AERGO Whitepaper

The Blockchain Fuel for Autonomous Business

Last Updated: 15 June 2018, **AERGO**

ABSTRACT

The blockchain is a form of technology that introduces for the first time, a cryptographic secure digital database of transactions that does not possess the points of failure and security issues of traditional databases. Its unique characteristics provide the potential for blockchain based products and services to disrupt many business models in many industries (for example, financial services, manufacturing, distribution, insurance, healthcare, government and the internet of things ("**IoT**")). Blockchain technology typically aim to provide three major characteristics that are important for businesses:

Security - Transparency - Trust

It achieves this through the use of a peer-to-peer ("**P2P**") network of distributed computers, where the data is securely deployed and stored using advanced cryptography.

To quote the previous Chief Operating Officer of UBS: "*the blockchain is a potentially transformative technology that will leave as deep a mark on our world over the next 20 years as the Internet has over the last 20"*[1].

The benefits of blockchain technology have not gone unnoticed, resulting in many blockchain implementations existing today. Most of these use and operate on computer networks that are easy to join and participate in. These permissionless implementations are often known as "public blockchain protocols" (such as Bitcoin and Ethereum). However, the use of an existing blockchain comes with many problems for existing businesses, mainly due to the lack of control over its features and development. Desired functionalities include throughput performance and the ability for systems to scale. While private/permissioned blockchains aim to fulfil the promise of becoming "fit-for-purpose", they entail immense costs in terms of infrastructure and forfeit the ability to evolve at the speed of open source.

The vast majority of both public and private implementations are in the early stages of their development (and currently use 3rd generation technologies). Projects typically focus on one type of blockchain versus the other. As such, most are only used for simple proof-of-concept ("**PoC**") test-cases. Despite many such projects, the evolution of the blockchain stack is still stagnating, due to difficulties with enterprise IT integration and a lack of developer-friendly and easy-to-use software tools. Many implementations also lack the enterprise grade capabilities that are critical to run real business applications in both private and public deployments. The technology behind blockchain needs to mature and become more accessible for it to become a widely used and deployed architecture. Additional services and capabilities are also needed for it to be a commonly used business platform. It also needs to be much easier to program and use for it to be adopted across many sectors.

Whoever can provide the protocol and needed supporting enterprise IT, developer and 3rd party services, has the opportunity to become as important to the future of the world-wide-web and "serverless utility computing" as TCP/IP became for the Internet.

The AERGO Project ("**AERGO**", "**Platform**" or "**AERGO Platform**") is a serious disrupter. It is also very different. It proposes to be a a 4th generation "enterprise ready" blockchain protocol

[1] Alex Batlin, et al. (2016). *Building the trust engine*. Available: https://www.ubs.com/microsites/blockchain-report/en/home.html

combined with an IT platform that uses new and more advanced technologies. It proposes to include a comprehensive ecosystem of complementary decentralized application ("**dApp**"), technologies and service providers that leverage secure cloud delivery models. Underlying technologies in AERGO are proposed to be made open source as it is truly an open and decentralised system.

AERGO is being built for **developers**, for **businesses** and the **IT suppliers** that enable them.

AERGO's platform seeks to enable enterprises and developers to easily design, build and deploy their own blockchain applications within the cloud. The platform aims to offer the possibility for creators to tailor their blockchain and applications to their needs, by giving them the choice to run across either a public or private network. Taking into account the differing characteristics private and public blockchain implementations present, the choice between the two aims to give enterprises and developers the flexibility they desire when designing a purpose-specific application. Hosting everything across a secure cloud-hosted distributed network, AERGO also aims to alleviate businesses from significant overheads through the elimination of needing to establish physical infrastructure themselves to run blockchain protocols and applications.

AERGO's core technology is based on COINSTACK[2] from Blocko Inc. ("**Blocko**"), a leading blockchain technology and enterprise IT integration-services company with operations in the UK, South Korea and Hong Kong. COINSTACK-based blockchain systems have already been deployed to 25 million users in over 20 in-production systems.

Blocko is now preparing and developing some of the core key technologies for AERGO. It proposes to provide comprehensive IT integration and support services for clients who wish to deploy and maintain new products and business services based on AERGO. Proposed new technologies include: a super-fast and efficient blockchain protocol; a new powerful SQL smart contract engine; advanced IT integration APIs; and easy to use developer tools. These are intended to be supported by a dApp orchestration and deployment framework to allow developers and businesses to install, manage and use these applications.

AERGO aims to advance enterprise blockchain, by opening up a new era of mass market usage of blockchain. An era where businesses can benefit from both public and private blockchain innovation, while focusing on building, deploying and managing new services. In short, the AERGO Project aims to provide:

1. advanced, yet friendly and easy to use technology for developers and contractors
2. a secure and fast public and private blockchain cloud architecture for businesses
3. an open ecosystem for third parties and businesses to connect and engage with

AERGO, the blockchain fuel for autonomous business

[2] A 3rd generation blockchain platform (including developer tools, blockchain operating system, integration APIs) www.blocko.io

DISCLAIMERS

This whitepaper and any other documents published in association with this whitepaper relate to the intended development and use of AERGO. They are for information purposes only and may be subject to change.

This whitepaper describes a future project

This whitepaper contains forward-looking statements that are based on the beliefs of Blocko Inc., which has prepared this whitepaper as part of its ongoing support of the project.

AERGO as envisaged in this whitepaper is under development and is being constantly updated, including but not limited to key governance and technical features. The AERGO Token involves and relates to the development and use of experimental platforms (software) and technologies that may not come to fruition or achieve the objectives specified in this whitepaper.

If and when AERGO is completed, it may differ significantly from the network set out in this whitepaper. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections or prospects and nothing in this document is or should be relied upon as a promise or representation as to the future.

Eligible purchasers

The information in this whitepaper is provided privately to certain prospective purchasers and is not intended to be received or read by anyone else. Eligibility is not guaranteed and is likely to be subject to restrictions

No offer of regulated products

The AERGO platform, AERGO Token or any token that operates on it is not intended to represent a security or any other regulated product in any jurisdiction.

This document does not constitute an offer or solicitation of securities or any other regulated product, nor a promotion, invitation or solicitation for investment purposes. The terms of the purchase are not intended to be a financial service offering document or a prospectus of any sort.

AERGO Token does not represent equity, shares, units, royalties or rights to capital, profit, returns or income in the platform or software or in any company or intellectual property associated with the platform or any other public or private enterprise, corporation, foundation or other entity in any jurisdiction.

This whitepaper is not advice

This whitepaper does not constitute advice to purchase AERGO Token. It must not be relied upon in connection with any contract or purchasing decision.

Risk warning

The purchase of AERGO Token and participation in AERGO Token sale carries with it

significant risks.

Prior to purchasing AERGO Token, you should carefully assess and take into account the risks, including those listed in any other documentation.

Views expressed in this whitepaper

The views and opinions expressed in this whitepaper are those of Blocko and do not reflect the official policy or position of any government, quasi-government, authority or public body (including but not limited to any regulatory body of any jurisdiction) in any jurisdiction.

Information contained in this whitepaper is based on sources considered reliable but there is no assurance as to their accuracy or completeness.

English is the authorised language of this whitepaper

This whitepaper and related materials are issued in English only. Any translation is for reference purposes only and is not certified by AERGO or any other person. No assurance can be made as to the accuracy and completeness of any translations. If there is any inconsistency between a translation and the English version of this whitepaper, the English version prevails.

No third party affiliation or endorsements

References in this whitepaper to specific companies and platforms are for illustrative purposes only. The use of any company and/or platform names and trademarks does not imply any affiliation with, or endorsement by, any of those parties.

You must obtain all necessary professional advice

You must consult a lawyer, accountant, tax professional and/or any other professional advisors as necessary prior to determining whether to purchase AERGO Token or otherwise participate in the AERGO project.

This whitepaper has not been reviewed by any regulatory authority in any jurisdiction. References in this whitepaper to specific companies, networks and/or potential use cases are for illustrative purposes only. Other than explicitly mentioned partners or providers such as Blocko Inc., the use of any other company and/or platform names and trademarks does not imply any affiliation with, or endorsement by, any of those parties.

Amounts are expressed in United States dollars (“USD”) unless expressly stated otherwise.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

When Satoshi Nakamoto introduced Bitcoin to the world in 2008, the new cryptocurrency was meant to enable electronic cash payments directly between individuals without the use of banks. Ten years later, the groundbreaking technology Nakamoto invented to power Bitcoin is being championed by enterprises in all kinds of industries as a way to radically improve their future products, services and businesses.

As the digital world moves towards a next generation utility computing model (where value is created across open networks and highly distributed ecosystems), blockchain has the potential to become one of the primary enterprise platforms to build these systems and ecosystems on.

In this new world, attention is likely to move away from developers having to understand and cater for complex IT architectures and the respective management and operation functions. This can help allow them to focus on application innovation and value creation at the front end of the process, where applications touch and interact with the end-user (and billions of future IoT devices). In this “serverless architecture” much of the IT complexity will be abstracted or simply hidden from the developer and the end-user. Applications will run as containers and microservices on a combination of secure private and public clouds, delivered from a wide variety of managed cloud delivery partners.

In order to achieve the promise to become one of the major platforms for this kind of utility computing world, a step change is required. Not only around core elements of the blockchain operating system itself, but in creating a completely new “enterprise blockchain platform” and associated ecosystem. These need to support the creation, deployment and management of new secure distributed microservice-based applications on blockchain.

To become mainstream (so that companies and third-parties can create value in this new world) the technologies, tools and methods need to be robust while being simple to use. They also need to be low cost.

This paper introduces AERGO: a next generation enterprise blockchain protocol and platform. AERGO aims to become one of the core mainstream IT architectures and models used by application developers and enterprise companies across a vast number of industries.

It is envisioned that thousands of innovative new products, services and business ecosystems will emerge that are built and run on AERGO.

In order to explain the current and future target market (i.e. describe the existing problem and business opportunity that lies ahead) this paper summarises a number of important enterprise needs, and fast evolving IT, technology and blockchain trends. Whilst many technical concepts are described, many of these have been simplified to explain them in a business-friendly manner. We also include more detailed information on each core topic by way of the included appendices (for example a blockchain “primer” in Appendix-A).

Core elements of AERGO are built on technologies developed by Blocko. Blocko is a leading blockchain firm that has helped some of the world's leading firms to design and deploy real business systems on a secure blockchain. Over the past four years it has learned a lot. Blocko believes that its existing core technology and advanced blockchain in-production capabilities

could form the basis of a new advanced blockchain platform for business. Proven technologies, that are already in use with over 25 million users.[3]

Blocko is contributing its core technology to AERGO. It may also deliver future services to the AERGO including consulting and maintenance services to future customers of AERGO.

As the open source platform develops and achieves higher levels of adoption with developers and businesses, it is anticipated that other companies may offer similar and complementary services to Blocko for AERGO.

[3] Gil, Jae-sik (2018). *"신한금융, 블록체인 기반 그룹 통합 인증 앱 만든다."* ETNews.com, 22 Jan. 2018, Available: www.etnews.com/20180122000304.

THE OPPORTUNITY

IMPORTANT CHANGES HAPPENING IN THE WWW AND IT TECH-INDUSTRY

The tech-industry is full of promise. It is also full of buzzwords and “the next big thing”.

In truth, what we have seen over the past 30 years is a gradual evolution and transition between what is called Web 1.0 and Web 2.0.

Web 1.0 brought us the basic internet. Dial-up modems, static (slow websites) and the most basic of mobile phones.

Web 2.0 advanced and changed this. The advent of iPhone and Android smartphones transformed the way customers interact and exchange information with one another (social media networks like Facebook, or instant multi-media messaging and video services like Twitter, Skype and Youtube). It also changed the way businesses could communicate with their markets (e-commerce via Amazon, or search and advertising through Google etc.).

Web 2.0 brought us interactive, hyper-connected, immersive, virtual, digital online ecosystems to create and share knowledge and collaborate and interact together. However, these systems were built on highly centralized mega-platforms. Platforms where vast amounts of user, customer and business data (including perhaps even more important, meta-data) are collected, mined and exploited by the owners of the platforms. Data became the new oil. However, much like oil production, few (business) parties could get into production to “extract” fair value from these ecosystems.

Many existing IT vendors support this multi-trillion industry. Building and selling the technologies and tools, that allows mega-platform providers to collect, manage, analyse and monetize this data in secure centralized (database) systems.

In short, Web 2.0 made new business models possible - but the largest benefits (and profits) primarily flowed into the balance sheets of a handful of digital global mega-firms.

Web 3.0 and so-called Web 4.0 are other buzzwords. Yet despite this, they describe the future state that promises a more “intelligent web”. One where data is used to provide hyper-personalized products and contextual services for customers. Many of these services will run on and connect with billions of mobile and other IoT devices. These connections will increasingly also be in real-time.

At the same time, IT technologies are going through some major enhancements and changes. In part these are driven by wider adoption of more secure cloud services in business. This is also due to wide adoption of increasingly open source based platforms (such as Linux as an operating system and Hadoop or TensorFlow to collect and leverage (big) data). The most commonly used development tools and middleware for software programmers are also now almost all based on open source projects. Developers increasingly want to create new apps that run on open platforms.

The above technology factors are enabling an entirely new way of developing new services on low-cost commodity-like IT architectures. This is what we call “utility serverless computing”.

In this “serverless architecture” the focus will move away from developers and businesses having to understand complex programming languages. They will also no longer have to cater for creating and managing complex IT architectures. The IT complexity will be abstracted or

simply hidden from the developer and the end-user; focus moves towards the application and the service itself. A shift in mindset and a shift in focus.

It is forecast that global IT spend will reach $3.7 Trillion USD by the end of this year[4]; it will also likely eclipse $4 Billion USD within three years. The International Telecommunication Union has separately estimated that about 3.2 billion people, or almost half of the world's population, would be online by the end of this year. Of them, about 2 billion are from developing countries.

These users will generate a vast amount of data that will be floating around, and as big digital corporations realised, personal information is an enormously valuable asset. Over the past 20 years, there has been a mass stockpiling of data in centralised servers, with Google, Amazon, Facebook and Twitter the biggest custodians. People sacrificed privacy and data ownership for the convenience of these services. Whether they knew it or not, their identities, browsing habits, searches and online shopping information were sold to the highest (advertising) bidder.

At the same time that these technology and internet innovations were happening, consumers, businesses and in fact governments across the world have become more savvy and demanding on how personal and business data is collected, stored and accessed (used).

New legislation has already been introduced in particular jurisdictions (such as the General Data Protection Regulation ("**GDPR**")[5].

Today, a few digital giants have created the leading solutions that have allowed them to capture a disproportionate piece of the Web 2.0 opportunity, with monopoly-like data-hungry services that ran in centralised and highly protected closed ecosystems and databases.

However, in the new emerging (and more data aware) next generation serverless utility computing world, there is a huge opportunity for new players to create innovative products and services, by capturing value in more open and trusted distributed ecosystems.

As this architectural methodology matures, we believe it will increasingly be taken up for many thousands of new business projects in almost every sector of industry that deals with digital asset exchange.

For example, Everest Group has predicted that blockchain will achieve accelerated adoption within the next few years in the banking industry (see Figure 25 on page 58).

We believe this new world is the next phase of the internet: the human-centered decentralized internet.

BLOCKCHAIN'S ROLE

Even though it is still young and immature in IT terms, blockchain provides probably the most innovative and secure, transparent and trusted way for developers and companies to capture value in more open and trusted future distributed ecosystems.

Democratisation is the idea. Blockchain provides the means.

---

[4] Anon. (2018). *Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018*. Available: https://www.gartner.com/newsroom/id/3845563

[5] EU Parliament. (2018). *The EU General Data Protection Regulation*. Available: https://www.eugdpr.org/

For the first time ever, we are able to create a decentralised architecture of the internet, whereby the consensus (regarding trust, data integrity and governance) across an entire network can be achieved securely and efficiently without a third party (controlling) intermediary.

Blockchain-enabled systems are intended to allow for the creation of a single, universal, absolutely trustworthy and indestructible record (ledger) of digital assets and associated transactions.

It can do so in ways that are often better and more efficient than the tools used today. For one, blockchain technology creates a viable, decentralized record of cryptographically encoded transactions (the distributed ledger), which allows for the substitution of a traditional master database with central points of failure and other security issues. The most critical area where blockchain helps is to guarantee the validity of a transaction by recording it not only on a main register but a connected distributed system of databases, all of which are connected through a secure validation mechanism.

Second generation blockchain technologies allowed for a network of peers to administer their own ‘smart contracts’ - computer programmes carried on the blockchain that execute their terms autonomously and without an intermediary once the criteria have been met.

At the platform level, we believe this has the potential to lead to radical simplification and cost reduction for large parts of many digital ecosystems, while making them more open, secure and reliable. User and business data is collected and stored in a secure distributed way. This also prevents (existing and future) tech-giants from hoarding and abusing the same data for their own business gain.

Perhaps the most exciting area of development, however, will be the dApps that run on a blockchain system.

A dApp is an abbreviated form for decentralized application. A dApp has its backend software code running on a decentralized peer-to-peer network. Contrast this with a typical app where the backend code is running on centralized servers.

Although the benefits of dApps to specific industries are still largely unknown by mainstream internet audiences, they show great promise.

Services that use dApps support the creation of a user-and-business-centric web where user and customers retain complete ownership of their data, identity and digital assets.

Some of the key potential benefits of dApps include:

- dramatic simplification of supply and value chains (removing many “middle-men”)
- ability to settle transactions and close deals automatically (anytime)
- Super accurate pay-as-you-go revenue business transactions
- improved security (in terms of immutability) of data and applications stored
- increased business (faster and more reliable transactions)
- reduced overhead costs (such as personnel and facilities)
- transaction fraud prevention (ultimate trust machine)
- significantly lower average transaction costs (simpler overall architecture)

Many potential use cases exist for dApp’s on serverless utility computing implementations.

While the adoption of serverless dApps is still very much work-in-progress, early indicators show that they will become a major force in how businesses deliver new services via secure and distributed cloud based services.

There is also much written about proofs-of-concept and even a few (simple) in-production deployments of blockchain. However there are a number of challenges today with blockchain, especially if it is to be adopted by enterprise scale businesses.

These include the following:

- it is hard for developers and IT contractors to write applications for blockchain
- there are (too) many conflicting implementation models to choose from
- the ability to design, test, deploy and manage is crucial for scaling and running dApps
- it often lacks the performance needed or data controls typical of businesses
- it can be very difficult to integrate a new blockchain project into existing IT systems
- it is likely there will be a need to build multiple blockchains within an enterprise firm

In short, businesses may find it very difficult to support multiple blockchain solutions.

Appendix-B provides more details of blockchain in this serverless utility computing world.

ENTER AERGO.

As noted there are challenges with blockchain today. However, we strongly believe that open, secure, distributed business ecosystems on blockchain will win in the long run.

What is needed for enterprise businesses and developers is a feature-rich, open and easy-to-use horizontal enterprise development and deployment blockchain “platform”. Not just another blockchain protocol, but a fully-featured ecosystem to enable and promote cooperation amongst the many stakeholders involved.

A blockchain platform that can support any industry and any sector.

This platform needs to include a “middleware and normalization layer” that serves to seamlessly connect legacy IT software to the new world of distributed serverless blockchain systems.

A platform that is built for business, developers, system integrators and other key third-parties who all have an important role to play in these emerging distributed ecosystems .

In our opinion, this is perhaps the most challenging (but also the most exciting) area of development for blockchain which we will see over the coming three to five years.

With Global IT spend at circa $4 USD billion, such an enterprise blockchain platform can both create and capture significant value for businesses and its creators.

This is the primary rationale and focus for the AERGO Project.

THE OBSTACLE

There are several obstacles for enterprises who want to adopt and use public and private blockchain environments. It is challenges like these that perhaps explain why we have yet to see numerous mass-deployed in-production systems built on blockchain in many industries.

LACK OF RELIABILITY

Lack of full control of their IT infrastructure raises operational issues for businesses. Public blockchains have been subjected to frequent "hard forks" (i.e. it was sometimes necessary to modify the underlying technology, thereby creating a totally separate variant of the original software program). When a public blockchain experiences a hard fork, the dApp applications are meant to continue to operate as usual on the new version of the protocol. When you consider the spider-web like relations between enterprise solutions, a hard fork on a simple user-application could potentially cause a critical business failure.

Hard forks can often increase the vulnerability of the IT network itself such that it may become susceptible to issues such as a network replay or denial-of-service ("**DDoS**") attack. As an example, there have already been a number of hard-forks of the original Bitcoin blockchain protocol (see Figure 1). More are scheduled in the very near future.

As the use of blockchain increases, the underlying technology needs to advance (for example to provide improved scalability). This also requires all nodes running the software to upgrade to the latest version of the protocol software. We strongly believe that the demand for blockchain technology will lead to further hard fork attempts. This makes enterprise blockchain use not only challenging but in some cases impossible for firms who need stable IT.

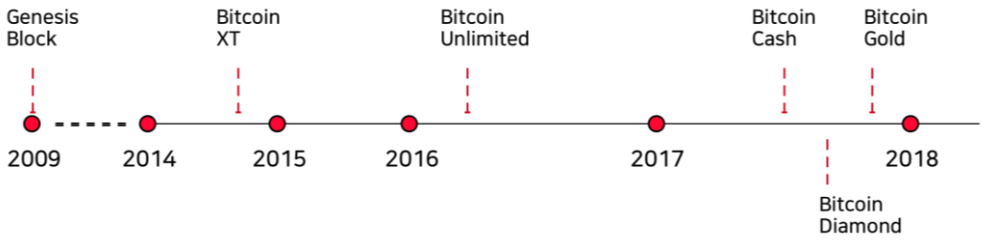


Figure 1. Bitcoin blockchain forks to date

Another issue is high volatility in transaction fees. We have seen the 90-day average per-transaction price [of Bitcoin] increase to $110.96 USD[6]. As of 18 March 2018 some 1,000 transactions were in the waiting pool to be included in the network. This volatility makes business applications on blockchain unpredictable and unsustainable. Generally, businesses do not like operational cost uncertainty, often rejecting promising new technologies as a result.

IT INTEGRATION DIFFICULTY

[6] Blockchain Info. (2018). *Average over 90 days from 2017.12.19 to 2018.03.18*. Available: https://www.blockchain.info

For several decades, enterprises of all sizes have been optimizing and transforming their businesses through the use of digital technologies. This has often occurred in waves, resulting in layers upon layers of different systems being tested and implemented. This in turn has led to complex operations and workflows. Enterprise infrastructures therefore tend to depend on a diverse range of technologies and processes.

Integrating a new disruptive technology such as blockchain into a traditionally complex (and often proprietary) system can be very difficult, risky and costly. While open standards such as security assertion markup language ("**SAML**") or the web access delegation standard and reference architecture for authentication (OATH) help, making a new IT system fully work with widely used products such as Active Directory, Oracle or SAP is a hugely complex task.

SOFTWARE DEVELOPMENT DIFFICULTY

New technologies such as blockchain often introduce new programming frameworks and languages. As the majority of enterprise developments tend to be project-focused, there is little room for developers to experiment and to learn new languages and tools.

Some of these are complex to understand, such as Solidity. With Solidity, developers are able to write applications that implement self-enforcing business logic embodied in smart contracts, leaving a non-refutable and authoritative record of the transaction. In our opinion, many firms simply do not have the software developer flexibility or capability to use these kind of new languages.

Companies often use part-time contractors to deliver IT project work. Many of these contractors are unlikely to want to pick up and learn a new language for a project. If these tasks are "outsourced", we believe it would be unwise to entirely rely on an external third party to write and codify the blockchain important business logic and rules.

We are of the view that instead of forcing developers to learn new languages to create smart contracts, we believe that enterprise blockchain should be easy enough to understand and to program. This would allow developers to leverage their existing expertise and experience with familiar toolchains (such as C++, Golang, JavaScript and Python).

SQL is also a very well understood and widely accepted language for programming and managing data - yet it appears to be almost forgotten in some blockchain implementations.

PRIVACY ISSUES

The business community has a stronger requirement for data privacy than is currently provided by public blockchains. While one way to achieve data privacy and improved security on public blockchain is to implement an encryption and decryption layer at the application level, enterprise blockchain implementations often need to provide a more robust, holistic approach for securing data, particularly where it involves sensitive and/or legally protected information.

As an example, a new and more stringent GDPR standard will be imposed and come into force in May 2018 across Europe. This will require that companies, including those that use blockchain (for their business), consider data privacy related issues in the design of systems by implementing security and data-privacy by design, and not as an afterthought.

SCALABILITY PROBLEMS

Many of the current blockchains are adequate for dealing with simple scalability. However, we believe that in many large-scale use cases, businesses need IT systems that can automatically deal with more demand from gradual or even sudden demand from the user(s) of the service.

This demand may require more immediate local computer resources, in what is called a vertically scaled-up system (for example more local memory, storage, computing, or network capacity for a specific high-throughput task). An example could be a business transaction that needs to be executed in the shortest time possible (e.g. secure the price of a stock traded on a regulated exchange at a specific moment in time).

Where there is a sudden peak in user demand, this requires the IT infrastructure to immediately add extra computer resources across a distributed system to share the extra load (in what is termed a horizontal scale-out system). An example here could be an immediate huge demand across the internet to purchase tickets for a just-announced and in-demand event (e.g. a new extra date is announced for a concert that has already sold-out for one of the world's most popular pop groups).

INTEROPERABILITY CONSTRAINTS

Even though the market is still currently in its infancy, there are over 100 different public blockchain protocols being used - primarily supporting Bitcoin and the many other crypto "altcoins". At the same time there are also at least 200 custom developed private blockchains developed and used by large enterprise companies. Each one of these implementations of blockchain is different. This reduces the possible benefits from economies of scale across these many diverse use cases.

As the market develops and matures (as was witnessed with cloud computing over the past ten years, and before that with Linux, another open source project), we predict that many of these blockchain implementations will disappear through lack of mass adoption. Others will continue to exist in smaller and specialist use-cases only. The most successful projects will eventually integrate with one another to form larger blockchain "ecosystems" and platforms.

We believe that the majority of future innovation in and around blockchain (as well as its mass adoption) will likely evolve around public ecosystems and not private blockchains.

Each of the resulting blockchain platforms and ecosystems will require specialist tools, IT integration know-how and deployment skills. Most firms will struggle to keep up with being able to deal with this interoperability and the manageability of the many variant private blockchains.

As mentioned earlier, it is very challenging to combine and work with public and private blockchains. Especially as this results in degrading performance and losing important characteristics from either system (the trust vs. performance paradox).

AERGO, the blockchain fuel for autonomous business

AERGO is a revolutionary concept and open source project.

AERGO PLATFORM

AERGO seeks to leverage and extend both public and private blockchains, supported by modern cloud architectures. We hope to create a technology and operational framework that supports an ecosystem of (dApp) developers, curated cloud delivery partners, and enterprise companies.

In short, we aim to create a platform that allows each party to create innovative and trusted business services.

AERGO intends to be a distributed modern ecosystem built around a high-performance, secure and easy to use public blockchain (that we call AERGO Chain).

Some of the key features of AERGO are depicted in Figure 2 that follows.

Figure 2. Key features of AERGO

Just like the development, evolution and adoption of "hybrid cloud" over the past 10 years, AERGO intends to facilitate the creation of hybrid blockchain based products and business models.

AERGO proposes to use state-of-the-art technology that is implemented and manifested as a simple to use practical blockchain protocol. This protocol is intended to be designed so that it can be used in any combination of (i) a public, (ii) a private or (iii) a combined public plus private blockchain architecture configuration. This is depicted in Figure 3 below.

AERGO aims to become the de facto enterprise blockchain. One that bridges the gap between both public and private networks. A platform that uses core blockchain technology and deployment blueprints that have already been proven in real-life in-production systems across the world by Blocko[7].

AERGO also aims to provide and support a developer friendly, feature-rich, multi-paradigm and consistent plugin-based smart contract infrastructure for programming each business implementation.

[7] Blocko has successfully delivered 23 in-production blockchain systems (for 20 companies) supporting over 25 million users

Making “design”, “deployment”, “usage” and “management” are key design principles for the AERGO project. Making things easy is not simple. This is especially true for blockchain today.

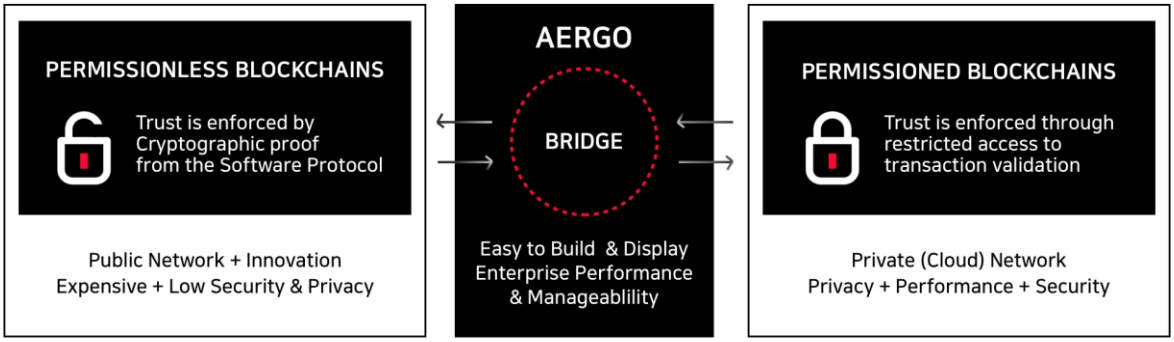


Figure 3. AERGO bridges the Public and Private blockchain worlds for Enterprise IT

AERGO intends to combine the practicality and innovation of public blockchains, with the performance and security provided by private blockchains.

Just as with cloud computing, we hope to develop the technology to enable companies to develop and run their (dApp) applications on a secure public infrastructure. When needed, these companies will be able to easily and seamlessly migrate some (or even all) of these applications to a more high-performance private blockchain.

All of this and without losing any of the benefits of their previous public blockchain model implementation.

To enable such a comprehensive hybrid blockchain architecture, innovative technologies and a novel data bridging framework (proxy) are required to make these different types of system work together. The bridging proxy would allow bi-directional communication between multiple public and private blockchain networks.

The ability to develop, compile and embed smart contracts into such a diverse architecture will also be required. This also needs to be supported by a very high-performance and efficient virtual machine engine for future and more comprehensive smart contract development.

This principle is depicted in the illustrative diagram below.

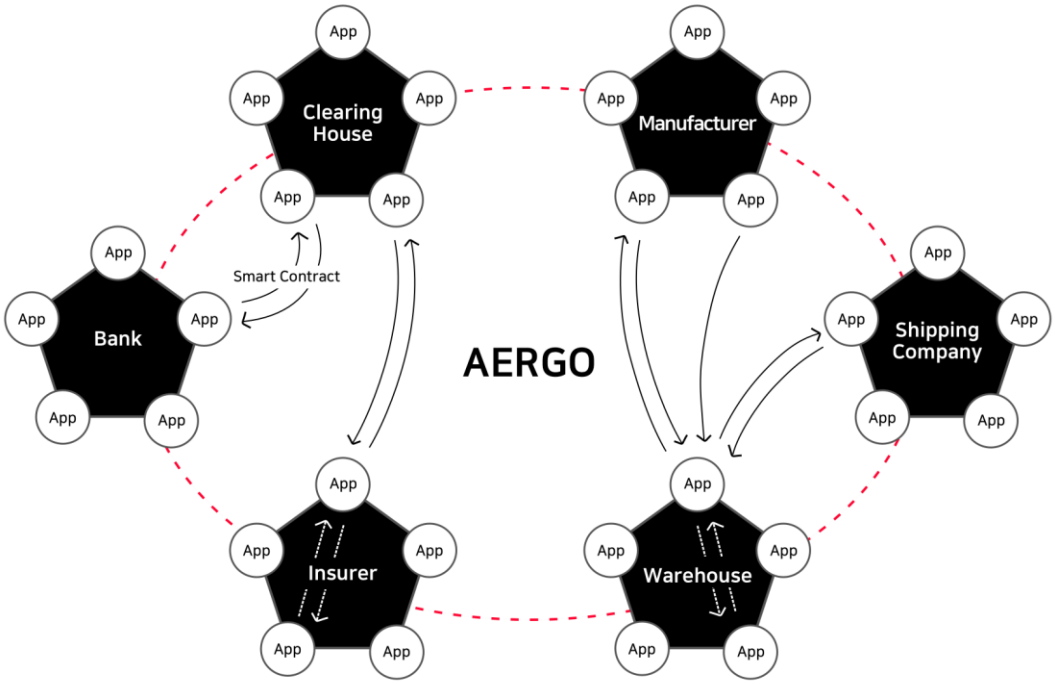


Figure 4. AERGO ecosystem network illustrating public and each private chain bridged

AERGO: SUMMARY ARCHITECTURE

AERGO intends to leverage and build upon Blocko's existing COINSTACK platform, which is a fully supported enterprise product that has been adopted by many of its existing clients.

AERGO aims to provide a complete framework for developing, orchestrating and deploying dApps on secure and high-performance cloud architectures.

Blocko will also help to cultivate a technology and supporting partner "ecosystem".

The key stakeholders in the AERGO ecosystem include any type of business wishing to use blockchain and their developers; as well as the IT contractors, infrastructure and service providers that provide value-adding services.

AERGO also intends to support open source developers who wish to use, develop, incubate and extend core features and projects within the AERGO technology stack. AERGO proposes not only be open-source friendly, it will *be* open source.

Attracting new ideas and projects to extend the value and utility of the AERGO ecosystem is a key principle for this initiative. The ecosystem partners will include special programs to support teams and research projects to enable these innovations.

The core elements of AERGO are shown below. Together these elements form the AERGO platform.

Figure 5. AERGO core elements

(I) AERGO CHAIN: a *public internet of blockchains.*

AERGO Chain is a the proposed new protocol consisting of a global public decentralized network of enterprise blockchains run by node providers.

It intends to contain **AERGOSQL**, a new canonical smart contract engine to easily create advanced smart contracts to enable innovative business products and services.

In summary, AERGO Chain can conceptually be considered to be an open source blockchain operating system.

(II) AERGO HUB: the *public interface into the underlying AERGO Chain*

AERGO Hub aims to work with and connects secure dApps with AERGO Chain.The dApps that are created are intended to be stored in one of two repositories:

- **AERGO Public Repository,** is a shared, open and decentralized underlying infrastructure for dApps (similar to GIT public repositories that is used to host open source projects, or automated build servers for public cloud computing)
- **AERGO Private Repository,** is a controlled, secure and private infrastructure for dApps. This aims to achieve access control, application security and performance, data compliance, as well as quality of service ("**QoS**")[8] that are required for enterprise IT systems

Both types of repositories inherit the industry tested implementation frameworks and API compatibility of COINSTACK, proven with clients across the globe.

These dApps (as well as other supporting software, computing resources and services that are optimized for blockchain) need to be orchestrated, provisioned, deployed and managed to be used on AERGO Chain.

[8] Wikipedia, The Free Encyclopedia. (2018). *Quality of service*. Available: https://en.wikipedia.org/w/index.php?title=Quality_of_service&oldid=836944975

This is intended to be achieved through **AERGO HORDE**: a public orchestration[9], management and software framework for infrastructure providers who want to participate in the AERGO Hub ecosystem.

For example: blockchain “node providers” or software vendors.

In summary, AERGO Hub is conceptually very similar to techniques found in current public cloud web services.

(III) AERGO MARKETPLACE: *a proposed one stop shop for software applications, computing resources and other services* optimized for AERGO Chain

- AERGO Marketplace software, computing and other services are intended to run on or work with AERGO Chain as part the ecosystem that supports the AERGO Platform
- These partner services are accessed via the AERGO Hub public interface
- These services are intended to be managed via AERGO Horde

AERGO - DETAILED FUNCTIONS AND CAPABILITIES

The following section describes in more detail the technical capabilities of the above (as well as other related) key functions within the AERGO Platform.

While this may be overly technical for some readers, we hope that by at least outlining these core functions some of the unique and innovative capabilities of AERGO are appreciated.

For more detailed information see the detailed AERGO Technical White Paper available at

www.AERGO.io

[9] Wikipedia, The Free Encyclopedia. (2018). *Orchestration (computing)*. Available: https://en.wikipedia.org/w/index.php?title=Orchestration_(computing)&oldid=831362994

AERGO CHAIN

AERGO Chain intends to be a public blockchain protocol designed to mitigate issues currently found on public blockchains. AERGO Chain intends to deploy a delegated-proof-of-state ("**DPOS**")[10] governance model. It also intends to implement a novel score based autonomous delegation algorithm to enhance reliability and quality of service ("**QoS**").

The AERGO Chain aims to feature an SQL based smart contract platform to increase usability. This is perhaps one of the most critical components in solving a number of major and current integration difficulties with blockchain.

We believe that an enterprise focused blockchain protocol layer needs to include advanced features such as distributed version control and concurrency control. These form the backbone of how users will create public and especially private dApp repositories. Collectively these new features will help to enhance the privacy of future enterprise blockchains.

A new parallel processing capability of smart contracts seeks to allow AERGO Chain to handle millions of transactions per second. AERGO is intended to be designed for optimal scale-up and scale-out of blockchain networks, to suit the demand of a wide range of products and services running on a blockchain. We believe it will also be capable of engaging and utilising a parallel throughput networking fabric, as well as supporting a multi-thread architecture for multi-core and ultra-fast cached memory computer environments.

Many of the techniques being developed for AERGO Chain are based on core capabilities from Blocko's COINSTACK operating system, coupled with their learnings from building in-production systems for large enterprise clients on their existing computer networks and in their secure and private data centres.

CONSENSUS ALGORITHM

Perhaps one of the most defining and important characteristic of a blockchain is the chosen consensus algorithm. A consensus algorithm is the key program that verifies that a block that is to be added to a blockchain is the real version.

Without a consensus algorithm, any actor could potentially add information to the blockchain, derailing the legitimacy of the entire system.

Whilst these consensus algorithms involve complex mathematics and logic (and are perhaps beyond the scope of the reader), it is important to at least understand the basics of the selected model that is being developed for the high-performance AERGO platform.

We therefore provide a simple description of the most relevant and associated technologies in the next sections. Further information on DTT can be found in the AERGO Technical Whitepaper.

AERGO Chain supports various consensus algorithms and allows its users to define and choose a consensus algorithm to best meet their business requirements. However, the fundamental and default choice consensus algorithm for AERGO is proposed to be Delegated Proof of Stake ("**DPOS**").

---

[10] Mycryptopedia. (2017). *Delegated Proof-of-Stake (DPoS) Explained.* Available: https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/

We believe this algorithm class provides enhanced scalability coupled with an economical operational model. In addition the AERGO DPOS algorithm will aim to promote and support businesses and important blockchain node providers to participate in the network.

This will help the long-term viability, efficiency and sustainability of the overall network.

Proof of Work

There is widespread belief in the blockchain community (public articles and other sources of reference) that Proof of Work ("**POW**") is the most genuine and useful consensus algorithm for blockchain. The benefits of POW are that it is concise, easy to understand and it has the potential to be the most democratic consensus method.

However, POW has a few very serious drawbacks.

POW may allow power and control to end up in the hands of a few large miners. We also believe network predictability, stability and sustainability are a fundamental requirement for businesses. They are major contributing factors for operational QoS in large-scale IT-systems.

Public blockchains designed for business will have to eliminate the possibility that external forces could impair both QoS and place control in the hands of fewer (or perhaps bad) actors.

Proof of Stake

Various algorithms are emerging around Proof of Stake ("**POS**"), including potential developments in the Ethereum platform. Some of this work is still not settled or even implemented. Many efforts are currently under way to solve some of the most important technical issues involving POS (such as the nothing-at-stake).

However, we believe, POS itself is unlikely to become a mainstream consensus method, until it addresses certain challenges, such as branches happening or so-called "coin slashing'. For example, if an error (or bug) breaks a POS rule, it will cause so-called coin slashing and thus create a very undesirable hard fork of the blockchain.

Hard-forks on public networks directly impact network reliability. They can also significantly increase the security risk of operating businesses that run on, or that are linked to, a public network. Figure 1 depicted earlier on page 13 of this report shows prior forks in Bitcoin.

Delegated Proof of Stake

Delegated Proof of Stake ("**DPOS**") is an alternative and promising consensus algorithm. DPOS is a progressive and network (energy) efficient model that has been used by a number of high-profile blockchain projects (such as EOS, Steem and BitShares).

It promotes decentralization (as it does not require huge, specialized - often concentrated - computer mining farms). DPOS also provides benefits for network stakeholders help to ensure that bad actors are removed from the network. This combined social and technological form of democratization recognizes valuable participants and supports goods behavior in the network.

In effect it's a self-monitoring and positive-promoting model.

We believe DPOS is both easy to understand and less likely to create hard forks. We also believe that acting as a participating node in a network where participants are enterprises and infrastructure providers reduces the possibility of hard-forks even further.

The important requirement for business process QoS would also be greatly enhanced.

In summary, POW provides purely economic incentives only. In contrast DPOS seeks to combine economic incentives with social consensus and has been chosen for AERGO.

SMART CONTRACT

AERGO Chain aims to support a well-tested and easy to use multi-paradigm smart contract infrastructure. It includes the Ethereum Virtual Machine.

This hybrid approach provides useful interoperability between different types of smart contract operations.

AERGOSQL

AERGOSQL is the term given to smart contracts operating on and within AERGO Chain.

AERGOSQL seeks to offer a relational data model for storing and accessing data and SQL-like scripting language for writing smart contracts.

We strongly believe that this new approach - based on traditional, well understood, and easy to use SQL technology - will enable the mass market of developers and business users to benefit from blockchain.

A simple indicative example of the resulting coding model can be seen in the extract below.

```
CREATE TABLE IF NOT EXISTS accounts   (
        owner VARCHAR NOT NULL PRIMARY KEY,
        balance NUMERIC (15, 2)
);

CREATE OR REPLAE FUNCTION
transfer (sender text, to text, amount numeric (15, 2))
RETURNS text
AS
$$
DECLARE
        sender_bal numeric ;
BEGIN
        SELECT balance INTO sender_bal FROM accounts WHERE owner = sender ;
        IF NOT FOUND THEN
            RETURN 'Sender not found' ;
        END IF
        IF sender_bal < amount THEN
            RETURN 'Not enough balance' ;
        END IF
        UPDATE accounts SET balance = balance + amount WHERE owner = to ;
        IF NOT FOUND THEN
            RETURN 'Receiver not found' ;
        END IF;
        UPDATE accounts SET balance = balance - amount WHERE owner = sender ;
        RETURN 'OK' ;
END
$$
```

Figure 6. AERGOSQL Coding model extract

For maximum performance, AERGOSQL intended to adopt advanced innovative technologies, such as a LLVM compiler infrastructure (providing intelligent JIT compilation[11]) and a high-performance b-tree data structure implementation (such as open source WiredTiger[12] for data storage).

Smart contract execution is a utility within AERGO (and is denominated as a native digital asset on AERGO Chain). It is proposed that smart contract execution (including the computing power needed for this task) in AERGO will be consumed as a running cost.

BRANCHING AND MERGING

One of the most complicated concepts involved in distributed version control systems, is the process of merging branches.

For blockchain (that must deal with real-time data) merging is even more difficult to achieve.

Due to its non-destructive process, we believe branching in AERGO will be a simple and straightforward process.

However, merging requires two different approaches:

(I) Automated Merging

- By default, Automatic Merging is the expected process for merging two branches. Automatic Merging is similar to a block-reorganization process in blockchains. In this case, the merging source's blocks are dissolved into transactions and absorbed in the merging target's merging-pool. Ultimately, the merging pool results in a new block attached to the merging target's best block. In the process, transactions inconsistent with the merging target branch are automatically excluded from the new block.

(II) Consistent Merging

- Consistent Merging happens only when a branch is created with the specified consistent merging logic. Consistent merging is similar to the merge functionality provided by version control systems such as Git[13]. Unlike automatic merging (which discards inconsistent transactions by default), consistent merging relies on the predefined conflict resolution logic to manage inconsistent transactions. The conflict resolution logic is implemented as a system-level smart contract.

We believe AERGO Chain will provide both friendly syntax and semantics for users accustomed to version control systems such as Git. Such functionalities can be accessed through the AERGO CLI client, as well as RPC (Remote Procedure Call) APIs.

---

11 Wikipedia, The Free Encyclopedia. (2018). *LLVM*. Available: https://en.wikipedia.org/w/index.php?title=LLVM&oldid=841209654

12 Michael Cahill. (2015). *A Technical Introduction to WiredTiger*. Available: https://www.mongodb.com/presentations/a-technical-introduction-to-wiredtiger

13 Wikipedia, The Free Encyclopedia. (2018). *Git*. Available: https://en.wikipedia.org/w/index.php?title=Git&oldid=841769346

AERGO Chain aims to be developer friendly. It seeks to allow developers to use technologies, tools and methods that are familiar and well understood.

CONCURRENCY CONTROL

Concurrency control is a critical function for blockchain networks. It ensures the DPOS consensus algorithm is deterministic (i.e. being entirely predictable) when delegates within a blockchain network schedule the important block creation transactions.

AERGO Chain will aim to provide two mechanisms for transaction serialization. These are (i) block-level serialization and (ii) pool-level serialization.

(I) Block-level serialization

- Since each branch of blockchain consists of a series of blocks, the transactions can be serialized by stacking one block after another.
- AERGO intends to provide Multi Version Concurrency Control (MVCC) which are based on block heights. Once a branch and block height are specified, it is therefore possible to provide consistent reads across different nodes in the repository.
- AERGO's MVCC functionality intends to provide both a snapshot isolation that is used for consistent reads and a form of optimistic locking, through row or document versioning. MVCC only works for block-level serialization.

(II) Pool-level serialization

- Persons accessing AERGO nodes can take advantage of the deterministic nature of the scheduled creation of blocks by delegates. This is a characteristic provided by the core DPOS consensus. It allows for execution of synchronous transactions, providing a strong guarantee on transaction finality.
- Since each delegated node in an AERGO network can apply uniform serialization ordering to process new transactions into the memory pool and create new blocks, clients do not have to wait for block interval completion to retrieve the result of transactions. As a result, the latency of executing a transaction decreases from seconds to milliseconds.

Pool-level serialization is depicted in the diagram below.

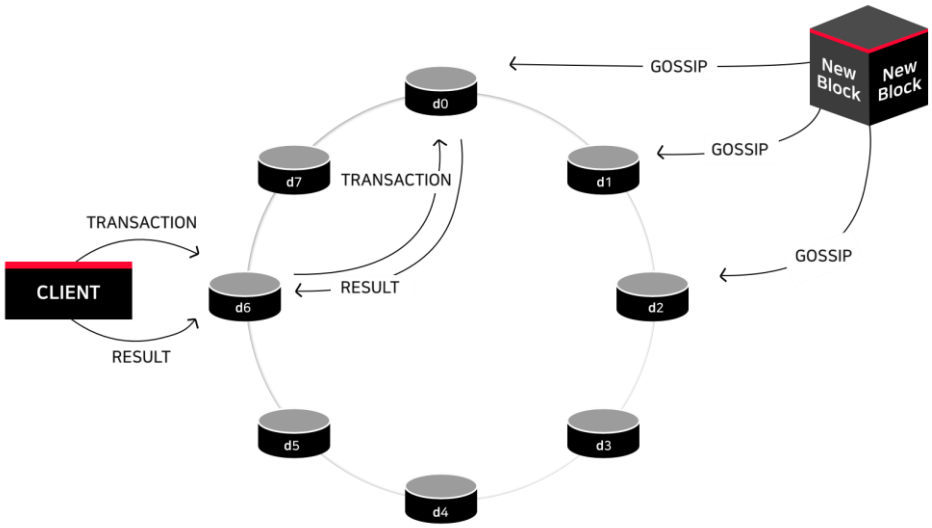


Figure 7. Pool Level Serialization in AERGO Chain

PARALLELISM

Performance in AERGO is intended to be maximised by a combination of transaction and block-level parallel processing.

The performance of a blockchain system primarily depends on:

(i) the efficiency of creating and sharing new blocks; and

(ii) the time it takes for each node to process the new blocks.

The entire distributed consensus protocol is involved in the block creation process of blockchain. While distributed consensus protocols have been studied (and are under the spotlight for various blockchain projects) we are of the view that the actual block creation process of each node in existing systems is often poorly designed and implemented.

Underperforming nodes are sometimes acceptable in public consumer-grade blockchain implementations (such as in Bitcoin and Ethereum). However, an enterprise-grade blockchain like AERGO, requires more robust performance. Ideally this should be near real-time. As a result, each node needs to be carefully implemented just as effectively and efficiently as with the consensus protocol itself.

AERGO Chain intends to introduce the concept of parallelism to various stages of the processing of blocks to maximise system performance.

Parallelism in a blockchain system involves the careful analysis and understanding of the dependencies between transactions included in each block. It also requires an efficient architecture, such as those inspired by a Staged Event-Driven Architecture ("**SEDA**")[14].

This (important) form of parallelism is depicted in the diagram that follows.

[14] Wikipedia, The Free Encyclopedia. (2018). *Staged event-driven architecture*. Available: https://en.wikipedia.org/w/index.php?title=Staged_event-driven_architecture&oldid=812633632

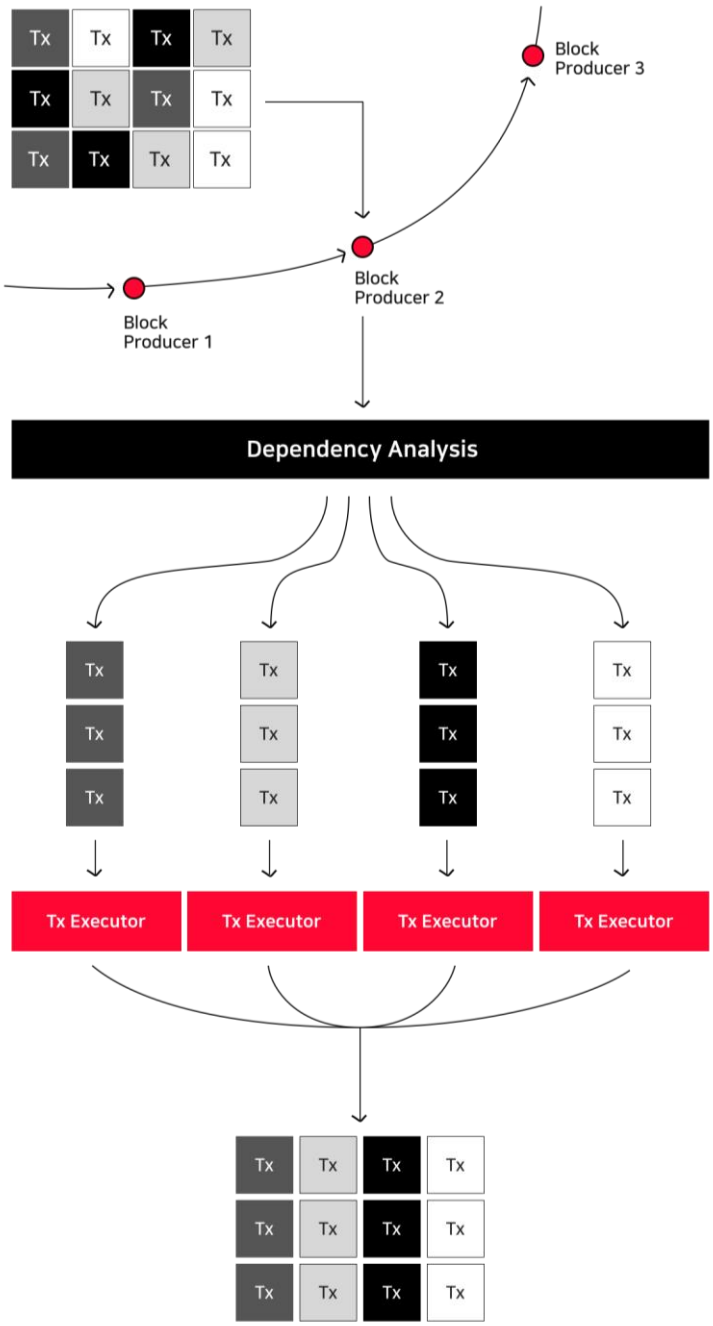


Figure 8. AERGO Parallelism

Dependency Analysis

Dependency analysis is a key factor that aims to enable AERGO's parallel processing capabilities.

AERGO aims to perform a dependency analysis among the transactions and blocks, to create a data structure of the execution order. It measures the deterministic results within the state machines affected by transactions. The data structure format is called Deterministic

Transaction Tree ("**DTT**"). Further information on DTT can be found in the AERGO Technical Whitepaper.

AERGO FILE SYSTEM

AERGO's own unique File System ("**AERGOFS**") seeks to further enhance AERGO's scalability, especially in regards to scale-out and scale-up IT systems mentioned earlier.

AERGOFS intends to operate much like a modern day distributed file system. It aims to provide structured and unstructured data storage capability for AERGO Chain. Unlike the Hadoop distributed file system ("**HDFS**")[15] with its chunked data storage, AERGOFS is intended to service a very large number of files.

AERGOFS is based on Facebook's Haystack[16] technology.

It is our design aim that AERGO Chain will support and enable its developers and users with adequate permissions to access the underlying ledger data by providing easy-to-use Git-like private repositories.

This is an important capability for developers.

DOMAIN-BASED PARTITIONING

Domain-based partitioning is the most basic strategy to secure scalability for AERGO. Domain partitioning seeks to be achieved through the distributed version control functionality of AERGO.

Unlike conventional blockchain implementations, AERGO proposes to be able to freely fork and merge its data through branches. This is referred to as **DVC**. As a result, the distributed ledger can be partitioned both logically and physically through different repositories.

Such an approach has already been used successfully by other established distributed version controls (such as with Git or Mercurial). For instance, the widely deployed Github system is able to host tens of millions of repositories.

However, the effectiveness of domain-based partitioning is primarily dependent on the structure and usage of the data. When a single repository needs to handle an unbounded expansion of data, partitioning data through branching is very difficult.

As a result, AERGO aims to utilize additional scalability approaches and capabilities using the AERGO File System (AERGOFS) and of AERGO Hub.

---

15 IBM. (2018). *Apache Hadoop Distributed File System*. Available: https://www.ibm.com/analytics/hadoop/hdfs.

16 Peter Vajgel. (2009). *Needle in a haystack: efficient storage of billions of photos*. Available: https://code.facebook.com/posts/685565858139515/needle-in-a-haystack-efficient-storage-of-billions-of-photos/

DISTRIBUTED DIRECTORY

Distributed directory ("**DD**") is a core functionality that is intended to be used as a building block within the AERGO implementation.

Each DD in a repository manages an independent and isolated namespace. Each namespace in turn contains information about different branches and tags residing in the repository, as well as the validity of various identifiers on the blockchain.

Each DD is a blockchain on its own, with its own genesis block and the best block. Unlike conventional blocks, DD blocks are limited in size with a relatively long creation interval between them. In addition, as DDs are used for managing metadata, they need to be compact.

In terms of its role and functionality, DD is comparable to data dictionaries in databases, zookeeper for Hadoop, or etcd for CoreOS[17].

In summary, **AERGO Chain** intends to be a powerful *public internet of blockchains*

[17] Lawrence Hecht. (2018). *CoreOS, Red Hat and Kubernetes Competition*. Available: https://thenewstack.io/coreos-red-hat-kubernetes-competition/

AERGO REPOSITORIES - PUBLIC & PRIVATE

AERGO Chain aims to support the creation of public and private repositories “out-of-the box’.

Repositories are a form of a code hosting platform for developers. They contain the actual software program code that is being developed for a project. They are also used for version control and collaboration. Repositories allow developers and others to work together on new projects from anywhere.

In effect, repositories manage a project, or a set of files, as they change over time

Repositories are actually the smallest forms of blockchains on AERGO Chain. A repository can effectively be either a private blockchain; or it can be a public blockchain that function independently of AERGO Chain.

Both public and private repositories in AERGO are free to use. Access to the repositories is established and controlled by the entity that creates them. Typically public repositories are open to anyone identified in the public network. Private repositories are only accessible to developers and users that are allowed into the specific private network.

This is depicted in the diagram below.

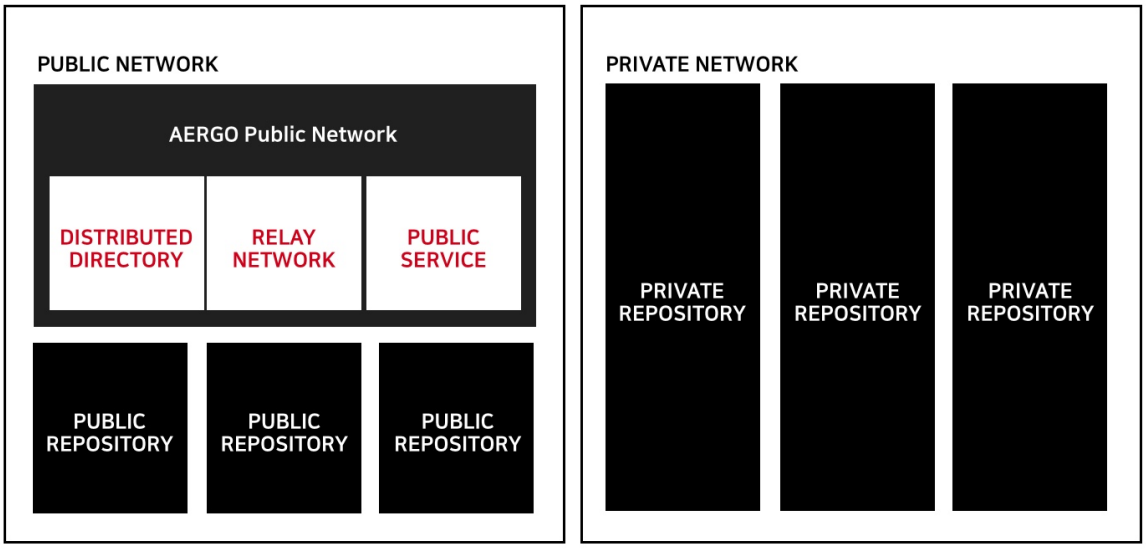


Figure 9. AERGO Public and Private Repositories

AERGO PUBLIC REPOSITORY

The AERGO Public Repository aims to be a shared, open and a decentralized underlying infrastructure for dApps (much like a public repository in GIT that is used to host open source projects, and automated build servers, for public cloud computing).

It is open for reading and writing, or alternatively it may even selectively grant permissions to anonymous users.

A common configuration is to create an AERGO Public Repository as read-only anonymous access.

AERGO PRIVATE REPOSITORY

The AERGO Private Repository, aims to be a controlled, secure and private infrastructure for dApps. This assures full access control, application security and performance, data compliance, as well as QoS all of which are necessary for enterprise IT systems.

AERGO Private Repository assures full access control for both reading and writing within the repository (only users with the right permission can work in these repositories). By creating a new branch from a remote parent branch, users can keep newly created blocks in a private branch that are isolated from the public. Only if permission is granted to the specific repository housing the branch, are users able to access the blocks within the respective repository.

AERGO also enables important GIT-like data models and command structures; this allows functions such as free branching out, or merging of blocks.

Within each repository, it is proposed that different branches can point to a different snapshot of the content in the blockchain, in order to create a specific status. New branches can also be created.

Finally, the concept of “best chain” in AERGO is analogous to the master branch.

Both types of repositories (public and private) inherit the industry tested implementation frameworks and API compatibility of COINSTACK (Blocko’s fully supported enterprise product and industry tested API framework).

Branching and merging in AERGO is depicted below.

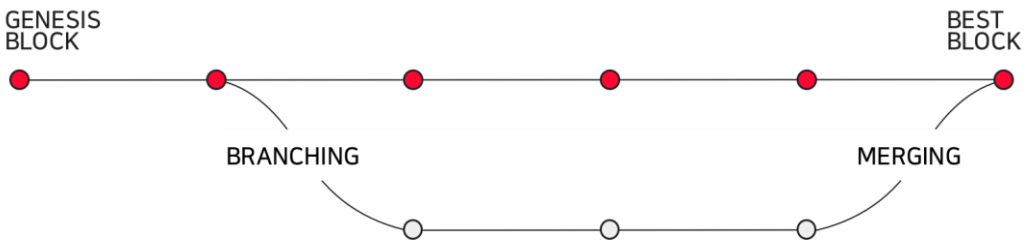


Figure 10. Branching and Merging

In order to create and connect to AERGO Public Repositories and Private Repositories, the users leverage features and services within AERGO Hub.

AERGO HUB

AERGO HUB is proposed to be the public interface, through which enterprise companies and dApp developers access computing power to run their business or applications on.

AERGO Hub intends to connect and work with dApps in the AERGO Chain. The dApps are created and stored in either of the two repositories described earlier. AERGO HUB aims to be similar in nature to current proven public cloud web services (such as Amazon AWS).

These offer a number of advanced capabilities (depicted in Figure 11 below), such as:

1) support for software microservices;

2) a content delivery network ("**CDN**")[18];

3) a serverless database;

4) interfaces for smart oracles (to connect a blockchain with separate data sources such as a separate database); and

5) a smart gateway to intelligently route data traffic / messages into a blockchain

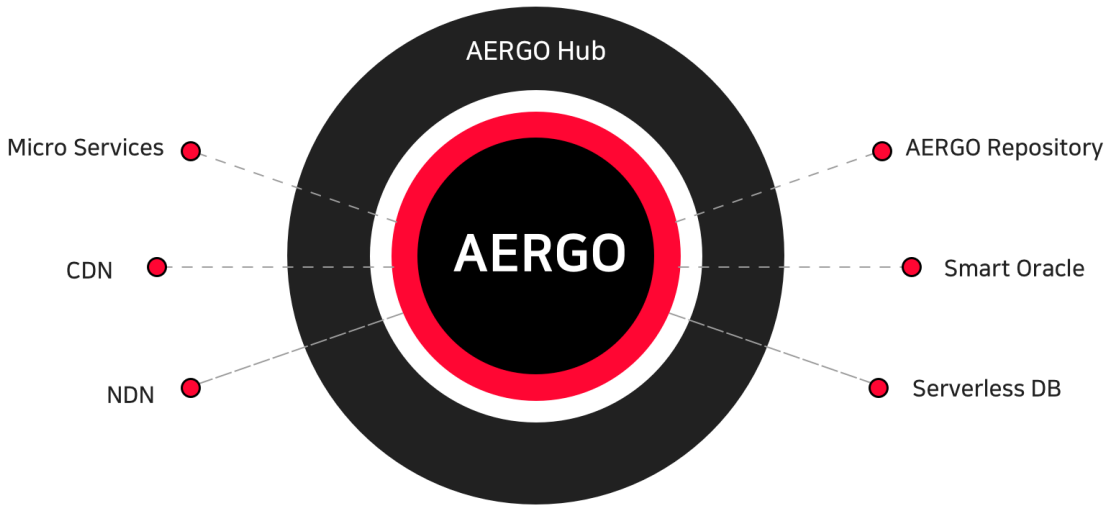


Figure 11. AERGO Hub Functional Illustration

In summary, **AERGO Hub** *is the proposed public interface into AERGO Chain*

[18] Wikipedia, The Free Encyclopedia. (2018). Content delivery network. Available: https://en.wikipedia.org/w/index.php?title=Content_delivery_network&oldid=841886968

AERGO Horde

AERGO dApps (as well as all other supporting software, computing resources and services that are optimized for blockchain) need to be orchestrated, provisioned, deployed and managed to be of use.

It is our intention to achieve this through **AERGO Horde**. This is a public orchestration management and software framework for infrastructure and other third party providers who want to participate in the AERGO Hub ecosystem. For example: blockchain "node providers" or software vendors.

These providers will need to install AERGO Horde in order to act and host as a node (in effect this allows them to "connect" their services to the AERGO ecosystem). AERGO Horde will be an open source, public-domain software project.

AERGO Horde is provided with its own specialised operating system for manageability and efficiency called **AERGO OS**.

This provides certain interfaces and components that interact and work with an embedded and high-performance Linux Kernel and associated services (as illustrated in the diagram below).

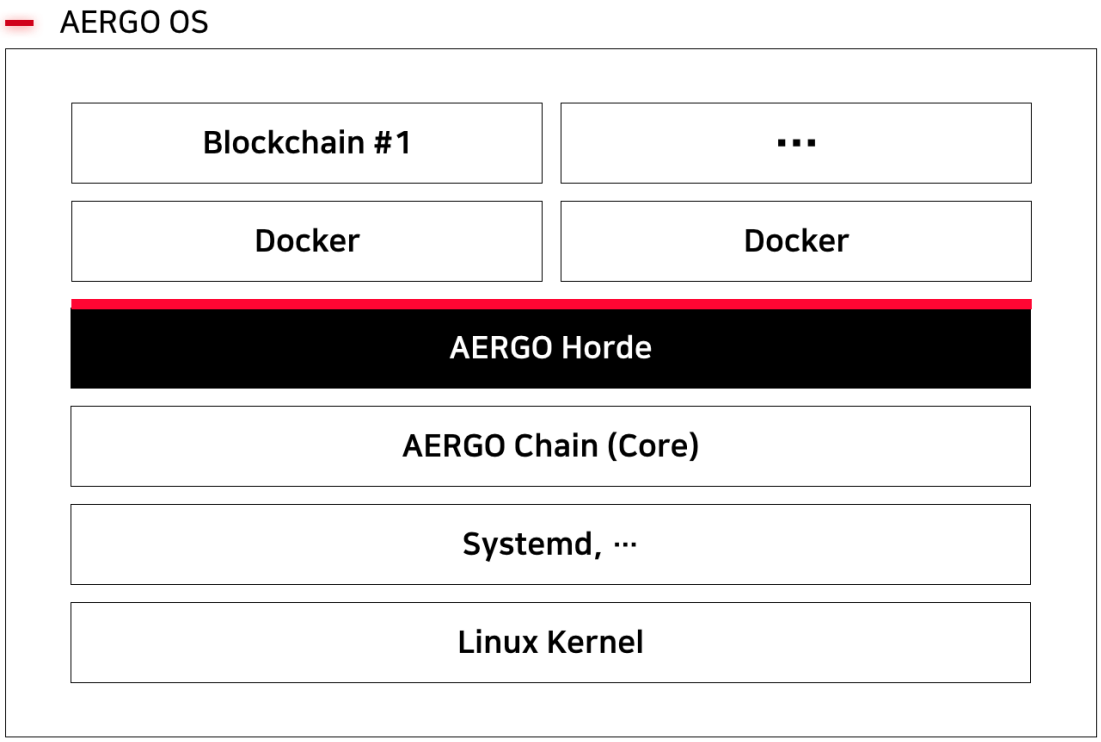


Figure 12. AERGO OS Architecture

With AERGO OS, we believe that a node provider will be able to perform a number of very useful system-level tasks, such as check node information, monitor resource usability, and the produced block information.

AERGO MARKETPLACE

AERGO Marketplace proposes to be a *one stop shop for software applications, computing resources and other services optimized for AERGO Chain*

The AERGO Marketplace software, computing and other services are intended to be compatible and run on or work with AERGO Chain.

It is proposed the AERGO Marketplace will be accessed via the AERGO Hub public interface and managed via AERGO Horde.

This flow is depicted in the diagram that follows.

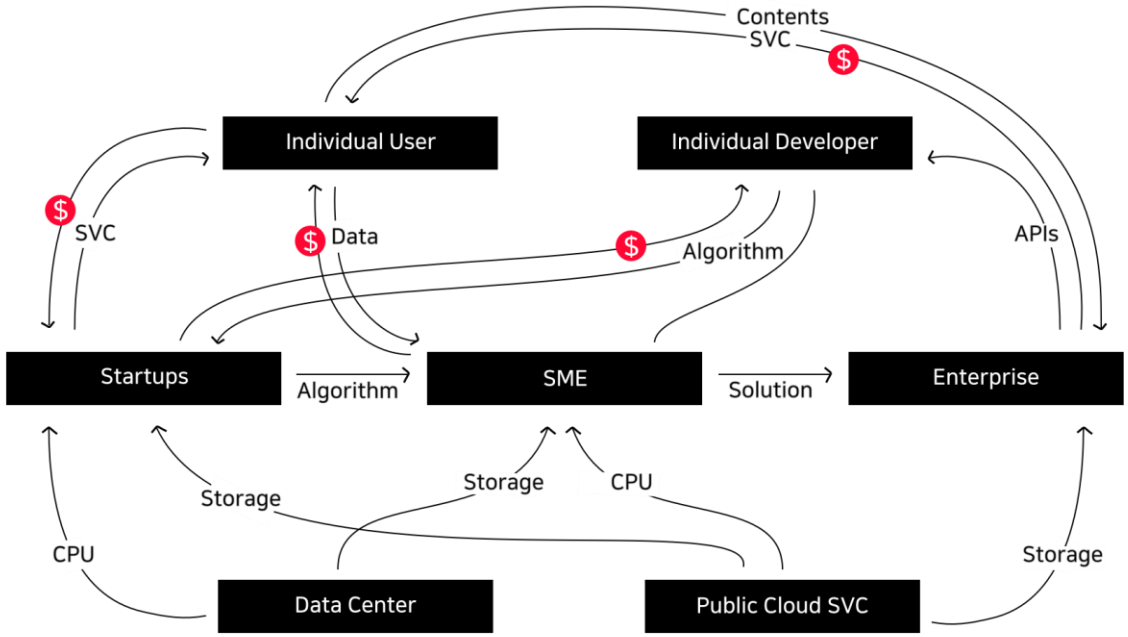


Figure 13. AERGO Marketplace Illustration

We propose to enable third parties, such as service providers, independent software vendors and cloud infrastructure vendors, so that they can make their products and services available to users of AERGO.

The end-users of AERGO will be software developers, and all types and size of businesses wishing to build, manage and run a blockchain project

Whilst similar in nature to traditional cloud marketplaces, it is our aim to ensure AERGO Marketplace significantly lowers the barriers to entry for its users. This includes individual software developers, IT contractors and companies (from small SMBs to large multinational enterprise firms).

We also plan to provide support for national and regional government agencies, who may wish to use AERGO to solve specific problems. An example of this is to provide a secure and anonymous citizen voting system based on blockchain (just as has already been implemented by Blocko with COINSTACK for a regional local government province in South Korea).

AERGO Marketplace will operate as a business and partner ecosystem. We plan to provide a wide range of digital capabilities that can be used to develop and deploy innovative blockchain solutions.

The Platform intends to support public, secure private and hybrid blockchain deployment models.

Examples of the digital capabilities that, over time, will be made available in the AERGO Marketplace include, may include:

- Computing Power (CPU)
- Storage (scalable - ultra fast), Solid-State Memory
- Content Delivery Network (CDN)
- Machine Learning Algorithms
- Digital Content (new algorithms and new software microservices)
- Specialised databases
- Smart Contract and Smart Oracle (templates)
- Blockchain IT integration blueprints
- Digital Identity blueprints
- Document Time Stamping (DTS blueprints)
- AERGO blockchain Training

The AERGO Platform will plan to consider including other modules and welcome new ideas from parties interested in engaging and cooperating with the AERGO ecosystem.

In summary, we aim to make the AERGO Marketplace a vibrant, open and sustainable ecosystem. A marketplace full of new technologies and innovations; whether these are provided from single developers or large software vendors.

These services will be promoted and hopefully employed to power the next generation of business running on a secure blockchain. The underlying IT architecture will also be based on a low cost distributed utility computing deployment model.

AERGO Token [NATIVE BLOCKCHAIN ASSET AND TOKEN MODEL]

AERGO Token ("**AERGO Token**") is the proposed utility token to operate on the AERGO platform. It aims to serve a multitude of different functions. The AERGO Token is broadly speaking intended to be the medium of exchange within the AERGO ecosystem.

These tokens aim to grant the holder the right to certain services available within the AERGO ecosystem.

More specifically, it is intended that the tokens are used for:

- running the smart contract (AERGOSQL);
- DPOS consensus algorithm
- payment method for Blocko's technical support on Coinstack 4.0;
- payment method for AERGO Hub services;
- payment method for services and assets on AERGO Marketplace; and
- payment method for the AERGO domain

AERGO Tokens are also intended to be transferable within the platform.

The AERGO Main-net is expected to go live in early 2019 (the current target release date being 1Q 2019).

It is intended that initially, holding AERGO Tokens can be used to access and purchase products and services on COINSTACK V4.0 (the latest proven enterprise blockchain platform release from Blocko).

The circulation and use of AERGO Token is depicted in the illustrative example below.

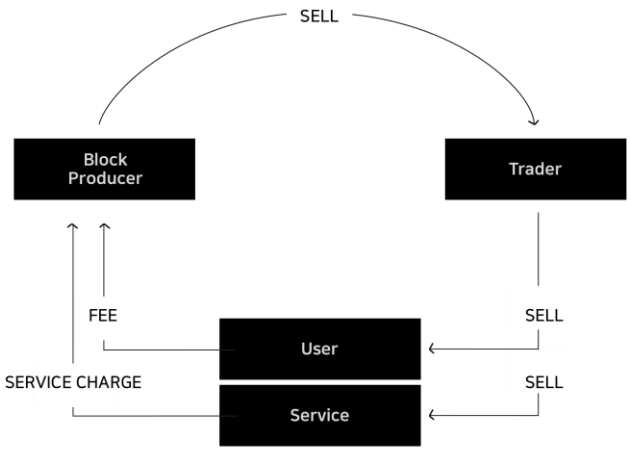


Figure 14. AERGO native asset circulation

TOKEN DISTRIBUTION AND USE OF FUNDS

TOKEN SUPPLY

A total of 500,000,000 AERGO Tokens will be issued.

The allocation and use of tokens will be in accordance with the table set out below, but is subject to change.

Proportion of Tokens for Sale	30%
Reserved by token issuer	35%
Employees of token issuer and affiliates	5%
Advisors and key backers	10%
AERGO community incentives and strategic partners	20%

USE OF PROCEEDS

The proceeds from the tokens for sale are intended to be used to develop and advance the technology programs and partner ecosystem development aspects of AERGO.

A breakdown of the proposed proceeds is depicted in the following table, but is subject to change.

R&D	40%
Marketing	15%
Ecosystem incubation	30%
Strategic alliances and business development	10%
Miscellaneous	5%

DEVELOPMENT ROADMAP

The proposed roadmap and release schedule for the AERGO Chain; AERGO HUB and AERGO Marketplace build-out is depicted in the following diagram.

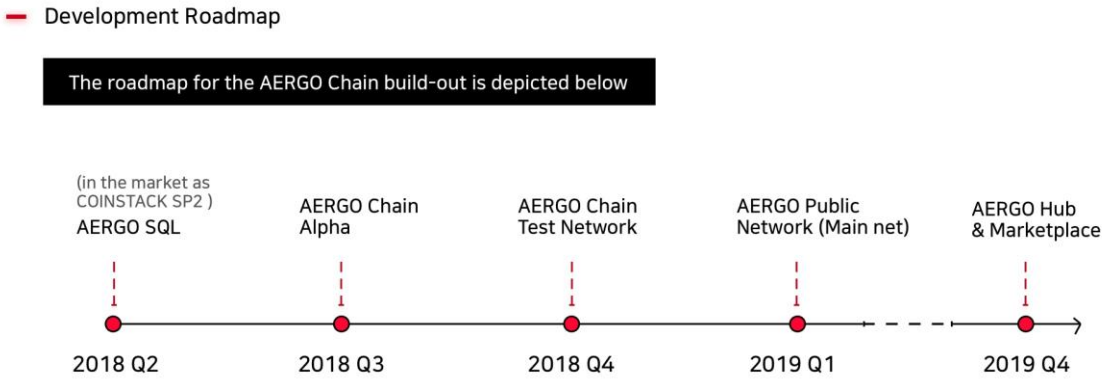


Figure 15. AERGO Development roadmap

This roadmap is subject to change.

It may also be influenced by specific early-tester and early-adopter enterprise customers who have already expressed an interest in using AERGO. This may result in certain capabilities being released earlier (or later) than the above plan suggests.

EXECUTION PLAN

We recognize that the AERGO Project has very ambitious long-term goals. However, frequent releases of key parts of the AERGO Platform are intended to be announced. Already significant components are under advanced development.

As part of the overall program for AERGO and to kick-start the project, we intend to use and leverage the following components from Blocko:

BLOCKO COINSTACK AND BLOCKO KNOW-HOW CONTRIBUTION

Blocko proposes to contribute a number of its existing products, services and know-how to the AERGO Platform. It will also leverage some of its existing customers who have expressed an interest in AERGO's future capabilities.

These (Blocko based) contributions are expected to include:

- COINSTACK AS A KEY INITIAL FOUNDATIONAL ELEMENT OF THE AERGO PROTOCOL

It is our intention that the AERGO protocol will inherit some of its key and proven functionalities (such as APIs which are intended to be backwards compatible).

- PROVEN ENTERPRISE DEPLOYMENT MODELS

Being able to provide secure and data-privacy-compliant deployment frameworks (e.g. proven and tested use-cases) are important for AERGO, if it is to be tested and adopted by future enterprise clients.

Blocko will share a number of these production-tested deployment frameworks with the AERGO and its users.

- BLOCKO'S EXISTING (AND FUTURE) ENTERPRISE CUSTOMERS

Blocko has to date secured over 20 paying customers and has implemented even more production systems based on its COINSTACK version of blockchain.

Blocko proposes to approach its existing clients to present AERGO as an enhancement to their existing deployments. This will be especially useful to those firms that originally moved away from connecting to public blockchains due to lack of operational control and privacy concerns.

- BLOCKO TO MARKET AND DIRECTLY SUPPORT AERGO BASED IMPLEMENTATIONS

Blocko proposes to present and actively sell AERGO as a preferred open protocol that it can configure and connect to its own COINSTACK solution for clients. It will also directly support enterprise deployments of AERGO based products and services.

- BLOCKO AS A STRATEGIC TECHNOLOGY PARTNER FOR THE AERGO

Blocko intends to provide technology development, as well and direct technical support, to

AERGO.

AERGO will also benefit from Blocko's leading edge and industry in-production proven Research and Development and IT integration and support capabilities (currently based out of South Korea, Hong Kong and London). Blocko continues to expand globally and intends to operate in may other countries and regions of the world.

➢ BLOCKO'S EXISTING INFRASTRUCTURE AND BLOCKCHAIN PARTNERS

Blocko will assist in helping to create the AERGO ecosystem. A number of its technology partners have expressed a desire to engage with and to help initiate the AERGO ecosystem. Examples include a specialist SQL development firm, a cloud infrastructure provider and large international Telecommunications firm.

➢ OTHER SUPPORTING THIRD-PARTY ECOSYSTEM ACTIVITIES

New technology innovations, curated value-adding partners, supporting open source and software developers are all critical elements of the AERGO ecosystem. Discovering and working with these AERGO stakeholders (and their expansion) is a fundamental part of the project.

This will also involve developing strategic, technology and IT service relationships in key industrial and governmental sectors.

Reserving a significant portion of the funding is intended to be used to promote and develop the above AERGO stakeholder ecosystem.

To support and help guide these efforts, the project has also secured the services of a highly experienced advisory panel.

This panel contains some of the world's leading experts in: blockchain, distributed databases, utility computing, digital communications, cloud computing, big data, machine learning/AI, virtualization, open source technology, open source licensing, computer programming, security, open source business development, financial and investment banking, government relations and strategic partner business development.

The AERGO Team can be seen in Appendix-D.

APPENDICES

APPENDIX-A: BLOCKCHAIN & OPEN PLATFORMS PRIMER

Bitcoin is to date perhaps the most well-known so called virtual crypto coin. It has gained a high degree of attention amongst public and government regulators. This is due to its frequent use in pseudonymous (sometimes illegal) transactions and its fluctuating value.

Bitcoin and the many other “altcoin” currencies that have appeared on the market are not the focus of this AERGO paper, but rather the novel technology architecture that these coins run and exist on is. This technology is blockchain.

At a very simplistic level, blockchain is just a database. A database that is both distributed (it runs on multiple computers) and secure. Just like Linux or Hadoop, public blockchains are also open source; that is, the technology is not owned by any single software company and is developed in an open and transparent process by developers around the world.

Blockchain is an ingenious technology that uses sophisticated cryptographic techniques and intelligent (so called consensus algorithms) to ensure an autonomous method by which digital transactions are approved and accepted within its ledger system. A consensus algorithm also effects how transactions and data are shared and pushed out to the computers within the blockchain network. Blockchain technology provides a tamper-proof version of the truth, so that transactions recorded in its system can be trusted. This trust applies to parties that have little (or indeed no) trust between them.

What is revolutionary is that blockchain operates as an intermediary and largely human free system. Even though database technologies have been in use for over 50 years, this had never been done before.

Blockchain-enabled systems are intended to allow for the creation of a single, universal, trustworthy and completely indestructible register of digital assets and associated transactions. The blockchain can be used to provide the basic services that are essential to any system where there is an exchange of digital assets (or even simply data). It can do so in ways that are often better and more efficient than the tools used today. For one, blockchain technology creates a viable, decentralized record of cryptographically encoded transactions, the distributed ledger, which allows the substitution of a traditional (and potentially less secure) master database for large numbers of distributed ones. We believe this has the potential to lead to radical simplification and cost reduction for large parts of many digital systems, while making them more secure and reliable.

Blockchain technology also allows for the creation of digital assets or tokens, which can provide a mechanism for direct and unambiguous transfer of value while keeping the advantages of digital networks.

We also believe that blockchain technology offers a far better means of establishing and using identity than what we use now. Identity can be stored cryptographically, with the ability for

individuals in a blockchain network to simultaneously authenticate their identities while protecting their privacy.

By providing unique, non-forgeable identities, along with an inviolable record of their ownership, the blockchain can potentially greatly simplify the direct transfer of physical assets and increase confidence in their origin.

Programming capabilities of blockchains are enabled through so-called “smart contracts”. Smart contracts are event-driven computer programs that possess the ability to take control of the underlying unit of value. In short, they are programs designed to automate execution and settlement of tasks. They are the application layer that allows dApp’s to unlock most of the value from a blockchain system (see Figure-16 below).

Smart contracts enable businesses to incorporate the value of financial transactions or other digital agreements into a form of cryptographically-assured business logic, giving it the ability to execute and move value autonomously. In short, business tasks are encoded and embedded securely within the blockchain itself - for auto-execution, auto-checking, auto-enforcement and auto-recording.

Smart contracts are therefore written and then compiled directly into the blockchain i.e. they are in effect embedded within the blockchain itself for this auto-execution to happen when called upon.

Figure 16. Smart contracts[19]

[19] Everest Group. (2016). Smart Contracts: Realizing the Benefits of Blockchain. Available: https://www.everestgrp.com/2016-

Blockchains cannot access data outside of their self-contained networks. Therefore, an important supplementary capability to smart contracts are so called “smart oracles”.

Smart oracles (in the context of blockchain) are external agents or programs that find and verify real-world occurrences and submit this information to a blockchain to be used by the smart contracts themselves. They provide external data and “trigger” the smart contracts. In effect smart oracles are third-party “data feeds”. They supply this information in a secure and trusted manner.

Smart oracles can in fact be software oracles, hardware oracles, consensus oracles and inbound and outbound oracles. As these are third party services, extra care (and techniques) are needed for these to be trusted.

Providing enterprise companies with trusted and secure information (when they use smart contracts in systems they build on blockchain) is crucial to users of the system. Mistakes can have serious consequences. Smart contracts execute autonomously and there is no so-called rollback in blockchain (due to its core immutability characteristic).

In summary, smart oracles can be seen as the “interface” between real word data and smart contracts.

The overall blockchain information technology (“**IT**”) stack is depicted in Figure 17.

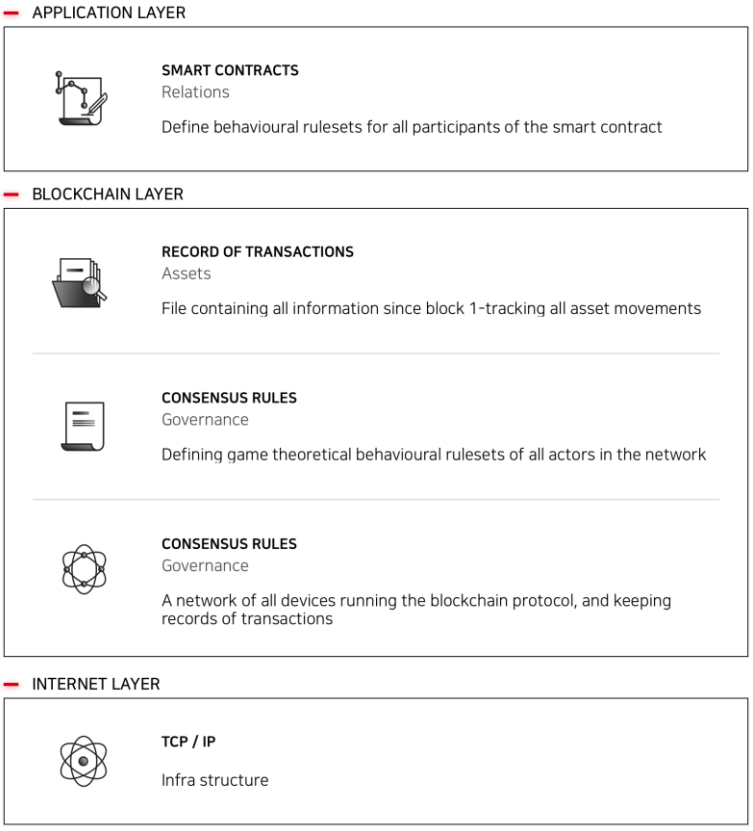


Figure 17. Blockchain IT Stack

10-smart-contracts-realizing-benefits-blockchain-36282.html/

Important functions of blockchain for business are depicted below in Figure-18.

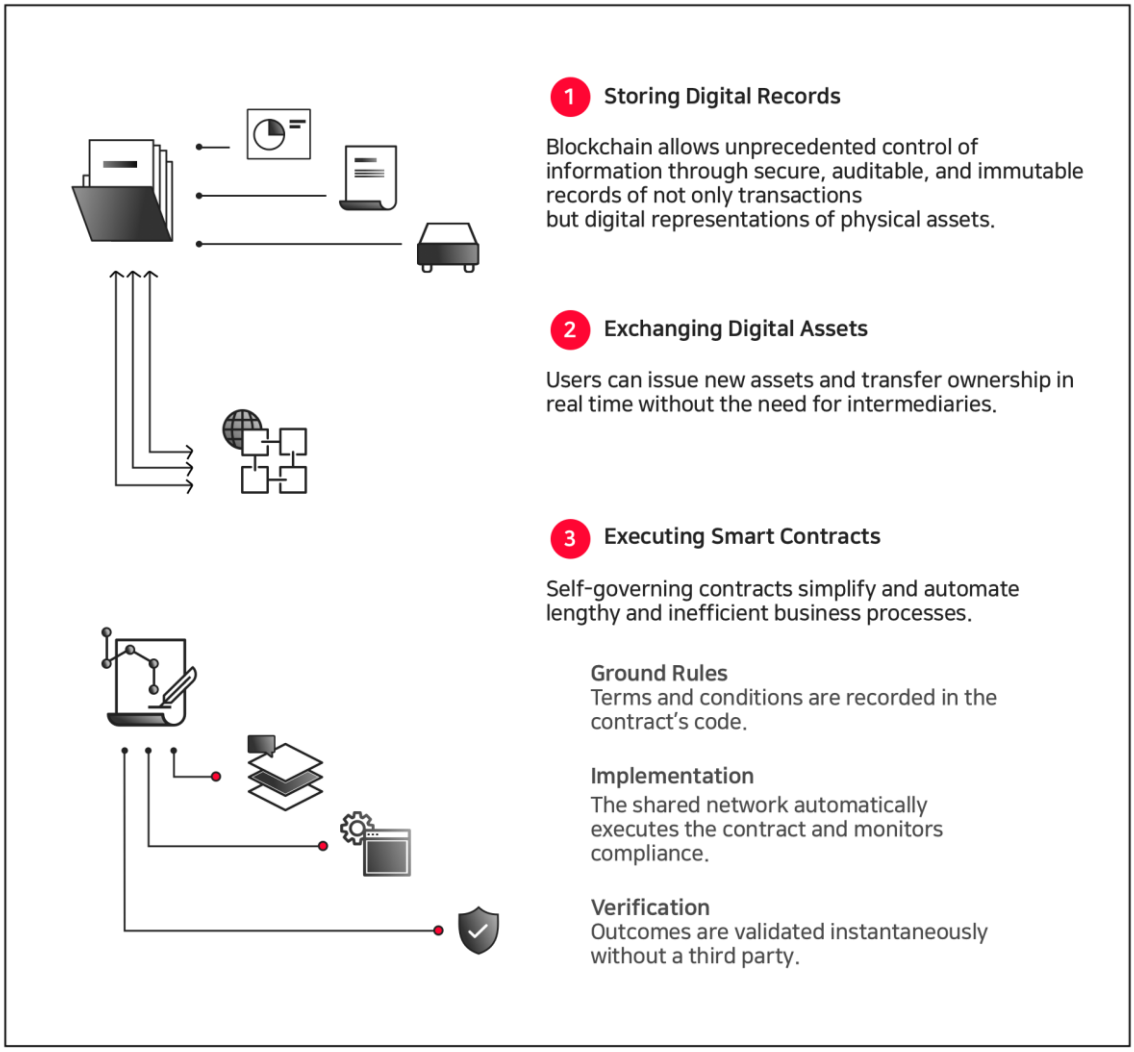


Figure 18. Functions of blockchain for business

The key distinguishing features of the two forms of blockchain (i.e. public and private protocols) include the level of trust and control in each system. Trust and control often vary depending on the nature of the blockchain architecture and the software consensus algorithms being used. Often increases in control can result in a decrease in decentralized trust, and vice versa. Performance throughput is also becoming a serious issue for blockchain as deployments grow.

Public blockchains, like Bitcoin, provide the potential for maximum participation and increase participation results in more computer "nodes" within the network. A larger network of nodes running a blockchain consensus algorithm increases decentralised trust. However, control can become a serious issue in this instance, if an entity gains a majority position over these computer resources. Large blockchain networks running current generation protocols and Proof-of-Work consensus algorithms are very inefficient. They draw a huge amount of energy to run the nodes and validate new transactions. The distribution of transactions is also very slow (especially for business-critical actions).

In private blockchains (such as Hyperledger Fabric) there is much more stringent control of which parties (nodes) are part of the specific blockchain network. Throughput can be increased by using state-of-the-art computers, memory and solid state disks; coupled with well-designed network interfaces between the nodes. However this often results in lesser decentralized trust as the networks tend to be much smaller in size than in public protocols. Newer and more innovative consensus algorithms are required (Figure 19 depicts the two models).

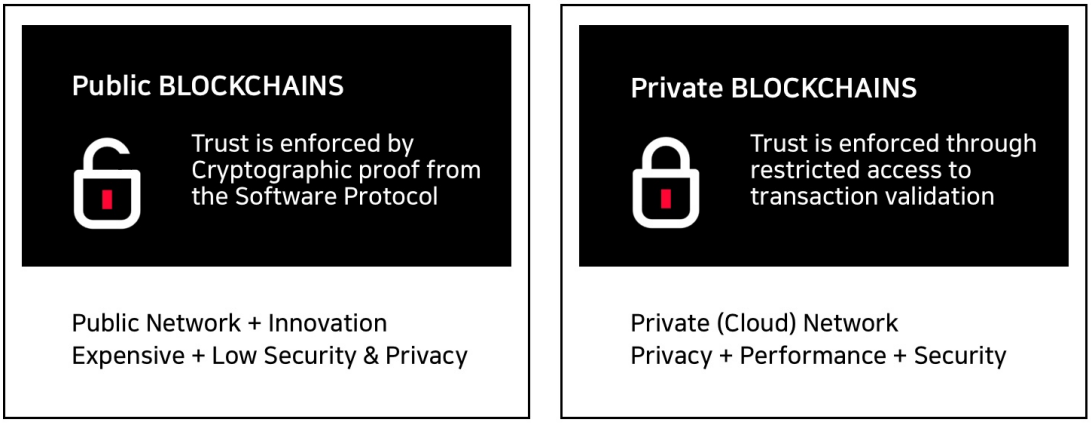


Figure 19. Permissionless (Public) vs. Permissioned (Private) Blockchains

The decision on whether a business chooses a public or private blockchain will depend on a few key considerations.

Such as a careful balancing act between

(i) the need to maximize trust in the transactions

(ii) control over the system and finally

(iii) overall performance throughput

For example, in banking - where trust and security are paramount - private blockchains are being designed to replace existing databases and systems. This is depicted in the following diagram.

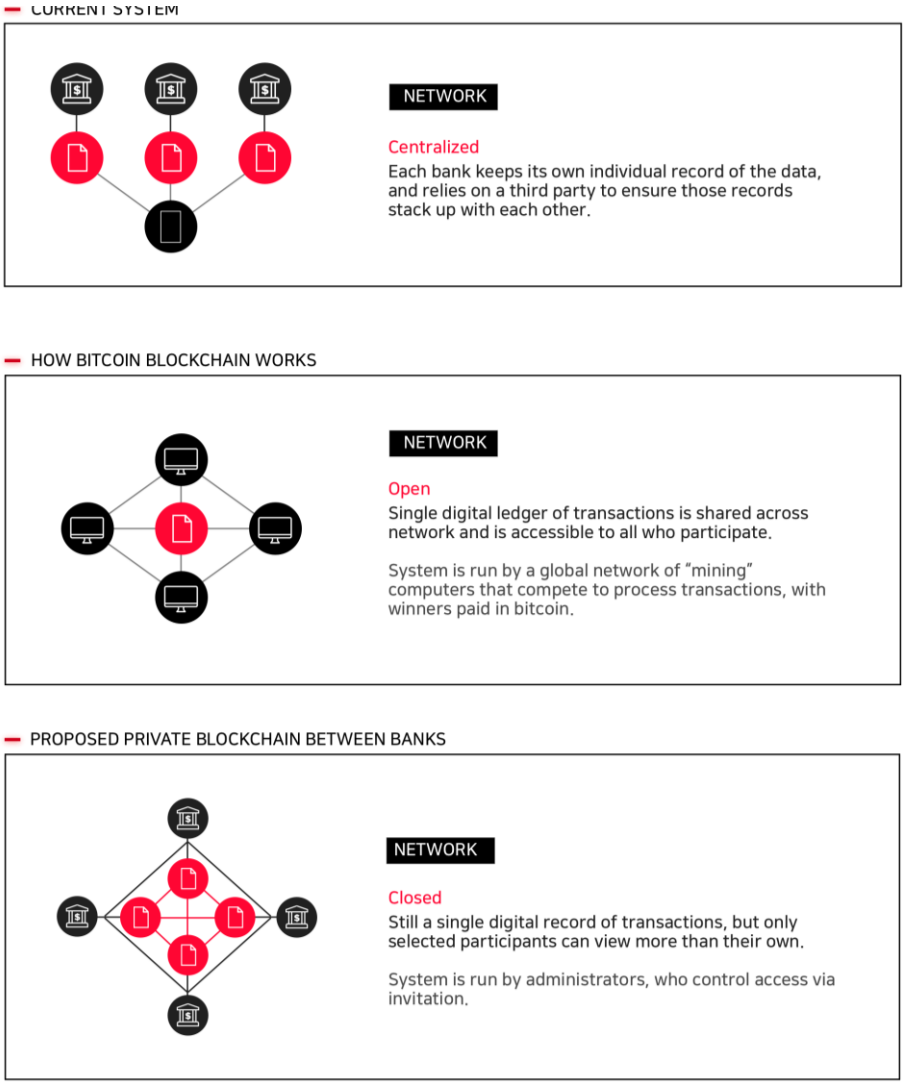


Figure 20. Example of blockchain network among banks

It is no wonder the market and customers are confused about which approach to back. This may (in part) explain why there are yet to be many in-production and at-scale blockchain deployments.

While blockchain is a great example of a peer-to-peer ("**P2P**") implementation, it is not always ideal for storing large amounts of data, due to:

(1) scalability: blockchains can be slow; and

(2) data protection: blockchain can create some data privacy related challenges (such as the-right-to-be-forgotten), particularly where the data is not appropriately secured and/or not subject to appropriate management access controls

These are areas currently undergoing much development in blockchain and where suitable solutions are expected to be found in the coming years.

Despite the above, we strongly believe blockchain will be a driving force of the next generation internet and the decentralized web. It can bring us true transactions without a middleman, with

Bitcoin as its first proven use case.

The same blockchain technology could allow companies in every industry to build new decentralized services in more open business ecosystems.

OPEN PLATFORMS ARE THE FUTURE

The combination of innovative dApp's, running on blockchain hosted on a serverless utility computing architecture - combined with mass mobile adoption use of secure e-commerce services - we believe will allow such "platforms" to transform many industries and business models in the coming years.

One only has to look towards East-Asia to see the largest example of such an open, developer and third-party friendly ecosystem - in the incredibly successful WeChat[20] messenger application.

Whilst not a reference model for blockchain per se, it is perhaps a reference model for how future open ecosystems will be built and operated. More importantly it showcases how new business value can be created when a modern digital platform (like AERGO) is open to users, developers, merchants, 3rd parties and businesses.

Introduced as a messaging app in 2011 by Tencent, WeChat has evolved into a lifestyle platform for users in China. With 1 billion monthly active users, it now offers to its users what Facebook, WhatsApp, Messenger, Venmo, Grubhub, Amazon, Uber, Apple Pay, offer together in the West.

WeChat has used strong user adoption to emerge as the one app that rules them all.

In the mobile-first world of China, WeChat has built a 'mobile lifestyle' that touches various aspects of users' lives, with an average user opening WeChat 10 times a day and spending circa 40 minutes per day[21] on the application. Initially launched as a pure messaging application to send texts in 2011 by Tencent (one of the three Chinese tech giants: Baidu, Alibaba and Tencent), it has evolved from just an 'app' to a 'platform'.

WeChat has benefitted from very strong network effects - both direct and indirect - in the Chinese mobile-first market. The more users they got onto the platform, the more other users wanted to join in order to be connected with their friends and families. Many Asian American people originally only got onto WeChat so they could remain connected with their relatives back in China.

WeChat was smart to open up the platform to third-party developers, who started offering their complementary or completely new services on the WeChat platform. Economies of scope effects applied here, the more users on the platform, more and more third party developers wanted to offer services on it, and vice versa.

With such strong network effects and little, if any, need to connect to different applications or services (i.e. a low so-called "multi-homing" environment), WeChat emerged as the app platform or rather an ecosystem that rules them all.

The following list shows some of the incentives of WeChat for its users - as well as the brands/merchants/third-party developers that engage within its ecosystem.

---

[20] Tech Node. (2017). *WeChat User & Business Ecosystem Report 2017*. Available: https://technode.com/2017/04/24/wechat-user-business-ecosystem-report-2017/

[21] Lily Kuo. (2014). *WeChat is nothing like WhatsApp—and that makes it even more valuable.* Available: https://qz.com/179007/wechat-is-nothing-like-whatsapp-and-that-makes-it-even-more-valuable/

For users, Wechat provides one integrated app that allows them to:

- Send text/voice messages to family and friends
- Share things on social media
- Follow celebrities and brands
- Book a taxi
- Order food delivery
- Book a doctor appointment
- Buy movie tickets
- Play games
- Transfer money to peers (red envelopes)
- Pay bills—utility bills, restaurant bills, etc.
- Find geo-targeted coupons
- Read magazine articles
- Meet strangers around them

For merchants/brands - Wechat provides one integrated app that allows them to drive user engagement through making APIs for payments, location, direct messages, voice, user IDs etc. available to these merchants.

Merchants also use WeChat as a CRM (customer relationship management) platform - to distribute news and to offer tailor-made promotions. WeChat has over 10 million (authenticated) official accounts including celebrities, banks, media outlets, and fashion brands to hospitals, drug stores, car manufacturers, internet startups, personal blogs, and more.

The platform is also very developer friendly. They are not forced to stay within the standard look and feel of WeChat so they can develop completely new differentiating services. The result is users gets the full web-app experience, without ever leaving the WeChat platform. The total annual lifestyle spending on WeChat was estimated to be $1.8 billion USD during 2014 (source: Tencent), mainly driven by entertainment and official accounts.

The WeChat ecosystem can be seen in Figure-21.

Perhaps most importantly, WeChat does not charge a user to sign up on the platform - it's completely free for users. Furthermore, WeChat tries to ensure trust in the ecosystem by vetting and authenticating all merchants that offer services on the platform.

Our understanding is that, the team behind WeChat, are now exploring how they could use blockchain to build and add even more new secure value-adding services to their platform.

In a recent post to a WeChat module called "Moments" (or "Friends' Circle," on Chinese versions of the platform), Ma Huateng (the CEO and Chairman of Chinese internet giant Tencent that is behind WeChat) declared, "*The time has come for a blockchain to decentralize a network.*" The technology, he said, *threatens to disrupt existing systems much like "the current TCP/IP, Packet Switching was able to defeat the giants such as AT&T*[22]*".*

[22] Sohu. (2018). *Ma Huateng made friends and commented on physicists' views on blockchain*. Available: http://www.sohu.com/a/218207096_117373

A very informative article on this truly innovative open platform ecosystem has been written by VC Andreessen Horowitz[23].

[23] Connie Chan. (2015). *When One App Rules Them All: The Case of WeChat and Mobile in China*. Available: https://a16z.com/2015/08/06/wechat-china-mobile-first/

APPENDIX-B: BLOCKCHAIN AND UTILITY COMPUTING

In the very near future, we believe the focus will move away from developers having to understand complex programming languages and having to cater for complex IT architecture management and operations. This will allow them to focus on application innovation and value creation at the front end of the process; where applications touch and interact with the end-user (and billions of future IoT devices in the coming years).

In this "serverless architecture" much of the IT complexity will be abstracted or simply hidden from the developer and the end-user. This concept is important to understand to fully appreciate this paper and one of the fundamental values that a future AERGO based system will provide.

Serverless architectures refer to applications that significantly depend on third-party IT services (known as Backend as a Service ("**BaaS**")) - or on custom code that's run in so called software containers (Function as a Service ("**FaaS**")), such as with Amazon AWS Lambda. By moving much behavior to the front-end of the process, this architecture reduces IT operational costs and enhances the performance for the end user.

"Serverless" does not explicitly mean that an application is running without compute servers. It means that the person who owns the system does not have to purchase the servers, does not have to provision them or does not need any virtual machines to run the back-end application code itself.

A typical three-tier web application (and that does not use a serverless architecture) is depicted in the simple illustrative example below (Figure 22).

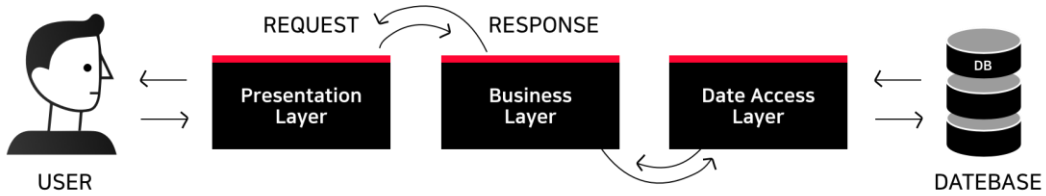


Figure 22. Example of "3-tier" web application

This architecture is composed of three different layers: the so-called (front-end) presentation layer, business layer and the data access layer (often called IT back-end).

When an end-user performs any action on the presentation layer, it calls the business layer to process the action (for example validation of an operation). It then calls the data access layer which interacts with the database. That in turn gives back a response to the business layer which then passes it back to the presentation layer (that is, the actual user interface).

This cycle is typical of many first generation three-tier web-based applications. Designing such systems requires developers to have an intricate knowledge of the whole system and to take care of how everything interacts and works together. In effect much of their time is devoted to making the various elements work together (often resulting in proprietary interface implementations).

This is contrasting to a more modern serverless architecture from Amazon (AWS)[24]

The architecture also has three layers: presentation, application and data layers. The biggest difference being that each layer connects with the layer above or below it through standardised interfaces (so called application program interfaces ("**API**")).

Another (simpler) way to therefore understand a serverless architecture is a system where the backend IT business logic can run on an arbitrary third party vendor's server infrastructure which developers do not need to worry about.

It does not mean that there is no server to run your backend logic, but rather that you do not need to maintain it. This serverless architecture is the business of third party vendors such as Amazon, Azure and Google. In effect it gave birth to cloud computing over the past ten years.

Serverless architectures have two variant models:

- BaaS or MBaaS (where M stands for mobile); and
- FaaS.

With BaaS or MBaaS, the backend IT logic will be run by a third-party service provider. Application developers do not need to provision or maintain the servers or the infrastructure which runs these backend services. In most cases, these backend services will run continuously once they are started. Application developers will simply need to pay a subscription (or in the future an "IT token") to the hosting vendor. In most cases, this subscription lasts for weeks, months or can run on a recurring yearly basis. Another important aspect of BaaS is that it runs on a shared computer infrastructure and the same backend service will be used by multiple different applications (in what is called multi-tenancy).

The second variant, FaaS, is even more popular these days. Most of the leading (current generation) technologies such as AWS Lambda and Microsoft Azure Functions, as well as Google Cloud Functions, fall into this category. With FaaS platforms, application developers can implement their own backend logic and run them within the serverless framework. The running of this functionality within a server will be handled by the serverless "framework". All the scalability, reliability, and security aspects will be taken over by this framework. Different vendors provide different options to implement these functions with popular programming languages like Java and C#.

As a developer or business running an application, it is possible to use the services of a third-party provider (such as Amazon API Gateway and AWS Lambda). This allows developers to build a serverless production application which is secure, scalable and highly available, without worrying about the complexities of key functions such as authentication, searching, updating and navigation of the underlying database layer.

There are few differences between FaaS when compared to BaaS:

- costs relate only to the amount of resources actually being used (for example per minute level charging);
- FaaS is ideal for use cases with highly fluctuating traffic; and

[24] Serverless Computing and Applications. Available: https://aws.amazon.com/serverless/?nc1=h_ls

- FaaS functions will run for a short period of time (typically a few mins only)

A simple way to understand when a developer will use a FaaS over BaaS is when the developer needs ultimate granular control of how the application works, performs and scales.

These innovative applications will connect and interact with other similar applications - whilst at the same time being smaller, more compact and more mobile. This is the essence of a so-called “micro-services” model.

These techniques are being used today by very advanced developers serving leading digital businesses (for example in B2B and B2C mobile e-commerce and mass consumer applications such as in social media, gaming and communications). Over the coming years these techniques will become common place; with all kinds of developers and firms and not be the preserve of simply the most advanced companies like Facebook, Amazon, Google, Apple and Alibaba.

Serverless Architectures will simplify the maintenance of future backend IT systems while giving cost and performance benefits for handling different types of decentralized micro-services based dApps.

In short, developers don’t see themselves as “plumbers of IT” any more; they want to focus on creative value-adding applications.

However, whilst there are many benefits, some aspects need to be carefully considered when dealing with these form of serverless architectures; such as:

- vendor lock-in could cause problems (for example frequent mandatory API changes, pricing structure and other future technology changes);
- speed issues across the network could occur and challenge the ability to meet enterprise service level agreements (“**SLAs**”) for many concurrent users;
- since server instances will come and go, maintaining the state of an application is really challenging with these types of frameworks;
- they are not suitable for running long-running business processes since these function services will be terminated after a fixed time;
- there are other very important limitations, such as the maximum possible transactions-per-second (“**TPS**”) which can be processed; often limited by the protocol used and the speed of interconnected IT services within the network; for example memory access speed, network speed, stability and network response time (latency);
- end-to-end testing or integration testing is not easy as these dynamic functions spin-up and come and go as and when needed; and
- lack of suitable monitoring and debugging capabilities into the production system and their behavior for the developer to be fully confident about their performance.

Despite these current limitations, we do believe that in the near future, microservices based dApps running on an AERGO based blockchain (in a serverless infrastructure deployment model) will become one of the dominant deployment model for many new services in the emerging distributed utility computing world.

In summary, we believe that the benefits of serverless architectures will be extremely important for the evolution of blockchain over the coming years.

They provide the ability to:

1. use multiple business application as service functions to reduce development costs;
2. reduce operational costs as developers do not have to consider infrastructure and maintenance costs;
3. scale resources quickly (as and when needed), plus it provides horizontal scaling of the application in a completely elastic and automatic manner;
4. manage and operate IT resources much more easily, as all physical IT involvement is managed by third party providers so there is no need to dedicate resources and time to these tasks; and
5. provide built-in availability and fault tolerance of serverless dApp applications.

The transition to new serverless applications has already started (see Figure-24 that follows).

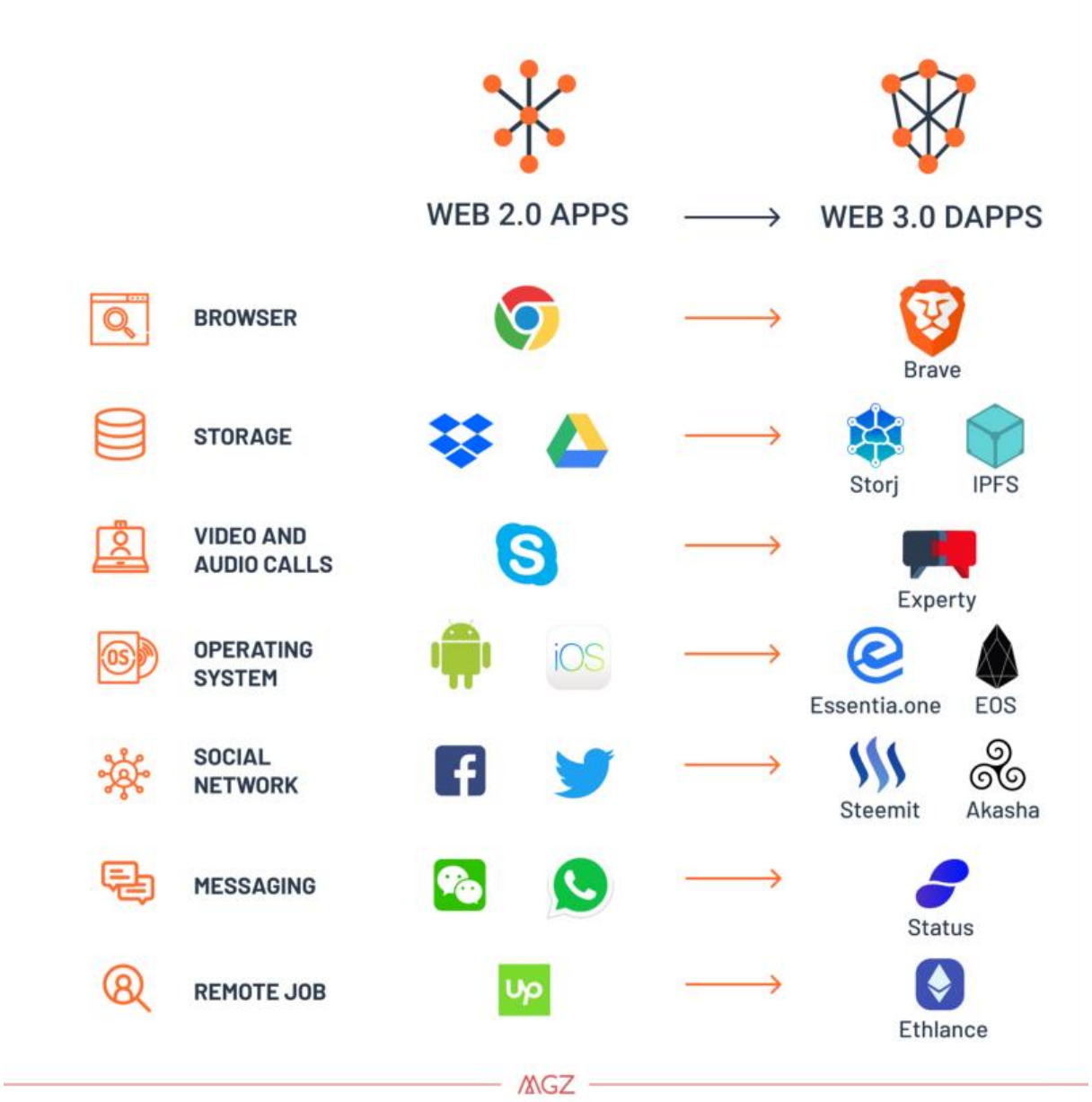


Figure 24. Transition from Web 2.0 to Web 3.0[25]

Whilst the adoption of serverless dApps is still very much work-in-progress, early indications are that they will become a major force in how businesses deliver new services via secure and distributed cloud-based services.

Some current mission-critical and at scale applications for businesses may not be immediate targets for this approach today (as some security capabilities and ecosystem tools still need to mature). However, the many potential use cases for serverless computing suggest that it is increasingly probable that it will become an "all in" decision for future firms. In fact it will be similar

[25] Matteo Gianpietro Zago. (2018). *Why the Web 3.0 Matters and you should know about it.* Available: https://medium.com/@matteozago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949

in many ways to the way that cloud computing has already been adopted in a diverse range of industries.

As this architectural methodology matures, we believe it will increasingly be taken up for many thousands of new business projects in almost every sector of industry that deal with digital asset and secure data exchange. For example, Everest Group has predicted that blockchain will achieve accelerated adoptions within the next few years in the banking industry (see Figure-25).

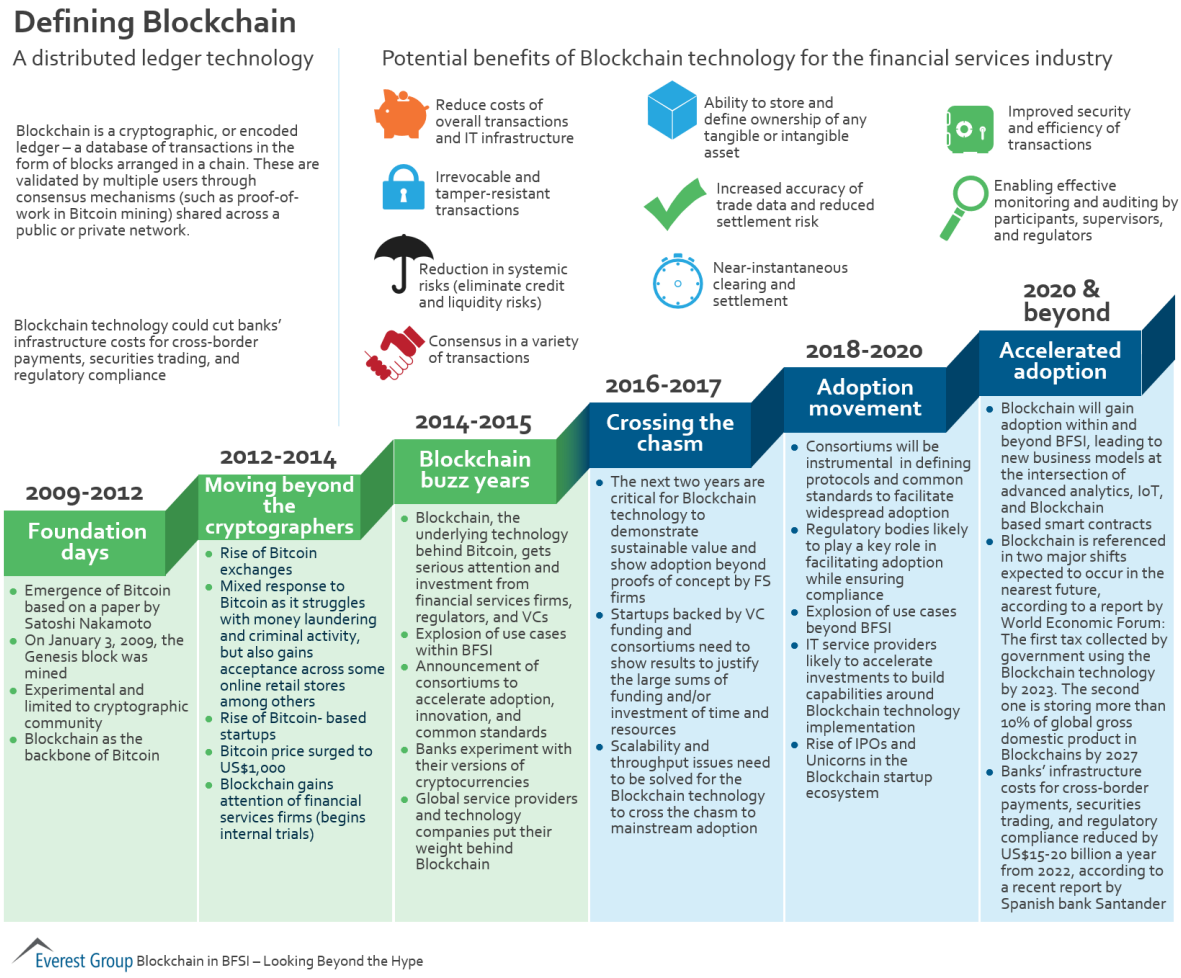


Figure 25. Adoption of blockchain in Banking (Everest Group)[26]

Today, many dApps are being built by various firms that use specific (perhaps immature) vertical blockchain solution implementations. There is little standardization; potentially leading to future fragmentation. This will lead to undesired cost, complexity and risk for companies seeking to leverage blockchain across many different business and product lines.

The level of fragmentation and complexity today can be seen in the following diagram.

[26] Everest Group. (2016). *Defining Blockchain*. Available: https://www.everestgrp.com/2016-05-blockchain-technology-bfsi-benefits-market-insights-20805.html/

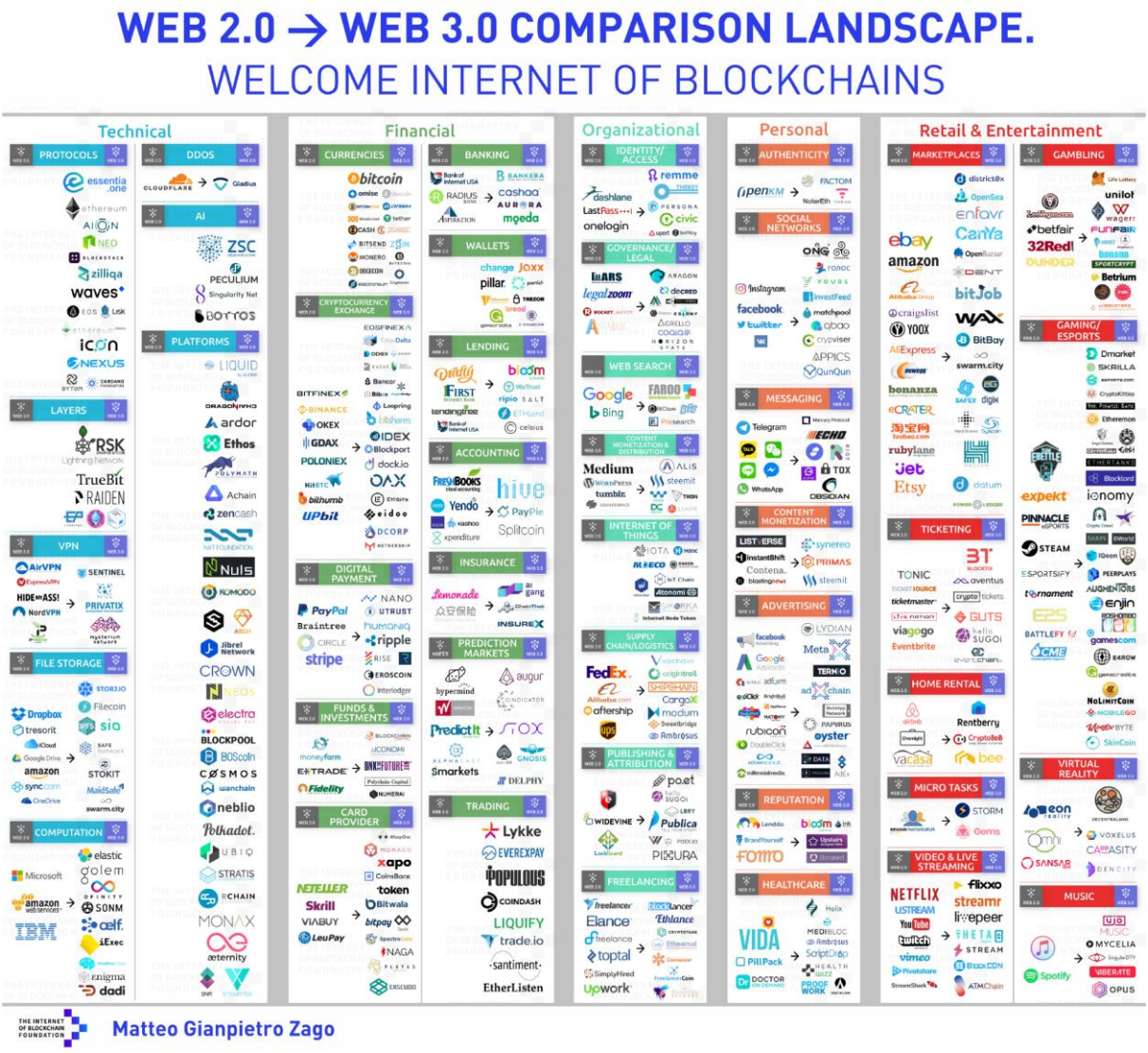


Figure 26. Complex landscape of blockchain solutions (today)[27]

Businesses will be challenged as they will find it very difficult to support multiple blockchain solutions (as described in the section: Obstacles to Blockchain Adoption, starting on page-14).

[27] Matteo Gianpietro Zago. (2018). *Why the net giants are worried about the Web 3.0.* Available: https://medium.com/@matteozago/why-the-net-giants-are-worried-about-the-web-3-0-44b2d3620da5

APPENDIX-C: PRIVATE vs PUBLIC ENTERPRISE BLOCKCHAIN

Public and private blockchain protocols have many similarities:

- Both are decentralized peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions
- In both cases, blockchain protocols provide data integrity and immutability (i.e. the data contained in blockchain (and specifically its recorded state) cannot be modified after it is created - even when some participants are faulty or malicious in a network)
- Both maintain the replicas in sync through a protocol referred to as consensus
- Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious (i.e. they work in a trustless network environment)

PUBLIC BLOCKCHAIN

At a conceptual level, the primary distinctions between public and private blockchain relate to who is allowed to participate in the network, execute the *consensus* protocol and maintain the shared ledger. A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.

One of the drawbacks of existing public blockchains is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale. More specifically, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem (called proof of work ("**PoW**")) to ensure all nodes are synchronised and trust is maintained.

This process is complex, slow and consumes vast amounts of energy (electricity).

Another disadvantage for particular users is the openness of many existing public blockchains, which provide little to no privacy for transactions (subject to pseudonymity). They also only support a weak notion of overall system level control as they are open to anyone to participate in the network.

These are important considerations for future enterprise use of blockchain.

However, despite the above, in a public blockchain, no one person, group or organisation controls the information which is on the blockchain; or the series of rules that underpin the protocol itself. No member can unilaterally change the protocols of the blockchain and the information contained within it. Users should be able to fully trust the public blockchain and therefore put their complete trust in a third party that uses the same blockchain.

In short, public blockchains can provide maximum trust but are slow and expensive to run. They can also be extremely difficult to upgrade, because they require consensus amongst a large group of participants, many of whom may have different (and even competing) interests. Further, their trusted status may be undermined by various factors, such as malicious activity (such as so-called

“front-running” by miners); by concerted behavior (e.g. when mining power is concentrated in a small number of participants); or even legal complexities that arise from having transactions recorded and validated in numerous jurisdictions all at once.

PRIVATE BLOCKCHAIN

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses that set up a private blockchain, will generally set up a *permissioned* network. This places restrictions on who is allowed to participate in the network, and in what transactions. Participants need to obtain an invitation or *permission* to join. The access control mechanism can vary: for example, existing participants could decide future entrants, a regulatory authority could issue licenses for participation or a consortium could make the decisions instead. Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner.

Private blockchains can (with careful system level IT design) permit greater scalability in terms of transactional throughput.

In short, private blockchains provide improved privacy, maximum throughput and are potentially cheaper to run, however they lack the level of trust and network effects that are gained from the more widely deployed public blockchains.

A lot of businesses are experimenting with building their own private blockchains. A number of these initiatives (and associated consortia) are facing difficulties to get these private blockchains into real life production systems.

Some of the reasons for this are perhaps:

1. building proprietary private blockchain systems requires specialist IT, cloud and developer skills and know-how that only very few firms possess

2. building these using an open source model - with the intention of using, enhancing and maintaining these longer term - is extremely challenging (and software development and maintenance is not typically a core-capability for these businesses)

3. the two above factors can significantly increase the long term costs of such systems

Therefore, for companies looking to integrate blockchain technology into their business processes, very careful consideration needs to be placed on the (i) trust plus interoperability (public) need versus (ii) performance plus privacy (private) requirement.

This is a fundamental paradox when dealing with combined public and private blockchains.

Most enterprise PoC efforts were apparently implemented in private blockchain networks. It appears that only a third of these were actually deployed on public networks (see Figure-27 below for a similar comparison in the banking sector).

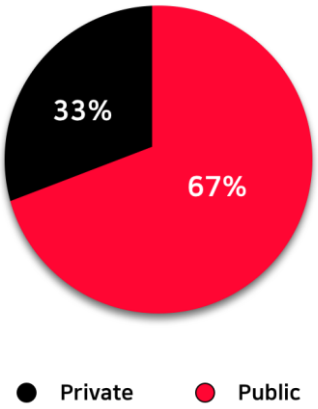


Figure 27. Type of Blockchain that were used in Bank driven PoC[28]

Due to stringent security and compliance requirements, large companies have traditionally implemented their IT systems in private computer architectures (such as private internal clouds). For the same reasons, many of these firms are experimenting with private blockchains, and choosing not to use any form of public protocol.

A number of industry consortia (such as R3 and Hyperledger) - may be limiting their potential long-term value and usefulness - by perhaps only considering one type of blockchain architecture.

In fact, much of the innovation in blockchain is actually happening in the public protocol space. This is evidenced by the sheer level of new ideas, projects and services that have been fueled by the many large scale (primarily crypto-currency driven) blockchain projects. The majority of these projects do focus on direct dApp development but this also drives certain innovations in the underlying (primarily public) blockchains that run them.

We believe that truly transformative business benefits can be achieved if a hybrid approach to blockchain is used. This approach would help maximize the benefits (and reduce the drawbacks) of a combined public and private blockchain architecture. We see the benefit in having a business architecture that - uses a public blockchain to provide enterprise integrity, immutability and a trustless network environment, for data and value (asset) transactions - coupled with a private blockchain that helps enable regulatory compliant record-keeping, privacy and that is configured and optimized for the required enterprise level performance.

A similar form of hybrid approach is already in use today with cloud computing. Enterprise firms combine private cloud (highly information-sensitive focused) data centres, with lower cost secure public clouds (for auto-scaling and performance throughput of business applications).

[28] Nivedita Bhattacharjee. (2017). *Blockchain is becoming more than a buzzword, and now there's tangible proof*. Available: https://www.techinasia.com/bankers-like-blockchain

APPENDIX-D: AERGO Team and Advisory Panel

AERGO represents a complex and comprehensive project that is being undertaken. Its development and successful deployment will demand a combination of an array of disciplines - namely, blockchain technology, cloud computing and open source know-ho.

AERGO has assembled a truly complementary team with stellar experience and proven expertise in these areas.

AERGO BOARD

Phil Zamani

- Global VP Sales & Biz Dev. Internet Embedded Linux Appliances for Redhat Inc.
- Global Head of Big Data & Cloud Biz Models at Santander
- Senior VP of Cloud Biz Unit at Deutsche Telekom

Hun Young Park

- Expertise in Machine Learning solution development
- 12 years of experience in Relational DBMS and distributed solutions
- KAIST, Computer Science. MS

Roderik van der Graaf

- Founder of Lemniscap, an investment and advisory firm in the blockchain space
- 7 years of PE/VC at Caldera Pacific and KCP Capital
- 13 years of equity derivatives trading at Deutsche Bank, HSBC, Rabobank, Bear Stearns, LIM Advisors and All Options
- Queen Mary, Univ. of London, Information Technology. MSc

COMMITTEE HEADS

Won Kim
Technology Committee Head

- 9 years of experience in Relational DBMS
- 6 years of research & development of distributed systems
- Boston Univ. Computer Science

Jane Lee
Finance Committee Head

- 7 years of experience in Strategy Consulting at Accenture
- Expertise in digital transformation, and technology commercialization
- Cornell Univ. Hotel Administration

Alison Shim
Ecosystem Committee Head

- 5 years of experience in Strategy Consulting at Accenture
- Expertise in go-to-market, and business development
- New York Univ. Economics and Communication studies

TECHNOLOGY TEAM

Yun Woo Park

- 7 years of experience in relational DBMS
- Principal software researcher in database R&D
- Korea Univ. Computer Engineering

Sung Jae Woo

- 11 years of experience in Relational DBMS buffer cache and IO subsystem development
- Expertise in Computational Physics
- Korea Univ. Physics. PhD

Pierre-Alain Ouvrard

- Python, Solidity developer
- Offchain scaling and plasma researcher
- INSA Lyon. Electrical Engineering

Kyung Tae Lee

- 12 years of experience in Relational DBMS and Query engine development
- Expertise in Graph database
- Kangwon Univ. Computer and Communication Engineering

Bernardino Ramos

- 19 years of experience on software development
- Expertise on SQLite database replication
- Creator of Binn, LiteReplica and LiteSync

+25 more

Blocko Team

BUSINESS TEAM

Mason Park

- 7 years of experience in Advertising and Marketing
- Innovator and expertise in branding, marketing strategy & execution
- Univ. of Wisconsin-Madison, Biochemistry

Han Kim

- 5 years of experience in Public Relations development
- Excellence in cryptocurrency dynamics and ecosystem
- HUFS, Social Science

Seona Kim

- 3 years of experience in IT Consulting & Cloud management service
- Strategy project manager and researcher for blockchain market
- HUFS, English-Korea Interpretation & Translation

Camron Miraftab

- 4 years of experience in innovation strategy and venture capital
- 3 years of experience in blockchain research and due diligence of blockchain businesses
- Newcastle Univ. International Economics and Finance MSc

AERGO ADVISORS

Eddie Alleyn

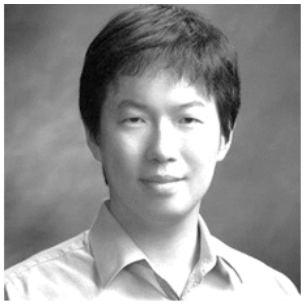
Eddie Alleyn is a technology entrepreneur and expert in security and secure communications. He spent thirty five years leading special projects for the UK Government, in the Ministry of Defence and the Foreign and Commonwealth Office. From 2011-2016 he was Chair and CEO of HMGCC, an agency of the FCO, involved in the design, manufacture and integration of secure communications and cyber systems for the UK Government. He is now an Exec and Non-Executive Director to innovative tech start-ups in the security and cyber security fields, and an Adviser to SANS Institute. Eddie knows how to get the best out of innovative technology and engineering teams to deliver ground-breaking security solutions.

Djamel Souici

Djamel Souici is a legal expert on open source technology, Licensing and business models. He is also a leading advisor and practitioner in Data Privacy and Regulation (such as GDPR). Djamel, a member of the German Legal Barr Association, has spent the past 19 years as General and Legal Counsel for a number of innovative software firms, leading their representations in respect of open source, data privacy and compliance. He has also developed a number of strategic partnerships with many Fortune 100 firms in diverse sectors such as Telecoms, Financial Services, Government, Automotive, Manufacturing, Petrochemicals, Logistics, Retail and Healthcare. Djamel is also a renowned negotiator and expert in international mergers and acquisitions.

Vincent Zhou

Vincent is the founding partner of FBG Capital. He has extensive experience in digital assets trading and investment. His professional experience has seen him work at leading technology companies including the likes IBM and Oracle. With an aptitude towards distributed ledger technology, Vincent has become an early investor in a broad spectrum of blockchain companies and projects.
His successes in the blockchain arena has led him to being considered as one of the most well-connected and visionary crypto hedge fund managers in Asia.



Joon-Hong Jake Kim

Jake Kim has a deep understanding of capital markets, strategic business development, as well as hands-on experience in system engineering and back-end computing. He is currently a venture capital and cryptocurrency fund manager based in Seoul where he specializes in corporate venturing, M&A, company building and (selective) Angel investments. He is a seasoned startup investor, adviser and enterprenuer with over 20 years of combined experience in capital markets, consultancy and large-scale back-end and middleware systems development. Jake currently manages Innobase, the corporate venture capital arm of Kolon group. He holds an MBA in Strategy and Corporate Governance from IE Business School.

Riad Hartani

Riad is a seasoned technology specialist and strategist with over 20 years contributing to the development of Internet, Mobile and AI technologies. He co-founded and led multiple high-tech startups (Caspian, Anagran, Wichorus and more) with some seeing very successful exits. He has advised over 10 leading technology corporations, numerous private equity houses and several governments and regulators. He also co-founded Xona Partners, a boutique technology and investment advisory firm and ivalley.co, a Fintech co-creation studio. Riad holds a Ph.D in in Artificial Intelligence. He is frequently invited as a lecturer, speaker and panelist at leading industry fora and academic institutions

Sinhae Lee

Sinhae Lee is a Partner at GBIC, leading blockchain investments and accelerating robust projects. Prior to joining GBIC, she has been deeply involved in the FinTech/blockchain industry in Silicon Valley. She led business development and operations at a payment start-up, Coin, which was acquired by FitBit in 2016 and later worked at NerdWallet, a FinTech start-up in San Francisco. She started her career as a management consultant at McKinsey & Company. She brings her Silicon Valley and consulting experience to the blockchain/crypto industry. Sinhae holds an MBA from Stanford University and a B.A. in Business from Korea University.

Pierre F. Suhrcke

Pierre Suhrcke is a leading Fintech expert and investor in Europe, having been active in this sector since 1999. Pierre spent more than 17 years in various senior executive management positions in Investment Banking at Deutsche Bank in London and Frankfurt (Equities, Risk Management and Head of Capital Venture Partners). Pierre is currently a Venture Partner at Tempocap, a European technology investment firm, and a board member of Acorus Capital, a Hong Kong based Private Equity firm. He is an angel investor, mentor and advisor to companies - having worked with and sat on the board of - over 20 successful private companies (US & Europe). He is frequently invited as an expert fintech panel member at leading conferences.

APPENDIX-E: Glossary of Terms

Branching: the duplication of an object under revision control (such as a source code file or a directory tree) so that modifications can happen in parallel along both branches.

Concurrency control: a database management systems concept that is used to address conflicts with the simultaneous accessing or altering of data that can occur with a multi-user system.

Content Delivery Network: a geographically distributed network of proxy servers and their data centres. The goal is to distribute service spatially relative to end-users to provide high availability and high performance

Decentralised Application (dApp): A dApp has its backend software code running on a decentralized peer-to-peer network. Contrast this with a typical app where the backend code is running on centralized servers.

Denial-of-service attack: a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Hard-fork: a radical change to the protocol that makes previously invalid blocks/transactions valid (or vice-versa).

JIT compilation: a way of executing computer code that involves compilation during execution of a program – at run time – rather than prior to execution.

LLVM: a compiler infrastructure project that is a collection of modular and reusable compiler and toolchain technologies used to develop compiler front ends and back ends.

Merging: combining the various versions and/or changes of a file or folder.

Microservices: a software development technique—a variant of the service-oriented architecture (SOA) architectural style that structures an application as a collection of loosely coupled services.

Orchestration: the effect of automation or systems deploying elements of control theory.

Parallelism: a type of computation in which many calculations or the execution of processes are

carried out concurrently.

Private Chain: a blockchain network with limited openness and decentralization compared with a public chain, where authorization under specific rules is required for a new node to join the network.

Proof of Stake: a concept that states that a person can mine or validate block transactions according to how many coins he or she holds.

Proof of Work: an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.

Public Chain: A blockchain network fully open and decentralized, where any participants can join the network if they follow the protocol of the public chain.

Serialisation: the process of translating data structures or object state into a format that can be stored (for example, in a file or memory buffer) or transmitted (for example, across a network connection link) and reconstructed later (possibly in a different computer environment)

Serverless Computing: a cloud-computing execution model in which the cloud provider dynamically manages the allocation of machine resources.

Smart Contract: a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

Smart Oracles: external agents or programs that find and verify real-world occurrences and submit this information to a blockchain to be used by the smart contracts themselves. They provide external data and “trigger” the smart contracts. In effect smart oracles are third-party “data feeds”. They supply this information in a secure and trusted manner.

Software Repository: a storage location from which software packages may be retrieved and installed on a computer.