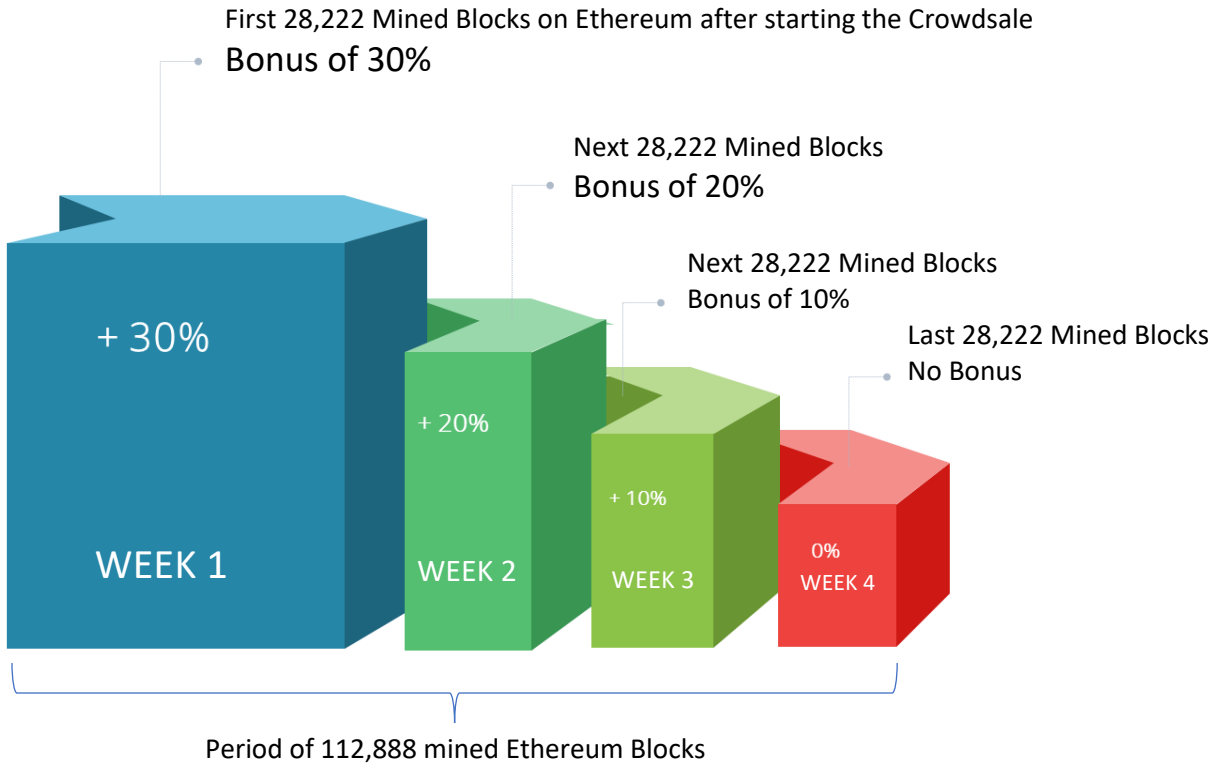
At the inception of the Crowdsale, the price per AMMBR in ETH will be set at the equivalent of $0.10 USD (Ten Cents). This value in ETH will persist for the duration of the Crowdsale.

Duration

The Crowdsale will continue for a period of 112,888 mined Ethereum Blocks.

Bonus Structure

To incentivise early but fair commitment to the Crowdsale, a sliding bonus structure will be offered. (*Periods of 28,222 mined Ethereum Blocks will used, and this roughly correlate to one week. Weekly periods are stated for convenience purposes only*.)



Token Sale Process

Individuals wishing to participate in the AMMBR Crowdsale will be presented with a number of terms and conditions to which they must agree, after which they will be directed to set up their target wallet, at which they will receive any AMMBR they purchase.

The process of setting up this wallet will be clearly explained and documented. The Ammbr 24-hour help desk will assist with any issues and queries.

Once the target wallet is set up, the participant will be presented with a form, wherein a selection is offered to make a contribution in ETH or BTC. The selection of either will result in a unique receiving address being generated and presented. The participant will then be able to choose to store and forward that address, or use the address to procure ETH or BTC directly from a listed exchange. Once the contribution is transmitted and received by the receiving address, the Crowdsale smart contract will issue AMMBR tokens.

Contributions to the AMMBR Crowdsale are paid to the Ethereum-based Crowdsale smart contract in either ETH or BTC at the receiving address created for the specific contributor. The purchased number of AMMBR tokens (pricing determined by the smart contract) are transferred to the contributor's target wallet. For the duration of this process, which should be no more than a few minutes, the contributed funds will be held in escrow by the smart contract.

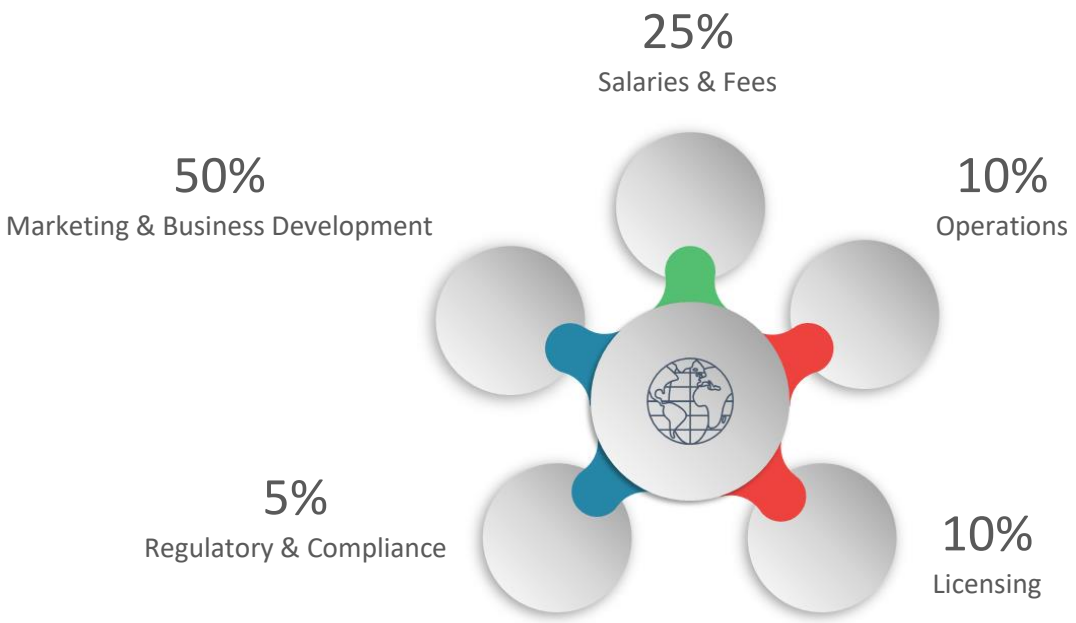
The (escrow) smart contract will then move these contributions to multi-signature wallets the instant the purchased AMMBR tokens are dispensed to the contributor's target wallet. The multi-signature wallets that will receive the contributions are hard wallets (Trezor and/or Ledger) that provide the highest currently commercial available level of security for cryptographic tokens. The multi-signature wallet co-signers are the directors of the Ammbr Foundation, and any use of funds requires signatures from three of the five directors (3 of 5 schema). The directors ensure that full corporate governance, including the diligent and accurate issuance of AMMBR in the Crowdsale, and the subsequent use of funds.

The funds are therefore protected should any issues be found with the smart contracts (as have been seen in the past with some projects or token sales). If the Crowdsale or token contracts have issues, or the Crowdsale fails to meet its minimum target, the Foundation can manually return contributions. In this case the Crowdsale smart contract can automatically issue a refund for all the participants. Funds will be moved back from the multi-signature hard wallets to the Crowdsale contract addresses and the participants will be able to initiate the transfer of the respective amount of ETH or BTC submitted to the smart contract from the smart contract's address back to the address used by that participant to transfer the ETH or BTC to the smart contract address.

This approach is preferred over leaving significant contributions in smart contracts or any centralised, online wallet. Any problems that may occur will not leave a large "honeypot" of funds subject to random issues or malign intent.

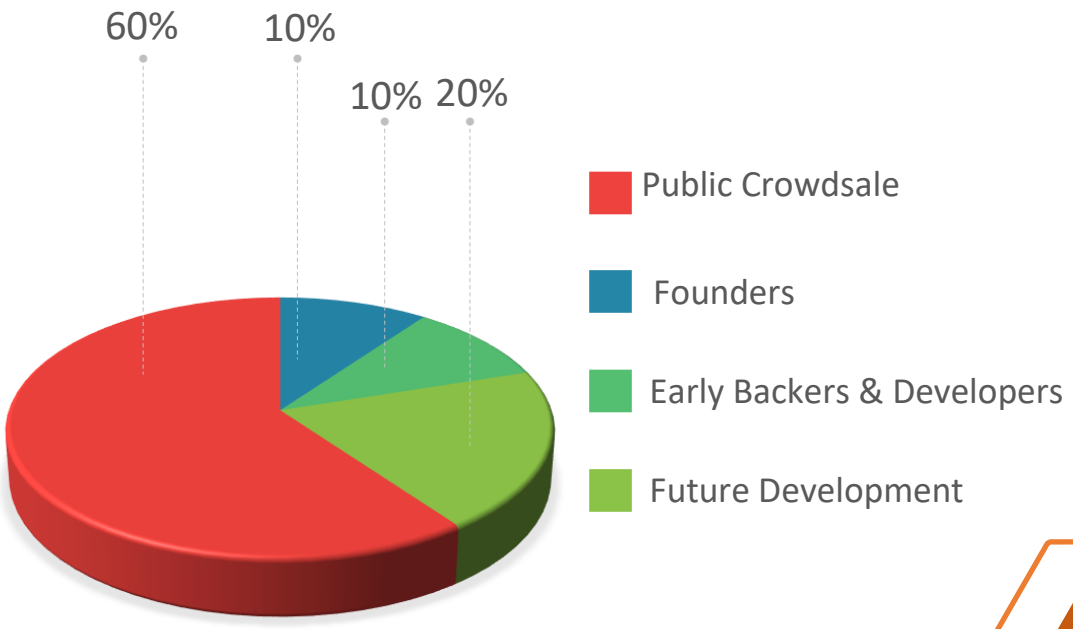
Use of Funds

The funds raised in the AMMBR Crowdsale will be applied to advance the development and implementation of the Ammbr network, and the global roll-out of the network.



Budget Allocation

AMMBR Allocation



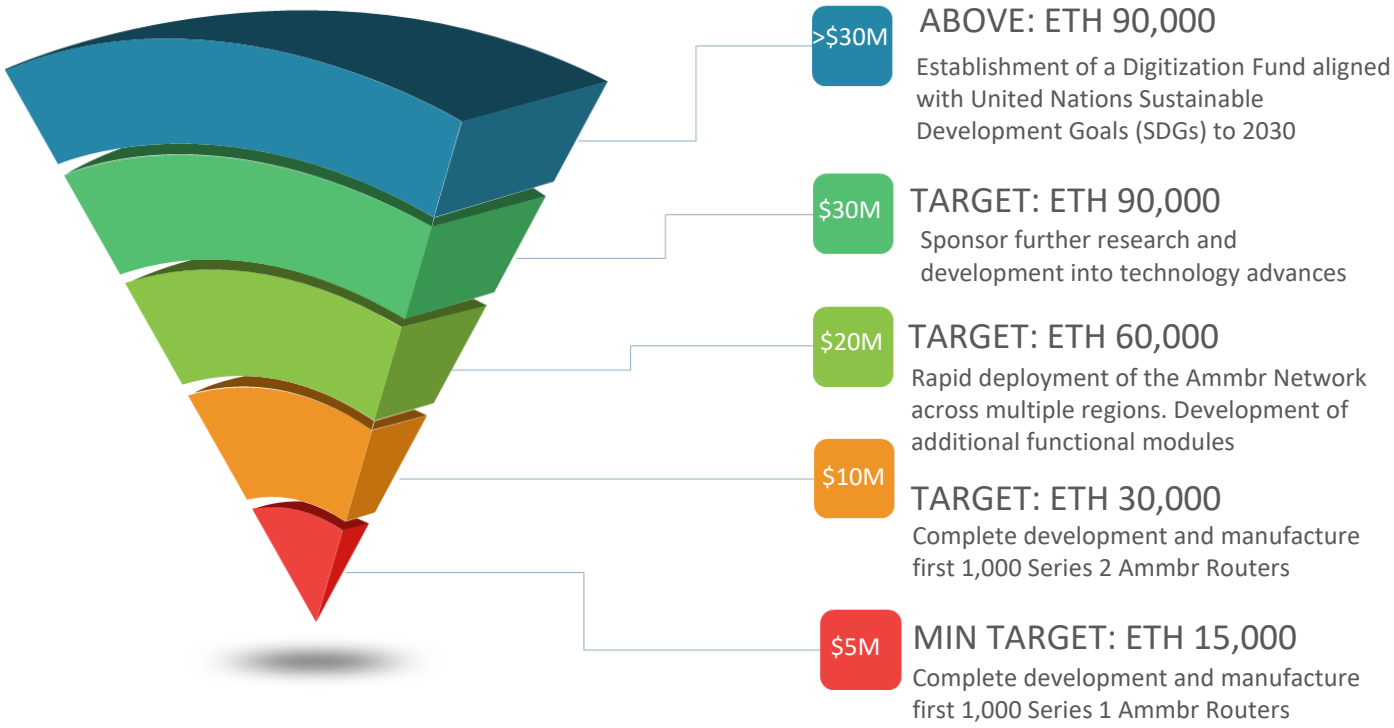
To Limit or Not to Limit

The decision was taken not to place a limit on the Crowdsale. The scope of our vision suggests that there is literally no limit - achievable through such a Crowdsale – to what can be spent rolling out a global telecommunications network. The marketing and advertising costs alone will be significant, and the opportunity to bring the so-called "Bottom of Pyramid" demographic into the market, while fantastic, will come at a cost.

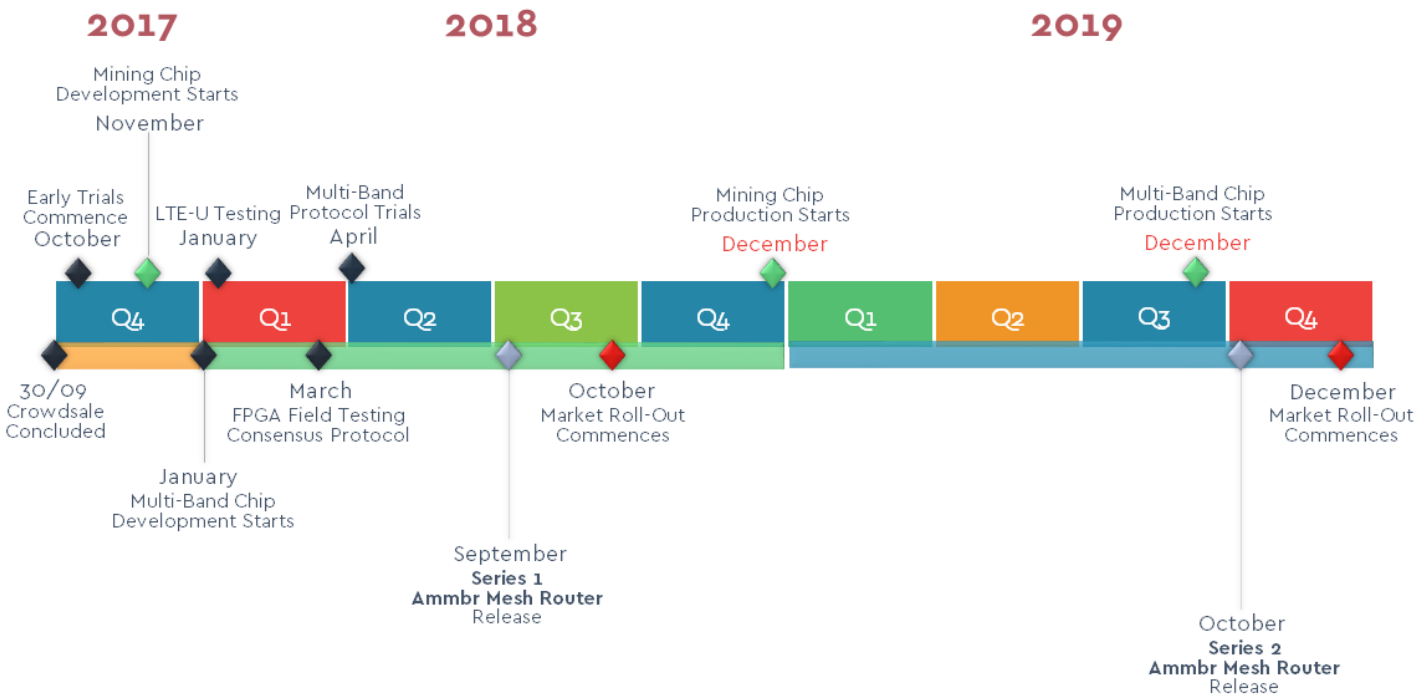
However, we also believe it is not healthy for a new venture to be handed enormous amounts of funds, well beyond their (unproven) ability to apply ethical governance. This is also potentially harms the very fundamentals which fosters creativity initially.

Our answer was to put in place a governance structure, with people who are able to apply the levels of ethical governance not normally found in a new venture, and to make it responsible for the sane application of funds raised. The Ammbr Foundation was the result of this decision.

So, while our goals are reasonable, the progressive application of funds to ever-larger goals laid out below will therefore be our response to whatever upper limits the market chooses to set.



Road Map



Risk Factors

Jurisdiction

The Ammbr Foundation is registered in Singapore, a jurisdiction that is well regulated and subject to the highest standards of governance. The Singapore MAS is the primary regulator administering the various statutes pertaining to money, banking, insurance, securities and the financial sector in general. However, the marketplace for the offered AMMBR is in its infancy and operates largely outside national boundaries in cyberspace. Regulatory standards are evolving, with segments of the market in the process of being regulated in certain jurisdictions, such as cryptocurrency exchanges. The ownership or resale of AMMBR tokens may therefore be subject to forces outside the control of the jurisdiction of Singapore.

Track Record

The Ammbr Foundation is newly formed (2017) and has no track record. However, the founding members have extensive qualifications and deep expertise that can be reviewed and evaluated. As with any early stage venture, the Foundation carries a significant risk in terms of its ability to deliver the products and services as described in this document.

Liquidity

The AMMBR tokens have no liquidity upon issuance, and only upon their inclusion among the offered cryptographic assets of the various exchanges targeted and described in this document will there be any practical means to achieve liquidity.

The liquidity of AMMBR tokens via these exchanges will be via other cryptographic tokens. There is a significant risk that the value of AMMBR on the exchanges, as well as any of the cryptographic assets they can be converted into, could decline, and then the initial investment made by a contributor could be lost.

Losses

Deposits made to, and holdings of cryptocurrencies are not insured or the subject of statutory protections in any jurisdiction. Any losses suffered through misappropriation, neglect, operational mistakes or other misadventures will likely be total and irrecoverable.

Viability of the Intended Utility Use

To the best of the available knowledge and information available to the Ammbr Foundation, both the technology and the envisaged sharing economy for telecommunications services could never materialize, or be proven viable or sustainable. This could prove severely detrimental to the value of AMMBR acquired in this Crowdsale.

Failure of the Token Sale

The Ammbr Foundation may not reach the target sale amount, and may subsequently not have sufficient funds to execute on its development and roll-out path.

Delays Due to Unforeseen Circumstances

The technology being built and the market dynamics involved in launching novel solutions and new business models involves significant complexity. Delays and failures on some or all of the facets are possible.

Ceding the Leading Position

While we are confident of our significant lead over current competing solutions, we are in a highly dynamic and fast-moving market sector - both in telecommunications and blockchain. It is possible that we may lose our leadership position, or simply be superseded by superior solutions.

Cybercrime

Token sales have come under attack from malicious players, and both the Ammbr Foundation and participants in the Crowdsale must remain highly vigilant throughout. Regardless, a risk remains that such an attack could occur and severely disrupt proceedings.

This white paper has been prepared in compliance with industry best practices and regulations as understood by the authors at this time. This white paper is not a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction.

A copy of this white paper has been delivered to the Monetary Authority of Singapore (MAS) for information purposes, although there are no pertinent regulations at this point that require approval or registration. Seeking approval, whether tacit or express, of this white paper by the MAS is not undertaken as an indication of the merits of the Ammbr Foundation or its cryptographic tokens. The cryptographic tokens offered in this white paper have not been approved or disapproved by the MAS or any other regulatory body in any jurisdiction.

Legal Discussion

The technology behind Ammbr is innovative, enabling a global peer to peer telecommunications network where ownership of bandwidth is distributed and where the operational infrastructure is not dependent on a single-provider model. The technology underlying the Ammbr Network, with hardware and software features, supports 'Net Neutrality' which does not discriminate based on applications and does not block content.

The Ammbr modular mesh router is designed for individual and SoHo usage and is deployed to create the distributed mesh network. The operative aspect of the network is conditional upon active involvement of Ammbr participants, either through ownership of Ammbr devices or as a user of network services. The Ammbr crypto token, AMMBR, is thereby a prerequisite for the operation of the Ammbr mesh network, through its primary intra-network usage as a micro payment medium of exchange among the network's participants.

Technically speaking, Ammbr network presents a 'next generation' blockchain technology, with its innovation being both on the marketplace level as well as on the governance level. In Ammbr, value is concentrated at the marketplace layer and exchanged among its users. The distributed nature of the marketplace is contrary to the centralization of value seen in the large organisations that currently capture the majority of value from the Internet substrate. Ammbr network's marketplace, built on blockchain technology, is constituted of its proprietary digital identity framework, its token driven value exchange and its mesh network utility.

Ammbr network's underlying technology allows the network to achieve scalability, security and transparency. The technology can address unresolved areas related to, among others, accessibility and trust between unknown online actors. In particular, Ammbr network is addressing the weaknesses of existing blockchain technologies by using a higher speed of transaction validation, better energy efficiency, self-sovereign digital identity-based security, and a generally more robust consensus mechanism. The Ammbr blockchain validation system for reaching consensus among participating nodes for proposed transactions is based on the Ammbr Foundation's proprietary Proof of Velocity (PoV). The Foundation's main responsibility during the Crowdsale is the diligent issuance of AMMBR to participants according to the terms described in its constitution. The Ammbr network ecosystem further consists of a team of developers, who have designed the network's consensus mechanism and networking features. The Team will continue developing Ammbr network's technical components, including the algorithms, after the AMMBR Crowdsale.

The nature of AMMBR is grounded in the PoV consensus mechanism and, as such, is pre-conditional to the successful creation, building up and functioning of the connectivity marketplace. AMMBR is restricted and limited to the exclusive use as a micro payment medium of exchange and its value would be determined by market forces such as supply and demand. The design of AMMBR as such is purposed for the Ammbr mesh network to achieve streamlining of specific transactions between Ammbr network participants, even though they may be unknown to each other. AMMBR, therefore, cannot be substituted by any other financial incentive in any form whatsoever.

No transaction on the Ammbr network can be considered as a pre-payment for product or services, like vouchers, despite the fact that the Ammbr network is facilitating the exchange of services and products against AMMBR. Contrary to vouchers however, there is no obligation by the Ammbr network ecosystem, as partly represented by its participants or users, to deliver or accept any of the possible product or service based transactions which may occur between participants and users. AMMBR is therefore a simple means of exchange subject to the time and venue of transaction and is not bound by any intrinsic obligations or rights.

With regards to blockchain functionality on the network, participants would make computer processing available on Ammbr mesh devices in exchange for transactional fees denominated and paid for in AMMBR. This would result in validation of a set of transactions recorded in blocks, which, after having obtained consensus through PoV from certain Ammbr nodes, are added to the network's decentralised payment ledger.

Participants, as independent operators, are in day-to-day control of the management of their property, forming part of the overall Ammbr mesh network. As such, they are intrinsic to the well-functioning of the Ammbr network collective ecosystem. The Ammbr blockchain component, in particular, would avoid the occurrence of double-spending or the introduction of counterfeit AMMBR. The rewards for participants' consensus work or networking facilities are received as a number of AMMBR and created via automated decentralised micro payment transactions. AMMBR can only be received by participants or users as a reward, donation or gift, from the volume of AMMBR in circulation and cannot be freshly created or issued as a result of activities performed. Owning AMMBR is, however, not entitling participants to any collective Ammbr network related ownership interest nor dividend from any fees or profits generated other than from the specific transactions under their control. In fact, there is no purpose or effect on the Ammbr network, which would allow any of the income, profits, rewards, donations or gifts received by participants to be pooled or controlled by any other operator than the participants themselves.

Moreover, AMMBR is kept in digital wallets used for storing cryptographic keys and transaction authentication codes, initiating transactions and providing an overview of transaction history. These wallets denote a core function to the Ammbr ecosystem and as such are exclusively linked to the digital identities of the individual participants.

Two types of wallets can be used on Ammbr network, online wallets (hot storage) and offline wallets (cold storage). Participants or users cannot initiate or authorise transactions on the Ammbr network without making use of the authentication provided by their individually controlled wallets. During the enrolment of a newly set-up wallet into the Ammbr network, participants and users are not requested to agree on a contract with the Ammbr Foundation or to pay a participation fee, nor is personal or sensitive payment data needed for making AMMBR micro-payments.

In particular, the Ammbr network's digital identity framework provides for full pseudonymity between parties for transactions, which, apart from enhanced security, is a relevant factor for data controllers or processors who, among others, in the EU, are required by law to limit their liability in relation to potential breaches of customer data privacy. Pseudonymity, as opposed to anonymity, allows for regulatory Know Your Customer (KYC) compliance, in particular in the case of AML/CFT (anti-money laundering, respectively the countering the financing of terrorism.[35]

It is our opinion that AMMBR is a micro payment medium of exchange distinct from alternative existing financial incentives, due to its functionality as a conditional part of the network's unique validation mechanism, as well as due to the non-obligatory, ad-hoc, nature of engagement by the network's participants. Moreover, the advanced levels of individual control exercised by participants, including the use of pseudonymity for digital identities, are part of the argument that would exclude AMMBR as an instrument defined as a unit of CIS or a security instrument under current Singapore and USA legislation.

[35] Payments on the Ammbr network cannot be linked to a payment instrument, payment account or person, but only to the participant's chosen pseudonymous digital identity.

Conclusion

The Team has brought together diverse experiences and training in a shared vision of technology advancement that can have material impacts in people's lives, and spawn innovations in the way we do business, organize and communicate. While the journey has just begun, we are all thrilled to be part of this venture into the unknown.

Over the coming months we will be releasing more information, and product that should evince robust debate, exhilaration, curiosity, and perhaps even outright dismissal from some quarters. In any event we love what we are doing, and the people we are privileged to work with in the process.

To those who have or will participate in, and contribute to our efforts, we thank you.

Full details will be presented on the website on or before 1 September, 2017 explaining how to participate in the Crowdsale

www.Ammbr.com

Final Disclaimer

The statements contained in this white paper are believed by the authors to be reasonably accurate in all material respects; however, during the offering period the authors reserve the right to revise or correct any statement contained herein in the event of any material change in circumstance, including any change of any applicable rule or regulation that becomes known to the authors.