GOLEM

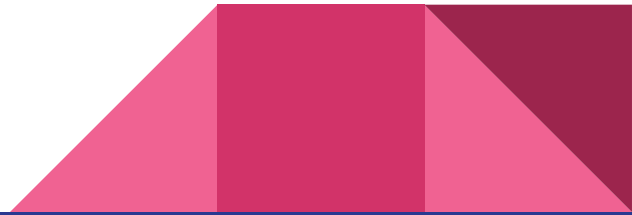
By:

Pushpendra Soni	:	RIT2015001
Pranav Maheshwary	:	RIT2015009
Priyank Agarwal	:	RIT2015029
Piyush Gupta	:	RIT2015083
Piyush Govil	:	RIT2015084

What is Golem?

Golem is the first truly decentralized supercomputer, creating a global market for computing power. Combined with flexible tools to aid developers in securely distributing and monetizing their software, Golem altogether changes the way compute tasks are organized and executed.

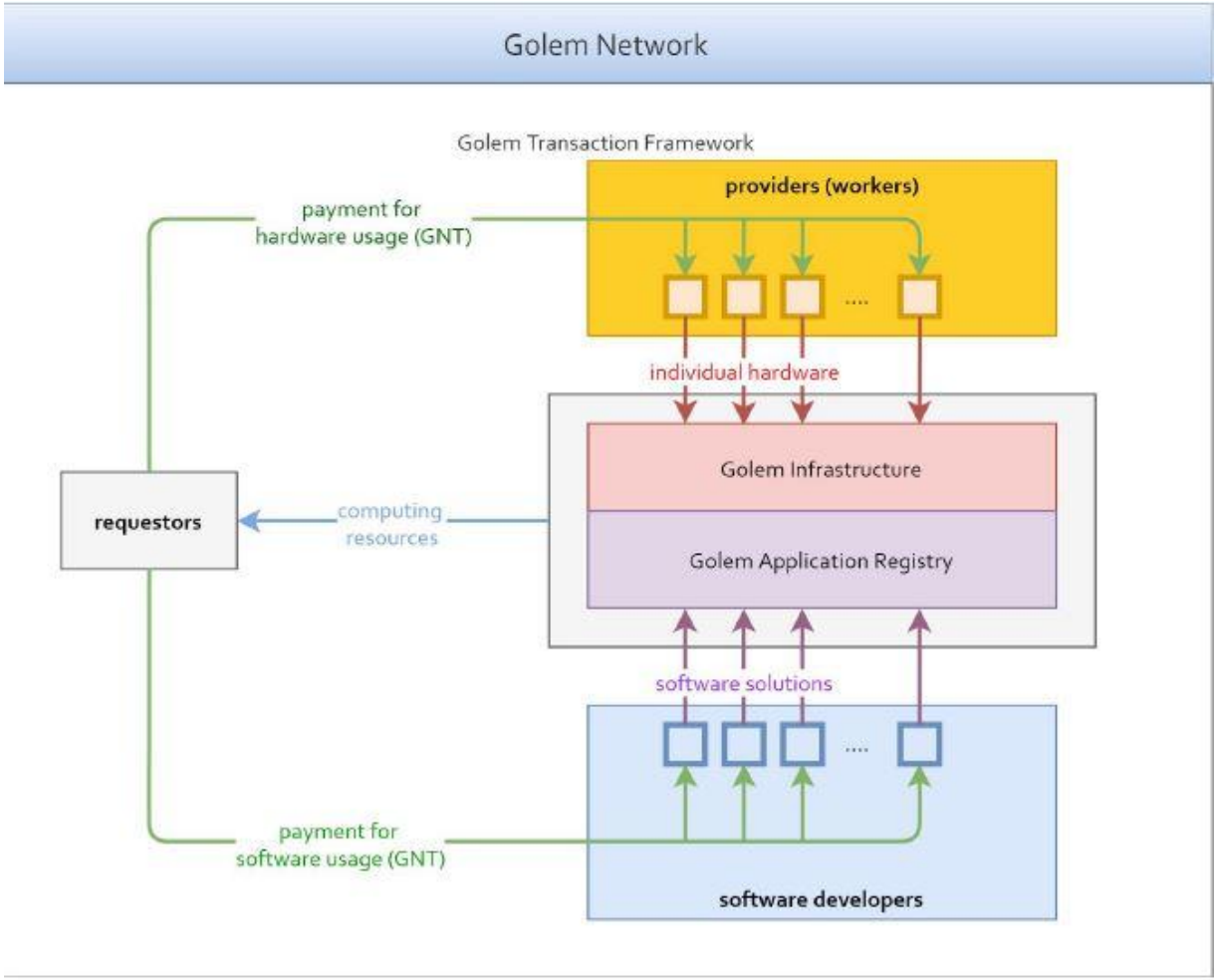
The Golem platform, put simply, is a marketplace for computing power. On the peer-to-peer network, unused computational resources can be rented out to users wishing to perform memory-intensive tasks, who pay the provider in Golem’s cryptocurrency.



- Basically, Golem aims to be the Airbnb of the computing world by allowing regular owners of idle PCs to rent out processing power to its infrastructure and get rewarded in golem’s network token (GNT).

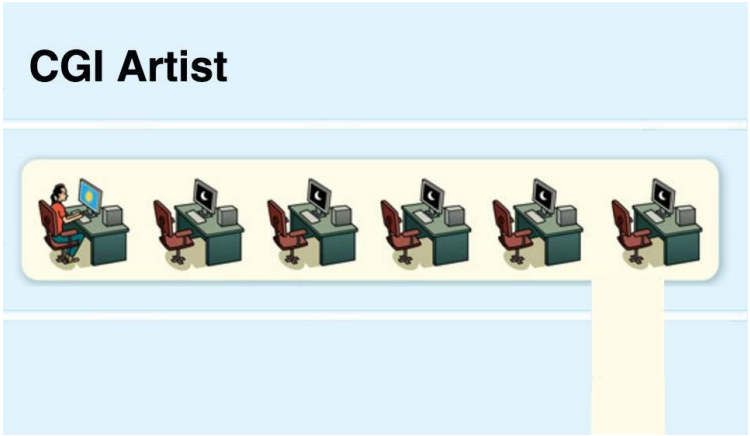
- Poised to be a futuristic internet service provider, it will not only make computation of complex applications available to the masses but also lower the cost of CGI rendering, machine learning and other computer demanding tasks that currently cost millions.

- Today, such resources are supplied by centralized cloud providers which, are constrained by closed networks, proprietary payment systems, and hard-coded provisioning operations.

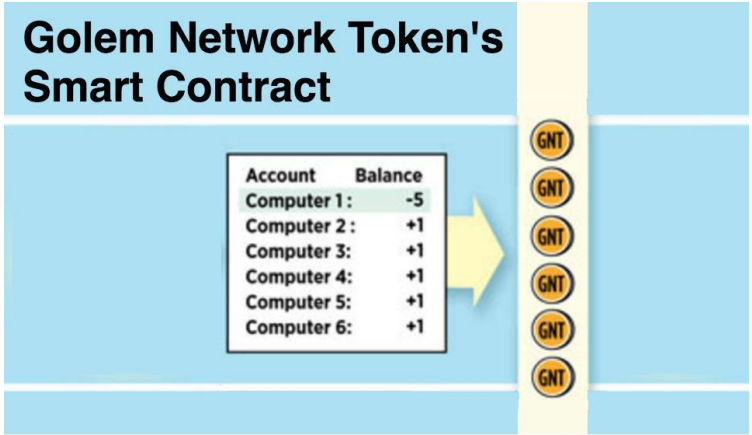


How Golem Works ?

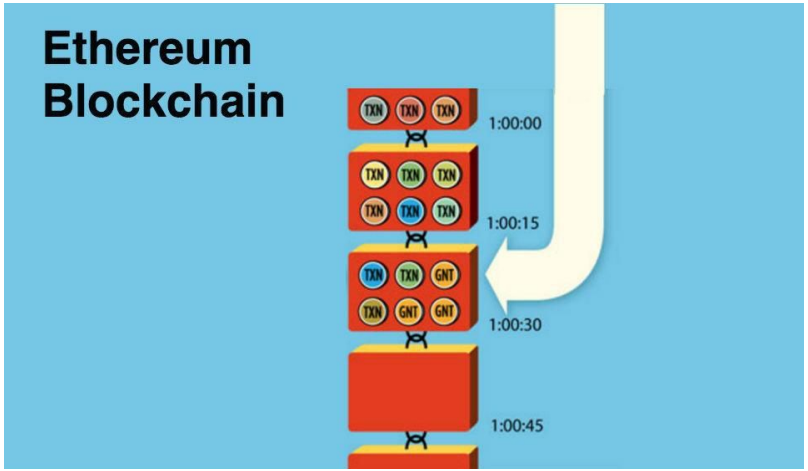
Any interested party is free to create and deploy software to the Golem network by publishing it to the Application Registry.Together with the Transaction Framework, developers can also extend and customize the payment mechanism resulting in unique mechanisms for monetizing software.



A computer-graphics artist who bought Golem Network Tokens to rent computing power on Golem tells her computer to render an animation. Golem determines the rendering can be completed by, say, five machines rendering for one hour each. (More likely, 100 for a minute each.) Each "idle" computer receives one GNT. This happens automatically.



GNTs aren't actually traded on the Golem Network itself. Ethereum makes it so easy to create tokens that the Golem Network (like many other networks) uses an Ethereum "smart contract" to trade GNT. The CGI artist's transactions are recorded onto the Ethereum blockchain, which updates the account balances of each computer that participated.



Computers supporting the Ethereum network, called miners, compete to solve a computationally intense math problem. The first to solve it wins the "block reward," which consists of newly minted coins (currently 5 ETH/block, or $1,350). The winning miner adds a new block of transactions to the ledger.

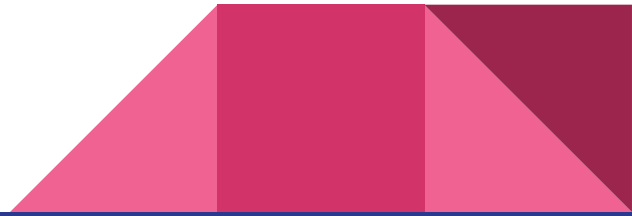
This time-stamped ledger contains every Ethereum transaction since the network launched in late July 2015. New transactions are added in blocks roughly every 15 seconds. This single source of the truth is nearly tamper-proof, as the 32,000 computers running the Ethereum software hold a copy of it. The CGI artist's GNT transactions are recorded here.

Who Is Golem For?

Golem's platform caters to a large audience: the current testnet has a focus on **CGI rendering**, but as it is refined, one can see the pool of requesters varying wildly, potentially including:

- Businesses wishing to handle large amounts of data
- Programmers running dApps
- Scientists simulating large-scale models
- Machine learning

Anyone can become a provider, renting their machines in exchange for cryptocurrency. It will be interesting to observe the variance in price from traditional centralised servers, given the low barriers to entry.



The problem it is solving

- As a decentralized supercomputer, Golem plans to **create a global ecosystem for computing power.**
- It is set to disrupt big time players in the computing market such as Amazon, IBM, Google and Microsoft, in an effort to **supply affordable computing resources** that have previously been the reserve of heavyweight market players.
- The long term use case, according to Golem, is to build a **Web3.0**. This will be a **completely decentralized network** that will enable users secure their content using **Blockchain's cryptography** while also allowing for **easy exchange of the same content** among users without the surveillance of centralized corporations and governments.

Golem's unique, interdependent ecosystem.

Group	Golem features	Incentive to participate
Requestors	Golem offers tools to execute compute-intensive tasks.	Requestors get access to affordable and scalable solutions, which combine hardware and software.
Providers	Golem combines and utilizes (almost) any kind of existing computing hardware.	Hardware providers get paid for renting out their hardware.
Software Developers	Golem is a flexible platform to deploy and monetize software.	Software developers use Golem as a distribution channel, associated with access to hardware.

Currencies and Tokens

In the unending tsunami of tokens flooding the market today, some have tried to establish a degree of stability when it comes to categorizing the new digital assets.

One such attempt is made by Pfeffer, where he makes the distinction of three types of tokens:

1. those maintaining the network backbone (tokens like Ethereum, which form the basis of the EVM),
2. those powering decentralised applications (dApps)
3. those aiming to be used as currency (Bitcoin and its many clones).

The GNT token is a perfect example of the second – the ecosystem runs on the native Golem token, with requestors paying providers in the currency for their computing power.

GNT

The Golem Network Token ("GNT") account is a core component of Golem and is designed to ensure flexibility and control over the future evolution of the project. GNT is created during the crowdfunding period (described in this whitepaper) and, following the first major release of Golem, GNT will be attributed a variety of functions in the Golem network.

- Payments from requesters to providers for resource usage, and remuneration for software developers is going to be exclusively conducted in GNT.
- Once the Application Registry and Transaction Framework are implemented, GNT will be necessary for other interactions with Golem, such as submitting deposits by providers and software developers or participation in the process of software validation and certification (as described in the Application Registry section).
- The general conditions for using GNT will be set in the Transaction Framework, but specific parameters of these interactions will be possible to define within each software integration.

The supply of GNT will be limited to the pool of tokens created during crowdfunding period.

How does Golem verify computations?

There will be different methods depending on the task type. In the future, a user who adds a new task can implement a new verification method that suits them. Possible solutions may involve:

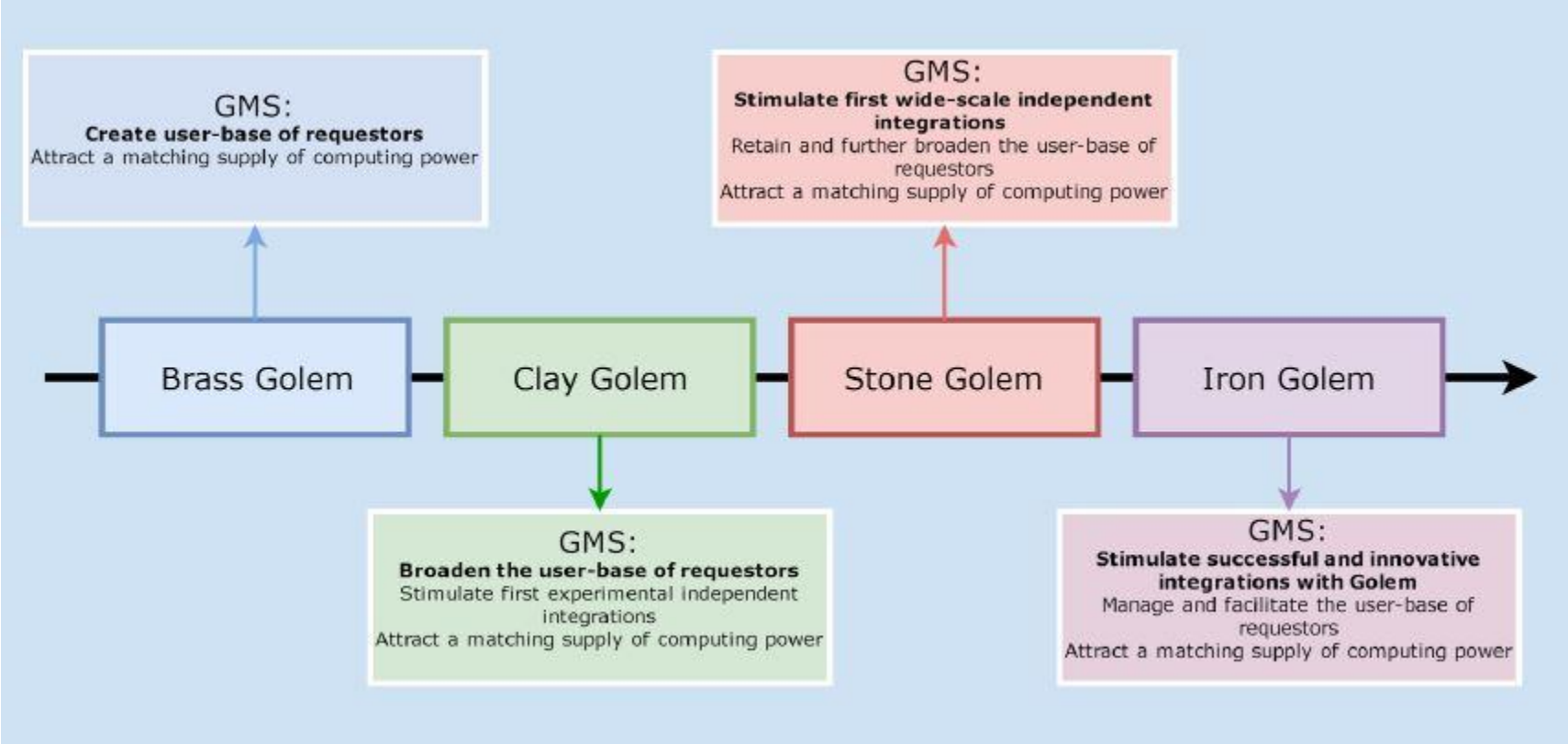
- simple correctness: checking of the result, eg. proof-of-work,
- redundant computation: ie. a few providers compute same part of the task and their results are compared,
- computing small, random part of the task and comparing this part with the result sent by the provider, ie. comparing the color of few random pixels in rendered picture

Why does Golem use Ethereum?

- Golem is building the transaction framework on top of Ethereum.
- Ethereum gives Golem expressive power, which is much-needed when implementing advanced, trustless schemes.
- Also it enables direct payments between requesters, providers, and software developers.

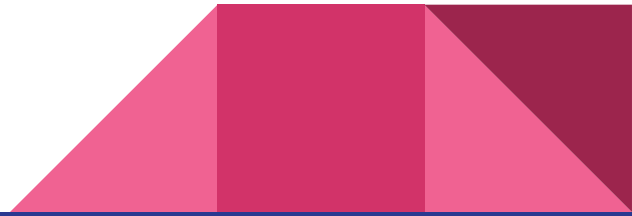
The various product milestones of the Golem Project:

1. Brass Golem
2. Clay Golem
3. Stone Golem
4. Iron Golem


GMS:
Create user-base of requestors
Attract a matching supply of computing power
GMS:
Stimulate first wide-scale independent integrations
Retain and further broaden the user-base of requestors
Attract a matching supply of computing power
Brass Golem
Clay Golem
Stone Golem
Iron Golem
GMS:
Broaden the user-base of requestors
Stimulate first experimental independent integrations
Attract a matching supply of computing power
GMS:
Stimulate successful and innovative integrations with Golem
Manage and facilitate the user-base of requestors
Attract a matching supply of computing power

1. Brass Golem

This version of Golem is only focused on rendering in Blender and LuxRender, and although it will be useful to CGI artists, we consider CGI rendering to be one use case among many, and also a training ground. This is the first decentralized computation market mainly focusing on requesters.



2. Clay Golem

Clay Golem is a big leap from the Brass milestone.

Clay introduces the Application Registry, which will make Golem a multi-purpose, generalized distributed computation solution.

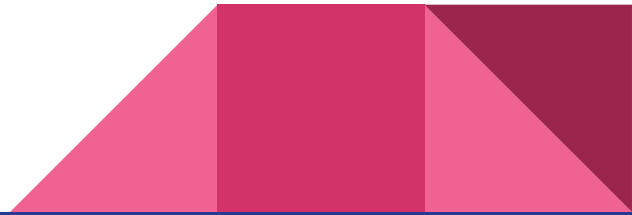
Developers now have the means to integrate with Golem. This advance, however, may come at the cost of compromised stability and security, so this version should be considered an experiment for early adopters and tech enthusiasts. Prototypes, new ideas and solutions will be built on Clay..

3. Stone Golem

Stone Golem will add more security and stability, but also enhance the functionalities implemented in Clay.

An advanced version of the Task API will be introduced. The Application Registry will be complemented by the Certification Mechanism that will create a community-driven trust network for applications.

Also, the Transaction Framework will create an environment that will allow Golem to be used in a SaaS model.

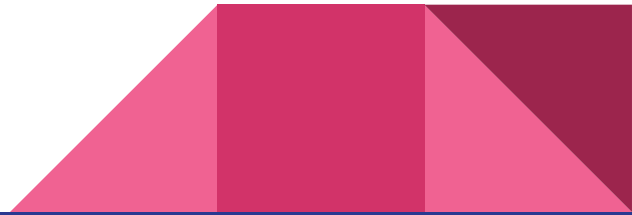


4. Iron Golem

Iron Golem, the final stage of the roadmap will be the most polished – the system will have been rigorously tested, and made more secure, stable and scalable.

Developers will have much more flexibility, being able to interact with resources outside of the network itself and gaining access to the Developer Toolkit.

A deeply tested Golem that gives more freedom to developers, allowing them to create applications that use an Internet connection or applications that run outside the sandbox.



Security Elements in Golem

Every new technology is exposed to attacks, some new and unpredictable. All components of the Golem application will be designed to be robust against attacks.

Key security elements will be:

- computations in isolated environments with minimal privileges and lack of external network connectivity.
- Well-known safety cryptography based on elliptic curves.
- Signed and encrypted messages inside the Golem network ensuring authenticity, which protects against man-in-the-middle attacks and passive data collection.
- Reputation system helping to detect malicious nodes and mitigate them. Evaluating these reputation metrics will assist in secure, efficient and correct task routing.
- Whitelist and blacklist mechanisms allowing providers to build trust networks and run only applications prepared by trusted developers.

Thank You