



THE END OF SURVEILLANCE

# PROMETHER WHITEPAPER

VERSION 1.1.0

ELTON BRAUER

ERIC J ANDERSON (EIJAH)



PROMETHER.COM



PROMETHERGROUP



@ENDSURVEILLANCE

## **ABSTRACT**

The rapid evolution and enabling features of science and technology has made us entirely dependent on connectivity. The limitless possibilities, offered by an always-on Internet, has ushered in a new era of human collaboration and creativity. We are now at the precipice of true global interoperability, with the power to change the future of humanity. And thus begins a third era of technological evolution we refer to as the Internet of Things (IoT).

The world has become a living interconnected organism, enabling us, and all our surroundings, to connect freely with access to more information, services, and means of communication. But this does not come without sacrifices. While the Internet introduced a borderless system, companies did what they do best – they took advantage of an opportunity and created their own borders with the goal of gaining control, making money, and self-preservation. Due to lack of awareness, people willingly handed over their data to companies, websites, and application providers, choosing convenience over security. It did not help that we combined this centralization of control and data with unreliable systems of user passwords, logins, security questions, and other means of authentication. Unfortunately, that turned people into products and drew the attention of malicious parties looking to exploit the system, leading our governments to start treating all citizens like criminals.

With all of its innovation, the Internet has served to unite the world, but also created means for the powerful to grasp more control and oversight – it became both our savior and executioner. Unless we begin to hold the tech industry accountable by building and using new secure and private solutions, there is no incentive for them to change, as they make too much money hosting our data and controlling our identities. This is why we believe there is a need for a new platform that puts privacy first, irrespective of the network topology or architecture. We have chosen to give power back to the users by building the first truly free, secure, and open decentralized network powered by the blockchain – Promether.

Promether is a new type of network called an Adaptive Symbiotic Network (ASN). Based on the principles of Artificial Intelligence (AI) and Ubiquitous Computing, Promether allows anybody to create secure and anonymous networks simply by deploying a series of reusable software components. Whether you're an individual trying to build your first app, a company who needs to develop a global service, or even a government that wishes to establish secure communications - Promether is flexible enough to adapt to everyone's specific networking needs. The vision for Promether is to become a global secure networking infrastructure for developers, miners, users, corporations, and governments. By merging blockchain based incentivization with secure decentralized networks and providing benefits for every participant, we will bring about the end of surveillance.

To build this sort of incentive-based decentralized network, Promether will develop an application building block, modular network, decentralized VPN, secure communications framework, decentralized data sharing and storage solutions, distributed computing platform, and fully self-sustainable ecosystem. These functionalities will allow Promether to become the decentralized network of the future. Additionally, unlike other decentralized and persistent networks, basic use of the Promether Network is completely free, irrespective of coin ownership. To accomplish this, a small percentage of total network capacity will be reserved up front. The remaining network capacity will be divided up equally according to the ownership of coins.

With an 18 month roadmap, Promether aims to create a network that draws inspiration from the Internet as a security driven decentralized social space. Now is the time to regain our individual control and safeguard our privacy, freedoms, and personal liberties from extinction. We will redefine the rules that govern the masses, and build a new paradigm of security on the Internet without authority, trust, centralization, giving up control, or the ever-watchful eye of Big Brother.

# TABLE OF CONTENTS

<b>ABSTRACT.....</b>	<b>i</b>
<b>TABLE OF CONTENTS.....</b>	<b>ii</b>
<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 The Age of the Internet.....	1
1.2 Virtual Globalization.....	1
1.3 Internet of Things.....	2
<b>2 PROBLEM STATEMENT.....</b>	<b>3</b>
2.1 Surveillance, Big Data, and The Centralization of Control.....	3
2.1.1 Corporate.....	3
2.1.2 Governmental.....	4
2.1.3 Individual.....	4
2.1.4 The Consequences Are Real.....	5
2.2 Privacy, Identity and Human Rights.....	6
2.2.1 The Compromised Universal Identity.....	6
2.2.2 Privacy and Obligation.....	7
2.3 The Broken State of the Internet.....	8
2.3.1 The Centralization of the Decentralized Internet.....	8
2.4 Summary of Problem Statement.....	9
<b>3 PROPOSED SOLUTION.....</b>	<b>12</b>
3.1 Motivation For Promether.....	12
3.2 Introducing Promether.....	13
3.2.1 Promether Demystified.....	13
3.2.2 Visions and Goals.....	13
3.3 Promether as the Future of Decentralized Networks.....	15
3.3.1 Promether as the Application Building Block.....	16
3.3.2 Promether as the Modular Network.....	16
3.3.3 Promether as the Decentralized VPN/Anonymity Network.....	17
3.3.4 Promether as the Secure Communications Platform.....	18
3.3.5 Promether as the Decentralized Sharing and Storage Solution.....	19
3.3.6 Promether as the Self-Sustained Distributed Computing Platform.....	20
3.4 Competitive Comparison.....	20
<b>4 TECHNICAL OVERVIEW.....</b>	<b>21</b>
4.1 Application Programming Interface (API).....	21
4.1.1 Networking Library.....	21
4.1.2 Security Library.....	21
4.1.3 Anonymization Library.....	22
4.1.4 Compatibility.....	22
4.2 Nodes.....	22
4.2.1 States.....	22
4.2.2 Features.....	23
4.2.3 Compatibility.....	24
4.3 Services.....	24
4.3.1 Service Types.....	24
4.3.2 Mutable Services.....	25

4.3.3 Immutable Services.....	26
4.4 Network.....	27
4.4.1 Network Architectures.....	27
4.4.2 Features.....	28
4.5 Applications.....	29
4.5.1 Integration Models.....	29
4.5.2 Compatibility.....	30
4.6 Data.....	31
4.6.1 Data Types.....	31
4.7 Users.....	31
4.7.1 User Types.....	32
4.8 Utility.....	32
4.8.1 The Growth Cost Problem.....	32
4.8.2 The Architecture.....	32
<b>5 COIN PROPERTIES AND ECONOMICS.....</b>	<b>34</b>
5.1 Overview.....	34
5.1.1 Distribution.....	34
5.2 Ecosystem.....	35
5.3 Economics.....	36
5.3.1 Stakers.....	36
5.3.2 Users.....	37
5.3.3 Funding.....	38
<b>6 CHALLENGES.....</b>	<b>39</b>
6.1 Perfect Security Does Not Exist.....	39
6.2 Awareness.....	39
6.3 Development Needs.....	39
6.4 Technical Considerations.....	40
6.5 Regulatory Considerations.....	40
<b>7 ROADMAP.....</b>	<b>42</b>
<b>8 PROMETHER TEAM.....</b>	<b>43</b>
8.1 Core Team.....	43
8.2 Advisors.....	44
8.3 Strategic Partners.....	46
<b>9 CONCLUSION.....</b>	<b>47</b>
<b>FOUNDER'S ACKNOWLEDGEMENTS.....</b>	<b>47</b>
<b>REFERENCES.....</b>	<b>48</b>

# 1 INTRODUCTION

## 1.1 The Age of the Internet

The progressive transition to the ever-changing digital age has brought about life-altering technological advancements and introduced us to a new world of endless possibilities in connectivity. Can one even imagine a world where computers, laptops, smartphones, television, and other connected devices are not part of our daily lives? For instance, the number of monthly texts sent alone increased more than 7,700% over the last decade, and that does not even count for app-to-app messaging (Statistic Brain, 2016). As science and technology evolved, lifestyle began to be connected to, and dependent on, connection, and as we continue to progress in this age, the influence and role of it is expected to grow even more.

*"Computers handle huge amounts of data, with power and accuracy which previous generations could have only dreamed of. Combined into networks, they enable wealth creation, pleasure, social life and the dissemination of culture and knowledge. They are so embedded in the way we live, work and play that we cannot function without them. We need it for private lives, for our social lives, for our household banking, transport, health and entertainment, and also to keep our public services and infrastructure running."*

(Lucas, 2015, p.37)

The backbone of it all, the Internet, has helped create a global nation – a world where with the power of the Web and connected devices, we can unite with anyone, anytime, and anywhere (Kotler, 2016). From entertainment to employment, from shopping to business and education, from relationships to how our brain functions, and much more, Internet has become the central nervous system of modern life.

## 1.2 Virtual Globalization

The rapid expansion of Internet-driven services have also played a major role in expanding the possibilities and scope of globalization – that is, a progression of growing possibilities for global interaction between people, facilitated by technology (Whittaker, 2002). One can possibly even refer to globalization as one of its defining features – after all, it is more of a social space than a "thing". We can argue, then, that the Internet has redefined what proximity and distance means, as well provided a shift in how we understand belonging and communities.

*"In fact, describing the Internet as a site of "exploration," "encounter," or "dialogue" means taking stock of one of the potentials this technology harbors: this virtual space can (potentially) provide a site of socialization that is an alternative to customary communities and, for this reason, help to redefine the relationship of individuals to "socialization" and "belonging."*

(Lagasnerie, 2017, p.109).

When taking Laganerie's (2017) theory of belonging as the foundational premise, belonging has changed to represent a choice where people are less constrained by the forced sense of associations that have been imposed upon us by nationality and location, often making it difficult to differentiate individual from the collective. In a world of the Internet, belonging is less constrained by those associations and opens possibilities to free oneself to global opportunities and belonging not bound by restrictions, borders, censorship, and societal duties. Communication, commerce, knowledge, forums, financial markets, media, different services, entertainment, Internet communities, and just about anything else – all of it is accessible without borders to anyone, making the world a global playground with universal language and us, as popularized by infamous hacker group Anonymous, "Citizens of the World".

### 1.3 Internet of Things

In an era where the distant world of yesterday has transformed into a connected, interactive social space of today, we have begun to exceed the limits of human collaboration and constraints of time and space. However, driven by the innovations of the Internet, the limitlessly connected human collaboration has also created the potential for connecting anything and everything to each other through the same technology – a third stage of interconnectivity (following the computer and the Internet) referred to as the Internet of Things (IoT). While the Internet has taken us on a new path of discovery, IoT attempts to take us on a new path of operational efficiency.

*"The Internet-of-Things (IoT) is a self-configuring and adaptive network which connects real-world things to the Internet, enabling them to communicate with other devices and objects. Advancements in science and technology enabled making smaller, cheaper and faster computing devices capable of sensing the environment, communicating and actuating remotely, which resulted to the increased interest of applying the IoT to vast aspects of life, such as smart cities, healthcare, smart home, etc."*

*(Negash et al., 2018, p.3)*

IoT is already taking over and is expected to connect more than 50 billion devices to the Internet by 2020 (ETCIO, 2017). It is also important to note that IoT has enabled us to not only connect between each other, but connect machines with machines, humans with machines, pets with machines, pets with humans, etc. As the now-global nation once separated by differences and conflict, the world has become a big living, interconnect organism, enabling us to connect freely – and the possibilities of connection have just began to reveal themselves, with much more to follow.

## 2 PROBLEM STATEMENT

### 2.1 Surveillance, Big Data, and The Centralization of Control

The Internet and connected devices have introduced a more interconnected society than ever before. People around the world have access to more information, services, and means of communication, but it does not come without sacrifices. Aside from companies and governments using this dependence to serve manufactured narratives, censor and filter information, and manipulate towards self-interests, there is also a drastic vulnerability in privacy. By giving data access and privilege to companies, websites, apps, etc., we make a choice to prioritize convenience over security – a phenomenon that has turned people into products, drawn the attention of malicious hackers, and incentivized the surveillance from even our own governments (Angwin, 2014). We have become obsessed with convenience to the point where we are willing to sacrifice anything for it, without even stopping to consider that the trade-off might help the benefactors (people with access to your data) more than the users. Putting trust in companies, websites, apps, and people online on the basis of fragmentary reasoning, has exposed us to three primary modes of surveillance - corporate, governmental, and individual – each with their own reasoning and agenda (Lucas, 2015).

#### 2.1.1 Corporate

How many read the Terms of Service of something they sign up for on the Internet – that is, the long list of text that we have to accept by ticking a box before pressing “Sign Up”. Truth is, most do not bother nor care, which is exactly what corporations use to their advantage. Put simply, they collect data about everything we do online – from what websites we visit, to personal information, to what we like, share, view, etc., and even statistics related to what time, location and engagement we issue to those things.

*“Commercial surveillance is indeed a powerful business tool. Businesses like to know as much as possible about their customers. Some of them may be more intrusive than others. Individuals do not have a general right to know what information is held about them.”*

*(Lucas, 2015, p.201)*

There are multiple reasons why corporations collect data, but the primary motivations are related to customer engagement, needs, and ultimately, profit. It is not unreasonable to consider surveillance as the business model of the Internet, since all bigger websites run by monetizing traffic – it is simply a game of ROI (Return on Investment), where the open marketplace of bidders try to capitalize on consumer data. Supported by Angwin’s (2014) conception of surveillance, it can be stated that the more personal and targeted that traffic is, the more potential there is to increase revenues, and as long as users remain the passive product without resistance, there is no burning incentive to provide any real privacy.

If that does not sound alarming, consider how Facebook collects information about everything we do online, and uses that data to predict users’ interests in the coming days, weeks, and months. In his interview with Stanford Graduate School of Business (2017), the ex-CEO of Facebook, Chamath Paliapitiya, indicated that the social media giant has created social feedback loops based on dopamine inducement, which encourages people to be stuck in their habits and systematic lives. He even made statements how Facebook exploits the very fundamentals of human psychology, leading to people being literally programmed through neurological pathways and rewiring of the brain and habits. Furthermore, Netflix decided to use big data to *design* a successful show called “House of Cards” - a series which success was predetermined based on patterns observed from user data (CIO, 2017). Keep in mind that this is all possible only due to the quantity of collected user data, allowing companies to analyze behavior patterns and design

ways to dictate and change them. When companies can start manipulating people and designing the society in a way they see fit, access to too much data is a threat, and it needs to be changed. As Bruce Schneier (2017) stated in his interview with openDemocracy:

*“There’s nothing wrong with public social media and social networks and how we communicate through them. But we start having problems when something as powerful as Facebook is run by a for-profit corporation. It’s not operating in the interest of its users, but in the interest of their customers – the advertisers. They’re making money in a regulatory world where they are allowed to exploit all of their users, spy on them, run social experiments and manipulate them for profit.”*

If we continue to *voluntarily* surrender any control and privacy over our data, which we are not obligated to do (neither socially or legally), we are greeted with a world infested by surveillance capitalism, and most importantly, we ourselves are the ones to blame.

### **2.1.2 Governmental**

Data collection for profit is certainly not the only reason for concern, or the way data is handled for that matter. Most of those corporations do not only serve their self-interests, but are also forced to facilitate the needs of the government. The issue is elevated by governments “piggybacking” on the tech company’s reach, influence, and capabilities, in order to conduct their own surveillance. Anyone remotely engaged in today’s society probably knows about the former NSA contractor Edward Snowden – a man now deemed national enemy at the risk of facing military trial and lifelong prison sentence due to “espionage” and “high treason”. While such introduction sounds illicit at first, Snowden is viewed as a national, if not global, hero by many. From June 2013 on, Snowden has engaged in exposing NSA and other intelligence services to the world – by publishing documents which show how the United States set up massive-scale data-gathering systems to monitor and spy on the people across the globe. Programs like PRISM, revealed by the same man, has brought to light how giant corporations like Google, Apple, Microsoft, Facebook, Yahoo, Youtube, AOL, Skype, Paitalk, and more, share data to the government and allow them direct access to confidential information. The following conception by Lagasnerie (2017, p.12) exemplifies the situation perfectly:

*“Anyone at all, the world over, is now exposed to the watchful eye of power: e-mails, telephone calls, and exchanges on social networks could be – or have long been – archived, collected, and examined by intelligence services, police agencies, and others. The state is increasingly installing systems of surveillance and data-gathering mechanisms that operate on an international level; this matter no longer concerns just individuals suspected of being involved in criminal activity or terrorist enterprises, but everyone.”*

With the increasing number of programs created for the sole purpose of surveillance, essentially nothing is allowed to remain foreign. PRISM was just the beginning, with countless others already being in the works, and potentially many others unknown to the public. To name a few, projects such as FAIRVIEW, CISA, STORMBREW, XKEYSCORE, BULLRUN, Edgehill, etc., have undermined the right to privacy and stripped us from our private life. When corporations are literally forced to hand over consumer data, and communications are constantly intercepted (TED Talks, 2014), we need to start taking steps to ensure, or at the very least consider, measures of keeping ourselves safe from the centralization of control.

### **2.1.3 Individual**

The centralization of private data by ISPs (Internet Service Providers), social media, e-mail services, marketing companies, and others in the tech industry is a fundamentally glitched system. By storing all that sensitive and extremely valuable information in one central location, companies put a target on their back – and not just in the eyes of government agencies, but also individual threats like malicious hackers, data thieves, and rogue employees. Businesses have come to



depend on electronic data and computer networking, which has created an incentive to grow databases of personal and financial information, and therefore expose that pool of data to privacy violations and breaches in data security. This leaves countless people vulnerable to identity theft and the use of their personal data for fraudulent activities. Eijah, the creator of Demonsaw, calls it “The Potato Chip Problem” - if you were offered a million USD to run a mile, you probably would, but if you were offered a potato chip for the same mile, you most likely would not. The same happens with the centralization of data, as all of that information in one location is a huge reward and extremely tempting, but what if there was only one file there – would an attacker still be tempted? Supported by Edward Snowden’s statements in TED Talks (2014) interview, trusting corporations and the government with the entirety of human communications and data is simply too big of a temptation to be ignored, and it exposes the users to immense breach in personal security and privacy.

But it is not just hackers who threaten our personal security as a consequence of centralized data. In fact, the focus is increasingly shifting towards safeguards against disloyal and rogue employees, who based on many security analysts, pose a greater threat to companies’ data than hackers. In his conversation with The Christian Science Monitor (2016), Avivah Litan, an analyst at advisory and research firm Gartner, stated that *“a lot of companies are really worried about employees walking off with their data. Insider threats have become a major issue because external criminals are actively recruiting insiders to help perpetuate their crimes, while disgruntled employees are actively making their insider services available.”* Therefore, users are not only threatened by hackers, but also employees working for self-gain or even worse, in allegiance with hackers. This means that people in privileged positions, working in data-rich organizations, are being recruited by individuals and organizations looking to get access to that data, expose it, or use it for some sort of personal advantage (e.g. corporate espionage). The same threat can also expose network credentials, backdoors, and confidential corporate data to criminals or people looking to use it for illicit gains - also often sold in the Dark Web. It is an industry wide-issue, as proven by the Grand Theft Data report by Intel in 2015, which reported that 43% of all data loss and illegal forwarding can be blamed on insiders.

### 2.1.4 The Consequences Are Real

Surveillance, big data, and the centralization of control has created a lot of opportunities for companies, but in its present form, it is simply not sustainable. Centralization definitely has its benefits, but it is too big of a security risk for users, backed by the countless failures in systemic centralization of data as evident from the following examples:

#### YAHOO

3 billion Yahoo accounts hacked and data stolen after massive server breach.

#### DROPBOX

68 million email addresses and passwords leaked. 2/3 of all customers exposed.

#### CLOUDFLARE

Massive leakage of private session keys and other highly sensitive information of clients.

#### ICLOUD

Over 500 private pictures of celebrities leaked due to iCloud API and phishing.

#### TARGET

110 million peoples’ highly personal credentials breached. Information sold and leaked.

#### EQUIFAX

Tax IDs, driver’s licence, social security numbers, etc. of 145 million customers exposed.

#### SNAPCHAT

90 000 Private Photos and 9000 Hacked videos leaked off the mobile app Snapchat

#### UBER

Data of 57 million Uber customers stolen. Uber paid \$100 000 to cover it up.

#### LINKEDIN

Personal credentials of 6.5 million users stolen and leaked by cybercriminals.

#### SONY PICTURES

Massive leak of confidential materials. Data exposed to malicious actors.

#### TELEGRAM

15 million user’s accounts, phone numbers, IDs and messages exposed.

#### SWIFT

\$81 million stolen. A typo by hackers avoided further \$1 billion in damages to SWIFT.

#### OPM

Records of 21 million people exposed, including breaches in government data.

#### ADULTFRIENDFINDER

Reports of 360 million users’ passwords and emails hacked and leaked.

#### IPHONE

All devices affected by major Intel bug. All customers’ sensitive data could be read.

#### DNC

Internal emails hacked within DNC servers. U.S. Presidential Election altered.

#### MYSPACE

Usernames, passwords, emails, and other sensitive information of 412 million users exposed.

#### TUMBLR

65 million passwords exposed after a massive data breach. Data sold on the darknet.

#### NSA + WANNACRY

NSA Cyber weapon leaked, allowing hackers to compromise over 300 000 machines

#### PETYA

Petya malware spread to FedEx, WPP, Rosneft, Maersk, etc. Users’ data exposed.

These are the companies, applications and intermediaries we use daily, and in which we place tremendous amount of trust and data - but is it really justified? If that seems too much, keep in mind that the indicated examples are just *some* instances brought out to make a case, but are far from the only breaches in the security of the centralized protocols we rely on. Data is the new oil, and it is the sole foundation of every major corporation's profits, making it one of the biggest targets and temptations for hackers and insiders. Even worse, once that information is out there, it will be out there forever, with victims being at the mercy of those who use it.

## 2.2 Privacy, Identity and Human Rights

### 2.2.1 *The Compromised Universal Identity*

Identity is what makes us human, and more importantly, what makes us unique – take that away and we are nothing but an empty shell. As we are no longer the definition of our physical presence in the world overtaken by devices and connectivity, it is our data that defines our existence and how the world sees and interacts with us. However, by giving away our information and allowing corporations, governments and criminals to handle it, we are stripping away from the very thing that gives us our humanity.

*"The single biggest danger we face online is to our identity and reputation. These are what make us people. A name is a person's most fundamental attribute. When we want to dehumanise a captive, you give him or her a number. Reputation – what people think about us – is our currency in society. With a bad reputation, your past misdeeds dog your steps into the future."*

*(Lucas, 2015, p.55)*

Our online identity may feel as secure as a bank vault, but it is wide open for an attacker who knows what he is doing. When we mix the centralization of control and data with unreliable systems of user passwords, logins, security questions and other means of authentication, a single mistake, ours or the company's, can give access to everything we do online. This means that in the modern world, if something happens with us electronically, it is also our real life that suffers as a consequence. There is a very strong idea put forward by Lucas (2015) about how identities guard a lot more than just private lives. He expresses how it is extremely unlikely for one to lose all personal possessions at once – things like keys, identification documents, driving license, wallet, etc., and even if it was to happen, a thief could not really use them simultaneously and instantly. However, as electronic identity is mostly stored in one location and combines the features of all physical possessions that govern access to one's life, it is much easier to get access to it and make use of it right away. And as for the consequences – they are correspondingly more damaging and endanger our identities, as the holder of this information can impersonate us without physical limitations.

*"Impersonation based on stolen credentials enables attackers to hijack computers, steal money and defraud other people. They can also be springboards for other, more sophisticated attacks. Many – probably most – victims will not know that they are at risk. Many of the sites from which the identities are stolen do not know they have been breached."*

*(Lucas, 2015, p19)*

The 2017 Identity Fraud Study, released by Javelin Strategy & Research, found that \$16 billion was stolen from 15.4 million US consumers in 2016, compared with \$15.3 billion and 13.1 million victims a year earlier. In the past six years, identity thieves have stolen over \$107 billion – and that is just in the US alone. Globally, the Center of Strategic and International Studies indicates an annual loss from cybercrime of somewhere between 375 and 575 billion US dollars, with numbers increasing every year. Stealing identities has become as easy as taking our card when we aren't looking, digging through

mail or trash for bank statements or other documents containing personal details, buying information from inside sources (such as company employees), skimming information from ATMs with special devices, swiping personal information from unsecured websites or public WiFi, stealing electronic data through data breaches – the list goes on and on (Investinblockchain, 2017). Is this the type of security we had in mind when trusting everything to centralized bodies? By allowing corporations, banks, governments and hackers to facilitate everything we do online, and giving them the means to handle all our information, we are not only targets of credit, debit, and checking and savings account frauds, but also subject to all sort of data leaks where our information is misused or manipulated for illicit gains. Essentially, the more information people have about us, the easier it is to get by the protocols and security systems set in place by companies to make sure they are dealing with the right person. But as the user does not need to be there physically, our information is everything one need to *become* us.

### **2.2.2 Privacy and Obligation**

What about our right to privacy, the basic principles of human rights, and our obligation, as citizens, to aid in running a well-functioning democratic system? As Edward Snowden has expressed, our privacy matters, because you never know when you might need it. What signifies the broken system of democracy, though, is the restriction to act within legal rights when it goes in conflict with our government. The mass media, NGOs, and even individuals involved in data-driven corporations have a significant role to play in keeping the society from being consumed by central authority and acts that go against human rights and privacy laws. We should be given the right and immunity to investigate allegations and publish our findings. Additionally, we need the freedom to force companies and authorities to pursue and combat those claims in a mutually beneficial manner. Unfortunately, we only have that right as long as it does not conflict with the views of the threatened parties. Instead of giving people the freedom to investigate, expose and publish illegal activities, they are crucified for espionage, treason, etc., and driven to serve life in prison. It poses the question: are we really living in a democratic world when heavy censorship and control is inducing fear and people are too scared to reveal what they know due to feeling afraid for their life. It should never be that way in a democratic society. It should be our right, and in fact, our obligation to help target those issues, not be forced to make a choice between the right = prison and the wrong = freedom.

*"If the state acts in a criminal manner, contrary to the constitution, it is the duty of citizens – not just morally but, above all, legally – to put a stop to it."*

*(Lagasnerie, 2017, p.41)*

Following this logic, Edward Snowden, Julian Assange and Chelsea Manning – as well as other lesser known political actors before them – have stepped forward to become the embodiment of a true democratic system by essentially "disobeying" in order to reveal and stop illegal measures undertaken by the US government. We discussed Edward Snowden already (see 2.1.2 *Governmental*), but those that are not aware, Julian Assange is the host of WikiLeaks – a website that publishes secret information, leaks and otherwise harmful information about the violators of human rights – and Chelsea Manning, who after observing mounting instances of illegal activity within the army, publicized the pressing issues. Chelsea Manning was charged for 22 counts of treason and sentenced to 35 years in prison, while *"Julian Assange, and everyone else who contributes to WikiLeaks, potentially faces the charge of collaboration with the enemy - in other words, the prospect of being brought before a military tribunal and sentenced to death"* (Assange et al., 2012, p.4). However, taking the basic premises of human rights, anonymity and citizens of democracy as a framework of protection against such acts, we could argue that those three militants merely served their obligatory role as citizens. When something illegal happens, we are required to report it, or we would become accomplices – however when we do it against the government, we become the violator and suffer tragic consequences. Therefore, why doesn't the same legal framework give activists the same protections that holds for demonstrators on the street – why is such activity deemed criminal in the virtual space, outside of legal boundaries, when it opposes the benefactors of the government?

*"Instead of discussing anonymity as a "negative" practice, one may define it as an instrument that enables us to reflect on the framework of our thought and actions."*

*(Lagasnerie, 2017, p.58)*

For instance, why should Chelsea Manning, after observing mounting instances of illegality within the army, risk her career, retaliation, and so on for reporting wrongdoings? She held no responsibility for the dysfunctions (Lagasnerie, 2017). Why couldn't she just report the illegal activity she witnessed without losing her human rights as a democratic citizen. When such issues are prevalent, we need to use our right to privacy as a framework of protection – that is, to be able to express ourselves in the public sector without being crucified. The right of our governments to withdraw information from public circulation, commit criminal actions, or incentivize private parties to perform illegal acts beneficial for the state, is in direct conflict with the legal system they helped build – but the very system does not apply to them. As they have shown no interest in serving within the context of the law, what we can, or are even obligated to do, is use our legal rights to privacy and cloak our contributions, so the information would be revealed without us being at risk of losing our freedom for serving the way we are expected to in all other areas of life.

## **2.3 The Broken State of the Internet**

All of the above mentioned problems, and more – state secrets, mass surveillance, the decline of privacy and civil liberties, the centralization of control, identity crisis, etc. - have erupted as a consequence of mass connectivity in the face of the Internet. Promoting narcissism, reducing people to numbers, intercepting human interaction, promoting censorship and false narratives, incentivizing total surveillance by corporations and government enforcers – it is a platform of human greed that seeks absolute control over every person and object in the society. The Internet, with all of its breakthroughs and innovation, has served to unite the world, but also created means for the powerful to grasp more control and oversight – it has served as both the savior and the executioner. The fundamental problem remains in the excessive emphasis on freedom, convenience and possibilities, while security, privacy and network threats have taken the back seat.

### **2.3.1 The Centralization of the Decentralized Internet**

The problem stems from the basic principles of centralized control (covered in 2.1), which creates too many temptations and incentives for corporations and governments for data collection. This means that sensitive information of everyone is stored in central databases waiting to be exploited and mishandled, and more importantly, people wonder why they should care. What many still do not realize is that decentralization was not introduced by blockchain nor cryptocurrencies, but it was the Internet itself that did it. The Internet is not owned by anyone and it is a mutually built social space comprised of millions of contributors – that is, the first real decentralized system based on limitless connection. The Internet already introduced a borderless system, but companies created borders within that borderless system to regain control and design, over time, the inability for the user to choose freely. The most basic example of such restriction is Facebook. If we want to use it, but not sacrifice data and identity in the process, we simply cannot, as Facebook would enforce their restriction to make us obligated to agree with their terms of service in order to participate. Essentially, we either comply or are left without the ability to communicate with the world.

Everyone who owns and uses an electronic device that is connected to other devices via the Internet is potentially at risk and should worry about their online activities. Connecting all of our accounts, keys and passwords with a computer, or uploading material to the "Cloud" can be extremely convenient, as we can access anything from anywhere. However, the same convenience creates massive safety holes, as it is extremely easy to get access to those materials for the government, hackers, rogue employees, etc., who can break into that user account at any time.

Big corporations and governments have full authority and power as we trade it all away for a little bit of convenience, and they act without restrictions due to limited oversight, evolved systemic corruption, and need of control. When we have a system where nobody is in charge (the Internet), with infrastructures built on top of it based on pure trust and poorly designed technology, it is a fundamentally flawed system – the makings of a looming disaster if you will. Therefore, we might need to face the reality that the entire business model of the Internet is broken, as we have given away any sort of control over the way we connect, without any access to the medium or the messenger. We can not be interconnected without having those security holes dealt with, especially as we transition to the new era of IoT connectivity, which can, again, bring massive benefits but also even bigger threats. Therefore, we need to collectively take a step back and figure out ways to create a new business infrastructure divorced from manipulation, authority, and the centralization of control. Unless we begin to hold the tech industry accountable and work on building a new, more secure, and private Internet - where companies can continue to make money – companies can continue ignoring the downsides and threats they have brought upon us, as there is no incentive to change.

But even the decentralized solutions put forward by various projects are fundamentally flawed, as they seek to follow a similar pattern of making money off its users, but in a different framework. We now wish to go from using centralized networks and paying with our data or our physical wallets to using decentralized networks and paying with coin from our electronic wallets. Is this really progress? We cannot have a platform that advocates privacy and the protection of human rights while charging fees to use it. Freedom and the guarantee of privacy rights should not have a price tag and technology can never solve the "greed factor" in humans, as long as there are profits to be made. The inherent greed of mining is what is making decentralized networks bitter sweet - instead of centralized authorities making millions, miners and exchanges are making millions. We have become slaves to a different set of masters by moving the power and authority and corruption from the middleman to those who have the money to support the network and its growth. Decentralization has the power to set us free, but the ability to use and support decentralized networks should not be limited to the entitled few.

## 2.4 Summary of Problem Statement

There is a lot to digest on the topic of Internet security, privacy, and the future of networking. Even this chapter, while thorough, is still just a generalization of the massive spectrum of problems we face today. However, the acknowledgement, conceptualization and understanding of the underlying issues presented is intended to serve as context to the need for a proper solution. To help the reader create a link between the prevalent issues of the connected world (chapter 2) and the proposed solution (chapter 3), here is a summary of the foundations that inform the following chapter:

### Security is really difficult

Security has become too difficult to use for most people. Technologies like PGP and exchanging public keys (strong crypto) are tedious, prone to error/frustration, and will never be adopted by the mainstream. Varying password rules, secret Q&A, and multi-factor authentication are all complicated things for the average user. Security doesn't need to be difficult to be effective. Why can't security simply cater to how we as humans think?

### Hackers are unstoppable

Hackers are unstoppable, because the biggest security flaw is always us. Anybody who ever tells you that something is "unhackable" is a liar. No amount of due diligence, secure development practices, or adherence to policies will be able to stop a hacker who is motivated to find and exploit vulnerabilities in a system. When we amass a large amount of valuable information in a single location, it becomes too tempting of a target for hackers. It is no wonder that large scale hacks have been increasing in the past few years as the Cloud continues to stockpile more and more data in centralized stores.

### *Social networks are rampant*

We've moved to a social networking model for most of our online interaction with a focus on ease-of-use, simplification, and convenience. The interaction model of social networks is completely different than the older 1:1 or 1:N models of the past few decades. Security hasn't adapted well to the transient and diverse N:M interaction model prevalent in social networks. Identify providers and single sign-on provide a seamless experience at the cost of Social Networks being the sole authority for our authentication. Do you really trust Facebook with your deepest secrets or your Bank Account information?

### *Decentralized networks are lacking*

Decentralized and persistent networks, while more prominent today than ever before, provide an extreme offering for users. These networks usually attempt to solve a huge, monolithic problem and force the end-users to buy into the whole system in order to access the underlying functionality. What we need is choice and flexibility, not another box.

### *Companies control our data*

Companies claim that handing over our personal data en masse is the only way to benefit from a heightened convenience offered by the modern & connected world. So, we trust them with our personal data. In exchange, companies become wealthy by hosting our data in the Cloud. They make billions of dollars a year providing this service. They aggregate, index, and mine our data, using it for targeted marketing for goods & services at absolutely staggering margins. They even sell our data to 3rd parties without compensating us. In the end, nobody will care about our personal data more than we will. Only we can save ourselves.

### *Governments control our lives*

Governments now collect more bulk data about their citizens than ever before. The irony is that most of this data has been offered up voluntarily by people posting personal information to Social Networks, or is directly paid for by taxpayer funded programs and initiatives. In addition to this, governments have manipulated companies into configuring backdoors into their systems to collect data about customers (PRISM), or found, exploited, and intentionally not disclosed critical infrastructure and software 0days for their own gain (Equation Group Toolkits). All of this is done in violation of End User License Agreements (EULA) and Terms of Service (TOS) agreements, and we, the customer, are never notified. To make it even worse, recently passed legislation (CISA) further incentivizes companies to share our personal data with governments in exchange for heightened privileges, including not being held liable in the event of a hack.

### *Applications reinvent the wheel*

Every application vendor must implement and test its own security solution as part of every product. This means that many companies are reinventing the wheel with respect to secure data transmission. Application providers spend unnecessary time implementing and testing security code when they should be concentrating on what they are excellent at – building great applications. Security is very difficult to get right, and many of these companies make mistakes that create vulnerabilities that will later be exploited by hackers. Small and medium sized companies can also find themselves at a disadvantage since they do not possess the finances or in-house expertise to properly build a security infrastructure. This can be a hindrance to launching new products.

**Overall, the whole business model of Internet has evolved accordingly:**

1. The Internet started as a decentralized network.

2. Companies then migrated to centralized networks due to scalability, performance, ease-of-modification, reduced complexity, and profits associated with centralization of data. Governments also saw an opportunity and started capitalizing on companies by “piggybacking” off their reach and information.
3. A small group of brave “pioneers” (hackers, evangelists, freedom fighters) started embracing decentralization for the benefits contained in distribution economy and decreased power of corporations and governments.
4. Fast forward to now, the reality we face is that that neither network is sufficiently balanced and overly superior or perfect, as both have their individual benefits and shortcomings – essentially, only the mode of power has shifted, but not the problems associated with control.

***“We believe that there is a need for a balanced new platform that protects privacy first, irrespective of the network topology or choice in architecture.”***

***Welcome to the first truly free decentralized network powered by the blockchain.***

***Welcome to Promether...***



## 3 PROPOSED SOLUTION

### 3.1 Motivation For Promether

In the “real world”, that is, the physical world, we plan security based on probability, eventuality, practicality and potential consequences. In other words, we often question convenience in relation to security and are willing to trade some freedom for increased sense of safety. However, what is often neglected is the transition to an era of virtual connectivity, and how the Internet has transformed the concept of the “real world”. Today, physical and virtual worlds combined form the real world, with each being connected to another on multiple levels. Thus, attitudes towards online security should not differ from our attitudes towards security in the traditional sense, as the two “worlds” are mere reflections of one another. Regardless, technology becoming increasingly difficult and overwhelming has allowed companies and governments to sell packages of convenience, promoting all the benefits, but making us ever more blind and tolerant to the problems – after all, privacy is not lost overnight, but rather over time through limit testing and conditioning.

Therefore, the motivation for Promether stems from the problem statement (chapter 2), as it is exactly those incompetences that have inspired us to come up with a solution. All of the exposed problems - security is difficult, hackers are unstoppable, social networks are rampant, decentralized networks are lacking, companies control our data, governments control our lives, applications reinvent the wheel – sound extremely bad and discouraging, but it is important to remind ourselves that these are not irreversible shifts. In order for change to happen, there are three paradigm shifts that need to be prioritized to create truly secure and mutually beneficial networking opportunities.

- First, there is the market change. We need to create new protocols for communicating and exchanging on the Internet, and create enough incentives for companies and individuals to not rely solely on data to make profits.
- Secondly, we need to use our right to privacy and data security and actually want to care for our human rights, not voluntarily surrender it despite everything. Everyone should have the ability to conceal private communications, data, and hide his or her identity on the Internet, and it should not be as inconvenient as current solutions have made it.
- And third, we need to create not-for-profit solutions that are created for the benefit of everyone, so there would not be access restrictions and discrimination as currently prevalent with both centralized and decentralized solutions.

Ideally, not much should change in our habits of using the Internet as we progress through those shifts, but additional benefits should be incorporated in already existing consumption habits. Additionally, some solutions need to be created to facilitate the needs of those who do not have access and the financial means to create opportunities for access. If we create decentralized networks for the purpose of making money then we are no better than the companies and governments who host centralized solutions - we need an altruistic solution for the good of all humanity. What if we could create a blockchain based ecosystem that were free and did not require any coin to use? A system that was not motivated by greed but by utility instead? By making the coin central to the utility of the system, we can install value beyond the coin itself. Solutions are only possible if we acknowledge the problems and actually take effort towards solving them, not dismiss them based on the ignorance and disregard of the people in control.



## 3.2 Introducing Promether

### 3.2.1 Promether Demystified

Promether is a new type of network called an Adaptive Symbiotic Network (ASN). Based on the principles of Artificial Intelligence (AI) and Ubiquitous Computing, Promether allows anybody to create secure and anonymous networks simply by deploying and configuring a series of reusable software components. Promether is not a Walled Garden, nor is it just another persistent network. It is an open-source and component-based, reusable system that abstracts the details of the secure network from the applications that use it. Supporting centralized, decentralized, distributed, meshnet, and hybrid topologies, any application can communicate and transfer data securely.

Promether is designed from the ground-up to be 100% customizable to meet any application need. Whether you are an individual trying to build your first application, or a company who needs to develop a global service, or even a government that wishes to establish secure communications - Promether is flexible enough to adapt to everyone's specific networking demands. By building a complete security networking infrastructure based on an incentivized networking model, Promether will supply a secure API, networking modularity, distributed computing platform, decentralized VPN, secure communications infrastructures, decentralized data sharing and storage solutions, and a fully self-sustainable and incentivized networking ecosystem. Simple, reusable, and effective end-to-end security for everyone.

### 3.2.2 Visions and Goals

In order to build a next-gen solution, we need to understand what needs to change. Surely, one can point fingers and say what is wrong, but what could we do to improve upon the system? In other words, how can we restore the value and meaning of privacy? How could we limit the power of the State without breaking the fundamental benefits of the Internet – connection and convenience? How is it possible to prevent companies from mishandling our data and arrogate themselves to know everything about us? How can we stop bad actors from accessing our personal lives and limit their reach? How will we ever get to enjoy all of the innovation, freedom, and openness the Internet has introduced, without sacrificing our basic human rights and identities in the process? How could we re-structure the incentive system so businesses could profit without enforcing centralized control?

Taking all of these considerations in mind, the vision for Promether is to become a global secure networking infrastructure for developers, miners, users, corporations, and governments. By merging blockchain technology, decentralized networks, and state-of-the-art encryption, Promether marks the end of surveillance and brings about a new era of online privacy, security, and anonymity. But before we can build out our vision, we need to first acknowledge the characteristics that modern networks should have, and use that as our baseline for development milestones. In essence, these are the traits that will define the next great decentralized network, the future of the Internet. The goal for Promether is to become...

#### Free

The decentralized network of the future needs to allow users free access at a level of reasonable capacity and subsidy, without enforcing network service fees, resource donation requirements, or discrimination based on privilege - negative reinforcement schemes never work.

#### Open

The decentralized network of the future needs to comply with the needs of every participant, commercial or non-commercial, by creating an open ecosystem that does not enforce control and restrictions - open source, open infrastructure and open application. In other words, free to use, no walled gardens, and support for any application, both legacy and new.

### Interoperable

The decentralized network of the future needs to provide capability for limitless exchange, interactions, and use of information between all products and systems, regardless of operating system, platform, chipset, protocol, or device. Furthermore, support for a variety of application architectures should be provided - decentralized, centralized, distributed, meshnet, and hybrid - for interoperable communication.

### Performant, Scalable and Adaptive

The decentralized network of the future needs to be able to scale to millions of users, and facilitate the demands of modern networking in terms of reliability and speed. Also, it needs to display distinguished attributes in the ability to adapt to traffic flow and real-time scenarios in order to cater to the needs and demands of everyone involved.

### Configurable and Extensible

The decentralized network of the future needs to support a multitude of configuration options to statically and dynamically customize the network based on individual needs. Therefore, a variety of programming and scripting languages should be supported and interfaced with the network.

### Secure and Evasive

The decentralized network of the future needs to provide the highest level of data protection, while maintaining the flexibility for the user to decide what data to encrypt and how to encrypt it. Therefore, end-to-end encryption and symmetric/asymmetric ciphers need to be supported, while the code needs to be open and audited by industry experts to ensure multiple security confirmations from unaffiliated parties. It also needs to be able to subvert and evade corporate and government firewalls, proxies, Deep Packet Inspection (DPI), network black boxes, and other anti-privacy techniques.

### Anonymous and Private

The decentralized network of the future needs to allow users to navigate the network without revealing their IP address or any other personally identifiable information (PII) - identity should be optional and not a requirement. It is also important to be user-centric and put privacy first - that is, segregate and isolate information to prevent unauthorized access of data.

### Persistent and Efficient

The decentralized network of the future needs to support the ability to have both a stateless and stateful network, as well as allow the serialization of data to more permanent storage, i.e. hard drives. Computational responsibility is also important, only expending energy and resources when needed.

### Redundant

The decentralized network of the future needs to work flawlessly without any single points of failure, by distributing the nodes. Any loss of a server in the network should be imperceivable to the users of the network, as there are always resources to compensate and pick up the slack.

### Modifiable

The decentralized network of the future needs to support a variety of modification - we need a network that allows us to change our mind. Immutable data structures can only take us so far, and therefore modifiable smart contracts and user data is absolutely essential.

### Easy

The decentralized network of the future needs to conform to the wishes and needs of every user, regardless of levels of expertise, and provide convenience and ease-of-use parallel to modern applications. Also, contemporary and intuitive user interface and user experience (UI/UX) needs to be standard procedure in order to facilitate those needs.

### Trustless and Equal

The decentralized network of the future needs to remove centralization, authority, or requirement of trust, by treating all distributed individual nodes in the network as equals.

### Incentivized, Rewarded and Participatory

The decentralized network of the future needs to incentivize growth and capacity participation by rewarding miners with coins, as well as give the users a stake in the network, with ownership mapped as a percentage of total network capacity.

Our vision and associated goals draw inspiration from the Internet as a decentralized social space, so that we can build the layers it was always meant to have - a system where a person can choose, not be forced to comply. By creating layers of security and privacy on top of a decentralized incentivized system, we can redefine what borders and belonging means and build a new paradigm of security on the Internet without the centralization of control. This allows us to have a choice to use other means of alternative methods where we, the users, control the communication and engagement mediums.

## **3.3 Promether as the Future of Decentralized Networks**

As proven by the problem statement, decentralized networks have huge potential in protecting the privacy of individuals, while breaking free from the control that corporations and governments have on our data and online identities. However, there are two key challenges that decentralized networks have struggled with for decades: 1) growth and 2) cost.

*Decentralized networks know how to **make use of system resources**, but have **difficulty incentivizing network growth**...*

Why do decentralized networks need to constantly grow? Because the success of the network is directly dependent on the unused and available capacity of the network itself. That is, features become irrelevant if the services provided by the network are not available and responsive. Therefore, the more popular a network becomes, the more users will want to use the network, and the more nodes must be available to provide acceptable service guarantees to the users. This symbiotic relationship between supply and demand is what makes a decentralized network work, and therefore maintain its dominance in the market. However, it is difficult to get people to allocate system resources up front, as there is no real incentive to do so aside from personal use.

*Inversely, **blockchains** know how to **incentivize network growth**, but have **difficulty making use of system resources**...*

The blockchain has never had any difficulty in getting new people to contribute their machines to the network. Why? Because the machines, or miners, get paid out in coins. As Gordon Gekko once stated, "Greed is good", and when it comes to blockchains, greed motivates the people to "give up" their system capacity for use by the network. The greatest contribution that blockchains have made to decentralization has nothing to do with creating a trustless network, solving the double spend problem, or fixing the byzantine fault problem - blockchain has solved all of these, but the greatest contribution is that blockchains have managed to incentivize network growth to the point of sustainability. Therefore, cryptocurrencies have become the norm for blockchain incentivization and solved the problem of network growth in the process, but created difficulties in efficiently making use of system resources.

***Promether will solve these problems by merging blockchain-based incentivization with decentralized networks and rewarding nodes for donating unused bandwidth and other capacity.***

In terms of privacy, security and anonymity, decentralized networks are the past, present, and future. Promether can create a reason - a catalyst - that will start the chain reaction of decentralization that cannot be undone. We will create an irresistible incentivization model for participation in the blockchain-based decentralized networks, and reward participation, in the form of system resource allocation, in a way that cannot be ignored.

To build this sort of incentivized decentralized network, Promether will develop an application building block (3.3.1), modular network (3.3.2), decentralized VPN (3.3.3), secure communications app (3.3.4), decentralized data sharing and storage platform (3.3.5), and self-sustained distributed computing platform (3.3.6). These stepping-stones will ultimately allow Promether to become the decentralized network of the future.

### ***3.3.1 Promether as the Application Building Block***

Whether it is for Android, iOS, Windows, OSX, or Linux... most successful applications created today are online applications. These applications send traffic across the network, and therefore must solve problems like confidentiality and integrity of data. It is very difficult to create a successful application, but it is a whole other matter to write the scalable network code and make sure that the network protocol is secure and protected from attacks. This takes a tremendous amount of effort that steals time away from the development of the core application and its unique functionality. Online applications must be able to secure themselves from parties who seek to harm or manipulate the system for selfish gains, but it is extremely easy to expose vulnerabilities in the software when not done right. Once an unauthorized party has broken into the application, millions of users are exposed, which can mean the end for the application. The trust of the users is the most important asset, and it only takes one small vulnerability to destroy it.

However, why do software developers need to worry about security or networking code? Why can't this simply be taken care of on their behalf by a flexible infrastructure component? Why reinvent the wheel as an application when you can simply reuse well-written and effective technology that already provides the security and network stacks? Promether is designed to solve this problem by being both a network infrastructure and services API layer that provides the majority of functionality for common application development.

Supplying a next-generation security based open-source API that supports a variety of languages (Python, JavaScript, .NET, Go, and C/C++), individuals and businesses can easily and rapidly build modern applications without having to devote any time nor energy in the areas they are not experts in - networking and security. We do the tedious security and networking work for developers and provide a fully documented and audited security and network stack, as well as incentives for a secure and efficient application development process. This means that Promether can, in the future, host a variety of applications, platforms, and programs to support the need of every user, as developers can use the API without using the network and are incentivized to build on top of it due to unrivaled conditions.

Not only does Promether help dramatically decrease resource allocation (money and time spent on hiring security experts, performing audits, or coding security layers) associated with developing applications, it will also ensure that programmers can focus on what they do best - building great applications.

### ***3.3.2 Promether as the Modular Network***

Decentralized networks of the future need to offer modularity and variety in function, as well as to provide the user a choice in how to use the network based on individual preferences and networking requirements. Based on these acknowledgements, a Promether network can operate in the following different ways:



### Private Network

Promether can operate as a Private Network running on an Intranet. Private networks require that the infrastructure be provided and paid for by the host. This model is best for those who value privacy and isolation, but do not need their applications to be accessible from the Internet and do not require the full benefits of a global network. Examples include corporate Intranets, universities, and home networks.

### Public Network

Promether can operate as a Public Network running on the Internet. Public networks require that the infrastructure be provided and paid for by the host. This model is best for those who need their applications to be accessible from the Internet but do not require the full benefits of a global network. Examples include corporate Internets, secure communications, encrypted email, file sharing, and Cloud storage solutions.

### Global Network

Promether can operate as a Global Network running on the Internet as public nodes. Global networks are provided and paid for through the initial public offering of coins. This model is best for those who need their applications to be accessible from the Internet, do not want to host a dedicated private or public solutions, and require the full benefits of a global network. Examples include any and all applications that are hosted in traditional Intranet and Internet networks.

As networking needs and applications are different for every individual, corporation, and agency, it is important to create a network that accommodates the unique demands of everyone involved. This is exactly why Promether aims to provide users variety in form and function, and become a modular network that anyone can find benefits in.

### **3.3.3 Promether as the Decentralized VPN/Anonymity Network**

Promether implements a built-in decentralized VPN (virtual private network) service, which involves technologies that aim to add a layer of security to both private, public and global networks. The VPN acts as a solution within the Promether network, allowing users to send and receive data, as well as remove access and censorship restrictions without

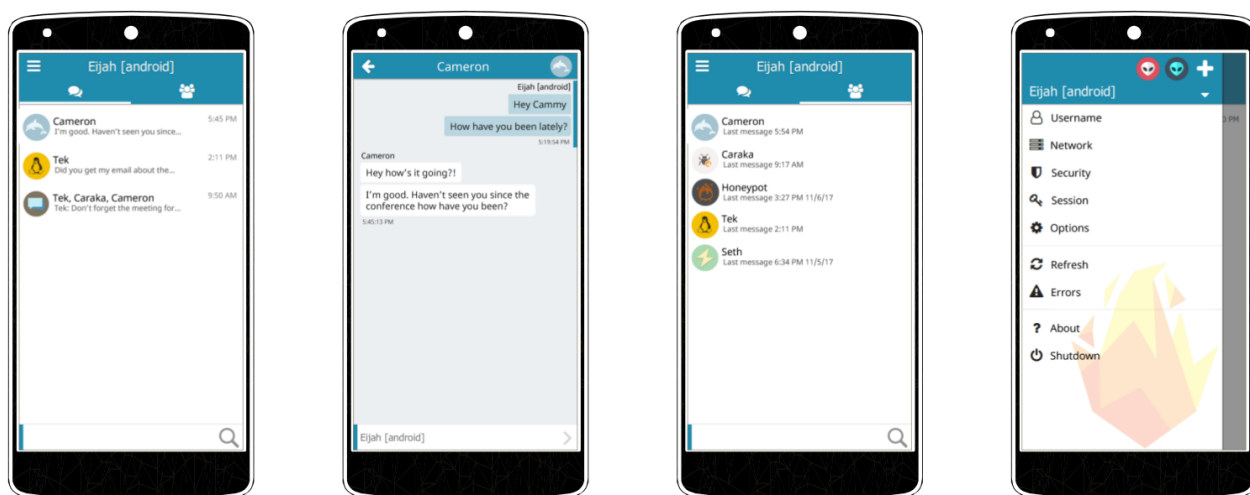
compromising any identifiable information. This also means that the data is encrypted and will not pass through one centralized VPN provider, but routed through any number of thousands of nodes at once, making it the safest way to interact and engage on the Internet.

Promether VPN is based on a fully peer-to-peer tunneling and serverless node networking, providing everyone the means to privacy, security, anonymity (routing and encryption), and access, while incentivizing the node operators when there is increased demand. Any applications (new or legacy) can also work with Promether via IP tunneling or SOCKS5 proxy functionality, ensuring increased flexibility for users, developers, corporations, and even governments. Promether will help protect user privacy and data, and provides the basic VPN services for no cost. While centralized VPNs and even decentralized VPNs have inseparable monetization model involved with their VPNs, Promether offers this functionality for free as one of the fundamental built-in services of the network itself. Surely, everyone can spare excess bandwidth with those who need more of it, but on certain level of capacity, those services are free and based on free network capacity (to see how participants are incentivised to offer capacity, refer to 5.2). Whether you are a traveler with access restrictions in certain areas, want to secure your connection in a public place (such as a coffee shop), want to express yourself freely without the fear of discrimination, wish to establish confidential communications between companies, are a whistleblower looking to anonymize your identity, etc., Promether VPN will have all the functionalities for everyone's privacy needs, while improving upon the existing centralized and decentralized VPNs concepts. The competitive advantage lies in the decentralized open network, unlimited scalability, free to use features, and different tunneling protocols, as well as node incentivization in case there is increased demand.

### 3.3.4 Promether as the Secure Communications Platform

The modernization of underlying technology does not necessarily imply the modernization of user interfaces, which is why it is important to understand the difference between them. While we associate modern user interfaces with innovation, the things that matter most - the underlying technology and architecture - are actually extremely outdated. Centralized communication applications run on private servers, are full of security vulnerabilities, provide multiple backdoors, and violate user privacy on so many levels.

Promether aims to solve the discrepancy between modern UI/UX and the underlying technology with a new state-of-the-art blockchain driven communications platform called Contact. Contact is part of the MVP that Promether launches with, alongside a built-in decentralized VPN network and a programmable API for developers. The truly secure VOIP/messenger will work with Android, iOS, Linux, Windows, OSX, and any IoT/embedded device, like the Raspberry Pi. It is powered by Promether network, fully decentralized, and built on top of open source software designed to protect the privacy of every individual through decentralized distribution protocols, flexible encryption, and advanced privacy functions.



Contact features will include encrypted group chat (such as dynamic group membership via NFC/QR Codes), audio/video streaming, secure messaging, VOIP, file sharing, sync, multi-device with identity, perfect forward secrecy (PFS), cross-platform/app communication, private file storage, video calls, conference calls, and message and account/identity self-destruction functions. We also strive towards interoperable integration, where Contact can be able to exchange information/content/value/data with other applications on the network through the API. Additionally, user has flexibility in choosing how messages are stored, with features to store everything in-memory (RAM) (which makes data almost unrecoverable once deleted), offline, or distributed around the world. Furthermore, as the application is powered by the blockchain-based decentralized Promether network, all data storage functionalities work in a distributed manner, removing central points of failure.

The secure communications platform is designed to give authority, security, utility, privacy and ultimately, ownership, of online communications back to users, and makes it extremely difficult for outside parties to gain access to any information. Creating a decentralized, secure, inter-operable and application-agnostic communications platform, Contact can connect everyone on the Promether network, regardless of the applications they use.

### **3.3.5 Promether as the Decentralized Sharing and Storage Solution**

Promether provides a solution for data sharing and storage without central control and reliance on third party providers. Instead, all trust is distributed across the entire network with client-side encryption and security protocols, which provides users full security, privacy and ownership of their data. Participants can set up a peer-to-peer network with anyone and share or store files on the decentralized storage network, or simply designate a folder on one's computer that can be shared with the entire network publicly. This means that users can either engage in private communications for file sharing, use the distributed network for file storage, or interact with all shared folders on the network (as public communications can be accessed by anyone), similarly to how torrenting and Google drive works (but in a decentralized manner).

The entire Promether network, and therefore the sharing and storage platform, is comprised of distributed nodes, making data handling secure, while all private communications and file sharing/storage is completely decentralized and anonymous, achieved by methods of advanced encryption and sharding. Essentially, when someone wants to upload a file via the Sharing and Storage platform, the file is sharded into pieces, each being encrypted and distributed around different participants in the network who share their storage capacity. Since that data can only be accessed with a corresponding client-side encryption key, which allows users to query the shards and reassemble them into the original file, it becomes very difficult for a malicious actor to retrieve one's data without having direct access to that person's computer. The owner of the content has complete control over the encryption, and therefore is the only one that can access that data. Furthermore, as the network grows, capacity grows alongside with it, thus making sharding significantly more effective, as with every shard, outside access will become more difficult. This also means that large files can be more efficiently distributed, decreasing capacity requirements per provider, and distributing the bandwidth demands more evenly as well - all of which will reduce the time of content upload and delivery by significant margins.

Additional features will also include caching (in-memory storage), persistent storage (on disk), archival, versioning (complete and incremental), streaming, etc. For example, if a user wishes to download something, the nodes will automatically cache that - a lot of things might be totally cached in memory and you can get it instantly. Persistence is another thing - used on disk - it is sharded, distributed, or both. You can store your messages offline, distributed around the world, or simply cache it in memory. By removing centralized points of failure, systemic corruption, and lack of privacy associated with walled garden solutions, while providing additional benefits mentioned above, Promether storage and sharing platform will allow users to abandon risky archaic platforms such as Dropbox, and set a new standard for how people share and store their files online.




### 3.3.6 Promether as the Self-Sustained Distributed Computing Platform

Promether is creating a self-sustainable ecosystem based on efficient coin circulation rewards. Essentially, this means that everything users have in excess, they can give, and anything users need more of, they can get. This creates an efficient circulation economy, where users can earn coins for giving excess capacity to the network, and then use those coins in order to acquire other capacities from the network - essentially, earning for what you have will pay for what you need. By allowing participants to earn capacities for contribution, it allows users to utilize the circulating coins instead of having to inject new money into the services. For instance, when a person has massive bandwidth speeds, but needs more storage, that person can offer bandwidth to the network in exchange for a set amount of storage from the network, creating a completely self-sustainable circulation ecosystem. Regardless, people who wish to acquire capacities without participating in contribution can still do so traditionally - by acquiring the Promether coin and using it to pay for services.

Another distinguishing element about Promether is that certain capacities are already freely offered to people who wish to use what they need, but not offer any capacity to the network in return. For that, 10% of the entire network capacity (provided by Promether Foundation and miners) is offered for free to people who have decreased capacity requirements and wish to use the network without having to contribute. This allows Promether to facilitate every user, based on different needs and requirements, as well as provide anyone access, regardless of status or coin ownership.

Promether can also be installed on existing computers and miners, which will make use of the available capacity and allows the miner to make more right away. This allows Promether to serve as a hybrid mining system, where a person does not have to choose which blockchain to support with his capacity, as it is possible to hybrid-mine both simultaneously on a given machine.

## 3.4 Competitive Comparison

		DECENTRALIZED NETWORKS				INDUSTRY	
		Siacoin	Ethereum	Substratum	MaidSafe	Microsoft	AWS
Marketcap (03.31.2018)	TBD	370M	47B	91M	137M	681B	190B
All in One Solution	✓	✗	✗	✗	✗	✗	✗
Fully Configurable	✓	✗	✗	✗	✗	✗	✗
Decentralized VPN	✓	✗	✗	✓	✓	✗	✗
Platform as a Service	✓	✗	✓	✓	✓	✓	✓
Secure Communications	✓	✗	✗	✗	✗	✗	✗
Diverse Monetization	✓	✓	✗	✗	✗	✗	✗
Resource Efficient	✓	✗	✗	✗	✓	✗	✗



## 4 TECHNICAL OVERVIEW

To build the next great decentralized network we need to think bigger than we have ever thought before, and even bigger than we have ever thought possible. We need to transcend the technological barriers placed upon us by companies and governments and create a vision for the future that positions the individual as the center of the computing universe. Then, we need to deliver on that promise for the good of all humanity. To protect the security, privacy and anonymity of everyone in the world we need to think outside of the blockchain. The next great decentralized network starts and ends with you.

Promether is many things, including:

- Application Programming Interface (API)
- Fully programmable nodes
- Suite of configurable services
- Interoperable and scalable network
- Environment to run applications
- Users who value security, privacy, and anonymity
- Data that constantly flows through the network
- A blockchain-powered utility that incentivizes growth

The following sections describe Promether in varying levels of detail, from the low-level design to high-level abstractions.

### 4.1 Application Programming Interface (API)

At its lowest level, Promether is an application programming interface that implements robust network, security, and anonymization stacks. It's free and open source. The API is not dependent on the Promether Network, allowing any application, legacy or new, to interface directly with the code.

#### 4.1.1 Networking Library

The networking library implements protocols that enable varying degrees of interoperability that allow computers to talk to each other irrespective of where they are located in the world.

##### Features

- UDP, TCP, custom protocols
- HTTP, HTTPS, SMTP, POP3, custom protocols
- UPNP, IP tunneling, SOCKS5 proxies
- Network discovery of hidden nodes
- Direct P2P (hidden and external), VPN, and Tor-like routed delivery
- NAT, firewall, and P2P active and passive tunneling

#### 4.1.2 Security Library

The security library implements all the cryptographic routines that secure data in transit and at rest.

##### Features

- |                           |                               |
|---------------------------|-------------------------------|
| • Hashing algorithms      | • Key agreement schemes       |
| • Public-key cryptography | • Elliptic curve cryptography |

- Encoding and decoding functions
- Checksums
- Compressions routines

#### **4.1.3 Anonymization Library**

The anonymization library implements evasive and subversive techniques that disguise data in transit, allowing applications to appear to be something that they are not. The API can circumvent firewalls, proxies, routers, Deep Packet Inspection (DPI), network black boxes, and other anti-privacy measures.

##### Features

- Protocol Transformation
- Packet Reordering
- Block Padding
- Chunking/Sharding
- Data Randomization

#### **4.1.4 Compatibility**

The Promether API is written in modern, POSIX compliant C/C++. The code is fast, optimized, and well-written. Because the API is coded according to ANSI ISO standards, the libraries will work on almost any chipset, compiler, device, operating system, platform, processor, and programming language.

##### Supported Compilers

The Promether API supports the following compilers:

- Clang
- Msvc
- Gcc

##### Supported Programming Languages

The Promether API supports the following programming languages:

- .NET
- JavaScript
- C/C++
- Python
- Go

## **4.2 Nodes**

Promether nodes are binary components that are compiled and built from the Promether API. Nodes interact with applications, users, and other nodes through one of many services. They can receive, view, analyze, modify, cache, persist, destroy, forward, and broadcast data.

#### **4.2.1 States**

A node can exist in one of four different states:

- Wait
- Process
- Input
- Output

### Wait

This state is active when the node is waiting for input. During this state the node will use its idle CPU time to perform background processing of low-priority tasks such as gossip, synchronization, and network updates.

### Input

This state is active when the node is receiving data from an application, user, or other node. Validation and decryption of the input stream occurs first, followed by any actions that need to be performed to determine the next steps. Depending on the outcome, the input is either dropped or forwarded to the processing state.

### Process

This state is active when the node is processing data from an application, user, or other node. During this state the node is able to view, modify, cache, persist or destroy data. This is an optional state and may not be implemented in every node.

### Output

This state is active when the node is sending data to an application, user, or other node. Validation and encryption of the output stream occurs first, followed by the sending of the data. This is an optional state and may not be implemented in every node.

## **4.2.2 Features**

- |  |                                   |
|--|-----------------------------------|
| • Autonomous                               | • Service-oriented                |
| • Self-preservatory                        | • Visible, hidden, and observable |
| • Network agnostic                         | • Abstracted                      |
| • Configurable, scriptable, and extensible | • Rewarded                        |

### Autonomous

Nodes can operate independently or as a part of a larger collective toward a temporarily shared goal. An entire Promether network can be comprised of just one single node, if so desired.

### Self-Preservatory

Although nodes can spend a good portion of their time working together, nodes ultimately have allegiance only to themselves and only cater to the interests of the collective inasmuch as it benefits their current goals. This greedy and self-preservatory nature of nodes is what drives their effectiveness/efficiency and maximizes individual capacity rewards. When nodes work together and win, the payout is greater than the sum of the parts.

### Network Agnostic

Nodes can only see a small portion of the network, primarily their neighboring nodes. As a result, nodes are able to operate equally well in centralized, decentralized, distributed, meshnet, and hybrid networks.

### Configurable, Scriptable, and Extensible

Nodes are configured by modifying configuration files. Scripts are used for more dynamic configuration. They provide a platform-independent way to extend node functionality. Scripts are optional and, if present, are invoked at runtime during the input, processing, or output states. Promether supports a handful of popular scripting languages including Python and JavaScript. Nodes are extended by writing new code, deriving from the existing code, and re-compiling the node libraries.

### Service-Oriented

Nodes support a variety of services that can be enabled or disabled in the configuration file by the node administrator. For a list of available services, please refer to section 4.3.

### Visible, Hidden, and Observable

Nodes can be either visible or hidden on the network. In a hidden state, a node's IP address is concealed to the outside world but its actions are observable via interaction by users, applications, and other nodes. The ability to hide nodes from view is a powerful feature that promotes privacy across a large number of devices, requiring group participation to review any amount of location detail.

### Abstracted

Nodes form natural abstraction layers between applications, users, and other nodes. Every node provides a barrier over which data can travel. When randomized across multiple nodes in the network with a max hop value, data can become sophisticatedly anonymized simply by network propagation.

### Rewarded

Nodes are interfaces into the Promether blockchain and record a variety of system resource transactions, such as network bandwidth, hard drive, memory, CPU, and GPU usage. Nodes are rewarded at preset intervals for the bandwidth that they consume. The more system resources they contribute to the network, the more nodes receive in reward.

## **4.2.3 Compatibility**

Nodes are fully compatible with the API. As a result, they will work on any chipset, compiler, device, programming language, operating system, platform, and processor that is also compatible with the API.

### Supported Scripting Languages:

- .NET
- JavaScript
- Python

## **4.3 Services**

Promether services provide a functional way for nodes to interact with applications, users, and other nodes. Services are configurable and can be enabled/disabled by node administrators. Promether supports the ability to write custom services. The unique selection of services enabled for a given node defines a node's scope of interaction with the network. The more services that a node supports, the more functionality that a node will provide to the network. The more services that are supported, the greater the contribution and ultimately the reward.

### **4.3.1 Service Types**

There are two types of services:

- Mutable
- Immutable

### Mutable

Mutable services can alter data as it moves through the network. They are also known as active services since they have the ability to read, modify, and write data as it flows through the network.

### Immutable

Immutable services cannot alter data as it moves through the network. They are also known as passive services since they only have the ability to read data as it flows through the network. Immutable services are limited by design to protect the integrity of the datastream.

#### **4.3.2 Mutable Services**

The following mutable services are available as part of the core Promether platform:

- Insertion
- Modification
- Deletion
- Encryption
- Compression
- Protocol Transformation
- Block Padding
- Chunking/Sharding
- Randomization
- Tracking

### Insertion

Nodes can insert new data as it moves through the network. Insertion can occur on new or existing datastreams.

### Modification

Nodes can modify data as it moves through the network.

### Deletion

Nodes can delete data as it moves through the network. Nodes can delete part or all of the datastream (also known as “null routing”).

### Encryption

Nodes can encrypt or decrypt data as it moves through the network. A variety of encryption ciphers are available such as AES (Rijndael), RC6, MARS, Twofish, Serpent, and CAST-256.

### Compression

Nodes can compress or decompress data as it moves through the network. A variety of compression routines are available such as zlib, gzlib, and lz4.

### Protocol Transformation

Nodes can transform protocols as data moves through the network. This is ideal as a technique for disguising traffic as something that it isn't for the purpose of subterfuge, such as bypassing network firewalls, proxies, or Deep Packet Inspection (DPI). For example nodes can change TCP traffic into UDP, change a proprietary binary messaging format into an HTTP GET request, or even change an HTTP response into a POP3 email request all with the intended goal of subverting and evading detection by network devices.

### Block Padding

Nodes can add/remove block padding to the data as it moves through the network. This helps normalize different sections of the datastream and prevent packets from being identified by their size.

### Chunking/Sharding

Nodes can break up data into smaller parts (known as chunking/sharding) for the purpose of redistributing the entire datastream as smaller portions across multiple nodes.

### Randomization

Nodes can add/remove random bytes to the data as it moves through the network. Random data can be placed anywhere in the datastream for the purpose of obfuscation and subverting detection. This helps normalize different sections of the datastream and prevent packets from being identified by their offsets.

### Tracking

Nodes can add/remove tags to the data as it moves through the network. This is helpful as a way to track end-to-end movement of data through a variety of autonomous nodes. An example of such a tag is a content watermark that's applied as data propagates through a node. Such a tag could be used to track ownership, expiration, or digital rights management.

## **4.3.3 Immutable Services**

The following immutable services are available as part of the core Promether platform:

- Viewing
- Proxying
- Forwarding
- Caching
- Persistence
- Versioning
- Synchronization
- Discovery
- Redundancy

### Viewing

Nodes can view and analyze data as it moves through the network.

### Proxying

Nodes can proxy data as it moves through the network. This achieves a level of anonymization as each node in the proxy chain will distance the sender from the target by one additional hop. The benefit of this redirection is that the sender's IP address is never revealed to the recipient of the datastream.

### Forwarding

Nodes can forward data as it moves through the network. This allows nodes to be responsible for the dissemination of data to a larger audience. The network will broadcast the original data to multiple users at once, guaranteeing that all packets arrive. This is helpful for social applications that use group functionality like secure chat and VOIP.

### Caching

Nodes can cache data in memory or on disk as it moves through the network. This allows nodes to identify highly requested bits of information and have them ready to future requests, thereby minimizing redundant calls across the network and providing a shorter path for data delivery.

### Persistence

Nodes can persist data to a more permanent storage as it moves through the network. Sometimes data needs to be stored to hard drives or databases as part of a longer term strategy for archival, backup or reporting needs.

### Versioning

Nodes can version data incrementally or completely as it moves through the network. The ability to retrieve prior versions of an archive is useful for long-term storage needs.

### Synchronization

Nodes share information with applications, users, and other nodes for the purpose of increasing effectiveness and efficiency. This gossip helps to normalize the network topology, giving a more accurate picture to all participants of the network.

### Discovery

Nodes are self-aware of their environment and have the ability to discover one another as data flows through the network. Nodes can discover network devices irrespective of whether they are hidden or IP-accessible.

### Redundancy

Nodes group together, forming natural clusters for the purpose of federation, scalability, redundancy, and fault tolerance.

## **4.4 Network**

Promether networks are decentralized infrastructures that allow applications to send their data through the network while opting in to various levels of security, privacy and anonymity features. They are macro-layer abstractions of the underlying API, providing a platform and programming language-agnostic way for applications to integrate without having to write low-level code. As discussed in section 3.3.2, Promether supports a variety of network types: private, public, and global. Promether networks contain nodes that abstract away the underlying complexities of end-to-end application security. All this is possible without sacrificing any performance due to the platform's focus on speed. Promether networks make it easy to secure all your applications.

### **4.4.1 Network Architectures**

Promether supports the following network architectures:

- Centralized
- Decentralized
- Distributed
- Meshnet
- Hybrid

#### Centralized

A type of network where users connect to a central server that acts as the authority for all traffic.

#### Decentralized

A type of network where users connect together in clusters, where each cluster has a single point of connectivity acting as network delegate to the outside world.

### Distributed

A type of network where users connect directly together and the data to be worked on is spread out across more than one computer.

### Meshnet

A type of network where users connect directly, dynamically and non-hierarchically to as many other users as possible and cooperate with one another to efficiently route data.

### Hybrid

Any unique combination of centralized, decentralized, distributed, or meshnet topology.

## **4.4.2 Features**

- 100% Free and Open
- Zero Transaction Fees
- Scalable and Performant Architecture
- Rewards-based Utility Network
- Full Application Ecosystem
- Flexible Decentralized Databases
- Proof of Stake (PoS) Blockchain

### 100% Free and Open

Promether is 100% open-source, open-infrastructure, and completely free to use for both commercial and non-commercial purposes. You control the code and how the network is configured and deployed.

### Zero API Transaction Fees

The world is full of decentralized networks that promise to solve every imaginable problem, so long as we hand over our money. It's time we demand more from decentralized networks and stop paying for what should be free. It is time to change the fact that exchanges, miners, and investors are the only beneficiaries of blockchain technology. It's time we bring the blockchain to the people - all the people. Everyone has the right to privacy, both rich & poor alike. The era of enriching the wallets of a few cryptocurrency elite is over.

Unlike other decentralized networks, Promether is completely free to use and has zero API transaction fees. A portion of the Promether network is subsidized, meaning that anyone in the world can use Promether with or without coin. Coin owners and those who contribute back to the overall capacity of the network are given prioritization. This ensures that anybody can use the network while minimizing leaching. To further incentivize the growth of the network, those who choose to donate capacity back to the Promether Platform will receive payment in coins.

### Scalable and Performant Architecture

Promether networks are fast, very fast. By default they're UDP-based networks that favor P2P interaction over routing, meaning that every transaction is optimized both from a data payload and network hop perspective. Promether networks are also unimaginably scalable due to the underlying distributed node architecture. The network can easily accommodate hundreds of thousands of transactions per second without even breaking a sweat. Promether can meet all of your performance network needs.

### Rewards-based Utility Network

Promether is a true utility network with ownership, rights, and privileges mapped to the percentage of coin ownership. The more coins a person possesses, the more options that are available. It's a self-sustaining and rewards-based network that



incentivizes a variety of participation models via coin-based, capacity rewards. Users can choose to stake their coins in one of many different ways, such as the ability to mine/forage in the PoS network, earn coins via participating in system resource sharing, or even receiving guaranteed capacity in the network for their personal use. For more information, please refer to section 5.

#### Full Application Stack Ecosystem

Promether provides a network and security layer that allows applications to connect in a easy & secure manner without worrying about the complexity of writing the underlying code. This allows developers to focus on implementing application features instead of worrying about the potential security vulnerabilities of the network and communication protocol.

Promether is a world-wide decentralized computer with an economy of scale-based architecture and infinite system resources. All applications, both legacy and new, are supported. Promether implements full, end-to-end encryption for all transactions. It's a user-friendly security, anonymity, and privacy framework for all applications.

#### Flexible Decentralized Databases

Promether networks are balanced and diverse, powered by multiple decentralized databases and ledgers. The ledgers are immutable while the databases permit modifications and deletions. Why? Just like in the real-world, sometimes we change our mind. The decentralized network of the future should accommodate for this. Mutable smart contracts are just one such example of the power of Promether's flexible data model.

#### Proof of Stake (PoS) Blockchain

Promether networks are powered by a Proof of Stake (PoS) blockchain that's magnitudes more efficient than traditional Proof of Work (PoW) blockchains used by other decentralized networks. Using a PoS blockchain is not only more environmentally-friendly, but it allows the network to offer a variety of stake-based incentives for coin holders.

## **4.5 Applications**

Promether applications integrate with the network in a variety of different ways. But no matter which integration option is chosen, application developers can rest assured that their security and network needs are taken care of. This allows developers to focus on creating great apps rather than having to worry about cryptographic routines, endpoint discovery, infrastructure costs, performance, or network scalability concerns. End-to-end application security has never been easier.

### **4.5.1 Integration Models**

Promether supports the following integration models:

- API
- Protocol
- Proxy

#### API

Integration to the Promether API is the lowest level of application integration. While this provides the greatest number of configuration options it's also the most complex type of integration. Applications will need to write a substantial amount of code and are responsible for directly handling all state machines, data packaging, callbacks, and errors. It's possible to use the Promether API at such a low level that applications aren't participants of any Promether networks.

### Protocol

Integration to the Promether protocol is a much simpler, albeit limited, integration model compared to the API. Although no code needs to be written, applications have substantially fewer configuration options and are required to use an existing Promether network for all communications. Besides not having to use the API directly one of the key benefits to this integration model is that it's 100% programming language and platform agnostic. In this integration model, messages are sent over standard protocols such as HTTP.

### Proxy

Integration to the Promether proxy is the simplest of all, although the most limiting. In this integration model applications are simply SOCKS clients of the Promether network and are therefore limited in the type of interaction they can have with the network. Any kind of data can be forwarded through the network as it acts as a proxy between endpoints. This is a highly desirable option for any applications that wish to remain unchanged and become more secure, such as legacy applications.

#### **4.5.2 Compatibility**

Promether applications will work on almost any chipset, compiler, device, operating system, platform, processor, and programming language. Whether you're creating the next secure communications/VOIP app, file sharing/sync network, VPN/Tor infrastructure, or dark web portal; Promether is flexible enough to adapt to your specific needs.

### Supported Chipsets

Promether applications support the following chipsets:

- 32 bit
- 64 bit

### Supported Devices

Promether applications support the following devices:

- Desktops
- Embedded
- IoT
- Laptops
- Miners
- Mobile
- Routers
- Servers
- Tablets

### Supported Operating Systems

Promether applications support the following operating systems:

- Android
- BSD
- Chrome OS
- iOS
- Linux
- OSX
- UNIX
- Windows

### Supported Platforms

Promether applications support the following of platforms:

- Application
- Command-line
- Service
- Web

### Supported Processors

The Promether API supports the following of processors:

- ARM
- x86/64

## **4.6 Data**

Any type of data can be sent across a Promether network. Data can be compressed, encoded, encrypted, hashed, authenticated, and cryptographically verifiable. Data with confidentiality needs can be encrypted using the following techniques, from basic shared keys to complex rolling ciphers that use any number of complex algorithms such as pre-hash authenticators, time-slicing, or even onion layering.

### **4.6.1 Data Types**

#### Application

Application data is unique to an application instance, defined by an application identity, i.e. cryptographic fingerprint, within a Promether network. Application data can be mutable or immutable. Application data can also be centralized or decentralized, depending upon application necessity. When stored in a decentralized way, a Distributed Hash Table (DHT) is usually used to propagate and index the data real-time across all users.

#### Network

Network data is unique to an instance of a Promether network and is shared across all applications, nodes, and users of that network. Network data is stored in the blockchain. The financial ledger that records the buying and selling of Promether coins is one such example.

#### User

User data is unique to a user instance, defined by a user identity, i.e. cryptographic fingerprint, within a Promether network. User data can be mutable or immutable. User data can also be centralized or decentralized, depending upon user necessity. When stored in a decentralized way, a Distributed Hash Table (DHT) is usually used to propagate and index the data real-time across all users. User data can also be stored more permanently as a mutable horizontal branch of the immutable blockchain.

## **4.7 Users**

Promether users interact with applications, nodes, and other users. Users control the level of identity and anonymity with which they interface with the network.

#### **4.7.1 User Types**

Promether supports the following user types:

- Anonymous
- Authenticated

##### Anonymous

Anonymous users don't reveal any real or digital identity. They are ghosts, able to conduct transactions without any form of correlation. There are many times when true anonymity is the most desirable form of interaction; such as in the case of whistleblowers, political dissidents, and missionaries.

##### Authenticated

Authenticated users assert real or digital identities. There are many times when it's desirable to know that the participants at the other end of a transaction are who they claim to be. Please note that identity authentication, although important, might not mean anything more than the verification of cryptographic primitives.

### **4.8 Utility**

Blockchains are exciting new technology, and not just because they solve the Byzantine Generals Problem or the Double-spending Problem. From a privacy standpoint blockchains are exciting because they solve the Growth Cost Problem that has plagued decentralized networks for decades.

#### **4.8.1 The Growth Cost Problem**

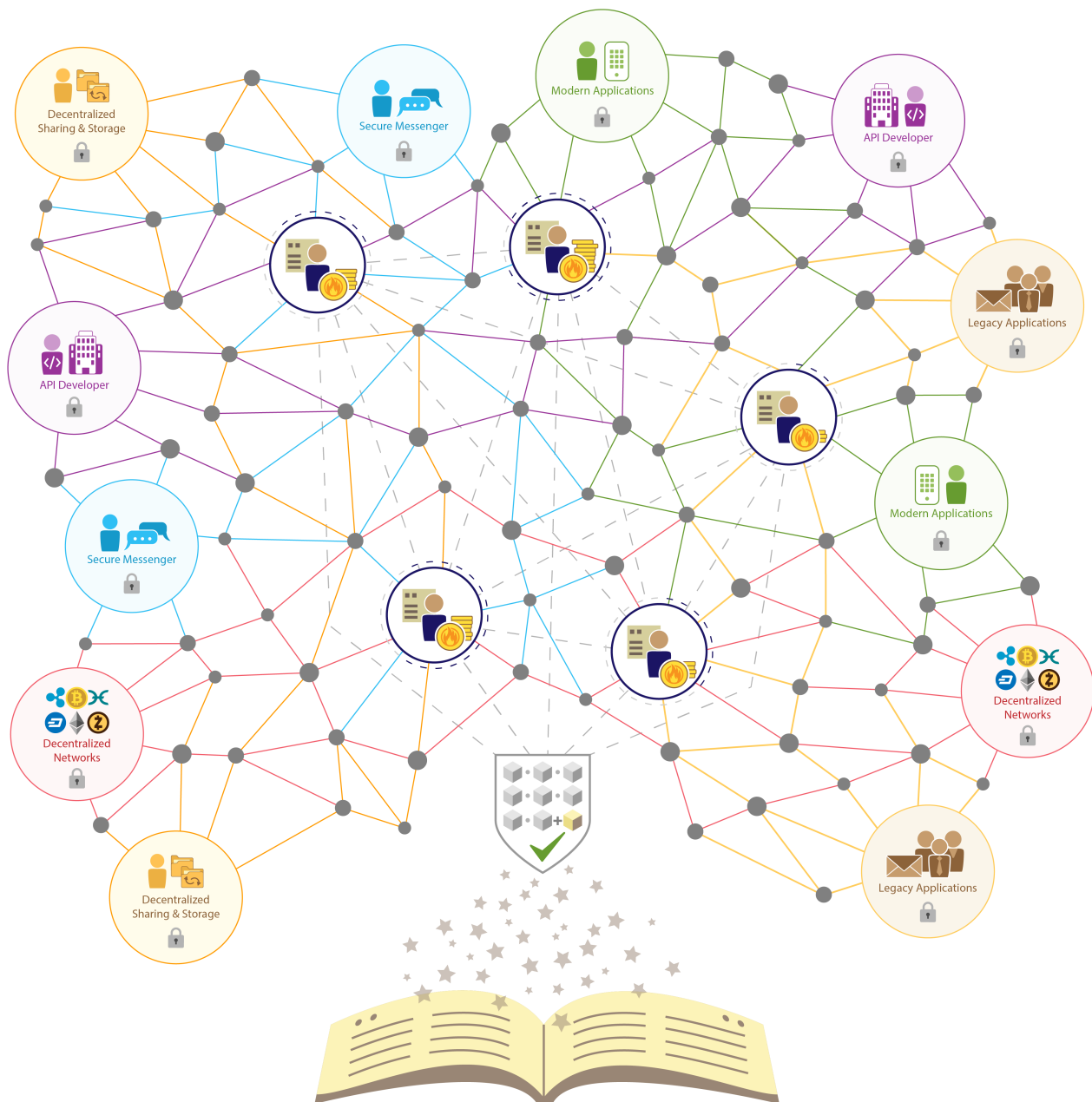
The Growth Cost Problem states that decentralized networks will be unable to grow beyond a certain point due to the overbearing weight of the associated costs of sustaining such a large network. Eventually the altruism and good intentions of a network's founding members will be unable to sustain and subsidize the increased demand of the network itself. Thus the more popular a decentralized network becomes, the more unlikely it will be to succeed. The irony is that the ideals of what ushered a network into existence is also the cancer that destroys it from within.

Keep in mind that the Growth Cost Problem isn't a technical problem - it's a human problem, dealing with the emotional core of what inspires and drives us as people. But it's a real problem. The Growth Cost Problem is the reason why the world hasn't embraced a single decentralized solution to protect individual privacy. To solve the Growth Cost Problem we will need to change the rules of the game and understand what motivates the human mind with regards to a better future. Gordon Gekko, a fictional character in the 1987 film *Wall Street*, once said that "greed is good." And he was right. As much as we would like to believe in a United Federation of Planets' futuristic society where altruism guides our decision making process, this just isn't true. The world is run by individuals who value self-preservation above all else. It's not our fault - it's in our nature to survive and protect those closest to us. It's in our nature to win.

#### **4.8.2 The Architecture**

Promether is greater than the sum of its parts. It combines an API, nodes, services, networks, applications, users, and data to achieve a balanced ecosystem that allows for secure, anonymous, and private interactions. Irrespective of how the parts might come together, the user always comes first.

The following is a high-level depiction of how a Promether network could be organized:



### Network

- The API provides security, networking, and anonymity libraries
- Services use the API to create language-agnostic network interfaces
- Nodes implement one-to-many services
- Networks are formed by one-to-many nodes working together
- Applications use the API or nodes interact with the network
- Users use applications to send data through the network

Please refer to chapter 5 for a detailed explanation of the Promether blockchain and coin utility model.

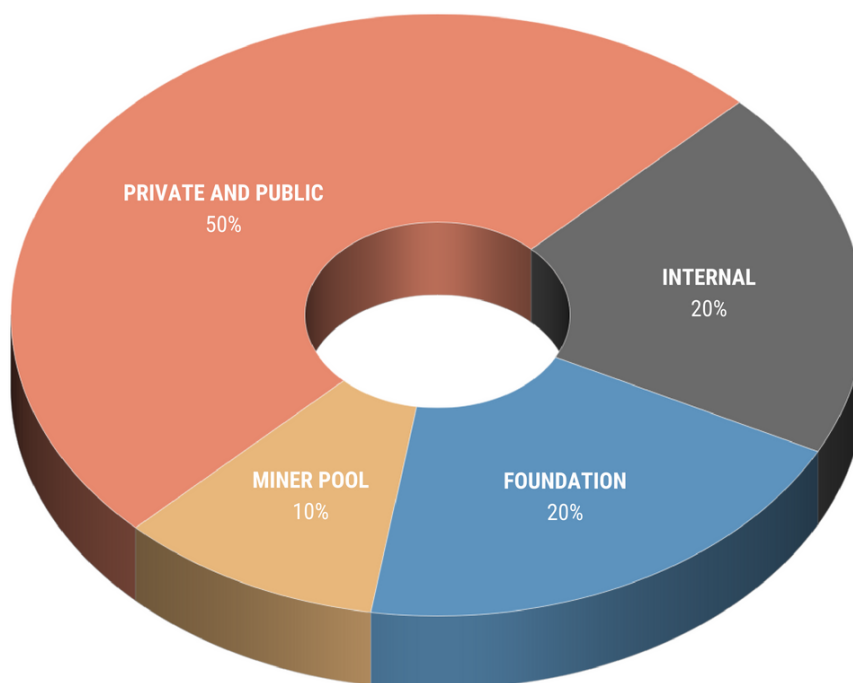
## 5 COIN PROPERTIES AND ECONOMICS

### 5.1 Overview

Promether has a Proof of Stake (PoS) blockchain with utility ownership, stake incentivization, and coin-based rewards. The Promether Coin (PYRO) will be created on the blockchain prior to the Initial Coin Offering (ICO) and derives value from its utility and functionality in the ecosystem. PYRO will serve to merge blockchain-based incentivization with decentralized networks and data structures, rewarding nodes for the servicing of the network, as well as for offering a variety of capacities, including (but not limited to) network bandwidth, system memory, hard drive, and CPU/GPU processing power. It is intended that PYRO's only utility is as a method of utilizing resources within the Promether network as detailed below. Specifically, PYRO will not represent or provide the holder rights to any assets, revenue, equity, voting or other investment-type or security-type rights.

#### 5.1.1 Distribution

In the minting stage of PYRO, a total of 300 million coins will be generated, of which 30 million coins will be held in reserve to be used only for supplemental miner incentivization until the year 2100. No additional coins will be generated afterwards. The total quantity of PYRO will be distributed as follows:



#### Miner Rewards Pool

30 million (10%) coins will be generated prior to the ICO and held in reserve for the sole purpose of supplemental miner incentivization. These coins will be used to reward the miners and incentivize the maintenance of the core Promether network until the year 2100, after which user and transaction fees will serve as the primary reward mechanism.

#### Private and Public Offering

150 million (50%) coins will be sold to investors during the private sale and the Initial Coin Offering (ICO). The private sale is open to accredited investors only and its purpose is to raise early capital, create strategic partnerships, consultations and advisory, and other business opportunities. Inversely, the ICO will be open to the public with no planned whitelist, although we reserve the right to create a whitelist if necessary to entice early investors. Any coins not sold at private and

public offering will be burned. Private sale\_coins are subject to an ethical 9 month vesting period (where ¼ of coins are available after 0, 3, 6 and 9 months), while the ICO coins will not be subject to any vesting period.

### Foundation

60 million (20%) coins will be reserved for ongoing ecosystem building. The foundation fund will primarily serve anything that is deemed most valuable to the network and ecosystem at the given time that they are allocated. Some examples include, but are not limited to, staker incentivization, community growth, bounties, all-purpose marketing, airdrop, user growth, independent applications funding, contributor incentivization, private sale bonuses, etc. As this is a reserve fund and not part of the circulating supply, all allocations and usage intentions will be notified well in advance.

### Internal

60 million (20%) coins will be reserved for the founders, partners, employees, advisors, and strategic alliances. These funds will support the building and growth of Promether through internal incentivizations, strategic partnership acquisitions, as well as development, maintenance and operations enticements. These coins are subject to a fair and reasonable vesting period.

## **5.2 Ecosystem**

Promether is true utility, meaning that PYRO is simply a form of digital representation of the total ownership in the network's ecosystem. A person who stakes a percentage of all the PYRO is fundamentally really just a percentile proprietor of the total capacity of the network, where capacity is a combination of network bandwidth, hard drive space, memory, and CPU/GPU processing power. Unlike other decentralized networks, basic use (i.e. small bandwidth usage) of the decentralized features are available irrespective of how much coin someone has in their wallet, however higher capacity demands are filled based on stake prioritization. To better understand the value of PYRO and how it functions, it is important to first understand the ecosystem in which the coin exists.

### Blockchain

- The core of Promether is a Proof of Stake (PoS) blockchain.
- The Promether blockchain stores financial ledger information, including addresses and transaction data.
- To achieve better scalability and performance, capacity information is not stored in the blockchain, but on a parallel data structure (see *DHT and DHG* section). Storing capacity information on the blockchain would be wasteful since this information is not required to persist forever.
- Promether also reserves the right to explore and implement other scalable and performant data structures (e.g. DHT, DHG, etc.) as the point of arrival for the network's financial ledger technology.

### Distributed Hash Table (DHT) and Distributed Hash Grid (DHG)

- User, application, or system data will be stored outside of the blockchain in a Distributed Hash Table or Distributed Hash Graph (e.g. capacity metrics, or user identity as in the case of Contact).
- Capacity metrics and reward multipliers will also be stored in the DHT or another type of distributed data structure like DHG, as capacity information does not need to persist indefinitely.
- The DHT/DHG data can be either mutable or immutable, depending upon specific needs.
- Storing the capacity log on a separate data structure allows efficient scalability and auto-truncation based on a set maximum log size, allowing any device to become a capacity node and participate in the network.

## Capacity

- The Promether network's utility is defined in terms of total available capacity.
- Capacity use is tracked by identity and transaction identifiers.
- A percentage of network capacity (contributed by nodes) is reserved up front, creating a limited subsidy that allows anybody, with or without coins, to send data securely, privately, and anonymously.
- The remaining network capacity is prioritizing those who hold a stake in the network or pay for expedited use.
- Ownership of capacity is adaptive, meaning that it is only offered to stakers when requested. When not in use, network capacity moves around and facilitates the needs of other users. This also redistributes guaranteed network capacity to be used by others as part of the free network.
- Contributed capacity is factored into staking rewards as a multiplier in the block reward algorithm (see 5.3.2 *Stakers and Staking*).

The amount of capacity that a node provides is difficult to accurately record in an objective manner without placing a heavy burden on the network itself. The ability to perform outside, 3rd party validation of reported capacity is desirable to discourage and/or prevent any sort of fraudulent reporting. Therefore, capacity metrics and the recording of capacity information is governed by a decentralized gossip protocol that insures consensus and fairness across the network, rewarding those miners who play fairly and disincentivizing those who do not. Users have the ability to report on others who do not provide the capacity services that they claim to provide. Negative feedback can accumulate to the point that nodes will become deprioritized in the validation pool, and therefore receive diminished rewards. The exact details of the gossip protocol will be documented in a future version of the Whitepaper.

## **5.3 Economics**

Promether's economics involves the constant circulation of PYRO coins in the ecosystem, specifically between the stakers and the users. By owning PYRO, a person owns part of the utility itself, including the rewards that come from that utility when coins are put at stake. Stakers are incentivized via block rewards that are funded by a unique combination of transaction fees, user fees, and until the year 2100, reserve pool payments (see 5.3.3 *Funding*). Additional incentivization elements involve a more capacious use of the API and the ability to utilize network's capacity in relation to the coins at stake. This is what funds and sustains the continued participation of the staking nodes, encouraging investors to put their coins at stake in the first place. The important distinction between Promether and other PoS blockchains is that the chance of being a block forger is not only influenced by the stake of PYRO, but also by the additional capacity that the staker makes available to the network (see 5.3.1 *Stakers*).

### **5.3.1 Stakers**

PYRO owners can choose to leverage, i.e. put at stake, their coins to be added to a block validation pool, acquiring the eligibility to become a validator and participate in the block forging process. As staking nodes are an inseparable element of Promether because of their role in sustaining, validating and securing the network, any blocks they forge will yield incentivization in the form of coin-based rewards for their contribution. In an effort to disincentivize fraudulent activity however, a minimum number of coins is required for staking (the specific amount will be announced at a later date) and an appropriate waiting period applies after coins are removed from stake.

## Overview

- Stakers provide capacity to the network as part of the validation/forging pool contract.
- Staker capacity bootstraps the network and provides the subsidy that allows free use of the network.
- Stakers also provide the capacity that is used by users that pay for expedited utility.



- Stakers can choose to make network utility available to them in relation to their stake amount, but also receive coin-based rewards upon forging blocks. However, there is a concurrency dynamic that affects the frequency of block forging when using capacity while staking (see *Stake Multiplier and Concurrency*).
- Staking PYRO is also directly correlated with extended network use through the API.
- In the event of licensing the API to third parties, the collected fees will also benefit the staking nodes as well as those who hold PYRO. The exact details of API licensing deals will be revealed in the future.
- Anybody can use the API, however users, applications or platforms that require more than basic capacity through the API are required to fulfill the appropriate staking threshold to use more of the network's resources.
- When becoming a staker for the purpose of extensive use of the API, the stake needs to be (at minimum) equivalent to the amount of capacity the application/platform is looking to use. This is important because without having an appropriate stake, they might not be able to utilize the amount of capacity required to avoid degrading performance.

### Stake Multiplier and Concurrency

In the Promether network, contributed capacity acts as a multiplier for a block reward chance. In essence, this means that greater contribution of capacity (for instance, a staker allocating X Mb/s of their network bandwidth, etc.) to the network increases that staker's chance of earning block rewards. This will incentivize people to add more resources to the service of the network, while allowing smaller stakers to unlock greater rewards by donating bandwidth, storage space, memory, and CPU/GPU processing power. However, since stakers can also choose to use the utility (i.e. capacity) of the network in relation to their stake, doing so will cause the multiplier to drop according to how much capacity they consume from the network, as the same coins cannot be simultaneously used to earn rewards and utilize network capacity. This essentially means that if 100 coins are at stake, but the staker actively uses 50 coins worth of capacity from the network, then their stake multiplier is affected only by the unused 50 coins. If all coins are unused, the multiplier is at its highest potential, while when all coins worth of capacity is used, the multiplier is at its standard rate. Therefore, the multiplier is in a constant state of adaption based on the dynamic formula between consumption and contribution, while the staker is not restricted and can adaptively adjust his incentives, requirements and demands from the network.

### **5.3.2 Users**

People who do not put any coins at stake are called users.

#### Overview

- Users can take advantage of the free capacity provided by the staking nodes (including the API), which can vary based on a number of factors such as total number of stakers, available bandwidth, number of capacity providers, etc. This subsidy is highly desirable and in limited quantity (approx. 10% of total network capacity).
- Users who opt in for the free bandwidth will be limited in the size of data payload. Their transactions might queue up and be subject to time delays. Free transactions are small payload size only, such as secure text messages. For increased demands, the user should seek to participate in the network via staking or by paying an expedited fee to incentivize staking nodes to deal with those requests.
- Users always have the option to acquire PYRO and spend it in return for guaranteed bandwidth. The proceeds go directly to the staker that forges the block. When a user purchases coins and spends it for bandwidth, they can use network's bandwidth without having to stake any coins. This allows users to have bandwidth above the free allotment while not having to share their own bandwidth.
- Users who do not pay for expedited capacity or do not use the free capacity can donate unused resources and receive free bandwidth in return from other users.

- Users can also engage in user-to-user provided bandwidth, which doesn't involve miners. This creates a fringe-layer, ratio-based capacity network, similar to BitTorrent. Fringe-layer provides a mechanism to scale the network indefinitely and places some burden on the users. Fringe layer network usage is totally free, relying upon a system of fair and equal capacity exchange, where users donate some of their own capacity to use the capacity of others.

### **5.3.3 Funding**

#### Transaction Fees

A small transaction fee is charged when users buy or sell PYRO. Unlike other blockchain-based networks, Promether does not take a percentage of these fees for itself. Instead, 100% of all transaction fees go directly to the miners who forge the blocks. We believe it would be unethical to take a percentage of the transaction fees from the miners.

#### Expedited User Fees

Users can optionally pay PYRO to receive prioritized queuing or expedited transaction times. The more users pay for expedited transactions, the faster the reward pool will fill up. There is no maximum cap for user payments during a given block creation. This means that user payments introduce an element of random rewards into the ecosystem, allowing miners to receive unexpected and higher payout for certain blocks. This overpayment of block rewards is driven by the user and network interaction and can happen at sporadic and indeterminate times. Users can also choose to tip miners who provide exceptional network services.

#### Reserve Pool Payments

A small amount of PYRO is taken from the 30 million coin reserve pool during block validation as a mechanism to reward miners. This helps keep transaction fees as low as possible without introducing any dilution, since the allocation of coins is determined prior to the ICO and factored into the economics of the network. Occurring at predetermined intervals, reserve payments will also halve over the course of the next 82 years, encouraging network growth earlier by larger payouts to those who receive block rewards prior to the event. Reserve pool payments will only come into effect in the instances where the rewards pool does not cover the minimum guaranteed reward amount. Eventually the rewards system will become self-sustaining without the need to pull coins from the reserve pool.

## 6 CHALLENGES

### 6.1 Perfect Security Does Not Exist

It is in human nature to pursue perfection in technology and deny anything that does not *claim* to provide it, but what is often forgotten is that the systems are only as perfect as the users themselves. Just as traffic will always have accidents and reckless driving, perfection in computer and network security is an impossibility. Providing the necessary tools and education will not automatically make the user safe, as ultimately it is up to the user's choice in how the tools and education is implemented. Even AI – something that a lot of proficient scientists and futurists claim to become the most advanced technological development in the history of the world – can not be perfect. In the future, AI can possibly monitor our body and offer a healthier diet, but it can not eat healthier food for us – all it can do is provide the basis to do so ourselves. These types of human flaws will always create possibilities for determined adversaries, and if a hacker with serious intent and resources wants to get hold of some data, they will most likely succeed, regardless of the precautions you think you are taking. Anyone who is selling something that *claims* to provide 100% guaranteed security is lying and most likely wants to monetize the associated misbelief.

After all, the biggest security flaw resides in the people, and therefore we can not claim Promether to be the perfect solution that removes flaws in human behavior. The only thing we can do is create the most convenient, beneficial, and secure protocol for everyone, and do so by doing the only thing that can stop the attackers - increasing the uncertainty, time, and effort involved in order to disincentivize the attacker. Promether does not claim to remove all security flaws there are and will ever be, but it will drastically increase the the time and effort involved for the person looking to gain access, while also decreasing the certainty of a reward. If a hacker knows he needs to allocate significant amount of time, money and effort to get access, while there is no certainty for the reward he was looking for to be there, the probabilities of such attacks will massively decrease.

### 6.2 Awareness

Another challenge resides in increasing awareness about online security among general population, as well as making it significant enough for people to take action. Security on the Internet is about everyone - governments, corporations, and every individual - adopting the profound shift in understanding how we perceive a secure society and ourselves. However, it is challenging to persuade people to shift from their current habits of consumption, as most can not visualize the threats that these invisible exploitations have. What does that mean? If someone were to follow us every day, listen to our conversations, sit next to us while we sleep, and count every mouthful we eat, it would feel like an imminent threat and would therefore incentivize change. Unfortunately, as we cannot physically feel or see the threat in an online environment, we perceive our safety, freedom and happiness not to depend on it. However, just because it is not physically visible does not mean it is not real, and just because we do not understand it does not mean that damage is not done. The attitude associated with online security is very stubborn, and because the threats are not imminent enough, it becomes very difficult to make people change their attitude towards it. Increasing awareness and invoking change is a journey, and will require patience, time, and fundamental shifts in the way we think about our security in a world of endless connectivity.

### 6.3 Development Needs

With every revolutionary concept, development is always something that will create a lot of challenges. Security in networking is still in its early stage, meaning that the development of real breakthroughs, such as Promether, might take time. We might not even fully grasp the extent of how Promether can be used in the future (with developments such as advanced IoT and Quantum Computing put in the mix), and only real-world application can reveal challenges, bring new

ideas, and inspire further innovation. While there are already significant benefits and use cases associated with Promether, the full potential is yet to be realized and put in practice, as with all great technology.

Moreover, in order to satisfy multiple requirements that human beings need in order to transact, communicate and create value, Promether requires additional layers (apps, platforms, etc.) on top of it to align the interests and incentives of everyone participating in the system. However, making it easily accessible for everyone to create additional layers (based on individual needs) on top of the platform can be tricky from a development standpoint, and might require a lot of patching, updates, and fixes along the way. Furthermore, this means that additional code can contain bugs, and therefore, during the early phases of development, there needs to be a good bounty system in place to incentivize (which does not guarantee it) potential attackers to claim bounty rather than attack with harmful intent.

Additionally, as most current security applications or protocols are off-putting due to their distinct use-cases and user experience, modern security applications need to follow the principles of ease-of-use and facilitate every user, regardless of levels of expertise. The user needs to be able to interact with interfaces that they can use seamlessly, without even having to pay attention to the security protocols that happen in the background. The challenge lies in creating interfaces that remain similar to how everyday applications function and look, while making the security be handled technically by the applications without user intervention. Tweaking should also be stashed away for technical users under advanced security settings, while the “mainstream” user experience needs to remain intuitive, easy and comply with current majority consumption habits.

## 6.4 Technical Considerations

One of the biggest challenges in the blockchain space right now is the lack of scalability in transaction volume. The sad truth is that the blockchain was never ready for mainstream use. In fact, it was really just a proof-of-concept, a cool academic and theoretical idea when the technology took off. In the documentary, *Banking on Bitcoin*, Satoshi himself admits that the blockchain is not yet ready for mainstream use. Satoshi pleads with Julian Assange not to accept BTC when Wikileaks is denied the use of traditional payment processors. Julian Assange ignores his advice and the Bitcoin revolution begins.

Right now VISA can handle at least 56,000 transactions per second (Vermeulen, 2016). Bitcoin maxes out somewhere around 3 - 4 transactions per second (Vermeulen, 2017). It is amazing when you consider that VISA has a capacity of 14,000 times greater than most current blockchain implementations. Why in the world would we even consider blockchain to be in the same league as traditional payment processors? It is not even close. In order for the Enterprise to take decentralized networks and blockchain technology seriously, concurrent transaction volume will need to meet or exceed that of VISA. Without the ability to scale to the needs of existing companies, the blockchain will fail.

Bitcoin, Ethereum, and Litecoin are currently using a Proof of Work (PoW) system for their blockchains. PoW is by far the least performant and scalable blockchain option. Proof of Stake (PoS), while a huge improvement, still is not good enough to compete with traditional payment processors. We need a better solution to move us into the future. One of the possible solutions being currently investigated by the Promether team is the use of an innovative and emerging technology called hashed graphs as a fully parallelized and concurrent solution to replace PoW and PoS blockchains. You can be assured that whatever solution is chosen, the goal of Promether is to ultimately exceed the transaction volume of VISA, American Express, and Mastercard.

## 6.5 Regulatory Considerations

We are ambitious and optimistic, but we are certainly not naive. We understand that both our mission and our technical and functional goals will likely be perceived to be a threat by existing governments, agencies, corporations, and even

portions of the general public, who may believe in the goals and tools of “big government”, “big business”, and even “big brother.” That is why we are assembling a team of experts in Internet regulations, privacy rules, and government privacy intervention laws to ensure that we create the most effective system possible, while understanding exactly how our system may be operated relative to country specific and international laws, rules, regulations and even political agendas. Our aim is to create the most effective system to meet the needs of the public, while being prudent about government power so we can remain in business to continue operating and improving our deliverables.

NOTE: Neither the private sale nor the ICO will be offered to residents of the U.S., Canada or China.

## 7 ROADMAP

With an 18 month roadmap, Promether aims to create a network that draws inspiration from the Internet as a decentralized social space, while building solutions it was always intended to have. Each of the milestone will act as a progression towards the ultimate goal covered in this whitepaper, and will allow us to set a new standard for privacy and security.



## 8 PROMETHER TEAM

### 8.1 Core Team

#### **Eric J Anderson (Eijah)**

##### **Founder, Technical Director**

Eijah is the founder of Promether and has 20+ years of software development and security experience. He is also the creator of Demonsaw, an encrypted communications platform that allows you to chat, message, and transfer files without fear of data collection or surveillance. Before that Eijah was a Lead Programmer at Rockstar Games where he created many games, including Grand Theft Auto V. He has been a faculty member at multiple colleges, has spoken about security and development at DEF CON and other security conferences, and holds a master's degree in Computer Science. Eijah is an active member of the hacking community and is an avid proponent of Internet freedom.

#### **Elton Brauer**

##### **Operations Director**

Elton is an experienced content and marketing specialist with a demonstrated history of working in the blockchain space. His background in corporate research and consulting has led Elton to work as researcher and marketing advisor at Invest in Blockchain. He owns and manages a consulting agency Starlike, which specializes in operations optimization, technical content, community management, public relations, and branding. Elton is also a co-founder of an upcoming blockchain based information sourcing and tracking solution Cloaktrack.

#### **Rishan Bhagawat**

##### **Business Director**

Rishan is the founder and managing director of the Sublime Group, an industry leading incubator based in Dubai that has been the guiding hand to 6 top 100 market cap crypto projects. He is an entrepreneur at heart that has founded, scaled and exited two successful multinational businesses. Advisor to FanLogic Interactive Inc.(TSXV:FLGC) (OTCQB:FNNGF), an angel investor in DroneClouds and RYDE Inc. and serves on boards of multiple companies which share his vision. His passion and expertise lies in leveraging technology and capital to make the world a better place.

#### **Daniel Bainbridge**

##### **Marketing Director**

Daniel is a blockchain investor and the founder of Investinblockchain.com and Coinad.com. Since 2014 he has been bootstrapping blockchain projects and investing in this blockchain space. He has given away over 1090 BTC (worth approximately \$12 million) through the "Bitcoin Aliens" mobile games and bitcoin faucets. He brings marketing consulting as well as online traffic reach and PR to the Promether project.

#### **J-F Simard (Tek)**

##### **Community Manager**

J-F is a Linux and hardware specialist, blogger and an active crypto trader. He also ran a computer business for 12 years setting up entire networks for enterprises and building custom made computers for gamers. He also has years of experience in the field of telecom and obtained a telecommunication degree in the Canadian Armed Forces. Tek is a

Python advocate and a bash script specialist. Online privacy and security are at the top of his agenda. He runs a crypto traders network on the Demonsaw platform and is also an avid supporter of Eric J Anderson (Eijah) and his work.

#### **Cameron Gaertner**

##### **Software Engineer**

Cameron is a C++ programmer, Internet privacy advocate, and hacker. Most recently, he was a UI/UX programmer for Demonsaw, a secure and anonymous information sharing application. Cameron has participated in several CTFs the past few years, focusing mostly on reverse engineering and vulnerability research. In his free time, he loves learning about new technologies, coding, and reading.

#### **Dan James**

##### **Software Engineer**

Dan James, better known as Bl4ckNeon, is a software engineer who specializes in web development, community outreach, and Information Security. He actively participates in the Demonsaw community by making tutorial videos, updating the wiki, implementing CSS themes, hosting monthly online meetings, and running the community twitter account.

#### **Eric Gillam**

##### **Creative Director**

Eric Gillam is the founder of Omnera, an augmented and interactive design studio focused on training the world through motion graphics and mixed reality applications. He has 20+ years of digital art, 3D animation and instructional design experience, and was an Art Specialist and Senior Lead on multiple projects for Activision, Disney, Marvel, Sony, Swift Transportation, America West Airlines, BNSF Railroads, the University of Advancing Technology and the Art Institute of Phoenix. He has served as the department manager for multi-million dollar software development teams at Activision, as well as the program chair for media arts at multiple universities. He holds a Master of Fine Arts degree in Media Design.

## **8.2 Advisors**

#### **Alex Heid**

##### **Strategic Advisor**

Alex Heid is co-founder & president of HackMiami, a South Florida hacking organization that hosts an annual information security conference in Miami Beach, FL. Heid is also currently an executive with SecurityScorecard, a cybersecurity firm in New York City. Previously, Heid worked within financial industry as a web application security analyst and was also a founding member of the SERT threat intelligence team at Prolexic Technologies. Heid's contributions during that period included the development and discovery DDoS neutralization and counterattack methods during the Operation Ababil campaigns of 2012 - 2013. Heid's work has been frequently cited by mainstream media, such as the feature story about HackMiami in Rolling Stone magazine entitled "The Geeks on the Front Lines."

#### **Steven Wilkinson**

##### **Blockchain Advisor**

Steven Wilkinson is a certified cryptocurrency, blockchain and information security professional. He brings more than 10 years of experience in technology leadership, IT and security consulting to Algebraix Data, Inc. While researching a solution for secure value transfer across the Internet, Steven discovered Bitcoin in early 2011 and began building multiple



mining operations around it. Since then, he has been working and advising on a variety of blockchain projects and startups in this emerging ecosystem, including multiple token crowd sales. In 2013, Steven founded the Bitcoin consulting firm, Austin Bitcoin, which is one of the first BitPay merchant integration partners. He is also one of the co-founders and Vice President of the Texas Bitcoin Association which produces the Texas Bitcoin Conference. Steven holds a Certified Information Systems Security Professional (CISSP) certification from (ISC)<sup>2</sup> and a Certified Bitcoin Professional (CBP) certification from (C4).

### **Richard Leckinger (Caraka)**

#### **Technical Advisor**

Richard is a long time crypto enthusiast, investor and package maintainer. He has worked as a Ministerial Advisor covering energy analysis, management and behavior change, and has stood for parliament 4 times. A key driver is the belief that technology should be our servant; not our master - bringing an end to surveillance capitalism. Realizing human potential through open data, open networks and protection of privacy are top line goals.

### **Bryce Case (YTCracker)**

#### **Hacker Advisor**

Bryce Case, better known as YTCracker, was exposed to computers by his father and mother, learning to program BASIC from age 4, and is a computer security professional most known for his high profile defacements of various government websites in the early 2000s. Since then, he has maintained close ties with the hacker community at large, and founded the grey-hat web board DigitalGangster.com. Case has consulted and performed penetration testing for businesses of all sizes, and has made regular appearances in the media explaining tactics used by hackers. Currently, Case runs a "celebrity cyber bodyguard" firm known as the Faction, protecting high-profile clients from unwanted intrusions and leaks.

### **Alexander Reay**

#### **IoT Advisor**

Alexander is a life long tech entrepreneur & pioneer in digital business models launching one of the UK's first digital publishing companies back in 1997. Alexander is passionate about disruptive technologies and new business models, with a keen interest in how Blockchain and AI can be utilised to improve humanity. As an early advocate for the merits of Blockchain and DLT, Alexander is a board director at the IDACB (International Decentralized Association of Cryptocurrency and Blockchain), Ambassador of the Nordic Blockchain Association, President and founder of the Nordic IT Association, a 2x Nominated Deloitte entrepreneur of the year and a recognised top 250 global authority on IoT, Automation & Strategic Management.

### **Randall Johnson**

#### **Legal Advisor**

Randall W. Johnson is a securities and finance attorney and a leader in international regulations affecting the blockchain industry. He is on the Board of Advisors of Cofound.it., one of Europe's leading blockchain project incubators, and has advised on more than 15 international blockchain token offerings. He also assisted the government of Anguilla to create its new Anguilla Utility Token Act. He is Senior Counsel at Sinnott & Company, an Atlanta based securities and finance law firm and a co-founder of ArtistCap Partners, a private investment firm and consultancy. Previously, Mr. Johnson worked for several years as a partner in a leading technology law firm, and senior counsel an international law firm.

## **Seth Wahle**

### **Hardware Advisor**

Seth Wahle is a hardware engineer who was featured in Forbes and BBC in 2015 for exploiting Android phones using an implanted NFC chip. He has since developed hardware for 4k streaming, detecting enemy I.E.D.'s, and radio communications equipment for the next generation of fighter jets. Most recently, Seth took first place in the 2017 Huntsville NASA Space Apps Challenge.

## **Jason Bissell**

### **Systems Advisor**

Mr. Bissell brings with him over 20 years of management experience in multiple I.T. sectors, with a focus on Critical Infrastructure & Security, software architecture and the design criteria of large networking systems. He has worked for multiple Fortune 500 companies, as well held consulting roles with many high-tech global entities, with a primary focus on cyber-security & defense. Familiar with DoD-Standard protocols and design logistics. He is also a member of a couple of the leading brain trusts in the early development of desktop and mobile encryption security and new technologies, with extensive knowledge of industry-specific regulations; (ITIL V3, AT101, SOX, PCI, HIPPA).

## **8.3 Strategic Partners**

### **Sublime Group**

The Sublime Group is a team of global market leaders with deep relationships and extensive experience in raising capital through digital token sales. Their strength lies in their unique combination of visionary technical and financial expertise, coupled with proven growth hacking and digital marketing skills from the performance marketing industry.

### **Sinnott & Company**

Sinnott & Company is a corporate law, project finance and advisory boutique serving domestic and international clients. Their areas of specializations include blockchain regulatory issues, securities law matters, domestic & international tax, international joint ventures, project finance and advisory, public-private partnerships, and more.

### **Holo**

Holo is a distributed cloud computing platform built on Holochain. Similar to AirBnB but for cloud hosting, users give up the spare resources, and space on their devices in exchange for Holo fuel, a new type of tokenless cryptocurrency which is tangibly asset-backed by hosting, and distributed computing on Holochain applications.

## 9 CONCLUSION

Despite all these problems, we should not be led to an anti-technological discourse and disconnect from the Internet – quite the contrary, we should become even more engaged and develop greater mastery of it to ensure that everyone can benefit with decreased exposure to the threats of an always-on Internet. While the past decade has been bad for privacy, we cannot forget that privacy is not just about us, but more importantly about the generations to come – our children, grandchildren and those yet to be born. We have laid an amazing foundation for limitless connectivity, but it is also our responsibility to not neglect the things that matter most in such an era - privacy, security, and anonymity. The problems we have created as the consequence of the “Lie of Convenience” and rapid innovation are challenging to overcome, but it is important to understand that they are not irreversible, as long as we continue fighting for our rights, identities, and personal liberties. Therefore, instead of discussing security, privacy and anonymity as a negative practice and associating it with extremists and hackers, we should consider how it can enable us, both legally and socially, to reflect our true selves through our thoughts, actions, belonging and sharing. Join us in building and enabling a securely interconnected infrastructure of tomorrow. The future is not yet written, but it is within our power to make it happen.

Choose the End of Surveillance. Choose Promether.

## FOUNDER’S ACKNOWLEDGEMENTS

I want to thank a few of my personal heroes for blazing the trail that led me to the place where I could envision a better future for privacy. Aaron Swartz, Bjarne Stroustrup, Kim Dotcom, Peter Sunde, Shawn Fanning, Julian Assange, Chelsea Manning, Edward Snowden, Noam Chomsky, Nikola Tesla, Gene Roddenberry, Erich von Däniken, Jean-Luc Picard, and John McAfee are just some of the courageous people who weren’t afraid to take a stand for what they believed in. These role models taught me that life is too short to sit idly by. No matter what happens, never stop believing in yourself. We stand on the shoulders of Internet giants as we move forward with Promether and take our turn at changing the world.

I leave you with a quote from Michael Ende, the author of *The Neverending Story*.

“It’s like the Nothing never was.”

–Eijah

## REFERENCES

- Assange, J., Appelbaum, J., Maguhn, A. M., Zimmerman, J. (2012) *Cypherpunks: Freedom and the Future of the Internet*. New York: OR Books.
- Brauer, E. (2017) "Cryptocurrency Security Debate: Is It Really Safer To Let Banks Store Your Money?", *Invest In Blockchain*, 23 December. Available at: <https://www.investinblockchain.com/cryptocurrency-security-debate/>
- Edward Lucas (2015) *Cyberphobia: Identity, Trust, Security and the Internet*. London: Bloomsbury Publishing.
- Equifax (2017) "Equifax Announces Cybersecurity Incident Involving Consumer Information", *Equifax*, 7 September. Available at: <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>
- ETCIO (2017) 50 billion IoT-connected devices by 2020: Report. Available at: <https://cio.economictimes.indiatimes.com/news/internet-of-things/50-billion-iot-connected-devices-by-2020-report/59589429>
- Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. 1st edn. London: Hamish Hamilton.
- Jason Whittaker (2002) *The Internet: The Basics*. London: Routledge.
- Javelin (2017) *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*. Available at: <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>
- Lagasnerie, G. D. (2017) *The Art of Revolt: Snowden, Assange, Manning*. California: Stanford University Press.
- Leslie Holmes (2015) *Corruption: A Very Short Introduction*. New York: Oxford University Press.
- Intel (2015) *Grand Theft Data: Data exfiltration study: Actors, tactics, and detection*. Available at: <https://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf>
- McCoy, K. (2017) "Target to pay \$18.5M for 2013 data breach that affected 41 million consumers", *USA TODAY*, 23 May. Available at: <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/>
- Morabito, V. (2017) *Business Innovation Through Blockchain: The B3 Perspective*. Cham, Switzerland: Springer.
- Negash, B., Rahmani, A. M., Liljeberg, P., Jantsch, A. (2018) "Fog Computing Fundamentals in the Internet-of-Things", in Rahmani, A. M., Liljeberg, P., Preden, J. S., Jantsch, A. (eds.). *Fog Computing in the Internet of Things*. Cham: Springer pp.3-13.
- Newcomer, E. (2017) "Uber Paid Hackers to Delete Stolen Data on 57 Million People", *Bloomberg Technology*, 21 November. Available at: <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>

Petraetis, G. (2017) "How Netflix built a House of Cards with big data", CIO, 13 July. Available at: <https://www.cio.com/article/3207670/big-data/how-netflix-built-a-house-of-cards-with-big-data.html>

Philip Kotler (2016) *Democracy In Decline: Rebuilding Its Future*. London: Sage Publications Ltd.

Pix, A., Schneier, B. (2017) "Surveillance is the business mode of the internet", openDemocracy, 18 July. Available at: <https://www.opendemocracy.net/digitaliberties/agne-pix-bruce-schneier/surveillance-is-business-model-of-internet>

Roberts, J. J. (2016) "3 Security Breaches That Freaked Out U.S Companies", *Fortune*, 21 September. Available at: <http://fortune.com/2016/09/21/biggest-security-breaches/>

Stanford Graduate School of Business (2017) *Chamath Palihapitiya, Founder and CEO Social Capital, on Money as an Instrument of Change*. Available at: <https://www.youtube.com/watch?v=PMotykw0Slk&t=12s>

Statistic Brain (2016) Text Message Statistics. Available at: <https://www.statisticbrain.com/text-message-statistics/>

TED Talks (2014) *How we take back the Internet | Edward Snowden*. Available at: <https://www.youtube.com/watch?v=yVwAodrjZMY>

Vermeulen, J. (2016) "VisaNet - handling 100,000 transactions per minute", *MyBroadband*, 17 December. Available at: <https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html>

Vermeulen, J. (2017) "Bitcoin and Ethereum vs Visa and PayPal - Transactions per second" *MyBroadband*, 22 April. Available at: <https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html>

Vijayan, J. (2016) "Why rogue employees may pose bigger threat to corporate data than hackers", *The Christian Science Monitor*, 7 July. Available at: <https://www.csmonitor.com/World/Passcode/2016/0707/Why-rogue-employees-may-pose-bigger-threat-to-corporate-data-than-hackers>