PROMETHER

THE END OF SURVEILLANCE

"He that would make his own liberty secure must guard even his enemy from oppression;
for if he violates this duty he establishes a precedent that will reach to himself."

~ Thomas Paine

V 1.0

Overview

Promether is a revolutionary new type of platform called an Adaptive Symbiotic Network (ASN). Based on the principles of Artificial Intelligence (AI) and Ubiquitous Computing, Promether allows you to create any type of network to meet your specific needs simply by deploying and configuring a series of reusable software nodes. Centralized, decentralized, distributed, and hybrid topologies are all supported. Once a network is configured, any application can then communicate and transfer data securely.

Promether is not a Walled Garden, nor is it just another persistent network. It's an open-source and component-based, reusable system that abstracts the details of the secure network from the applications that use it. By doing this, Promether removes the overhead and risks associated with building out traditional security infrastructures. This allows developers to focus on implementing application features instead of worrying about the potential security vulnerabilities of the network and communication protocol.

Simple, reusable, and effective end-to-end security for all. The end of surveillance is here.

Welcome to Promether.

PROJECT GOALS

WE NEED **CHOICE** AND **FLEXIBILITY**. A PLATFORM THAT **ADAPTS** TO USER NEEDS.

The primary goal of Promether is to bring about an end to surveillance by creating a reusable, node-based infrastructure that can be configured as any network topology to allow applications to communicate and share data securely. We need choice and flexibility, a platform that adapts to our needs. Building future applications on top of a ASN foundation will empower us to regain control of our data.

Other important goals of Promether:

- Open and permissive code (MIT license)
- Open and permissive infrastructure (no walled gardens)
- Secure Infrastructure details abstracted from applications
- Platform (OS), language, application, and protocol agnostic
- 100% POSIX compliant code and API (32/64 bit, x86/x64/ARM support)
- Easily configurable security and anonymity
- End-to-end symmetric and asymmetric encryption
- Modular and dynamic architecture
- Centralized, decentralized, distributed, local and hybrid network topologies
- Vertical and horizontal scalability
- Evasive and subversive firewall circumvention (Palo Alto), DPI, Great Firewall of China
- Lightweight and portable with low memory and CPU requirements (PI, IoT, etc.)
- No logging, no tracking, nothing to hand over to governments
- 100% configurable, adaptive, mutative, reusable and component-based architecture
- C/C++ and Python API Support

In the future, we won't...

- Be subject to data collection by abusive governments
- Be spied upon by rogue agencies who seek to harm us
- Trust companies with our personal information
- Be victims of preventable cyber attacks

In the future, we will...

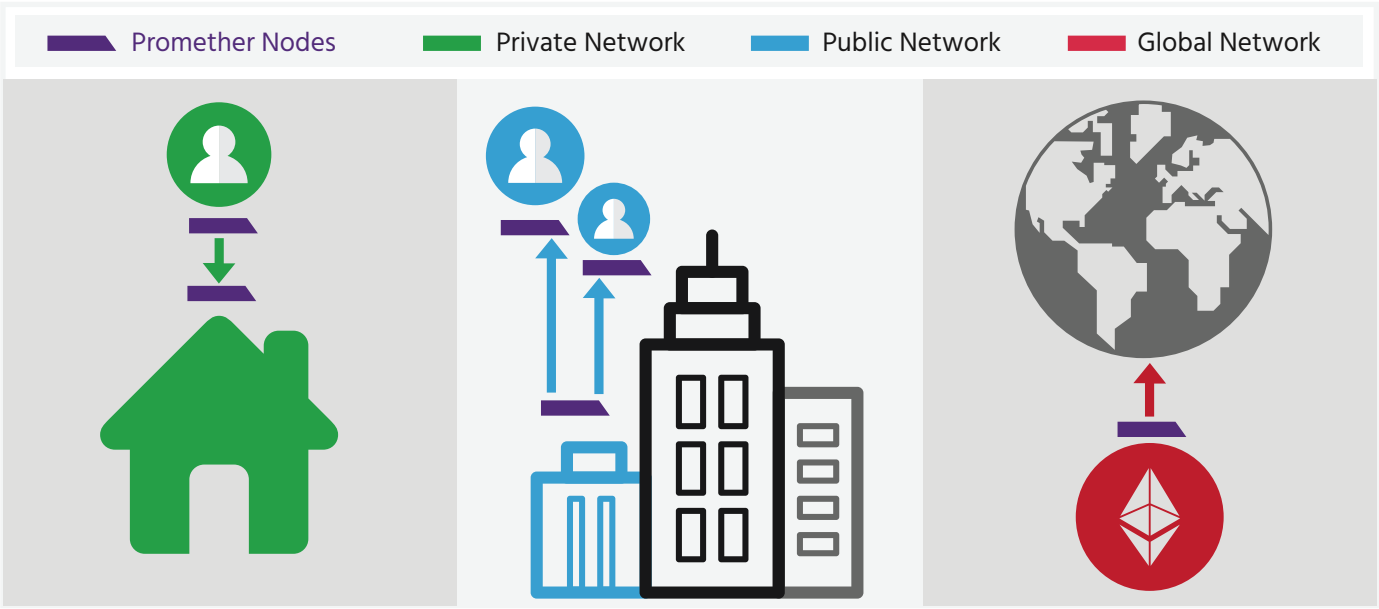
- Empower the people to take back control
- Remove the corporate middleman, giving us a competitive advantage
- Create powerful and innovative technologies to protect our privacy
- Bring about an end to surveillance

PROJECT VISION

POWER AND CONTROL OVER DATA SECURITY CAN BE ONE CLICK AWAY

A Promether network is made up of a collection of small software components, called nodes that can be deployed in many configurations. A key benefit of a node-based, ASN architecture is that the nodes handle the secure transmission of data, abstracting these details away from the underlying applications. Giving flexibility to network topology, while remaining agnostic to the data they transmit. This gives power and control to the application developers, allowing them to focus on making their applications great, rather than having to worry about the complex details of network and infrastructure security.

A Promether Network can operate in the following different ways:



Private Network or Intranet

As a Private Promether 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 Deployment

As a Public Promether 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 Deployment

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

TEAM

2 DECADES OF EXPERIENCE BUILDING OUT REAL WORLD ENTERPRISE SOLUTIONS

Founder

Eric Anderson (Eijah) is the creator of Demonsaw, a secure communications platform that allows you to chat, message, and transfer files without fear of data collection or surveillance. He has over 20 years of software development and IT Security experience. His career has covered a broad range of Internet and mid-range technologies, core security, and system architecture. He is also an active member of the hacking community and an avid proponent of Internet freedom.

Technical

- Creator of Demonsaw
- Lead Programmer for Rockstar Games on Max Payne 3, Grand Theft Auto 5, and Red Dead Redemption 2
- Lead Programmer for Activision on Guitar Hero 5, 6, and Band Hero
- Security Portfolio Architect for American Express, authored their Application Security Vulnerability whitepaper
- Hacked Bluray and released the first AACS Device Key

Academic

- Multiple certifications and degrees, including a Master in Computer Science
- Adjunct faculty member at two community colleges where he taught 18 accredited courses on a variety of Computer Science subjects

Business

- Led teams of programmers locally and globally
- Most recently he was the Chief Technology Officer (CTO) of MGT
- Worked with industry leaders such as Kim Dotcom, John McAfee, Nolan Bushnell, Joshua Corman, John Fanning, as well as many others

Speaking Engagements

- Speaker/Workshop Leader at DEF CON for 4 years and HackMiami for 3 years
- Numerous podcasts, interviews, and published articles about his work

Community

- An avid proponent of Internet freedom
- Ran the public Demonsaw community for two years
- Open-sourced many codebases, including the most recent 100,000 lines of Demonsaw code released under the permissive MIT license
- An active advocate of diversity and inclusion, including a 2017 sponsorship of Queercon at DEF CON 25

Team Members

Eric has brought together a diverse team of leaders in a variety of technical fields including hacking, programming, network administration, executive leadership, marketing, sales, and strategy/planning.

HISTORICAL TIMELINE

MORE **DATA,** MORE **PROBLEMS.** THE UNDERLYING PROFITS OF LOSING **PRIVACY**

In 1795 when Thomas Paine wrote the words "He that would make his own liberty secure must guard even his enemy from oppression; for if he violates this duty he establishes a precedent that will reach to himself." It was with coastal borders and suffrage in mind, but it holds true with information security today. We have sold our liberties and our fundamental rights to privacy at an astoundingly cheap rate, topped off with an unbelievably low return. We are at the brink of very big data meeting very big security flaws, and the fallout will be in history books.

Let's look toward the future without forgetting the past:

1940s

Project SHAMROCK/MINARET
1945
AFSA/NSA/Western Union/RCA/ITT intercept all telegraphic data entering/exiting US – no warrants

UKUSA Treaty
1946
AUS/CAN/NZ/UK/US ('Five Eyes') bound in a secret bilateral joint intelligence collection agreement

1960s

Project FROSTING
1966
'Five Eyes' establishes program for collecting and processing all data from communications satellites

Project ECHELON
1971
'Five Eyes' creates global eavesdropping network that can collect millions of records on individuals.

1970s

Network Email
1971
Ray Tomlinson sends test email to himself with 2 computers sitting side by side on ARPANET

TCP Implemented
1974
Vinton G. Cerf & Robert E. Kahn, publish "A Protocol for Packet Network Intercommunication"

Project BLARNEY
1978
NSA "upstream" surveillance & collection in-house at top-level telecommunications companies

.com Introduced
1985
Created on the Domain Name System, administered by the Department of Defense

1990s

WWW Proposed
1989
Tim Berners-Lee submits a proposal for a distributed information system at CERN

Mosaic Developed
1993
NCSA at the University of Illinois Urbana-Champaign create a multi-protocol browser

Google Incorporated
1998
Formalized in Susan Wojcicki's garage in Menlo Park, California

Patriot Act Signed
2001
Controversial Act including indefinite detention, asset forfeiture, and expanded surveillance

2000s

Google Acquires Keyhole, Inc
2004
CIA Non-profit In-Q-Tel sells Keyhole, Inc for $35m, this becomes Google Earth in 2005

PRISM Begins
2007
NSA partnership between Microsoft, later Yahoo, Google, Facebook, Youtube, Aol, Skype, Apple, etc

Google/NGA Partnership
2008
National Geospatial Agency and Google partner to launch the high-resolution spy satellite GeoEye-1

DOJ Admits Domestic Oversteps
2009
Deparment of Justice acknowledges NSA large-scale overcollection of domestic communications

Patriot Act Extended
2010
President Obama signs extention on expiring portions of the Patriot Act

2010s

Utah Data Center Built
2010

Construction started on $1.5billion NSA data center, initially known as "Massive Data Repository"

FISA Extended
2012

Congress extends the FISA Amendments Act for another five years, Obama signs off

Amazon/CIA Contract
2013

After a court battle with IBM, Amazon is awarded a $600million cloud computing contract with the CIA

Snowden NSA Leaks
2013

Edward Snowden's leaked NSA documents published in the Guardian and Washington Post

Cambridge Analytica Founded
2013

Data mining company involved in 100s of political races, models over 230 million personalities in US

FASCIA Database
2014

As reported in 2014, FASCIA location database can process 5 billion records per day

2017

TOR Fully Funded
2015

Through the Broadcasting Board of Governors tor receives $6.1 million between 2007 and 2015

USA Freedom Act Passed
2015

Mandated an end to bulk-collection of metadata, but allowed mandatory retention under FISA Court

James Clapper IoT Spying
2016

US Director of National Intelligence in Senate Testimony admits spying via Internet of Things

GOOG Surpasses Apple
2016

Alphabet Inc. surpassed Apple to become the world's most valuable publicly traded company

VAULT 7 Leaks
2017

Wikileaks releases troves of documents outlining CIA surveillance, and exploit programs

Equation Group Leaks
2017

The Shadow Brokers release 0day exploits created by the NSA/CIA/Private Contractors

PROBLEM STATEMENT

SECURITY IS AN ILLUSION
YOU HAVE THE POWER
TO SAVE YOURSELF

Why create an ASN framework to facilitate the creation of endless secure and anonymous networks? Because the following problems are prevalent in our world today and it's time that we put an end to surveillance.

Hackers are Unstoppable

Hackers are unstoppable, because the biggest security flaw of all is always people. No amount of due diligence, secure development practices, or adherence to compliance and regulatory mandates will be able to stop a hacker who is motivated to find and manipulate vulnerabilities in a system. Anybody who says otherwise is trying to exploit us. When we amass a large amount of valuable information in a central location, it becomes a tempting 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.

Security Is Difficult

Every application vendor must implement and test its own security solution as part of every product. This means that many companies are re-inventing the wheel with respect to secure data transmission. Application providers spend unnecessary time implementing and testing security code when they should be concentrating on building great applications - something that they are excellent at. 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.

Times Have Changed

We've moved to a social networking model for most of our online interaction with a focus on ease-of-use and simplification. The interaction model of social networks is completely different than the older 1:1 or 1:N models of the past 2 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?

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 all complicated things for the average user. Security doesn't need to be difficult to be effective.

Corporate Betrayal

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.

Government Deception

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 tax-payer 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.

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.

ARCHITECTURE

EASY TO **CONFIGURE** AND **DEPLOY** TAKE BACK **CONTROL** OF YOUR NETWORK

A Promether network can be configured in a variety of ways to create different network topologies, each with its own benefits. The following are just a few of the endless possibilities.

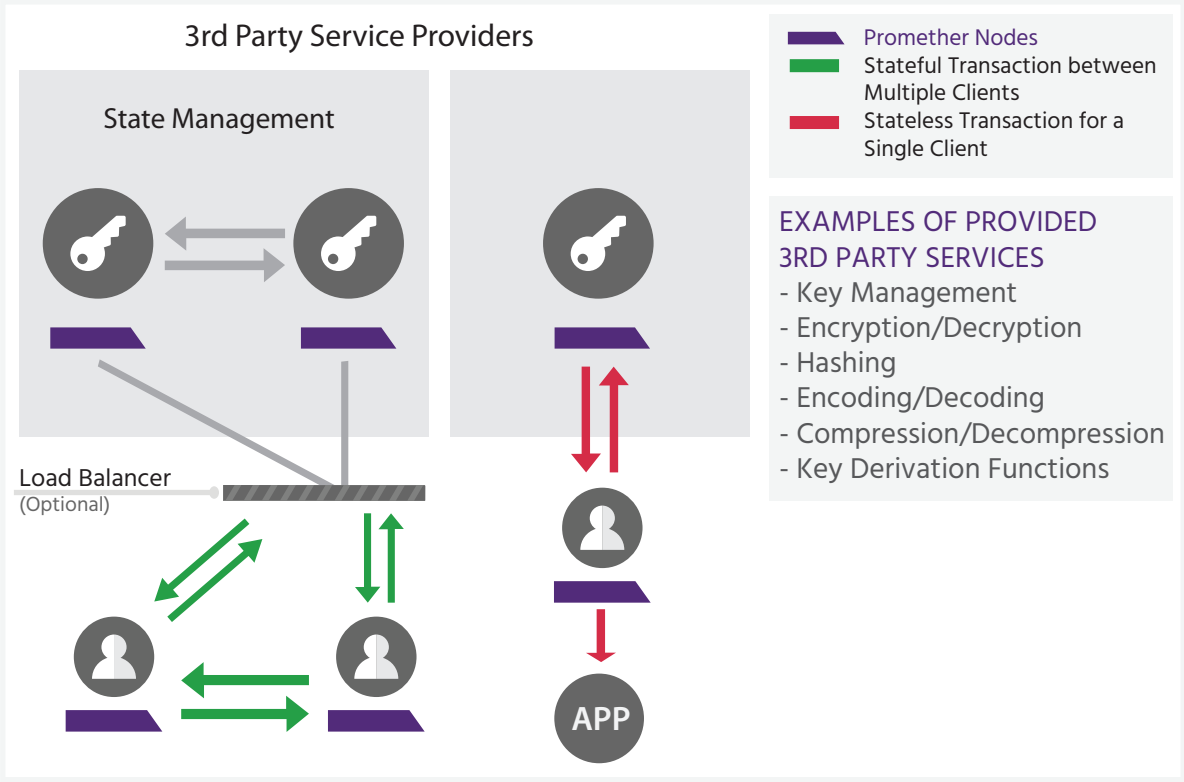


Fig. 1 3rd Party Encryption Provider Services

3rd Parties can provide isolated and scalable utility services such as encryption, compression, and cryptographic key management.

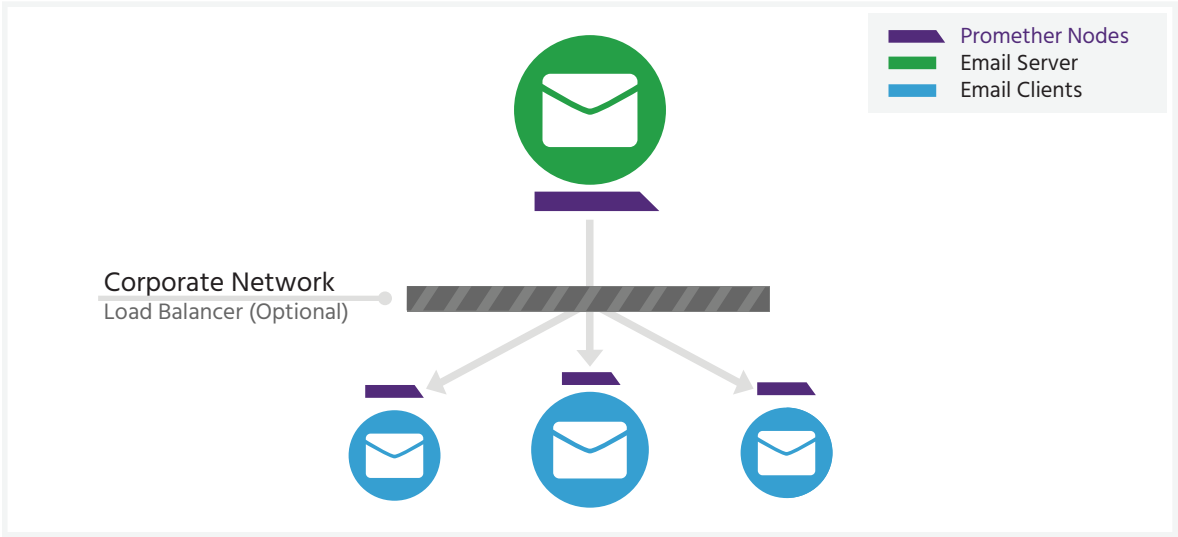


Fig. 2 Secure Email (PGP Alternative)

Insecure applications and protocols become secure, end-to-end encrypted platforms.

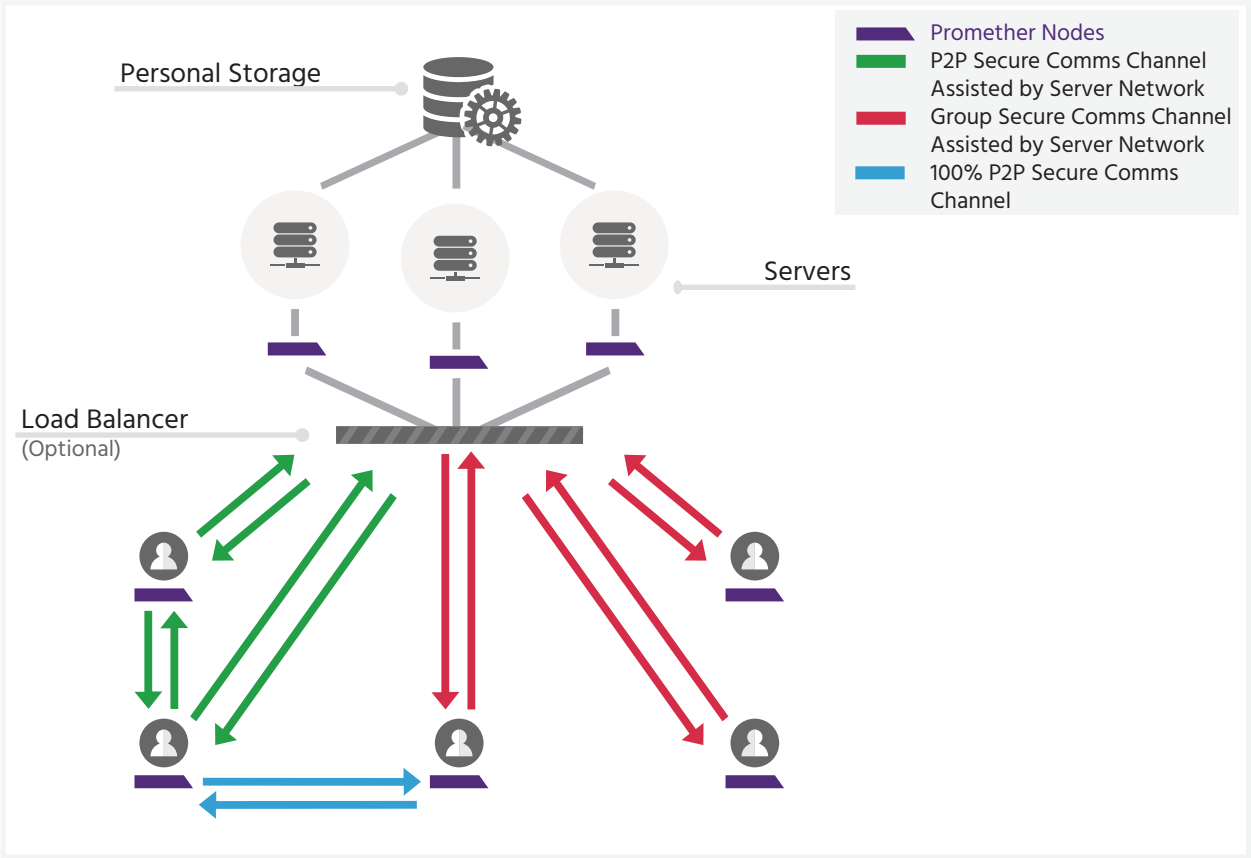


Fig. 3 Secure VOIP and Chat Platform

Create secure communication channels between clients for chat, VOIP, or document sharing.

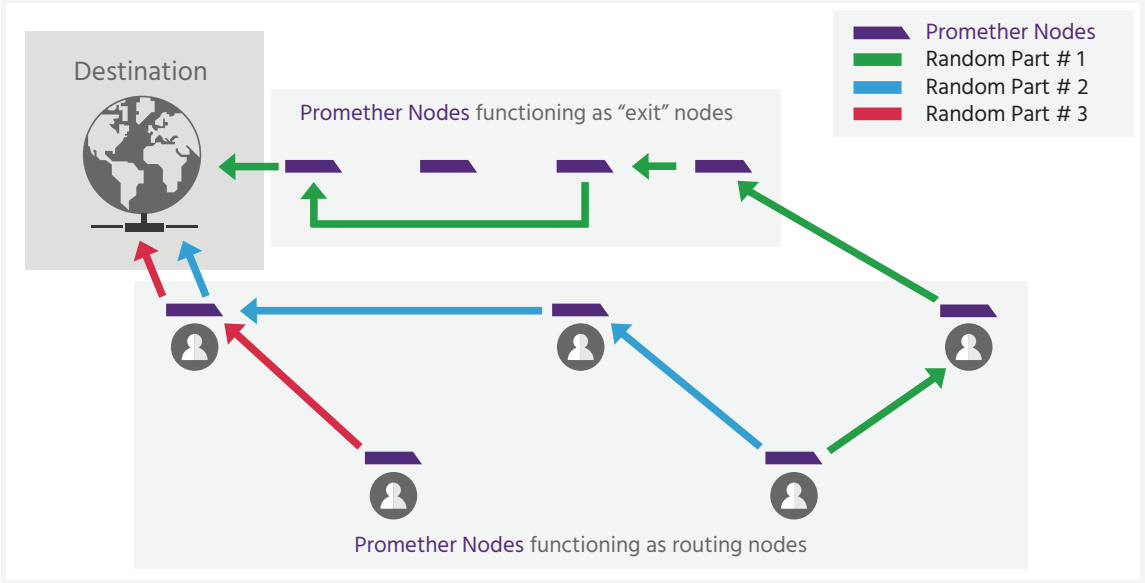


Fig. 4 Anonymous Traffic Routing (TOR Alternative)

Route traffic dynamically through your network to safeguard anonymity.

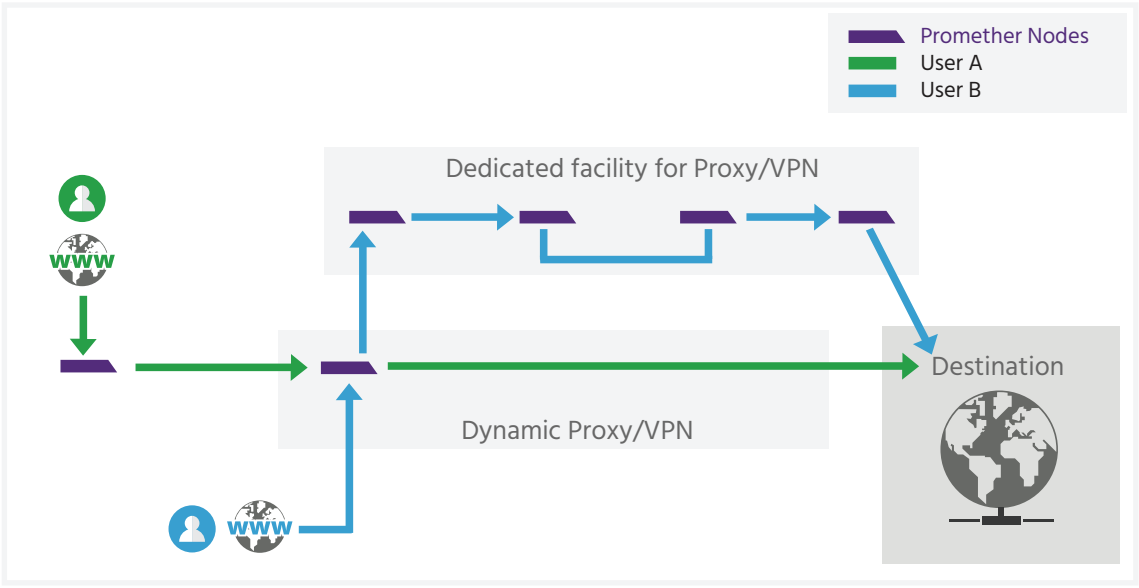


Fig. 5 Secure Web Browsing (Proxies/VPN Alternative)

You have complete control over where your data goes and who has access to it.

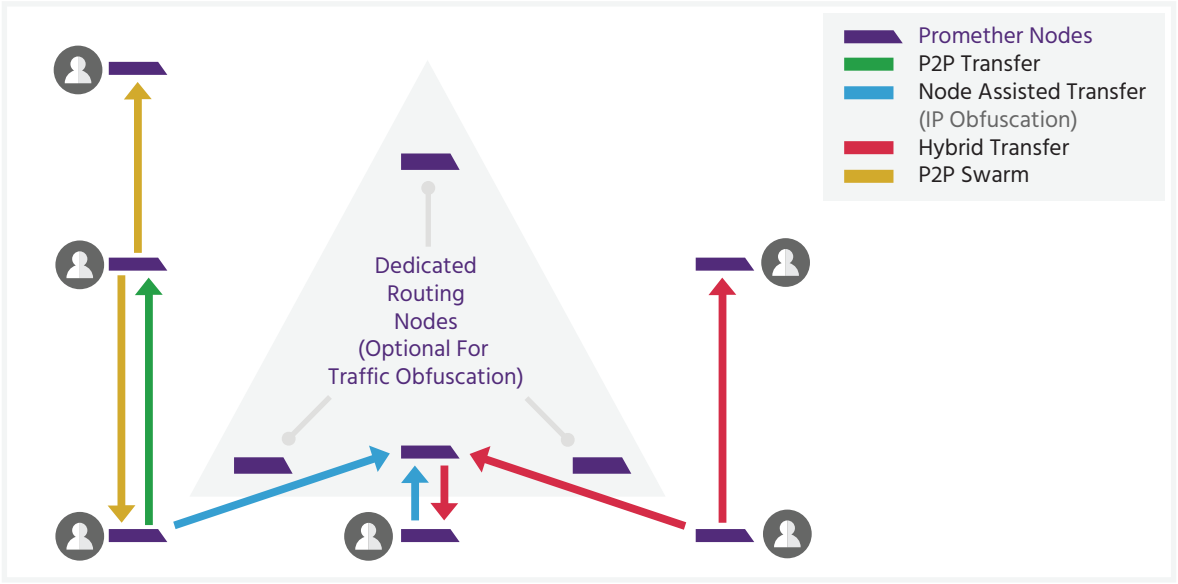


Fig. 6 File Sharing/Syncing Network

Centralized, decentralized, distributed, and hybrid applications are supported.

TECHNICAL DESIGN

THE **FUTURE** IS **CLEAR**
THE GEEKS SHALL **INHERIT**
THE EARTH

Promether is a secure ASN infrastructure that businesses, consumers, and developers can use to protect their privacy and put an end to online surveillance. The following information is a more technical analysis of the network, along with how the tokens will integrate into the global network.

NETWORK

A Promether network is made-up of a collection of nodes that provide limitless services to end-users.

Overview

- Networks can operate in a centralized, decentralized, distributed, or hybrid model.
- Networks can route their traffic in a proxy-based or peer-to-peer manner.
- Networks are protocol agnostic and can use either TCP or UDP to send data.
- Networks can be private or public

Topology

- Networks can be stand-alone or participate in federations.
- Federations provide a proxy layer between nodes within the same network, further obfuscating client node IP addresses from being identified on foreign node endpoints.
- Federations also provide fault tolerance and redundancy to remove any single points of failure.

Scalability

- Networks are able to scale both vertically and horizontally.
- Vertical scalability is a function of the addition of new networks, either isolated or federated.
- Horizontal scalability is a function of the addition of nodes to a specific network, thereby increasing the total computation power of a given network.

Hosting

- A network can be self-hosted or participate as a part of a larger network
- Self-hosted networks are completely disconnected from the global network, allowing complete autonomy and flexibility of configuration
- The global network is a publicly hosted network integrated into Ethereum and supports Smart Contracts to incentivize node creation in the network (via tokens) that contribute to the overall scalability of the network. It incentivizes users who contribute to the scalability of the network by rewarding contributors with tokens. The tokens, in return, are used to guarantee levels of service for the overall network. For example, a higher token ownership will generate faster speeds and access to additional levels of scalability. Users without tokens will be granted a minimal amount of bandwidth and overall network access.

NODES

Nodes are lightweight software instances that form the foundation of a Promether network. Nodes can be grouped together to form more complex networks that elicit neural network-like behaviors.

Overview

- A network can have 1:N nodes.
- Nodes can add, remove, modify, cache, proxy, persist, forward, or broadcast data.
- Nodes can choose to support all functions, or a subset of available functions on an as-needed basis.

Behavior

- Nodes operate autonomously
- Nodes collectively form a neural network which increases the overall capacity of the network as the number of nodes increase.
- The unique permutation of nodes in a given network defines the network itself, allowing networks to accommodate the current network requests.
- Nodes have the ability to propagate (i.e. hop data) across 0:N other nodes.

Data

- Nodes can host/share any type of data to provide file sharing and dark net web hosting functionality.
- Nodes are 100% agnostic to the data they send, allowing data to be end-to-end encrypted without risk to violating confidentiality of data.

DATA

Any type of data can be sent across a network.

Overview

- All data within a network must have at least one layer of end-to-end encryption.
- There is no limit on the number of layers of encryption (asymmetric and/or symmetric) that can be applied.
- Encryption keys are never shared across the network.

APPLICATIONS

Any type of application can run on a network.

Overview

- Applications can integrate in a loosely coupled manner via proxies (e.g. SOCKS5) or in a tightly coupled manner via a programmatic API.