WHITE PAPER

PLEXIO : The Flexio Platform A Decentralized architecture for enterprise security and storage & makes integrating Web 3 protocols quick and seamless .

DISCLOSURE STATEMENT

Forward-Looking Statements: This Informational Presentation and the information on our website contains or may contain certain statements, estimates and projections that are or may be deemed "forward-looking statements." All statements other than statements of historical fact on this Informational Presentation and our website are forward-looking statements and include statements and assumptions relating to: plans and objectives of management for future operations or economic performance; conclusions and projections about current and future economic and political trends and conditions; and projected financial results and results of operations. These statements can generally be identified by the use of forward looking terminology including "may," "believe," "will," "expect," "anticipate," "estimate," "continue", "rankings," “intend,” “outlook,” “potential,” or other similar words. DecentraWeb, it’s employees, staff, affiliates, assigns, principals, advisory board, governing board and advisors do not make any guarantees, representations or warranties (express or implied) about the accuracy of such forward-looking statements. Forward-looking statements involve certain risks, uncertainties, and assumptions and other factors that are difficult to predict. Readers are Cautioned that actual results of the statements referenced in this informational presentation and the accompanying website could differ materially from forward-looking statements; and readers are cautioned not to view forward-looking statements as actual results or place undue reliance on forward-looking statements. Conduct your own Due Diligence when Reviewing this Material.

CONSULT YOUR OWN ADVISORS BEFORE MAKING ANY DECISION WITH REGARD TO ANYTHING WRITTEN IN THIS MATERIAL. Additional information is available on our website: http://flexioplatform.com but it is not exhaustive of all risks and is subject to all disclosures. Before using or participating in Flexio, please perform your own due diligence. Digital Assets carry a high level of risk. Decentralized Finance (DeFi) is experimental, and code can be flawed. Nothing in this Informational Presentation is an offer of an investment or a solicitation of any kind. We have taken the position that FLEXIO is a utility token that aims to be a pillar of the decentralized internet allowing for active participation on the Flexio platform. Before participating in Flexio, you must read and agree to our Terms and Conditions.

No Recommendations, Offerings, Advice or Solicitation: Nothing in this Informational Presentation or written on our website should be construed as, and may not be used in connection with, an offer to sell, or a solicitation of an offer to buy or hold an interest in any blockchain, cryptocurrency, security or investment product.

Nothing in this Informational Presentation is or should be deemed an offer of an investment or a solicitation for an investment. We have taken the position that FLEX is a utility token that aims to be a pillar of the decentralized internet and for all intents and purposes we believe it should be viewed as such. We make no guarantees that the legal and regulatory regimes governing at any period of time will view this in the same or similar manner and offer no advice or conclusions.

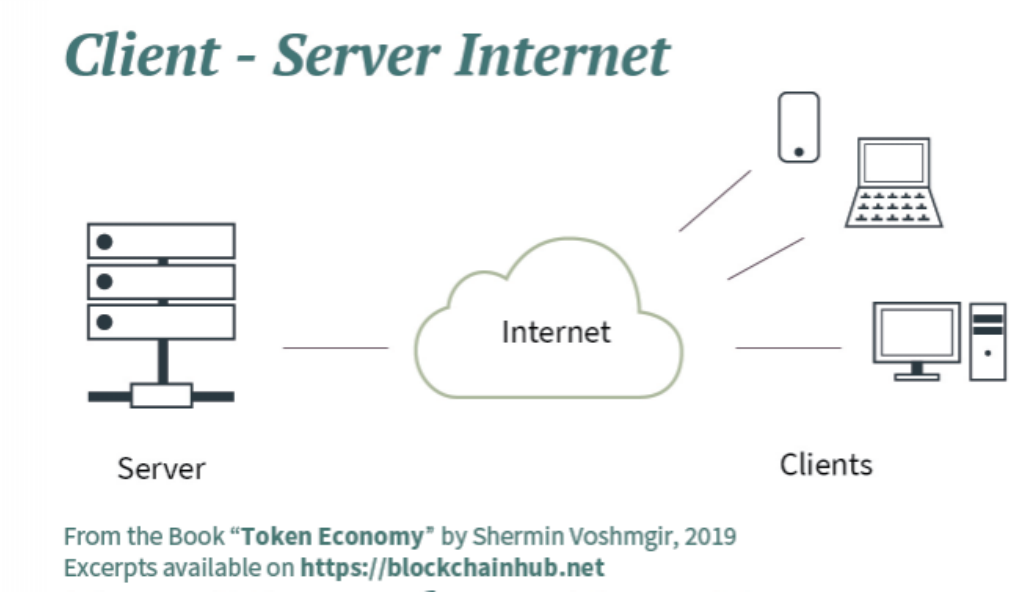
Inherent Risks of Cryptocurrencies: The Flexio Project is not responsible for the costs and fees associated with the purchase, sale, transfer and/or liquidation of FLEX and/or the corresponding currency and/or platform used to transact in FLEX. Everyone acknowledges that cryptocurrency is volatile, prices can swing in any direction at any time, cryptocurrency is highly speculative and FLEX like any other cryptocurrency carries the same or similar risks. Any decision regarding FLEX should be made in coordination with careful consideration and professional tax and financial advice where applicable.

FLEXIO IS A TOKEN TO BE USED ON THE DECENTRAL WEB PLATFORM. ANY PAST PERFORMANCE IS NOT INDICATIVE NOR A GUARANTEE OF FUTURE RESULTS. No content in this document shall be viewed as a guarantee of future performance of Flexio Platform or FLEXIO for that purpose.

1. ABSTRACT

The Internet we have today is broken. We do not control our data, nor do we have a native value settlement layer. Thirty years into mass adoption of the Internet, our data architectures are still based on the concept of stand-alone computers, where data is centrally stored and managed on a server, and sent or retrieved by a client. Every time we interact over the Internet, copies of our data get sent to the server of a service provider, and every time that happens, we lose control over our data. Even though we live in a connected world, with more and more devices getting connected with the Internet – including our watches, cars, TVs, and fridges – our data is still centrally stored: on our computers or other devices, on the USB stick, and even in the cloud. This raises issues of trust. Can I trust those people and institutions that store and manage my data against any form of corruption – internally or externally, on purpose or by accident?

Each time we interact over the Internet, copies of our lives are made and sent to the other computer, and when this happens, we lose control over our data on the other end of the Web, behind the walled gardens of a server. This is not only an issue when it comes to the privacy of our personal data, but it also produces a lot of inefficiencies in the backend of operations along the supply chain of goods and services. The current Internet – with its client-server-based data infrastructure and centralized data management – has many unique points of failure, as we can see from the recurring data breaches of online service providers. It furthermore produces high costs of document handling, as well as non-transparencies along the supply chain of goods and services.



There are historic roots to these issues. We first had the computer, then the Internet was invented, which connected these stand-alone computers with each other through a data transmission protocol. In the early days of personal computers, we used to save data on a floppy disc, eject it, walk over to the person who needed the le, and copy the le onto their computer so they could use it. If that person was in another country, you would need to mail the oppy disc to them. The Internet and the emergence of the WWW put an end to this by providing a data transmission protocol – TCP/IP – that made the transfer of data faster and massively reduced the transaction costs of information exchange. Ten years later, the Internet became more mature and programmable. We saw the rise of the

so-called Web2, which brought us social media and e-commerce platforms. The Web2 revolutionized social interactions, bringing producers and consumers of information, goods, and services closer together, and allowed us to enjoy P2P interactions on a global scale, but always with a middleman: a platform acting as a trusted intermediary between two people who do not know or trust each other. While these platforms have done a fantastic job of creating a P2P economy, with a sophisticated content discovery and value settlement layer, they also dictate all rules of the transactions, and they control all data of their users.

The Internet we use today predominantly builds on the idea of the stand-alone computer. Data is centrally stored and managed on servers of trusted institutions. The data on these servers is protected by firewalls, and system administrators are needed to manage these servers and their firewalls. Trying to manipulate data on a server resembles breaking into a house, where security is provided by a fence and an alarm system.

In this context, blockchain seems to be a driving force of the next-generation Internet, what some refer to as the Web3. Blockchain reinvents the way data is stored and managed. It provides a unique set of data (a universal state layer) that is collectively managed. This unique state layer for the first time enables a value settlement layer for the Internet. It allows us to send files in a copy-protected way, enabling true P2P transactions without intermediaries, and it all started with the emergence of Bitcoin.

The Bitcoin blockchain and similar protocols are designed in a way that you would need to break into multiple houses around the globe simultaneously, which each have their own fence and alarm system, in order to breach them. This is possible but prohibitively expensive. In the Web3, data is stored in multiple copies of a P2P network. The management rules are formalized in the protocol and secured by majority consensus of all network participants, who are

incentivized with a native network token for their activities. Blockchain, as the backbone of the Web3, redefines the data structures in the backend of the Web, now that we live in a connected world. It introduces a governance layer that runs on top of the current Internet, that allows for two people who do not know or trust each other to reach and settle agreements over the Web.

The Flexio platform is a hybrid decentralized data processing architecture designed for secure, scalable management of online data storage, file sharing, document editing, user access, email, messaging and other cloud-based applications within businesses, enterprises, government organizations and for individual consumers. This decentralized technology designed by Flexio Inc utilizes Flexio Tokens (or FLEXs) to power an open source cyber-security platform benefitting all industries that are susceptible to cyber-security breaches including banking, finance, law, insurance, healthcare, transport, logistics, media, construction and government. This technology seeks to displace single source Cloud Storage Providers (CSPs), Cloud Access Security Brokers (CASBs), Cloud Security Gateways (CSGs), Storage Partitions, Anti-Virus Scanners, Threat Monitors and other security products. The Flexio ecosystem manages security for data-at-rest (storage), data-in-motion (email / chat / payments) and data- in-use (file editing / sharing / collaboration). The ecosystem is structured to provide scalable benefits and incentives for all participants to grow the security, integrity, financial competitiveness and performance of Flexio technology for the benefit of the Flexio token or FLEX value (and hence all its participants). Blockchain based networks that use a large number of consensus driven processing nodes are ideal for managing network security. However, they are not well suited for managing file storage and sharing applications because of the inherent latencies of the order of tens of seconds or more. Instead of storing files on a consensus-driven node structured blockchain network, the Flexio ecosystem uses a low latency, decentralized cloud platform with multiple dedicated cloud storage providers as file storage nodes. In addition to a decentralized multi-cloud platform for file storage, the hybrid ecosystem integrates a private blockchain platform for a secure immutable record of all user access sessions and file transactions. This

double-decentralized platform uses the Flexio digital token to drive all of its blockchain components, pay for its development, and generate revenues from its security and storage services. This design architecture meets the security, performance, compliance, speed, cost and usability requirements for managing all forms of confidential data between business enterprises, their employees and their customers. It also provides for the secure and cost-efficient transfer of confidential data between allied or federated enterprises and benefits individual consumers with free storage and security services.

2. BACKGROUND

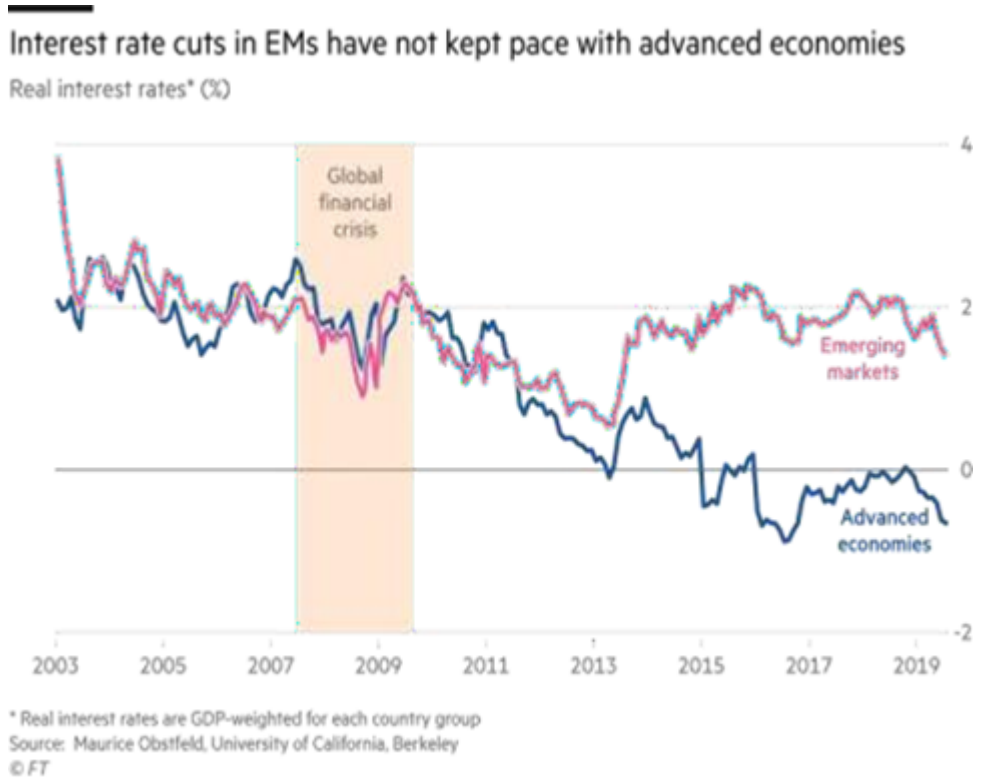
Since the Bitcoin whitepaper was published in 2009, researchers, entrepreneurs and investors have been trying to change the current fiat-money system and to create a digital currency that is decentralised, fair and easy to use. After years of development, the industry has evolved from digital cash to a vibrant ecosystem of decentralised applications. Noticeably, the term decentralised finance or open finance was brought to the market after the cryptocurrency bull run in 2017 and start to ramp up in volume in 2020. It broadly includes financial applications built using blockchain technology that are aimed to disrupt intermediaries in the traditional finance industry .

Decentralised finance (DeFi) changing FinTech

Decentralised money market protocols allow users to access high yield financial products without border

Global interest rates varies a lot across different markets. For instance, developed countries offer close to zero interest rates on saving accounts and that more complex financial market products are not accessible for average bank customers. However, it is hard to exploit different returns in the world of traditional finance due to restrictions in foreign currency exchange, account restrictions in equity markets and so on. As demonstrated in Graph 1, there are

significant gaps between the interest rate in emerging markets and advanced economies after the global financial crisis, and that both are exhibiting a downward trend.



Graph 1

With the growth of crypto market capitalisation and the number of users, offering financial services for crypto assets now makes sense for companies. We have witnessed a significant surge in assets locked in DeFi protocols. It has been an exciting movement for DeFi assets to cross the US$10 billion benchmark from less than US$1 billion in less than six months - it demonstrated that there is real demand from users and that the current blockchain networks could support relatively large-scale asset transactions.

Graph 2: Total Value Locked in DeFi quickly ramp up in the second half of 2020

Moreover, the interest rates offered for assets deposited in DeFi protocols are much higher than traditional fiat-based products because of vibrant trading opportunities in crypto. It is common to achieve APY above 6% through either centralised or decentralised service providers for holding in stablecoins.

3. INTRODUCTION

3.1 PROBLEM

Enterprises are increasingly storing more of their confidential data online via cloud storage vendors. They are also increasingly using online applications that run on the cloud to create, collect, manage, use and sell information for business management operations. The advantages of the cloud to any business or enterprise include greater employee mobility, reduced operational costs and the elimination of capital expenses for storage hardware. However the biggest risk, largest cost and major operational concern involved in migrating an enterprise to the cloud is security. While cloud storage costs may have dropped to very low commodity level pricing (around $5 - $10 per TB / user / month), enterprise-class security remains an expensive premium priced service (around $40 - $80 / user / month). Moreover, cloud security technologies are very incomplete and imperfect solutions. This explains why global cyber- security losses are now approaching $1 trillion annually despite a global cyber-security industry worth over $100

billion. Existing security technologies may act to reduce the risk of security breaches but they do not mitigate the risk entirely. Over time all cloud storage vendors will eventually be compromised, and all information stored by enterprises in the cloud will eventually be exposed to security breaches.

The fundamental weakness of existing cloud storage and enterprise security technologies lies in their centralized design architecture that relies on trusted third-party vendors. Every cloud storage vendor is vulnerable to cyber-security attacks, and once a security breach has been successfully achieved enormous amounts of confidential data can be readily stolen from a centralized network. We can identify the five main security threats to enterprise networks:

(1) External threats from remotely located syndicated hacker groups.

(2) Viral threats from malicious software programs such as viruses, malware and ransomware.

(3) Operational failure threats and denial of service attacks.

(4) Internal threats from bad actors, disgruntled employees.

(5) Surveillance intercept threats or man-in-the-middle attacks.

The total cost of a complete enterprise-class security solution for cloud applications can typically vary from between $40 and $80 / user / month and this is the major cost factor when determining cloud adoption strategy. Nonetheless, most large enterprises who adopt these conventional cloud security solutions will still suffer significant losses due to security breaches every year.

3.2 SOLUTION

In contrast to conventional centralized enterprise security and storage technologies, the Flexio platform presented here describes a decentralized data management architecture designed for highly secure, scalable control of data storage, data management, file sharing, file editing, user access, emails, and data compliance. While there exist other decentralized file storage platforms based on blockchain technology such as Sia and Filecoin, the hybrid Flexio platform

described here does not suffer the inherent latency problems of blockchain-only storage technologies. Existing blockchain storage technologies typically demonstrate large access latencies in excess of 10 – 20 seconds and as much as several minutes or more. This effectively makes real-time file management, data-in-use and data-in- motion applications too slow and unusable for multi-user enterprise environments. Hence existing blockchain-based file storage technologies are primarily focused on individual, libertarian minded public consumers who want to upload large files as opposed to large file numbers. Blockchain-only storage simply doesn't meet the security, performance, latency and usability requirements for enterprise customers.

Moreover, the Flexio ecosystem provides much more than a secure, usable, low-latency file storage platform for enterprise environments. It also manages user access control, file tracking / logging / auditing, email / chat security, internal threat monitoring, policy enforcement and industry / legal compliance. The ecosystem represents a simple, complete enterprise security and storage solution that protects a business, organization or enterprise against all five main cyber-security threats (or attack vectors) of migrating to the cloud. As a complete enterprise security and storage solution in a single product bundle for enterprise customers, the Flexio ecosystem can displace many conventional cyber-security and storage technologies.

The Flexio ecosystem incentivizes enterprise customers with a complete security solution, simpler deployment, easier management and lower overall costs. The platform addresses the security problem at the fundamental data storage level itself, thereby not requiring the complex, piecemeal, after- thought approaches of conventional security and storage solutions. Security encryption is written into the decentralized storage process for passive protection of file storage. There are also inherent benefits for the enterprises' customers (ie: the individual public consumer) with limited free storage and security services provided by the enterprise. The ecosystem further incentivizes the processing of information for FLEX token participants (or FLEX miners) with rewards for

verifying user ID, file uploads, file sharing, data integrity and secure user access sessions. It also incentivizes the open-source development of future platform features and encourages rapid trial and adoption by all customers. In terms of architecture, the hybrid platform consists of three different but complementary decentralized platforms integrated with a security engine and user-interface to form a complete security and storage solution.

3.2.1 HYBRID CLOUD COMPUTING

A hybrid cloud is a type of cloud computing that combines on-premises infrastructure—or a private cloud—with a public cloud. Hybrid clouds allow data and apps to move between the two environments.

Many organizations choose a hybrid cloud approach due to business imperatives such as meeting regulatory and data sovereignty requirements, taking full advantage of on-premises technology investment, or addressing low latency issues.

The hybrid cloud is evolving to include edge workloads as well. Edge computing brings the computing power of the cloud to IoT devices—closer to where the data resides. By moving workloads to the edge, devices spend less time communicating with the cloud, reducing latency, and they are even able to operate reliably in extended offline periods.

3.2.2 THE BENEFITS OF A HYBRID CLOUD PLATFORM

A hybrid cloud platform gives organizations many advantages—such as greater flexibility, more deployment options, security, compliance, and getting more value from their existing infrastructure. When computing and processing demand fluctuates, hybrid cloud computing gives businesses the ability to seamlessly scale up their on-premises infrastructure to the public cloud to handle any overflow—without giving third-party data centers access to the entirety of their data. Organizations gain the flexibility and innovation the public cloud provides by running certain workloads in the cloud while keeping highly sensitive data in their own datacenter to meet client needs or regulatory requirements.

This not only allows companies to scale computing resources— it also eliminates the need to make massive capital expenditures to handle short-term spikes in demand, as well as when the business needs to free up local resources for more sensitive data or

applications. Companies will pay only for resources they temporarily use instead of having to purchase, program, and maintain additional resources and equipment that could remain idle over long periods of time.

Advantages of the hybrid cloud:

Control—your organization can maintain a private infrastructure for sensitive assets or workloads that require low latency.
Flexibility—you can take advantage of additional resources in the public cloud when you need them.
Cost-effectiveness—with the ability to scale to the public cloud, you pay for extra computing power only when needed.
Ease—transitioning to the cloud doesn't have to be overwhelming because you can migrate gradually—phasing in workloads over time.

3.2.3 WHAT IS A PUBLIC CLOUD?

Public clouds are the most common type of cloud computing deployment. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the internet. With a public cloud, all hardware, software, and other supporting infrastructure are owned and managed by the cloud provider. Microsoft Azure is an example of a public cloud.

In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud "tenants," and you access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Advantages of public clouds:

Lower costs—no need to purchase hardware or software, and you pay only for the service you use.
No maintenance—your service provider provides the maintenance.
Near-unlimited scalability—on-demand resources are available to meet your business needs.
High reliability—a vast network of servers ensues against failure.

3.2.4 WHAT IS A PRIVATE CLOUD?

A private cloud consists of cloud computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization.

In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organizations with business-critical operations seeking enhanced control over their environment.

Advantages of a private cloud:

More flexibility—your organization can customize its cloud environment to meet specific business needs.
More control—resources are not shared with others, so higher levels of control and privacy are possible.
More scalability—private clouds often offer more scalability compared to on-premises infrastructure.

3.2.5 . FLEXIO SUMMARY

the Flexio platform comprises of a decentralized, multi-vendor cloud storage platform called VAULT for encrypted file storage and file sharing, a decentralized blockchain platform called NODE for immutable storage of all user access sessions and file transactions, a decentralized database map for storage of file encryption keys, transaction data and audit logs, a user control interface called FOLDER for managing file storage / sharing, security policies, user access and file permissions, and a central security engine and backend called CENTER for the integration of all platform components and the enforcement of security policies, user access controls, file settings, participant incentives and the Flexio Token ecosystem.

All three decentralized storage platforms (multi-cloud, blockchain and database) interact with each other via the CENTER security engine to perform complementary tasks for the benefit of all participants in the Flexio ecosystem. They also protect against different types of security threats in various manners to provide an enterprise customer with a complete data security and storage solution against all five potential security threats. In summary, the Flexio platform and FLEX ecosystem is a complete enterprise security and storage solution that leverages a viral network effect among

enterprises and their consumers to increase the adoption, performance, security and value of the platform for all participants.

4. TECHNICAL

4.1 TECHNICAL BACKGROUND AND CHALLENGES

While decentralized platforms offer significant potential benefits for enterprise customers and users in terms of security and scalable throughput, the exact design and size of a decentralized platform can dramatically affect numerous other product performance and usability characteristics for the user. Of particular relevance is how the type and number of storage nodes (or information processing nodes) can affect both the potential attack surface and access latency of the platform. In addition, migrating confidential data from a centralized architecture to a decentralized architecture should typically benefit enterprise customers in terms of cost-effectiveness. Despite the potential of improved platform security, widespread adoption of a decentralized security and storage platform is highly challenging unless there exists significant cost savings for the paying enterprise customer. Consequently, identifying the sweet spot in terms of node number, attack surface, latency and cost benefit is critical to the optimal design of a decentralized network solution.

4.2 LATENCY IN DECENTRALIZED SYSTEMS

Conventional centralized storage platforms such as Google Drive, Amazon S3 and iCloud and other content delivery networks exhibit very low access latency while still delivering reasonable throughput speeds for data upload and download. Access latency is an important performance and usability issue for real-time applications requiring the frequent upload, download and management of lots of small sized files (typically < 1MB). Online cloud-based applications such as file / folder management, file sharing and live editing generally demand access latencies no larger than a few hundred microseconds to be considered

usable in real-time. Regardless of the upload or download speed of a storage platform (ie: throughput), large multi-second access latencies can render real-time file storage, management and editing applications unusable for most users. Most consumers and users of cloud based storage platforms do not want to wait tens of seconds or more to initiate the upload of a small file that may take less than a second to upload via conventional cloud storage services. Consequently, existing centralized storage systems with high throughput and low latency are better suited to real-time online file storage, management and editing applications. They only suffer one major problem in that they exhibit large potential attack vectors and poor data security characteristics.

Conversely, decentralized blockchain storage platforms such as Sia and Filecoin are ideal for the upload or download of very large files and data payloads . Decentralized platforms can be configured to exhibit improved data security, throughput and download reliability compared to most centralized storage platforms, given their reduced potential for data bottlenecks or operational failures to interfere with data transfer operations. This is important when uploading or downloading large files and multi-file batch processing applications such as back-up storage drives. In this case the user does not typically mind waiting tens of seconds to initiate an upload or download process that may take tens of minutes or more to complete. Moreover, decentralized storage architectures can be designed to impart a high level of file security to the stored data. However, the large access latencies characteristic of

decentralized blockchain based platforms (typically 10-20 seconds or more) make them highly unsuitable for most individual online file management, sharing and editing applications. Furthermore, most enterprises require seamless fast management of all file storage, editing and sharing applications between hundreds or thousands of employees, clients and customers. Consequently, using a blockchain based storage platform in an enterprise environment becomes impractical and cumbersome for the user.

4.3 COST STRUCTURES FOR ENTERPRISE SECURITY AND STORAGE APPLICATIONS

Every business appreciates the value of data as it relates to competitive advantage. What is less appreciated is the value of relating through data to drive competitive advantage. Companies that understand this distinction, like Amazon, Netflix, Airbnb, are quickly displacing the leaders across many industries.

It is tempting to point to the more visible artifacts that have led to their success, such as adopting new tools, API and microservice infrastructures, and the DevOps practices that enable rapid iterative change. But underneath this is a different relationship to data than others. Data is not something orthogonal to application development. It is actually at the center of it.

In most companies, data infrastructure is built to manage the sharing and collaboration of data across different applications, services, analytics, and AI models. Companies talk about harnessing data exhaust through expensive new staging platforms such as data warehouses, data lakes, and even data lake houses. The fundamental problem with this approach is that data is considered almost as an afterthought that must be integrated, secured, cleaned, and wrangled to create value.

Some of the signs of this misalignment are the significant costs incurred on integration, security, and data engineering. IDC estimates enterprises spend about a third of their AI lifecycle time on data integration. Companies are burdening developers with more security-related development in response to the rise in API-related security incidents. One survey found that 91% of companies experienced an API security incident in 2020. Finally, companies are discovering they often need five data engineers for each data scientist to get the data into the form and location required for good data science.

Making the lead to data as collaboration requires a significant shift in mindset. However, organizations can ease this transition by addressing three key pillars of data as collaboration:

Factor in the effects of time through immutability;

Enforce identify and trust directly on the data; and

Adopt a shared vocabulary around data.

Factor in the effect of time through immutability

Time is an ephemeral quality that gets woven into data either on purpose or by accident. It is easy for developers to ignore this fact in the rush to get a new service running. But when time is not considered, applications can break in funny ways, data can get lost, and enterprises need to invest in complex data integration efforts.

Developers often gloss over how data might be used outside of their application context. For example, standard practice is to perform create, read, update, and delete operations on data. But important information about time is lost when data is simply updated or deleted. Ensuring data reuse requires addressing changes to data to ensure traceability across all applications.

Enforcing data immutability ensures that other applications have a consistent view of the individual account balance and bank portfolio reflected in audit statements, regulatory reports, and business analytics. Different variations of this problem can create challenging problems in microservice orchestration, intermittent failure, inconsistent report page layouts, and customer service

frustrations communicating about price changes. Data has many tentacles. If we do not understand the traceability of data, we will be at a disadvantage.

Reducing online storage costs is not the decisive factor for an enterprise because storage costs are relatively insignificant compared to the cost of deploying a complete security solution for file storage. It is important to note that while decentralized platforms offer greater protection against security breaches, this is only for protection against external threats and operational failures. Decentralization by itself does not offer any added security against internal, viral and surveillance threats. Of prime importance to all large enterprises and organizations is the ever-present security threat from internal sources (ie: employees) which is not typically an issue for individual consumers. To mitigate against internal, viral .

4.4 THE PROBLEM THAT FLEXIO SOLVES

Blockchains currently operate in silos, meaning they are incapable of interacting with one another, a limitation that can be regarded as one of the main hurdles to making the technology genuinely viable for mainstream adoption. An array of projects and platforms have been developed that attempt to solve this precise issue.

The majority of current efforts predominantly revolve around cross-chain token transfers (the ability to send a crypto asset from one blockchain to another), while overlooking one of the key value propositions of blockchain technology, smart contracts. Smart contracts are protocols on a decentralized network that are designed to execute according to the terms of an agreement. As smart contracts are relatively straightforward transactional protocols, and input results in a defined output, they offer the foundation upon which the decentralized services of the future can be built.

Currently smart contracts are limited to operating solely within the context of the blockchain on which they are deployed, whether that be Ethereum, Polkadot, Cardano or any other smart contract platform. This not only limits usability but also the number of users any smart contract application can serve, as well as fundamentally precluding connectivity between different blockchains. Flexio has been created to offer a solution to this problem.

5. FLEXIO PLATFORM ARCHITECTURE

Low cost cloud storage services for data-at-rest applications are a fundamental weakness for all conventional security solutions that are complex and expensive to deploy. Building a complete enterprise- class security solution must also incorporate cloud storage as a fundamental building block to ensure an optimal security profile. The design philosophy that underpins the hybrid Flexio architecture is based on optimizing specific characteristics of three different decentralized platforms to meet the varying multitude of critical performance requirements for both enterprise security and storage applications. Not every decentralized platform is ideal for every online application and it requires the integration of three different but complementary platforms to meet the broad performance and usability demands for a complete enterprise-class security and storage solution. Flexio digital tokens or FLEX are an essential ingredient that powers the entire Flexio platform architecture by:

· Enabling the three different decentralized storage platforms (VAULT, NODE and CENTRAL) to operate with each other and provide multiple layers of security,

· Allowing enterprise customers and individual users to purchase a complete range of security and storage services,

· Providing incentives for enterprise customers to initially trial and deploy security and storage services,

· Providing incentives for open source developers and alliance partners to support the FLEX ecosystem by developing an expanding range of compatible API and plug-in products,

The benefits for both enterprise and individual customers include :

(i) dramatic improvements in security profiles,

(ii) simpler trial and deployment of products via a single product solution,

(iii) lowers total operational costs for online security and storage.

6. FLEXIO TOKEN MANAGEMENT

Flexio will issue a native token in the network to facilitate decentralised governance and to bootstrap early users. The token economics are designed so that users could actively participate in trading, providing liquidity and also sharing the upside in network value growth.

Flexio digital tokens (ie: FLEXs) are essential to power the Flexio hybrid platform and allow each of the three decentralized platforms to communicate with each other to provide a complete, interoperable security and storage solution for the customer. Consequently, efficient management of the supply, demand and flow of FLEXs is critical for the scalable, profitable growth of the entire ecosystem according to fundamental crypto-economic principles.

6.1. Token Utility

● Decentralised governance

The design and implementation of the protocol would be determined by token holders. For parameters like pool staking fees, transaction fee burn, liquidity mining ratio are initially set by the protocol itself; token holders could update the numbers and the smart contract itself based on the voting process. In order to encourage users to participate in the process, there could be some profit set to reward the voting participants.

● User incentives

As a decentralised product, getting liquidity is crucial for the user experience and platform adoption. Therefore, a large proportion of the Flexio tokens are reserved to encourage users to add liquidity to the platform and to use the products. By depositing assets to the protocol, users could automatically market the protocol.

In designing the user incentives, the protocol also takes into consideration the long term sustainability of the token. As there are more liquidity mining programs launched by DeFi protocols, users tend to participate in those programs in order to earn tokens rather than to fulfil their true needs. In the meantime, as more tokens are generated, there is continuous selling pressure to the network if no strong use case is designed to create demand for the token. Therefore, in designing the liquidity mining program, priorities would be given to long term supporters and market makers for the protocol.

● Asset staking

Flexio tokens could be staked to participate in the base layer consensus and earn system rewards. It is also the staking currency to share platform revenue and ensure that the debt positions are safe.

6.2 Crypto-Economics and Token Value Analysis

The Flexio platform utilizes a viral crypto-economic model comprising two different but complementary business models for decentralized network architectures. The primary benefits of using a decentralized multi-cloud platform for file storage and sharing are low access latency, minimal attack surface, large scalability, high data resiliency and commodity level pricing from large trusted cloud storage vendors. This multi-cloud file storage platform encourages viral adoption via file sharing between enterprise employees and their external customers and clients .

The primary benefits of using a decentralized private blockchain platform for managing user access and file tracking / auditing activities are:

· Customizable permissioned access to a permanent immutable record of all user access and file sharing activities within an enterprise and between an enterprise and its customers,

· Initial user base to stimulate the initial trial and adoption of Flexio products and services via a supportive community of Alliance Partners, Open Source Developers and FLEX investors,

· Viral network effect that encourages the utility and exchange of FLEX tokens for security and storage services more than it encourages speculative investment in FLEX token value growth as listed on crypto-currency or token exchanges, and

· Inevitable long-term growth in FLEX value with increasing customer adoption by enterprise customers, regardless of short term speculative fluctuations in FLEX value from investors.

Critical to driving these benefits for the FLEX ecosystem .Furthermore, customers may pay for security and storage services with either FLEX. Moreover, this design

also encourages the large pre-purchase of FLEX tokens by customers to pay upfront for services over the long term.

The Flexio ecosystem is designed for high product utility that drives inevitable price increases in FLEX value over the long term, scaling directly with increasing customer adoption. No merchant adoption is required by the FLEX ecosystem and customer adoption is driven purely by the massive demand in the enterprise market for more secure, simpler and cheaper cloud storage and security products. Moreover, the manual injection of FLEX's into the ecosystem by the Flexio Foundation offers an efficient method for adjusting market liquidity in FLEX's to counter speculative volatility.

6.2 Token Distribution

There will be **500M FLEX** tokens at the launch of Flexio Network and it is a fixed token supply.

25% of the tokens will be distributed through token sales;

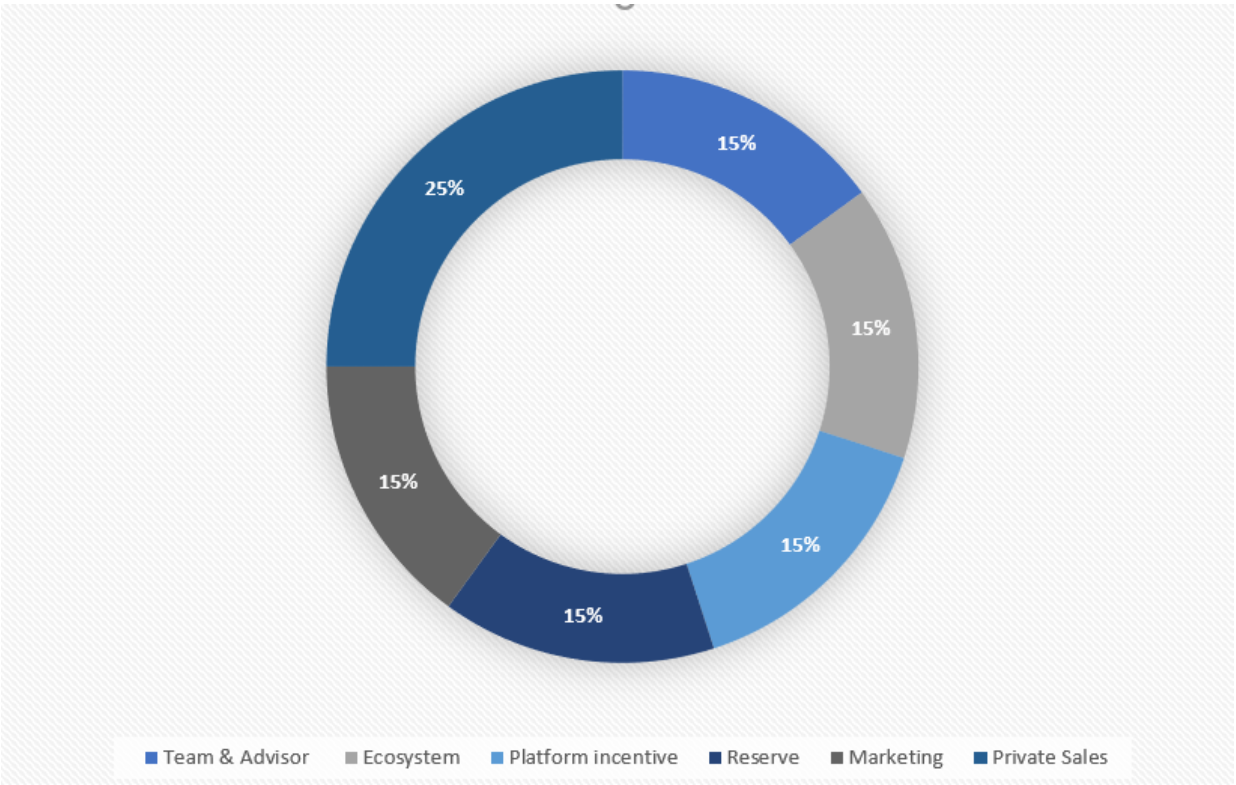
15% of the tokens will be used for marketing and linear vesting for 24 months;

15% of the tokens will be reserved for ecosystem development and partnerships;

15% of the token s will be reserved to the foundation and locked for 1 year;

15% of the token will be distributed through incentive plan to users who participate in the network;

15% will be reserved to teams and advisors who support the project.



6.3 Conclusions

A hybrid decentralized architecture for enterprise security and storage has been designed and described in detail. A simplified prototype version of the Flexio platform with limited user interface features has been built and tested for security performance and access latency behavior. Dramatic improvements in security profile and significant reductions in attack surfaces have been observed for the hybrid decentralized platform when compared with conventional centralized security and storage solutions. The platform also has exhibited low sub-second latencies for configurations that use 3 to 8 storage nodes. This is considerably more usable than the 10-20 second latencies of other blockchain storage platforms such as Sia and Filecoin (only suitable for long duration back-up applications) and enables real-time enterprise cloud applications such as secure file sharing, live editing and chat. The Flexio ecosystem also benefits from the viral network effect that occurs through token exchange and file sharing activities. Consequently, the hybrid architecture exhibits the security, performance, latency usability and cost-efficiency requirements for enterprise-class security and storage applications.

A token management ecosystem and token economy infrastructure has also been proposed that offers ever-increasing incentives over time to enterprise customers, individual consumers, digital currency miners, open-source developers, strategic alliance partners, token sales investors and Flexio shareholders. The financial viability of the architecture is underpinned by the common alignment of all participant incentives for increased FLEX payments and usage which will result in increased FLEX value. The more customers that adopt Flexio products the more the FLEX token will rise in scarcity and value. It will also provide a huge financial opportunity for FLEX investors, miners, vendors, alliance partners and open source developers. The Flexio platform architecture and token ecosystem promises a truly complete, scalable and cost-effective solution that solves the critical security and storage problems for tomorrow's businesses, enterprises and large organizations.