DISCLAIMER

This paper and any other documents published in association with this paper relate to the intended development and use of the Akropolis platform ("Akropolis platform"). They are for information purposes only and may be subject to change.

- **This paper describes a future project.** *This paper is draft, and subject to further legal and regulatory advice.* It contains forward-looking statements that are based on the beliefs of Akropolis Decentralized Ltd, a company incorporated in Gibraltar (company number: 116430) ("**Company**" or "**Akropolis**"), as well as certain assumptions made by and information available to the Company.

  The Akropolis platform, as envisaged in this paper is under development and is being constantly updated, including but not limited to key governance and technical features. The AKT and AIT tokens ("**Tokens**") involve and relate to the development and use of experimental platforms (software) and technologies that may not come to fruition or achieve the objectives specified in this paper.

  If and when the Akropolis platform is completed, it may differ significantly from the network set out in this paper. 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.

  Regulatory licences and/or approvals in respect of Akropolis platform are likely to be required in a number of relevant jurisdictions in which the Company intends to operate. It is not possible to guarantee, and the Company does not make any assurances, that any such licences or approvals will be obtained within a particular timeframe or at all. This means that the platform may not be available in certain markets, or at all. This could require fundamental restructuring of the platform and/or its unavailability. The Company intends to operate in full compliance with applicable laws and regulations and obtain the necessary licences and approvals in key markets.

- **No offer of regulated products.** The Tokens are 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. The Tokens do not represent equities, shares, units, royalties or rights to capital, profits, returns or income in the Akropolis platform or software or in the Company or any other company or intellectual property associated with the platform or any other public or private enterprise, corporation, foundation or other entity in any jurisdiction.

- **This paper is not advice.** This paper does not constitute advice to purchase AKT tokens. It must not be relied upon in connection with any contract or purchasing decision.

- **Risk warning.** The purchase of AKT tokens and participation in any token sale carries with it significant risks. Prior to purchasing AKT, you should carefully assess and take into account the risks, including those listed in any other documentation.

- **Views of the Company.** The views and opinions expressed in this paper are those of Akropolis 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 paper is based on sources considered reliable by the Company but there is no assurance as to their accuracy or completeness.

- **English is the authorised language of this paper.** This paper and related materials are issued in English only. Any translation is for reference purposes only and is not certified by the Company 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 paper, the English version prevails.

- **No third party affiliation or endorsements.** References in this paper 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.

DRAFT

AKROPOLIS: A GLOBAL BLOCKCHAIN PENSIONS INFRASTRUCTURE

ANASTASIA ANDRIANOVA, PAUL HAUNER,
DR. KRISTIAN MCDONALD, DR. ADRIAN MANNING, AND MEHDI ZEROUALI
TEAM@AKROPOLIS.IO

VERSION 1.0

Abstract. Globally, the pension industry is in urgent need of serious reforms. The global deficit between pension assets held and existing liabilities is projected to grow rapidly in coming decades and risks triggering a pension-induced global financial (and social) crisis. Furthermore, workplace changes are increasingly atomising the modern workforce whilst legislative agendas are transferring the burden of managing the pension deficit back onto the individual. Complex fee structures that lack transparency are further eroding the performance of pension funds and exacerbating the problem. The Akropolis platform aims to leverage decentralised technologies to deliver a transparent, accountable and portable pension infrastructure that provides services to meet the needs of the modern workforce. Industry participants such as Pension Funds and Fund Managers can benefit from reduced regulatory overheads, access to new (token-based) mechanisms of engaging with clients, and marketing/promotional opportunities derived from new (verifiable) reputation and ranking systems. Individual users gain from the improved visibility, auditability and portability of a blockchain-engaged pension platform that acts as a single source of pension truth for the individual. Furthermore, protocols for accountability and transparency incentivise good behaviour by institutional participants and reward individuals and/or institutions that reveal bad behaviours. The challenges facing the pension industry are non-trivial and intricate, yet they must be addressed. Akropolis believes that leveraging new decentralised technologies to empower the community to unite and tackle the pension problem offers the best hope for both rectifying existing systemic failures and building a sustainable future.

Akropolis (Greek, Ακροπολις): *a citadel or fortress, the defensive core of a city, a city within a city.*

Acknowledgements

We would like to acknowledge Ian Grigg, Jason Dehni, and Peter Robertson for the many valuable discussions and expert industry advice which has helped shape this work.

Preface

This paper introduces the first iteration of a novel solution to a complex problem. The authors' goal was to construct a document containing sufficient detail to enable an initial implementation-effort based on the content of the paper. However, it is understood that empirical testing and analysis undertaken throughout the implementation process will inevitably necessitate modifications to the envisioned specifications. Accordingly, one anticipates deviations from the structures and methods detailed herein. As such, the mechanisms and processes described in this document should not be considered as final nor binding — they represent a considered first iteration, informed by the current capacities and limitations of blockchain technologies, and the present understanding of the problem.

1. Introduction

The state of the global pension industry is rapidly deteriorating. Many pension programs around the globe are under-capitalised and are effectively drifting into insolvency. A global discrepancy between pension assets held and existing liabilities looms large as a major economic challenge, both for individuals, whose retirement will likely be under-funded, and the larger global economy, which must manage the fallout. Pension funds are increasingly overburdened by the stresses of increased life expectancies [1], global decreases in voluntary pension contributions [2], and decreasing ratios of active employees to retirees [3]. The dire state of the global pension industry is quantified by the global pension deficit, namely the gap between existing pension liabilities and assets held. This deficit is expected to grow faster than global GDP[1] [4] and to reach $400 trillion (or five times global GDP) by 2050 [5]. The scale of this astounding discrepancy has the potential to create a full-blown global financial crisis, and some authors argue that the severity of this crisis will exceed anything previously experienced [4, 5, 6, 7].

[1] Gross Domestic Product.

DRAFT

The systemic issues plaguing the pension industry are intricate and complex, though some key requirements of candidate solutions are readily articulated. Any solution aimed at addressing the pension crisis will need to support the current pension ecosystem, ensuring that upcoming retirees are not unduly punished for systemic failures. In addition, a viable pension protocol must be capable of supporting the growing needs of an aging population whilst simultaneously facilitating a global intergenerational transition to a new, economically sustainable system.

A new pension protocol must also recognize that workplaces and legislative agendas are rapidly changing. Whereas earlier generations could rely on the stability of a lifelong job within a single company or industry sector, the modern worker must navigate a completely different landscape. The workforce is being increasingly atomized, with workers frequently changing jobs (and even careers). Furthermore, the tendency towards freelancing and the sharing/gig economy has eroded many traditional mechanisms for building pension savings. Workers are also increasingly mobile, having to move between geographical locations and different legal jurisdictions, with very little, in the way of inter-jurisdictional support protocols, available to help the atomized worker accrue an adequate pension. Traditional pension structures, which rely on geographic or regional stability, and are often administered by the employer or state and lack the flexibility necessary to meet the modern worker's pension needs. In addition, as the discrepancy between pension assets and liabilities grows, states are increasingly liberalising pensions and/or increasing the retirement age, to both reduce pension liabilities and shift the burden of funding retirement back onto the individual. Thus, the pension protocol of the future must be capable of accommodating existing collective-based pension frameworks, in which individuals pool their resources collectively within state- or employer-defined pools, whilst also ushering in the transition to an individually-oriented pension framework compatible with changing workplace and legislative agendas. The modern worker requires a pension system that is compatible with the atomization imposed on workers by both the modern state and workplace.

In addition to the excess costs brought about by archaic systems, the pension industry suffers from a number of systemic problems such as poor visibility around fund management, unnecessarily complicated (and often hidden) fee structures, stringent portability limitations due to geographically localised fund management, and vast compliance regulations which, at times, are manually enforced. Moreover, the incentive structures between end-user investors, the pension funds to which they contribute, and the fund managers who oversee the underlying assets, are often egregiously misaligned.

From a technological perspective, there has been a plethora of recent developments relating to distributed and decentralised systems. The advent and subsequent interest in blockchain technology has radically altered the spectrum of research and developmental possibilities relating to decentralised systems. In addition to Bitcoin [8], the subsequent creation of Ethereum [9] ushered in the era of "Blockchain 2.0" technologies.

Ethereum introduced the Ethereum Virtual Machine (EVM), which enabled arbitrary calculations to be performed and verified on all nodes of a network, without the need for a centralised governing body. This development was not without limitations. As with most public, fully decentralised systems, Ethereum suffers from (a) scalability issues which, in-turn, limit transaction speeds; (b) game-theoretic incentives to break consensus;[2] (c) environmental concerns stemming from the underlying Proof of Work (PoW) consensus mechanism; and (d) limited privacy capabilities for concerned parties. A number of ongoing projects are aiming to rectify these limitations. For example, Raiden [10] and Plasma [11] both aim to tackle the scalability issues, and the concept of sharding [12] also promises significant advancements on this front. Casper [13, 14] is a Proof of Stake (PoS) mechanism aiming to address shortcomings of the current PoW consensus approach. Research into partial and fully homomorphic encryption schemes [15, 16], along with Zero Knowledge systems [17, 18, 19],[3] are being introduced to address the privacy limitations of public blockchains. This research is further supported by the so-called "Blockchain 3.0" technologies, which aim to link multiple blockchains together to form a mesh-like network. Projects such as Polkadot [20], AION [21], and Cosmos [22] fall into this category and show promise for building a relaying infrastructure capable of unifying various underlying blockchains. Despite their current limitations, these bleeding-edge technologies show great promise. Importantly, they have the potential to revolutionise many traditional industry sectors and the pension industry is no exception. In particular, the transparency, automaticity, and auditability of decentralized ledgers offers new tools for juggling the competing demands of workers, Pension Funds, and Fund Managers, whilst simultaneously ensuring the flexibility, accountability, and regulatory compliance required of a pension service.

Akropolis is a new pension platform that aims to unify recent technological advancements to create a long-term sustainable solution to the myriad of issues that plague the existing pension industry. The Akropolis platform aims to facilitate the transition from existing pension structures to an atomized, individually tailored pension protocol capable of meeting the needs of the modern worker. Demands of both legislators and the modern workforce are pressing individuals to bear greater responsibility for their own retirement outcomes. The Akropolis platform will

[2]External actors can spend resources to perform a 51% attack on the network, whilst shorting the internal currency to profit.

[3]The Ethereum community is actively working towards some Zero Knowledge solutions, which is evident by the cheapening of some elliptic curve operations in a recent hard fork to allow for their verification within a block.

DRAFT

provide a pension infrastructure capable of supporting the modern worker throughout their individual journey in an environment beholden to changing legislative demands and workplace conditions. Akropolis will work directly, and in conjunction with, current leading industry experts to iteratively design and build a platform that simultaneously supports the current pension ecosystem whilst facilitating the much needed inter-generational transition to a more robust retirement savings model.

Fundamentally, Akropolis is a global platform that seamlessly connects everyday users with a diverse range of experienced pension funds and fund managers. The distinguishing features of Akropolis include transparent fee structures, built-in regulatory compliance, stringent fund vetting and, most importantly, game-theoretic incentive structures that mitigate the excessive fees traditionally borne by users in the pension industry.

Akropolis will leverage the unique characteristics and advantages of blockchain technologies to underpin its technologically advanced pension platform. Specifically, Akropolis notes that (*i*) the blockchain's public, immutable ledger will improve visibility and audit trails relative to existing pension funds, whilst permitting mechanisms for maintaining a suitable level of privacy; (*ii*) the asymmetric key infrastructure utilised by blockchains for authentication will allow on-chain (off-platform) direct communication necessary to facilitate a global system (i.e., blockchain technologies readily support the global portability required of modern pension services); (*iii*) the blockchain's decentralised processing capabilities permit the development of decentralised on-chain processes to handle compliance and provide transparent fee structures, whilst also permitting the construction of crypto-economic incentive mechanisms to re-align disjoint incentive structures in traditional pension schemes. Finally, it is also noted that slower transaction times, often experienced in a blockchain environment, are not problematic for a pension platform - typical transaction timescales in the pension sector do not possess the time-sensitivity of, e.g., infrastructure supporting high frequency trading algorithms.

The forthcoming pension crisis represents a complex and difficult problem. While the utilisation of blockchain technology is not a cure-all for the industry, it is clear that emerging technologies offer new solutions to the challenges faced by the pension sector. Akropolis is partnering with leading experts in the pension industry and leading blockchain projects to tackle the global pension crisis as a community. The goal of the Akropolis project is to leverage new technologies to develop a transparent, accountable and portable pension infrastructure capable of delivering sustainable pensions that meet the needs of the modern workforce, while acknowledging and accommodating the realistic constraints imposed by existing legacy systems.

This paper outlines the Akropolis platform, its vision for the future and the complications within the pension industry it aims to remedy. The paper is organized as follows. Section 2 gives a high level overview of the Akropolis platform, detailing its major components and their connections, and highlighting the benefits of the platform compared to current legacy systems. The sections following, provide extended detail into selected core components of the Akropolis platform before concluding with a brief summary of the project and its future direction. A glossary of key terms and acronyms appears in the Appendix.

2. The Akropolis Platform

2.1. Overview

The ultimate aspiration of Akropolis is to develop a decentralised pension platform (or more abstractly, protocol) that spans a variety of blockchains and delivers trustless retirement savings products. The goal is to leverage recent technological developments and offer transparent, accountable, and portable pension services for the modern worker. Due to the infancy of the technologies surrounding decentralised systems,[4] this goal will necessarily be attained in progressive stages, paralleling technological advancements in the space. Consequently the initial implementation of the Akropolis protocol, as described in this white paper, will be a hybrid of decentralised components managed by a centralised trusted entity, which we refer to as the Akropolis Foundation.

The platform will initially be built on Ethereum [9], as this is the most appropriate currently-operational chain to supply the service features required of a pension platform. However, the ultimate goal of Akropolis is to be a blockchain-agnostic pension provider that utilises the most efficient and appropriate technologies to deliver the required services and features. This may entail non-Ethereum based decentralised chains such as EOS [23], Cardano [24] and RSK [25]. The blockchain-agnostic goal aligns with the principles of various *Blockchain 3.0* technologies (such as Polkadot) which could ultimately be the core underlying technology used for a multi-chain Akropolis platform. It is probable that Ethereum will continue to play a role in the long-term implementation of Akropolis, however, it is important to emphasise that Akropolis' priority is to deliver sustainable, reliable pension products. Accordingly, choices regarding specific technological implementations will necessarily be informed by the needs of pensioners rather than adherence to specific technologies. Ultimately Akropolis is focused on delivering a product to the market that meets users' needs and developmental decisions will be made with this goal in mind. Nonetheless, throughout this paper it is assumed that Ethereum will underpin (at least) the early phases of Akropolis and future references to blockchain implementations in this paper will assume Ethereum as the underlying chain.

[4]Specifically issues of scaling, availability of cost-effective decentralised oracles, and stability of decentralised stable coins.

DRAFT

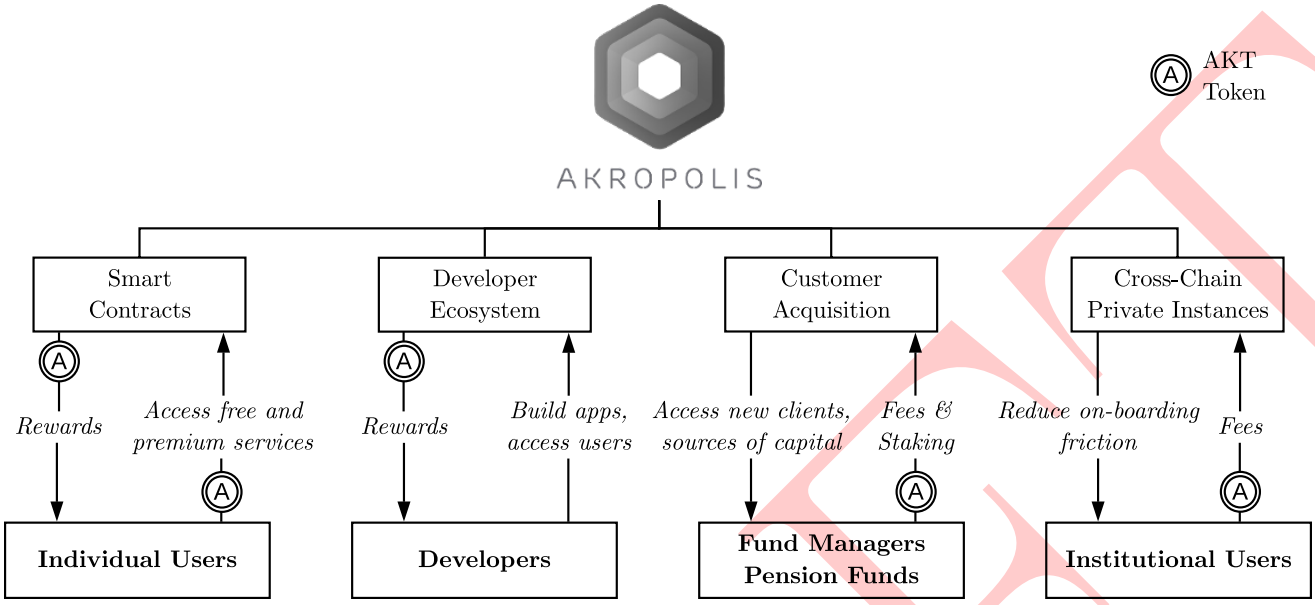

FIGURE 1. Institutional users access valuable data from the Akropolis system, while individual users are rewarded directly. Rewarding opportunities are created for both institutional funds and developers alike.

The Akropolis platform provides an efficient gateway between both individual users and institutional pension funds, and the fund/asset managers who traditionally manage pension investments (as shown diagrammatically in Figure 1). The fund/asset manager's conduct on the system is enforced through a number of incentive mechanisms to obtain an optimal outcome for all participants. FMs, who invest on behalf of individual and institutional clients, build a portfolio of assets which are tokenised on the blockchain and distributed to investors. Investors then maintain a global, portable, on-chain portfolio which represents their pension investments. The tokenisation of value within this system allows Akropolis to leverage blockchain technologies to automatically enforce various compliance rules specialised to specific assets and geographic regions. Incentive structures incorporated into the platform will also be built on-chain, though it will be necessary for dispute resolution mechanisms and procedures to initially be managed centrally by the Akropolis Foundation. This arrangement will act as a stepping stone and future implementations will aim to decentralise these dispute resolution components, to the extent that this is compatible with regulatory demands.

Importantly, although an individual user will have a single account that is tied to their identity, the totality of the user's on-chain operations will not be tied directly to a single identity/address/public key. Instead, the user's transactions will be pseudo-anonymous, similar to identities on various cryptocurrency systems, such that each new transaction and/or class of transaction is tied to different addresses generated by a single seed[5].

Blockchain technologies are oft espoused for the privacy they afford users and Akropolis' philosophy with regard to user's data errs in favour of the individual's right to privacy. Akropolis will seek to ensure that data ownership is rightfully granted to the individual user. However, given the capacity for users to leverage their data to access products that better suit their needs, or to acquire rewards (i..e., pension top-ups), the Akropolis platform will provide options that permit voluntary participants to allow agents of their choosing to access various aspect of their private data. Data can be exchanged for tokenised rewards that will further strengthen the individuals net pension position.

In summary, the Akropolis platform is a hybridised trust/trustless system that acts as a gateway between users, Pension Funds and Fund Managers. The platform seeks to re-align the incentive structures between agents in the pension sector, while leveraging the accountability afforded by blockchain technologies to deliver transparent pension products.

2.2. Platform Agents

The present section details the main agents that participate in the Akropolis system. An overview diagram summarising the actors and their interactions appears in Figure 2.

Individual User — The individual user (referred to in this paper simply as a *user*) represents a singular, non-institutional individual who uses the Akropolis platform for their pension savings. More abstractly, when discussing elements on the blockchain, a user refers to a

[5]Typically wallets of Unspent Transaction Output (UTXO) blockchains, such as Bitcoin, have this behaviour.

DRAFT

singular identity which is mapped to a collection of public keys via a generating seed.

Pension Funds (PFs) — Pension Funds are institutional entities that may (or may not) currently exist in the pension industry and who maintain their own platform and collection of users. These institutional funds will act similarly to individual users on the Akropolis platform.

Fund Managers (FMs) — Fund Managers are institutional entities charged with purchasing or acquiring assets on behalf of users and/or PFs. They must undergo stringent vetting processes to obtain access to the Akropolis platform and must regularly report on the assets under their management.

Asset Tokenisers — Assets procured on the Akropolis platform must be tokenised in order for the decentralised components of the system to function effectively. Asset Tokenisers hold assets, either directly or through verifiable third parties, whilst minting and distributing tokens which represent a share of the held asset. These are centralized entities that provide a source of truth to the blockchain layer (through the minting of tokens) and as such are key actors in the trust model of Akropolis.

Developers — Developers are community members who contribute to the Akropolis platform, building extended/advanced services for pension users.

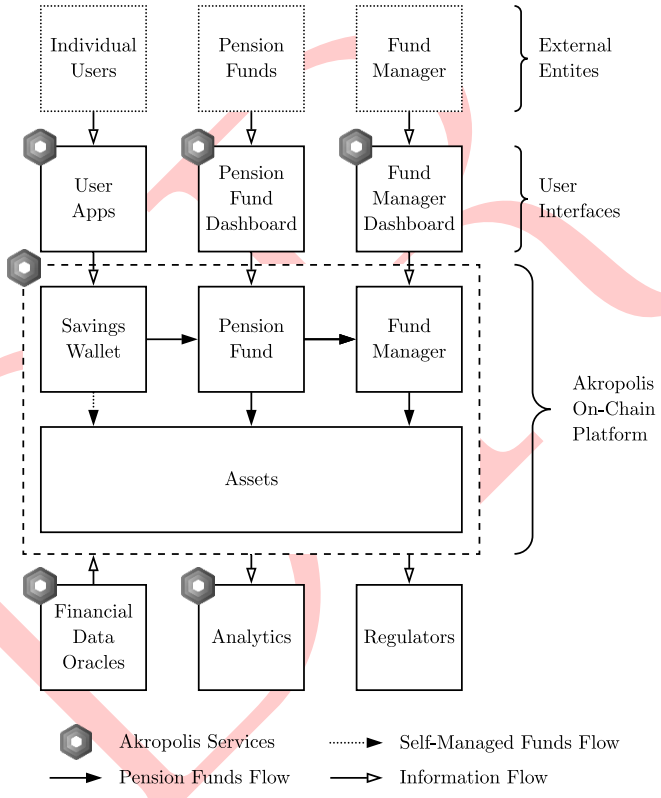

FIGURE 2. Akropolis component overview, detailing information and capital flow.

2.3. Benefits of the Akropolis Platform

The Akropolis platform provides benefits for individual users, who create and manage pension accounts on the platform, and for Pension Funds (PFs), who manage large numbers of pension accounts on behalf of individual clients. Fund Managers (FMs), who manage assets and supply pension products to PFs, also stand to reap benefits by participating in the platform. The present section outlines the features and benefits of the Akropolis platform for these different classes of participants. More details regarding these features are elaborated in the sections that follow.

2.3.1. User Motivations

From the perspective of individual users/workers, the motivation for Akropolis follows from three key observations:

- Firstly, many PFs around the globe are undercapitalised relative to their liabilities.
- Secondly, to avoid further amplifying the discrepancy between assets held and liabilities, state- and employee-operated pension schemes are increasingly pursuing systemic changes that transfer the liability for funding retirement expenses onto the individual (as manifest by, e.g., the tendency for pension liberalisation).
- Thirdly, changes in workplaces and working conditions, as manifest by the sharing/gig economy, freelancing, and the increase in global workforce mobility, mean individuals are increasingly self-employed, engaged in short-term employment, and/or working transiently in geographic regions subject to varying regulatory requirements. These changes further exacerbate the problems with existing pension models, which typically rely on employment and/or regional stability.

Thus, the individual worker finds themselves increasingly responsible for navigating a career that involves a series of short-term employment engagements, often in geographically diverse locations, while simultaneously bearing a greater responsibility for procuring adequate savings to fund a reasonable quality of life in retirement. The individual is now, more than ever, a global citizen who cannot rely upon their employer nor the state to guarantee a satisfactory quality of life in retirement.

The individual requires a pension system allowing them to collect and assemble pension savings accrued from multiple employers, in combination with voluntary contributions, both of which may be obtained in diverse jurisdictions. If the individual is to be responsible for funding their own retirement, they require a system with (a) sufficient flexibility to easily function in accordance with the demands of their working life; (b) sufficient regulatory compliance to support this flexibility; and (c) sufficient transparency to permit informed fund allocation decisions,

DRAFT

despite the absence of traditional workplace/lifestyle stability, whilst minimising the mental transaction costs [26] associated with proactive pension engagement.

The Akropolis platform is designed to meet these needs by delivering a flexible, regulatory compliant, transparent and accountable pension protocol. The goal is to construct a central source of pension truth for the individual, namely a single account, attached to their identity, which contains detailed information on their existing pension accounts, manages their voluntary contributions, and provides options to allocate savings to PF products. All PFs will be governed by strict transparency and accountability rules, enforced by blockchain-supported technologies. Future iterations of the platform will aim to support self-managed pension products (e.g., support direct user-FM engagement). This functionality is not an initial priority, however, as only a tiny minority of individual users are likely to possess the motivation and/or expertise to self-manage their holdings.

2.3.2. User Benefits

In addition to the general features described above, the blockchain-based Akropolis platform will offer individual users the following improvements relative to existing pension systems:

- Secure and immutable pension records, transparent record management and ease of auditing with real-time feedback.
- A decentralized, portable, single source of pension truth.
- Capacity to leverage smart contracts for secure peer-to-peer lending (e.g., family members can send *pension contribution coins* to younger adults, which can be used to acquire pension products that remain locked within the platform for designated time periods).
- The ability for users to monetize their own data.
- Transparency of governance protocols and outcomes (e.g., avoids difficulties with fund seizures encountered in Poland, Hungary and Argentina).
- Common protocols for fee and performance reporting.
- Incentivised accountability and ranking mechanisms for PFs to showcase good actors and filter out bad actors (acts to revert misaligned interests in the current system).
- Modern products and services that meet the needs of a generation that is familiar with real-time data and feedback (i.e., supersedes outdated legacy systems)
- New capital pools, such as cryptocurrencies. Users can incorporate cryptocurrency assets into their pension portfolio with options to time-lock the assets within smart contracts until the user reaches a pension age. Akropolis will advocate for regulatory changes that provide crypto-assets (held in verifiable time-locked pension contracts) with the same tax benefits afforded to traditional pension investment assets.
- In-built global automated compliance.
- Singular onboarding event.
- Simplified proxy voting with end-to-end accountability.
- Certificate-like global standard of FMs.

2.3.3. Pension Fund Benefits

PFs also benefit from joining the Akropolis platform. The current pension system is rife with regulatory and compliance overhead expenses, relating to auditing requirements, system development and administration and monitoring of relationships with FMs. Furthermore, the relation between FMs and PFs is fraught with transparency issues and often mediated by middlemen who erode the value of pension returns. The Akropolis platform will deliver the following benefits for PFs:

- Easy verification of document authenticity by counterparties.
- Singular onboarding event.
- Able to engage multiple pre-vetted FMs, with full regulatory compliance, from a single platform (avoids burdensome regulatory overhead that is rampant in the present system).
- Simplified internal administration and reduced reporting overheads.
- Improved transparency in relationships with FMs.
  - Transparency of fee structures.
  - Blockchain auditability.
  - Well-defined terms/conditions of services, independently verifiable.
- Reduced inefficiencies with platform integration and middlemen.
  - Eliminates intermediaries, allowing direct investment in assets.
  - Unified infrastructure for frictionless engagement.
  - Blockchain-enabled triggering of direct payment and asset movements.
- Alleviates redundancies in IT infrastructure across PFs and compliance expenses for engaging new FMs.
  - Blockchain-based common infrastructure with access to pre-vetted FMs
- Tamper-proof data storage that provides an independently verifiable source of truth.
  - Reduces costs of compliance reporting and the need for external audit trails.

2.3.4. Fund Manager Benefits

The Akropolis platform also offers benefits to FMs:

- Quality verification. Good actors will have a source of truth to verify their good behaviour and the quality and reliability of products they supply.

DRAFT

- Simplified onboarding. Joining the platform requires a single onboarding event. Thus, the need to establish regulatory-compliant relationships with each individual client PF and/or individual is ameliorated.
- Access to many clients. The single onboarding event provides FMs with access to multiple PFs and individuals to whom they can deliver services and products.

2.4. Akropolis Tokens

There are two main tokens within the Akropolis platform. The AKropolis external Token (AKT) and the Akropolis Internal Token (AIT). The former primarily facilitates functions of external users participating with the system, whereas the latter abstractly represents a stable coin and accounting mechanism to track and record capital flow internally within the system.

2.4.1. The Akropolis External Token

The Akropolis external token is a fixed-supply token whose value is subject to market forces. AKTs can be used for the following operations:

- Onboarding and platform access (see Onboarding/Vetting)
- Purchase premium services on the platform (see Premium Services)
- Purchase platform data (see Akropolis Platform Data)
- Stake in various platform incentive mechanisms (see Incentive Structures)

A key function of the Akropolis External Token is to serve as an onboarding utility token that allows participants to access the Akropolis platform. However, by default, the platform will operate on a freemium model, meaning that individual users can interact with the system without requiring AKT tokens. All underlying blockchain operations and system expenses relating to the basic operations of the freemium model will be paid for by the Akropolis Foundation. This model is adopted to ensure that all individual users can access the platform, consistent with Akropolis' desire to develop a pension platform to meet the needs of a global community of workers. Individual users will also have access to a number of extended services offered on the platform (see Premium Services), though access to the premium features will require AKTs. We note that a mechanism is required to decouple the price of the volatile AKT to the fixed stable cost of services on the platform. In the initial implementation, a trusted price oracle[6] will perform this task.

As the platform matures, users' data will accrue both on and off chain[7]. This data will be valuable to a variety of external agencies and options will be available to monetise the data (i.e., receive rewards for delivering data access), for the users' benefit (see Akropolis Platform Data for further details). Users that opt-in to share selected aspects of their data will be rewarded in AKTs.

Various incentive structures are outlined in the Incentive Structures section. These require the staking of a value-store in order to incentivize good behaviours by actors within the system. One could use the AKT as a staking token, however, this exposes platform participants to unnecessary volatility risk - good actors, whose stake is returned in full, may be punished if AKT market volatility pushes the value of AKTs in unfavourable directions on timescales comparable to the staking period. An incentivization mechanism that unduly punishes good actors is unlikely to prove successful as many platform actors will be risk-averse. Thus, demanding that staking-based incentivization mechanisms do not create undue volatility risk for good actors necessitates the introduction of a stable token.

2.4.2. The Akropolis Internal Token

The Akropolis Internal Token (AIT) is an independent token which abstractly represents an arbitrary stable coin. Due to the long-term nature of staking, this token is required to give participants a volatile-free option when engaging the staking incentive mechanisms (i.e., staking in AKTs would subject a staking entity to undue volatility risks which would undermine the efficacy of the staking mechanism). AITs also serve as an accounting bookkeeping tool within the Akropolis system. User's funds are represented digitally by AITs (i.e., users acquire AITs after depositing funds into the system) which can be converted to other tokens that represent ownership in different asset classes. AITs can be exchanged for both cryptocurrency and fiat deposits, and fundamentally act as an internal accounting tool whose audit trail lies on the public blockchain.

The AITs are entirely independent from the AKTs (i.e., Akropolis uses a decoupled two-token system). Akropolis opted for a decoupled two-token system as an investigation of existing coupled two-token systems revealed inherent weaknesses. For example, some systems use two coupled tokens, with one (volatile) token used to access the platform, and a second (stable) token that is pegged to some real-world value store (like a fiat currency). Furthermore, the volatile access token is converted into stable tokens upon entry into the system (i.e., stable tokens are generated by conversion of volatile tokens, which 'couples' the tokens). Any such coupling necessarily entails collateralisation of some form to mitigate against the volatility of the stable token. Collateralised coupled two-token systems have an inherent risk relating to under-collateralisation in the event of strongly unfavourable moves in the value of the token. These risks are systemic, in the sense that the viability of a platform based on such a system could be

[6] A service that sets the price of AKTs relative to a fixed fiat currency which is used to statically price services (in fiat values) on the blockchain.

[7] For privacy concerns, see the Privacy section.

DRAFT

cast into doubt in the face of highly unfavourable volatility. Systemic volatility risks are unacceptable for a pension platform (and, one could argue, for other existing use cases) and, accordingly, Akropolis adopted a decoupled model for AKTs and AITs.

2.5. Incentive Structures

A core economic principle of the Akropolis platform is to better align the incentives of all actors within the current pension system. Specifically, Akropolis attempts to converge on the idyllic case that fund managers act reputably and reliably on behalf of investors while receiving a transparent and reasonable fee for their service. Three main mechanisms will be initially deployed in an effort to realise the idyllic scenario.

2.5.1. Onboarding/Vetting

Pension products demand a certain type and calibre of institutional fund management. This is one of the key properties that distinguishes a pension-related platform from an arbitrary marketplace of fund managers. As such, it is vital that the Akropolis onboarding and compliance processes, which dictate who is allowed to manage and advise users' funds on the Akropolis platform, are not only thorough but also align with pension-based regulatory frameworks for relevant jurisdictions.

Akropolis proposes an onboarding/vetting system that requires candidate FMs to stake AIT or AKT. The staked tokens will be held for the duration of the FMs engagement with the Akropolis system. To be commercially viable, it is envisioned that this stake should be proportional to traditional cost funds must pay to adhere to standard compliance and regulatory demands during their engagements with clients; i.e., the FM stakes tokens once and gains access to multiple PFs and individual users, alleviating the need to repeatedly incur administrative and regulatory overheads when engaging new clients. The overall goal of this staking mechanism is two-fold:

(1) To provide a barrier of entry for funds applying to participate in the system, to avoid excess costs in vetting un-suitable fund applicants.
(2) To enforce reputable behaviour once acting within the platform.

The first point is intended to mimic the logic and behaviour of a token curated registry (see the Token Curated Registries section). Although the initial implementation will be managed by a centralised Akropolis Foundation, it is anticipated that, as elements of the platform transition to a more decentralised structure, this mechanism will be replaced by a suitable (proven) token curated registry.

The second point is to discourage participant FMs from acting against the interests of pension holders in ways that may occur in traditional pension schemes. In particular, the onboarding system aims to actively discourage the following behaviours:

- Off-mandate investments
- Fraud of various degrees
- Misleading or missing information regarding investment/asset status and/or management

To achieve these goals, a set of slashing conditions will be employed, such that bad-actors of the system lose all or portions of their stake when any or all of the above behaviours are demonstrated. The exact set of conditions to enforce these behaviours requires careful analysis and simulation. Such studies will be published as the project develops.

The size of the onboarding stake initially supplied by FMs will be bound from below (i.e., a mandatory minimum stake size will be specified) and asymptotically bound from above (i.e., a maximum stake), allowing the staker to select a value in between. It is anticipated that the size of the stake provided by an FM will act as a quantitative measure of the FMs commitment to the principles of transparent and accountable pension fund management advocated by Akropolis. In essence, the stake demonstrates the extent to which the FM "backs them self" to comply with the transparency requirements of the platform. Akropolis has a built-in reputation-based system (see Ranking and Reputation) which ranks/compares funds on offer. As such, the amount of stake a fund manager is willing to contribute will feed into the reputation system, in a transparent way, and reflect the FM's degree of commitment to behaving reputably on the platform. More formally,

$$S_L \leq S(\omega) \leq S_U : 0 \leq \omega \leq 1,$$

with

$$S(0) = S_L, \text{ and } S(1) = S_U,$$

where S_L and S_U denote the lower and upper fixed staking bounds, respectively, $S(\omega)$ denotes the stake a FM wishes to contribute, and $\omega \in [0, 1]$ serves as a quantitative measure of the FM's commitment to upholding the values of the Akropolis platform. Further, the parameter ω can be fed into the ranking system. We expect $S(\omega)$ to be non-linear with respect to ω, taking a form akin to $\tanh(x)$, which should shift the FM distribution toward a normal distribution.

2.5.2. Asset Reporting

As with traditional systems, fund managers will be required to regularly report on the state of their asset portfolio. The Akropolis platform will incorporate protocols to incentivise accountable reporting by FMs (see the Incentivised Accountability section). FMs will be able to stake tokens as part of the reporting process, with the stake serving as a bounty for individuals/entities able to demonstrate falsities within the report. Similar to the onboarding stake, the amount staked by FMs during reporting may be optional but will serve to represent the FMs confidence in, and commitment to, the validity of their report. This information will naturally feed into the reputation and ranking system of the fund (see Ranking and Reputation).

DRAFT

The staking mechanism is designed to encourage a new class of (potentially anonymous) actors who can profit by demonstrating the existence of inconsistencies in a fund report. These actors must provide supporting evidence to verify their claims, either in the form of documentation that demonstrates wrongdoing (i.e., whistle-blowers) or a detailed analysis that demonstrates falsities in the report. A more formal discussion of this mechanism is deferred to the section titled Incentivised Accountability. The key point is that tokens staked by a fund during reporting will be partially dispersed to any actors able to prove (more practically, convince a set of stakeholders) that the report is misleading, inaccurate or invalid. Funds are incentivised to participate in the staking process as good behaviour is rewarded by reputation points that can be used for marketing and promotional purposes within the platform (and, in principle, for external marketing).

2.5.3. Ranking and Reputation

Any actor managing funds/assets on the Akropolis platform must be extensively reviewed to comply with both internal platform standards and all relevant laws and regulations. In addition to ensuring platform users that all FMs engaged with the platform are regulatory compliant, Akropolis also provides a ranking system for FMs on the system. Expected performance, actual performance relative to expect performance and other measures allow the construction of a single overall ranking for all funds on the platform. Additionally, more-detailed rankings, that incorporate factors such as reputation, ethical policies, relative risk-profiles etc., will also be available, allowing users to categorize funds based on a variety of metrics (see the Ranking section for an in-depth discussion). Ultimately the ranking score will be representative of how reliable (i.e. How often a fund meets it's own targets and how much it's willing to stake to be reputable) and trustworthy Funds are on the platform.

The overall rating given by Akropolis will likely feed in a number of fundamental metrics, such as track record of meeting expected returns, size of onboarding stake, amount staked during reporting periods and relative performance compared to other funds. Ultimately, it is envisaged that a high Akropolis rating could provide a type of universal gold-standard for pension-based fund/asset managers.

2.6. Asset Tokenisation

A blockchain-engaged pension protocol offers new ways to provide transparent auditing trails for pension holders, PFs and FMs. Excluding cryptocurrency assets, value-stores held as part of a pension portfolio generally map to real-world assets such as precious metals, fiat currencies, properties, or businesses. Real-world assets need to be tokenised in order to be represented within a blockchain protocol. Thus, it will be necessary to tokenise various assets to provide a digital record of user's pension holdings.

Initially, it is envisioned that users will acquire AITs after depositing funds into the system. These AITs can be used to acquire tokens representing various pension products provided by PFs. The initial phases will see a small number of options available, aimed primarily at unsophisticated investors, with a greater range of products being incorporated over time.

Token ownership entitles a user to the underlying assets but also gives access to services, features and products offered by PFs. For example, data feeds specifying asset performance, marketing material related to the given asset class, or information regarding better-performing assets, will be available to users (if they opt-in to receive it). Thus, the token permits new ways of client engagement, such as reward schemes and other benefits, all of which can be accessed with a transparent, independently verifiable audit trail.

Future implementations of the Akropolis platform will include more options for sophisticated investors and individualised pension products, including a larger and diverse range of tokenised asset classes. Regulatory and practical requirements will require different degrees of central oversight for the diverse range of asset classes, though Akropolis' long-term vision is to decentralise as much of the process as possible (see the Future Directions section for more discussion).

2.7. Blockchain Wallet, Asset Ownership and Identity

Decentralised identity, key management, and recovery are very popular and active areas of research and development in the blockchain community (an example of a mature project in this space is uPort [27]). Akropolis intends to eventually integrate with decentralised identity platforms, such as UPort, however, due to the sensitive nature of data that Akropolis will need to maintain, the initial implementation will operate a traditional centralised database maintained by the Akropolis Foundation.

Identity and KYC[8] information, along with all personal data, will be stored off-chain and maintained by the centralised Akropolis entity. User's monetary transactions and asset holdings will be stored on-chain. Each user will possess their own blockchain wallet (and associated private key(s)), which cryptographically verify ownership of all assets in their holdings. Technically, a user's wallet will actually correspond to a collection of Ethereum addresses, generated from a private seed, for new transactions on the platform (see the Privacy section for further details). For KYC and AML[9] purposes, each newly generated address will be registered with the centralised Akropolis database. Thus, Akropolis also maintains a database that maps users to their public keys on the blockchain. We note

[8]Know Your Customer.
[9]Anti money laundering.

DRAFT

that this measure of pseudo-anonymity has many caveats whose discussion is left for the Privacy section.

2.8. Key/Asset Recovery

No pension platform will be successful if it is possible for a user to lose their life savings simply because they forget/lose their authentication credentials. This topic poses some slight contention with the use of decentralised systems, which typically offer no recourse against lost keys.

Akropolis will mitigate this issue. One possible resolution is to offer users the ability to split their wallet secret (more technically, the seed that generates the series of Ethereum private keys) into n pieces amongst friends and family, such that k pieces are required to recover the secret. Processes that facilitate this practice are well-known; for example, Shamir's secret sharing [28], and the promising blockchain-focused project Tenzorum [29], offer possible implementations.

Ultimately, and as a last resort, Akropolis can utilise the centralisation aspects of asset tokenisers to re-assign assets to new wallets for users who have unrecoverable wallets. Such a re-issuance is in principle feasible, as the Akropolis Foundation holds a central database of users' asset holdings. In practice, Akropolis will not have the control/ability to re-assign assets but, as a trusted entity, Akropolis can submit requests to individual asset tokenisers to re-assign the specific assets/holdings to ensure a user's account is entirely recoverable.

2.9. Platform Developers

The lifespan of the Akropolis platform will require constant development as it transitions to its final decentralised state. For this reason, the Akropolis platform will retain a reserve fund of AKTs to incentivise community development. The contributing developers will assist with extending services and features available on the platform, through development on the underlying blockchain layer, or, the application stack above. As such, their contributions will be rewarded in AKTs from the reserved development fund.

2.10. Akropolis Platform Data

There are two major classifications of data that exist in the Akropolis platform. Data that is public (i.e., put on the public blockchain and visible to the world, known as "on-chain" data) and data that is private (i.e., stored privately and securely by the central Akropolis Foundation, known as "off-chain" data). A deeper classification and discussion of these are given in the Data Model section below.

When users join the Akropolis system, they may opt-in to complete a financial profiling questionnaire, which will be undertaken entirely off-chain (private) and the data will be stored by the Akropolis Foundation[10]. Financial profiling data will be used to help users access funds and pension products that best suit their risk-profiles and financial goals.

Users' monetary transactions and their portfolio, consisting of the past and present totals of the funds/assets that a user has accumulated, are abstractly stored on the public blockchain. Further details appear in the Privacy section.

Akropolis gives users the ability to monetise this data. Users can opt-in to add their profiling data and potentially elements of their on-chain data (maintaining anonymity) to be marketed and sold in bulk by the Akropolis foundation to analysts and marketers. The resulting profits (in AKT) will be distributed evenly to the participants who chose to share their data. Ultimately, users are paid for sharing their data.

2.11. Regulatory Compliance

The pension industry is heavily regulated, as appropriate for a core social and financial infrastructure intended to maintain the living standards of a nation's citizenry in retirement. Though necessary to ensure a functioning pension sector, the dense regulatory environment surrounding the pension industry provides one of many hurdles that PFs and FMs must navigate to ensure compliance in relevant jurisdictions. Akropolis aims to streamline regulatory compliance by leveraging features of the platform.

Firstly, through the Onboarding/Vetting process, Akropolis will verify and check compliance for all FMs participating in the system, ensuring they comply with all necessary standards, locally and globally (where appropriate).

Secondly, it is often the case that the assets procured by FMs will themselves be bound to specific geographic regions and must therefore comply with regionally applicable rules and regulations. The asset tokenisation process will allow specific regulatory and tax requirements to be built into the token itself. This will allow seamless global on-chain compliance at the blockchain layer. For example, consider an investment in Australian property. An individual property may be fractionalised into a set of asset tokens. Australian law prohibits certain volumes of property being sold to foreign investors. Given that participants in the Akropolis system have been KYC'd, it is possible to programmatically ensure (with a verifiable audit trail) that the tokenised assets can only be transferred to accounts within the platform that are either Australian-owned or manifestly consistent with the demands of this particular regulation. Similar automated compliance protocols will be applicable, and readily implemented, for a wide range of assets.

Thirdly, the nature of pension investments often requires time-locking of investment assets, to comply

[10] See Privacy for further details discussing privacy concerns.

DRAFT

with either regional regulatory policy or the specifications/requirements of the fund products themselves. Compliance with time-locking requirements is another area that can be easily automated using a decentralised blockchain layer. Publicly verifiable locking of investments for specific periods of time aids platform auditing and ensures compliance with fund products and regulations.

To further this point, Akropolis will offer time-locked contracts, where users can opt to lock their funds for various periods of time, either for security, personal or regulatory reasons. We envisage that three such wallets will be regularly used; a retirement wallet (withdrawable after a certain age, e.g., after turning sixty-five), an intermittent release wallet (withdrawable at regular intervals) and an emergency wallet (withdrawable after demonstrating an emergency, consistent with predefined standards). These wallets are optional and can be designed to help users manage their investments. As a general rule, however, in order to comply with regulatory requirements regarding taxation and access to pension funds, time-locking of (at least) some portion of a user's funds is anticipated. Implementing such time-locking is, of course, a key advantage of blockchain-engaged systems such as Akropolis, which permit automated secure time-locking with full transparency.

The issue of regulatory compliance, for a pension platform intending to facilitate the flexibility required of a mobile global workforce, is a non-trivial matter. It is important to emphasise that the above discussion does not intend to over-simplify the complexities of regulatory demands. Principally, there are two classes of regulatory demands that must be integrated into such a system. One set of requirements relates to the local or regional regulatory requirements that apply to a citizen of a given state/jurisdiction. It is relatively easy to ensure that regional compliance is afforded by the Akropolis platform. KYC requirements ensure that users' data is tied to a particular jurisdiction and the platform can automatically apply the relevant regulatory framework to a user's account.

A more complicated issue relates to the global or total regulatory demands applicable for such a system. It is trivial to reapply a new set of regulatory demands as an individual updates their KYC information, thereby transitioning the governing framework for the user's account to the newly applicable jurisdiction (when appropriate). However, ultimately it is desirable that a (minimal) set of regulatory demands can be implemented on a global scale, reducing the friction experienced by modern workers engaging with the demands of an atomized, transient work environment. The changing demands of the modern workforce, and the forces they impart upon the individual as they attempt to accrue an adequate pension, would ideally be matched by an evolving regulatory framework that enables the global workforce to meet its needs. In principle, a unified set regulatory demands could be applied to part or all of an individual's pension accounts, and an idyllic vision for the future regulatory environment would see the regulatory framework evolve to increasingly respond to the demands of the modern workplace. For example, international trade agreements could include efforts to provide common unifying regulatory frameworks to steer global pension regulatory structures towards a suitably homogeneous configuration. The Akropolis platform is ideally suited to implement (and advocate for) a global regulatory framework while incorporating relevant jurisdictional-unique regulatory demands. The same applies for the current tax landscape, whose framework is heavily localised to specific geographical regions. In fact, Akropolis intends to liaise with several regulatory bodies of various countries to work towards recognizing the Akropolis platform as a pension fund structure (for individual contributors), allowing users to benefit from pension-specific tax treatments, including the tax relief on voluntary contributions.

It is emphasised that a perfectly homogeneous regulatory environment is unlikely in the near future, though regulatory homogeneity across regions such as, e.g., the Euro zone, offer some hope for such developments. The Akropolis platform will, in practice, be a provider of services that navigates a net of heterogeneous regulatory frameworks. Nonetheless, the larger goal of Akropolis is to design and advocate for a pension system that meets the needs of workers, as both the workplace and legislative agendas push greater responsibility for funding retirement onto the individual. Decentralised implementations are perfectly suited for nudging pension regulatory frameworks towards the modernisation necessitated by the needs of global citizens. The capacity for technologically-driven efficient protocols to advance outdated regulatory frameworks is evidenced by advances in the sharing/gig economy and the development of new monetary systems such as Bitcoin itself. Services such as Uber and Airbnb both forced regulatory environments across the globe to adapt to the modern era. Service-driven technological advances that better meet the needs of the population can source the legislative change the population requires. Thus, Akropolis is focused on developing a pension platform for the future, a system that learns from the failures of the past, and leverages technological advances to meet societal needs, while satisfying existing legislative requirements and advocating for legislative changes that ensure that users' needs are met.

Akropolis will need to consider and implement futuristic developments, such as the notion of a universal basic income, or related means of allocating basic resources to ensure that individuals can meet their needs in a workplace heading towards mass-automation. Akropolis does not advocate a particular position on such issues. However, Akropolis notes that the design of the Akropolis platform, in which individuals possess a unique pension account that is tied to their identity and acts as a portable source of pension truth, as the individual navigates the globe, is well suited to implement such futuristic programs.

DRAFT

2.12. Premium Services

The Akropolis platform is designed to help users transition from existing pension infrastructures to a more flexible, transparent and accountable system. As such, the platform adopts a freemium model, whereby users can join and the base services are offered for free. In addition to the base-level services, there will be extended (premium) services available on the platform. The range of extended services will inevitably expand as the platform develops. To give the reader a sense of the expanded services that may be offered, the following list contains some examples:

- Ability to add beneficiaries (family members, partners, friends, charities);
- Creation of Testament/Will Smart Contract (automatically assign holdings to a beneficiary in case of death);
- Add a controller/manager (implement a programmatic power of attorney, allowing users to appoint a person or a group of people to manage investments).
- The platform will incorporate stress-testing features for users, providing analysis of sector allocations and probable portfolio responses to extreme market/sector movements. It is envisioned that basic options will be available to all users (perhaps for a small fee) while more advanced stress-testing will be available as premium services.
- Cross-border assistance for expatriates, including access to information regarding the pension system in new host countries and tools for navigating inter-jurisdictional transitions.

2.13. Fees

All fees referred to in this section will be paid for in AKT tokens.

To combat the often complicated and hidden fee structures in traditional pension systems, Akropolis will implement a transparent and sustainable fee structure that both encourages good behaviour and adequately remunerates participants for their services.

There are four primary areas in which fees are taken within the Akropolis platform.

Premium Service Fees — While Akropolis adopts a freemium model for basic services, Premium Services are offered at additional cost. These fees vary depending on the service offered.

Onboarding Fees — FMs who wish to participate in the Akropolis ecosystem will need to be on-boarded and vetted in accordance with strict governance and regulatory guidelines (cf. Onboarding/Vetting). A flat fee is charged in this process to cover the platform's cost in undertaking the vetting process. This fee also acts as a deterrent to spamming and *trolling* attacks which can plague Token Curated Lists.

Enterprise License Fees — In parallel to the public Akropolis platform, an enterprise solution shall exist for PFs to manage and track their investments across the Akropolis platform (see the Enterprise Instances section). This enterprise solution will allow FMs to interface with specific PFs who wish to use a private or permissioned blockchain implementation, mainly for data privacy reasons. A license fee to use and access the platform will be charged to FMs and PFs. These licence fees will help support and grow the Akropolis platform, both in the private and public domains.

Performance Fees — Performance fees are key in the Akropolis model to ensure that FMs are incentivised to provide the best possible investment services to the Akropolis community. These fees will be based on transparent templates (see Templated Transparent Fund Fees) that will be released to FMs according to the performance of the assets under their management. This element can be automated on-chain using smart contracts, whereby fee withdrawals are permitted based on agreed values of the effective returns compared to an FMs expected/promised returns.

2.13.1. Templated Transparent Fund Fees

Given that contributions and returns are represented on-chain in the form of AIT transactions, the fee structures implemented by PFs and FMs can be implemented in smart contracts. Akropolis may issue a set of "standard" fee-templates as smart contracts. These contracts can be easily implemented by a fee-charging entity with their own variables (e.g., percentage fees, etc.), providing transparency to assure users that there are no hidden fees. These template fee contracts are reusable. Accordingly, it is reasonable to expend the requisite effort to ensure that these templates are clearly explained and understood, providing a significant improvement over the obfuscated and unnecessarily complex fee structures often used in the present environment.

In the event that a fee-charging entity wishes/needs to implement their own fee-structure contract, the Akropolis Foundation will be required to white-list the relevant contract prior to acceptance onto the platform. During the white-listing process, Akropolis may review the contract and ensure that the fee structure is not unnecessarily complicated and accurately reflects promises made to users.

2.14. Summary

The present section gave an overview of important elements of the Akropolis platform. Some mechanisms outlined above were intentionally communicated in a general sense. Throughout the development of the Akropolis

DRAFT

platform, each aspect of the system will be carefully analysed and fine-tuned to ensure that the platform remains commercially viable and technically feasible. Further papers, detailing technical specifics for elements of the system, will be forthcoming after sufficient real-world testing is completed.

The remaining sections of this document provide more-detailed discussion of key elements of the described system. These sections aim to be relatively self-contained and, where applicable, appropriately general.

3. Incentivised Accountability

The present section describes a general protocol for incentivising good behaviour by participants in a marketplace comprised of service providers and service users [30]. This Incentivised Accountability Protocol (IAP) has immediate application within the Akropolis platform but can also be used in more-general marketplaces to incentivise good behaviour by participants.

Participants who offer pension products on the Akropolis platform (either FMs of PFs, generically referred to as FMs in this section) will be required to inform the marketplace of the status and performance of their Funds Under Management (FUM). Akropolis will require FMs to deliver FUM status reports at regular specified periods as a condition for continued access to the platform. In order to (a) facilitate market transparency, (b) penalize bad actors, and (c) reward good actors, Akropolis will incorporate incentivisation mechanisms designed to hold FMs accountable for claims made in FUM reports.

The incentivisation process works as follows. Prior to releasing a FUM report, FMs must lodge an amount of AIT within the Akropolis system. These AITs are staked as part of the accountability process. Once the stake is received, the FM is authorized to release their report, a hash of which is sent to the smart contract holding the staked AIT. Upon receipt of the report hash, the smart contract specifies that the stake is locked for a specified period of $T_{S,A}$ days. During this period, the staked AIT acts as a bounty that incentivises market participants to provide evidence indicating that the FUM status report contains falsities. In principle, any interested individual/entity can analyse publicly available FUM reports and attempt to access the bounty, though two classes of market participants are clearly incentivised to verify the tenacity of reports:

- Users invested in the product offered by the FM are incentivised to verify the reported status of assets held.
- Individuals with inside knowledge of false reporting may wish to inform the marketplace of the FMs false claims (i.e., whistleblowers).

To make a claim of false reporting, an individual must submit supporting evidence, a hash of which is submitted to the smart contract storing the staked AITs. Submitted evidence will be analysed and a judgement will be made (see details below) regarding the tenacity of the FUM status report. Two outcomes are possible at the conclusion of the judgement period:

- The FMs status report is deemed valid. In this case, the AIT staked by the FM is returned to the FM after $T_{S,A}$ days have passed (i.e., the FM avoids punishment for bad behaviour). Furthermore, the FM gains positive reputation points, which can be used for marketing purposes within the platform to promote the quality of products offered by the FM (i.e., the FM receives rewards for good behaviour).
- The FM status report is deemed invalid. In this case, the staked AIT are forfeited and an amount of reputation points are subtracted from the FM (i.e., the FMs bad behaviour is punished).

Initial implementations of the IAP will require the outcome of the assessment process to be inputted by the owner of the staking contract. In the event of bad behaviour by an FM, the seized AIT are used to reward the individual who submitted evidence demonstrating the falsity of the report and to reimburse any authorities engaged to assess the validity of the evidence. Specifically, the staked AIT are split between the address that provided the hash of the evidence and an address that stores AITs used to fund the assessment process.

A challenge to the validity of a FUM report begins once the smart contract receives a hash of the evidence of bad actions. When submitting a claim of falsity or misleading conduct, the submitting entity (i.e., the claimant) may also be required to lodge a small amount of AIT in the staking contract. In the event that a ruling is made in favour of the FM, the claimant forfeits the submitted AITs, whereas the staked AIT is returned to the claimant if a ruling is made in the claimant's favour. Staking by claimants may not be enforced in all scenarios employing the IAP on the Akropolis platform, though one envisions some scenarios where claimant staking will be necessary, from a game theoretic perspective, to disincentivise bad actions by claimants. In any case, it is anticipated that claimant stakes will be relatively small, to allow genuine claimants to submit their case without undue burden, yet the claimant's stake should also be sufficiently non-trivial to discourage repetitive bad action on behalf of claimants.

Two phases are envisioned for the decision-making process engaged to determine the tenacity of a claimant's evidence (i.e., the evidence assessment process). In the initial implementation of the IAP, oversight will be provided by Akropolis, representatives of whom will act as the owner of the staking contract. The contract owner must:

- Undertake a preliminary assessment of the evidence to ensure it is not clearly false.
- Initiate the evidence assessment process, in the event that the evidence appears reasonable.

DRAFT

- Input the outcome of the assessment into the smart contract, at the conclusion of the evidence assessment process.

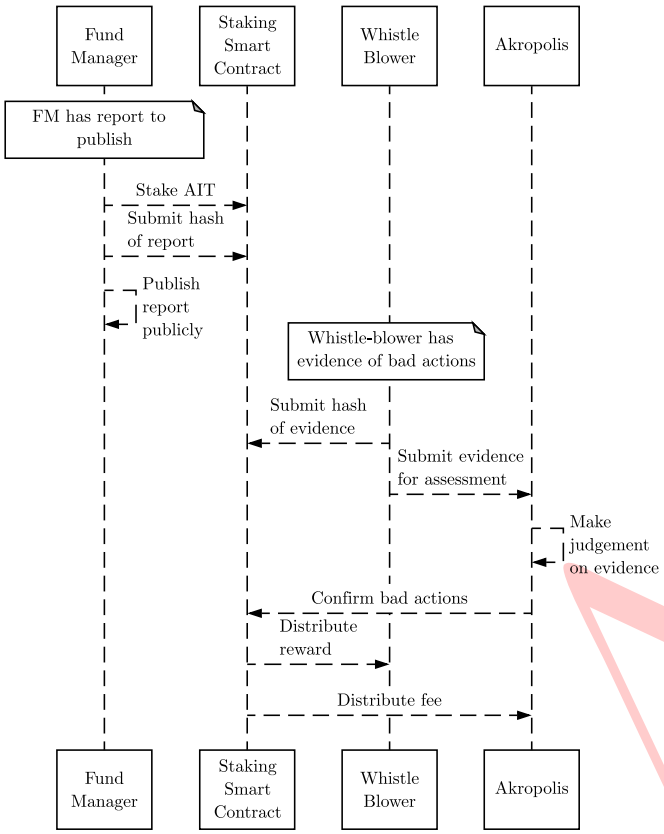

FIGURE 3. Sequence Diagram: A FM publishes a report that is found to contain falsities.

This initial implementation clearly requires a central authority. Ideally, a future phase of the IAP would remove the need for central oversight. The extent to which the evidence assessment process can be decentralized depends on the range of offences deemed punishable by the Akropolis system. It is beyond the scope of the present document to analyse the legal complexities relevant for the range of candidate bad actors, though it is evident that in cases of overt criminal behaviour it may be necessary to involve the relevant authorities. A sequence diagram summarising the IAP, for the case of a published report that is found to contain falsities, appears in Figure 3.

Ideally, some components of the evidence assessment process could be decentralised by employing a staking mechanism analogous to Augur [31]. The evidence assessment process could use Augur itself or a purpose-built variant of such a system, constructed for internal users of Akropolis. The decision-making process would work roughly as follows. The staking smart contract receives a hash of the FUM report and a hash of the evidence purportedly demonstrating false reporting. These documents are made publicly accessible, so that the relevant hashes can be verified. Any individuals interested in analysing the evidence and forming an opinion regarding the tenacity of the report can stake some AIT and participate in the decision-making process. All parties participating in the evidence assessment process then vote as to the tenacity of the report. The outcome of the vote is recorded by the staking smart contract. All AITs staked by participants that voted against the majority are forfeited and redistributed to participants within the majority. If the majority votes in favour of bad action by the FM, the AITs staked by the FM are included in the redistributed AITs, modulo the percentage of the stake provided to the address that supplied the hash of the evidence. This provides a decentralized process for assessing the quality of FM reports.

A couple of comments are in order. Firstly, there may be instances in which the FUM report, and the evidence of wrongdoing, are only made accessible to users holding assets with the given FM. In such cases, only those users possessing tokens associated with the relevant investment product could stake AIT and participate in the decision-making process (i.e., voting is only permitted by those with a vested interest in the tenacity of the report). Secondly, it is likely that the above decentralized IAP would still require some degree of central oversight. Given that assets and FUM are ultimately held externally in the physical world, there may be instances in which legal authorities are required to take action against FMs. The decentralized accountability incentivisation mechanism would likely require central oversight to determine whether it is appropriate to conduct the evidence assessment process in-house via Akropolis or whether the matter needs to be forwarded to legal authorities. The aspiration of Akropolis is to construct a system that is maximally decentralized, while acknowledging the reality that the pension sector imposes inherent constraints that will require some degree of central oversight.

3.1. General comment regarding this class of incentivisation models

The above discussion describes an IAP for accountable reporting of product information by FMs. Ultimately this general mechanism can be used in a variety of contexts within the Akropolis platform and the above discussion, which focused on the use case of FUM status reports, is just one possibility. An alternative use case would relate to product information and advertising material released to Akropolis users by FMs. A similar incentivisation structure would be possible - the FM submits an amount of staked AIT to a smart contract, along with a hash of the product information, advertising material or product disclosure statements. Users could investigate the reliability of claims made within the material, drawing attention to unrealistic assumptions regarding anticipated returns on FUM or any other information which may reasonably be considered misleading. Akropolis users are incentivised to police the reliability of material posted by FMs, while FMs are incentivised by the receipt of positive reputation

DRAFT

points for marketing and informational material that has been vetted by the staking process and deemed void of misleading information.

Regarding the number of staked AITs required to implement this mechanism, one possibility would be to allow FMs to decide on the amount of AITs they're willing to stake when submitting material to the system. The number of positive reputation points awarded to the FM for good behaviour could be determined by the size of the stake put forward by the FM to incentivise market scrutiny - the stake size would represent the strength of the FMs conviction regarding transparent and open engagement with investors. Accordingly, an FM willing to submit a larger stake should be rewarded with more positive reputation points. Similarly, FMs that submit a large stake that is ultimately forfeited due to bad behaviour may lose less reputation points than FMs that forfeit a smaller stake, with the loss of the stake itself considered an acceptable component of the punishment.

4. Ranking

Users of the Akropolis platform will benefit from ranking metrics that can aid fund allocation decision-making processes. Akropolis will provide multiple metrics for assessing the performance of PFs and/or FMs. One important metric will be an overall ranking of raw fund performance, i.e., a pure measure of fund returns, relative to alternative funds on the market. Other measures will assess the overall reputation of the fund provider, user satisfaction, the clarity and transparency of marketing material, and the FMs track record of meeting return forecasts.

4.1. Relative Fund Rankings

There are multiple ways to rank the relative performance of funds. One approach would be to employ a generalized implementation of the Elo rating system [32]. Elo developed a rating system for two-player games that can be applied to, e.g., chess or video games. Participants begin with a specified amount of ranking points and gain (lose) points, at the expense (benefit) of their opponent, whenever they win (lose) a game. Over time, players receive a ranking that encodes their relative number of victories and losses (or draws), while also factoring in the relative-ranking of opponents they have beaten/lost to. The relative ranking of two players also encodes the probability that each would be expected to emerge victorious if they competed.

For present purposes, it may be necessary to generalize the Elo rating system to games with n players (in the present case, players are individual funds). Denoting the rankings of the players in a two-player game as R_i, with $i \in \{1, 2\}$, the two-player Elo rating system proceeds by defining an estimated score for the players, defined as

$$E_i = \frac{1}{1 + 10^{(R_i - R_j)/D}}, \quad (1)$$

where $i, j \in \{1, 2\}$ with $i \neq j$. Note that the estimated scores sum to unity, $\sum_{i=1}^{2} E_i = 1$. The constant D is chosen such that an advantage of D rating points over an opponent translates into the player's expected score being magnified by ten times, relative to the opponents expected score. At the games conclusion, the players actual score is determined by a scoring function. For example, a suitable scoring function for chess is

$$S_i = \begin{cases} 0 & \text{if player } i \text{ loses} \\ 1/2 & \text{if player } i \text{ draws} \\ 1 & \text{if player } i \text{ wins,} \end{cases} \quad (2)$$

and the players ranking is updated as:

$$R_i' = R_i + K(S_i - E_i.) \quad (3)$$

Here K is a numerical factor that can be used to encode the relative impact of the outcome of the new game, on the player's ranking; i.e., a "master," with a large number of prior victories, may have a smaller value of K, such that the impact of a single loss is not severe, while a "beginner" may have a larger value of K, so that a single loss has a considerable impact on their ranking.

The Elo rating system can be generalized to an n-player game by treating the n-player game as a set of games in which every player is competing against every other player. Thus, the single n-player game can be treated as $n(n-1)/2$ two-player games. The players estimated scores can be cast as

$$E_i = \frac{1}{n(n-1)/2} \times \left\{ \sum_{j \neq i} \frac{1}{1 + 10^{(R_i - R_j)/D}} \right\}, \quad (4)$$

where once again the estimated scores sum to unity, $\sum_{i=1}^{n} E_i = 1$. The scoring function for the n-player game, for which the n participants are ranked from first to last, can be written as

$$S_{i,p} = \frac{n-p}{n(n-1)/2}, \quad (5)$$

where player i, who finishes in place p, receives the score $S_{i,p}$. Player rankings are again calculated as:

$$R_i' = R_i + K(S_{i,p} - E_i). \quad (6)$$

This generalized Elo rating system provides an example for a method to rank fund performance on Akropolis. Fund performance would be ranked at some regular interval, producing a relative ranking for all funds that evolves with time. The constant K could start out being equal for all funds, in the first phase of the Akropolis platform, and subsequently evolve to ensure that a fund with a strong history of reliable performance is not unduly penalized for a single bad year, while the volatility of the ranking for a new fund is more sensitive to the fund's yearly performance in its initial years.

DRAFT

4.2. Reputation Rankings

The Akropolis platform will provide additional classes of ranking measures for the benefit of users. The platform includes incentives to encourage accountability and transparency of FMs and part of these mechanisms includes the reward (or removal) of reputation points for good/bad actions. For example, funds that deliver their promised returns can receive reputation points, and similarly funds that stake AITs to incentivize scrutiny of their reports will be rewarded with reputation points in the event that their reports survive the scrutiny. It will also be possible to acquire reputation for delivering transparent and informative marketing and/or product material to the marketplace. Other sources of reputation measures may also be possible. These alternative measures of fund performance will be available for users to aid their decision-making and will also serve as marketing tools for funds on the platform.

The factor K that feeds into the overall fund ranking could also be given a sensitivity to the reputation measures derived by the platform, such as measures of user satisfaction and fund transparency and accountability. For example, if a fund has r_p reputation points, and one takes $K \propto r_p^{-1}$, funds with a stronger reputation will be less sensitive to a poor performance than a fund with a poorer reputation. More generally, including the factor ω that quantifies the FMs commitment to the principles of transparent and accountable reporting (see The Akropolis Platform), the K factor may take the form $K = K(\omega, r_p^{-1}, \ldots)$, where the dots denote additional relevant dependencies.

The platform will provide overall rankings both with and without the reputation sensitivity, allowing users purely interested in returns to select funds based solely on that measure, while users applying other fund allocation strategies may utilise rankings that incorporate various reputation factors. It would also be possible to include reputation systems that rank funds according to ethical factors such as environmental impact, employee conditions, gender equality in leadership, etc., allowing users to apply various ethically-oriented fund allocation strategies.

5. Governance

Akropolis' long-term objective is to maximise the degree of decentralised functionality available on the platform.[11] Within the maximally decentralised vision for the platform, the centralised oversight initially provided by the Akropolis Foundation will be largely replaced by a Decentralised Autonomous Organisation (DAO). In practice, the degree of decentralisation ultimately achieved will be subject to legal/regulatory requirements and the functional benefits for the platform. Furthermore, even after the Akropolis platform transitions to a system with a DAO governing body, it is envisioned that a small, elected body of curators will still be required to oversee the platform and rule on specific crowd-proposed issues. This body, hereafter referred to as the Akropolis Council, will coexist with the governing DAO and assist with various operational functionality.

The detailed implementation of any DAO requires careful consideration of a number of issues. In particular, it is crucial that the decision-making process avails a legitimate and provably-fair framework for organisational governance. The present section explores existing research on DAO governance models and considers possible DAO implementations that may be compatible with future versions of the Akropolis platform. It is emphasised that the implementation of decentralised oversight within Akropolis is a long-term vision. Initial implementations of Akropolis will include central oversight by the Akropolis Foundation and no move to decentralisation will be made without detailed consideration, rigorous testing, and careful implementation. The motivation for decentralised oversight stems primarily from the view that individuals should be empowered to control their financial future, not only in terms of building a pension fund, but also by determining the rules governing the functionality of the systems that control and implement their pension decisions. As the platform evolves, the extent to which decentralisation is appropriate and desired by platform users will be assessed and serve as the basis for future platform planning; i.e., decentralisation will not be imposed but will instead be utilised if it serves the needs of platform users.

5.1. Immediate Challenges

The immediate challenges that must be overcome for a DAO implementation to be successful include the following:

Governance scalability — It can be extremely difficult to mobilise a community to achieve a quorum for voting on organisational resolutions. The difficulty of attaining this goal typically increases with the number of participants in the system. This issue is well known and was encountered in many votes that occurred within The DAO [33].

Governance resilience — Naive DAO implementations often employ a majority vote, requiring more than 50% of participants to vote in unison to pass a resolution. Such systems can be vulnerable to 51% attacks - failure to carefully design optimal DAO implementations can allow malicious external actors to acquire 51% of votes

[11] See the Future Directions section for further discussion.

DRAFT

and implement various attacks, such as stealing staked deposits.

Game-theoretic equilibrium — DAO implementations that permit a wide range of voting proposals can be susceptible to attacks in which proposals that benefit the majority of participants are put forward and rapidly endorsed. Such proposals introduce bias into the voting system and can produce undesired outcomes. A trivial example would be a proposal that splits profits with participants who vote yes.

Governance extensibility — Fully decentralised systems can often be a double-edge sword. They provide a trustless deterministic framework but issues can arise if the framework itself is flawed. Mechanisms should be implemented, within the governance framework itself, that permit the governance framework to be extensible and upgradeable.

Dormant Tokens — Systems that do not offer key-recovery are susceptible to tokens/assets/votes gradually being lost and/or removed from circulation. If a system's tokens are used for voting, the assumption that all tokens are capable voting becomes less accurate over time. This is known as the dormant token problem [34]. A successful DAO should account for dormant tokens and adjust internal variables accordingly.

5.2. Approach

Several authors have investigated governance issues for decentralised systems and organisations [35, 36, 37]. In the present context, the modular design proposed and built by DAOStack [38] is of particular relevance. This design, coined the *Operating System for DAOs*, allows for replacement/modification of individual components that constitute the overall governance framework. It addresses many of the immediate challenges listed above and provides an extensible framework on which to build a governing protocol.

In the design of an over-arching governing protocol, Akropolis will also include the following extended principles:

- **Monetisation of attention**:
  - Incentivising voters to participate in important votes by compensating voters for their time. This could be achieved, for example, by remunerating voters using tokens from the community-pool.
  - Attention can also be monetized via a reputation-based system: the more often a member votes on proposals, the more reputation points they receive.
- **Delegation**:
  - Passive/dormant token holders will have the ability to delegate their vote to other members of the network or to the Akropolis Council. This allows idle participants to contribute their voting power with minimal effort.
- **Token-holder individual sovereignty**:
  - In the event that a token holder's opinion contradicts the vote submitted by his/her delegate, Akropolis will allow for vote overriding, enabling token holders to express their opinion at all times. This significantly mitigates the risk of coercion and collusion and aids the prevention of cartels.

Monetary incentives are not the only way to encourage good behaviour and/or discourage bad behaviour in DAO structures. The Akropolis reputation system (see Ranking and Reputation) can be integrated into many of the modular components that constitute the governance protocol. Thus, reputation-based incentives can also be used to encourage the above behaviours. We explore this possibility in more detail in the following section.

5.3. Akropolis Reputation System

Reputation-based incentivised governance models have been explored by the community (see Ref. [38] for an example). The present section considers the potential for incorporating the Akropolis reputation system into a decentralised governance model. A governance system that utilises governing members' (or participants') reputation must ensure that reputation points (which abstractly represent an increase in reputation) are non-transferable. Furthermore, the system protocol must clearly elucidate the ways in which reputation points are distributed amongst users. Below, a set of general guiding rules for awarding reputation points, within the context of decentralised governance models, are proposed. These may serve as the basis for the development of a more fully-fledged reputation-based governance system.

(1) Community-assigned reputation points: A process whereby community members may submit proposals for a given platform participant to be awarded reputation points. The recommendation is only enacted after the proposal is voted on.
(2) Algorithmic reputation flow: A set of rules which dictates a system for dynamic reputation-point assignment, including but not limited to:
   (a) Automatically assigning reputation points for the submission of approved proposals.
   (b) Automatically assigning reputation points for early votes in accordance with the majority.
(3) Platform usage: Reputation points can be awarded to users that actively/regularly participate in the system, either as users or developers. Various metrics can be used to quantify a user's level of participation, ranging from the amount of pension assets stored within the platform, the

DRAFT

number of votes participated in, or the frequency of platform activity.

Similarly, a set of rules can be enforced to decrease the reputation of specific participants. The rule-set could be based on events such as:

(1) Submission of a rejected proposal.
(2) Inactivity (Dormant-tokens): Token holders who do not delegate their voting power and do not participate in the last x proposals.

It seems fitting to decrease a user's reputation to disincentivise the occurrence of these (and related) events.

5.4. Akropolis Council

Decentralised systems often require a core group of participants who are responsible for casting final rulings on decisions initiated by the wider community of participants. Such agents, referred to as *curators*, are often elected from the participating community and given specific privileges on the system. In the present context, the curators of the decentralised Akropolis platform are referred to as the Akropolis Council.

It is anticipated that the initial body of curators will be chosen from the founding Akropolis team and leading experts in the industry. This includes reputable figures with relevant experience, such as pension advisors and consultants, asset/fund onboarding specialists, investment managers with specific sector expertise, financial planners and regulators.

The council of experts will be elected and maintained by the governing DAO. In the event of curator inactivity, the DAO may propose the removal of a member and elect a replacement. At any point, proposals may be made to replace council members to mitigate centralisation and prevent council member misbehaviour.

The responsibilities of the Akropolis council will include the maintenance of the FM registry, which functions as a token curated registry (see the following subsection). Council members will act as the curators of the registry.

5.5. Token Curated Registries

Token curated registries have recently received much attention in the decentralised community. In particular, a number of authors have explored the concept of DAO-maintained token curated registries [39, 40, 41].

Functionality of the Akropolis platform necessitates that a list of vetted Fund Managers, who are authorised to interact with contributors (individual contributors and pension funds), is maintained. Within the initial implementation of the Akropolis platform, the list of vetted platform participants will be maintained by the Akropolis Foundation. However, as the platform transitions to a more decentralised framework, it is anticipated that this centralised aspect of the system will be converted to a DAO-maintained token curated registry.

The purpose of a token curated registry is to provide a decentralised, self-sustaining registry of elements that conform to some externally agreed-upon metric. Any entity interested in adding an element to the list is required to stake some monetary value as assurance that the element confirms to the agreed upon metric. The wider community may challenge the purported suitability of an element and, if it is decided that the element does not conform to the metric, obtain the elements stake.

This logic can be applied directly to realise a decentralised tool for constructing and maintaining a list of FMs on the Akropolis platform. In the event that the governing DAO issues challenges to FMs that (supposedly) don't conform to some requirement, the Akropolis council could be tasked with performing the necessary background checks to ensure that the requisite standards are being met. At any given time, challenges against listed FMs could be issued by token holders or external pseudonymous/anonymous actors (see for example, the Fisherman-like protocol [20]). The Akropolis Council will likely be responsible for reviewing these challenges and deciding (through voting) if it is appropriate for the selected FM to remain on the token curated registry.

As a final comment, it is noted that the well-known issue of passive token-holding, which leads to easier exploitations of 51% attacks (majority validator attacks) can be mitigated in the event that Akropolis includes a voting-delegation mechanism. Such a scenario would, in principle, incentivise token-holders to either participate in the curation of the registry or delegate their vote.

5.6. Voting Mechanism

Voting mechanisms must be carefully developed and deployed in order to ensure that voting processes do not admit biases that can influence the outcome of votes. If, for example, participants' votes are public, the information can bias future votes cast by participants yet to submit their vote. Here, a potential implementation is outlined which provides vote secrecy at the cost of greater user participation. It is based on the well-known partial-lock commit-reveal commitment scheme [42, 43].

The basic strategy is outlined in the following steps

(1) Proposal submission: A token holder may submit a proposal to be voted on by the community. Votes are either in favour or against.
(2) Votes submission:
    (a) Commit stage: users who wish to vote on the proposal submit a hash of their vote and a salt.[12]
    (b) Reveal stage: users reveal their votes by submitting their choice (either yes or no) along with the salt used.
(3) Proposal outcome: Once the reveal period has ended, the result is automatically recorded by the voting smart contract.

[12] A random bit of information that makes the hash unique.

DRAFT

5.7. Final Comments

The above discussion provides an overview of candidate issues and solutions that are relevant for a decentralised implementation of the Akropolis platform. The purpose of the discussion is to provide a general sense of relevant considerations involved in the development of such a platform. As already mentioned, the move towards a decentralised framework (or even features) will be carefully considered and only implemented if it adds value and quality of services for platform users. The preferred goal of Akropolis is to embrace the community-oriented perspectives inherent in the decentralised developmental community and focus these perspectives to deliver optimal pension products that protect individuals from regulatory uncertainty and centralised points of weakness, while empowering individuals to secure their own financial future. To the extent that decentralisation serves the broader goals of the Akropolis platform, Akropolis will investigate and embrace promising decentralised implementations. However, decentralisation will not be pursued purely for its own sake - ultimately the governance and functioning of the Akropolis platform must serve the interests of pension holders, and developmental choices will reflect this priority.

6. Data Model

A guiding principle of the Akropolis project is to provide transparency and accountability through the use of distributed ledgers. However, it is important that this objective is attained whilst simultaneously ensuring that platform users maintain sovereignty over their private and personal information. Akropolis will be required to handle sensitive information (e.g., during onboarding and vetting) and maintain records of (some of) this information. Storing such information in the present regulatory context necessarily involves a private, permissioned database.

To achieve the competing goals of transparency and privacy, it is helpful to envision splitting the Akropolis data model into two broad categories, namely private and public data. Information on the public database is assumed to be public to the Internet and as such must be non-sensitive or sufficiently encrypted. The private database is expected to be fully-encrypted and only accessible by Akropolis. Accordingly, it may contain personally identifiable and sensitive information.

This section outlines the requirements of the public and private databases and the entities involved in their main processes. The overall role of the private database is also briefly discussed.

6.1. Public Database

The public database is assumed to involve a blockchain, such as Ethereum [9]. Implementation considerations will determine whether the public database is truly public to the Internet, or resides within a permissioned network (such as a corporate network). The Akropolis protocol is intended to be blockchain agnostic, however, for initial implementation considerations, Akropolis functionality will be designed to be compatible with the capacities of the current public Ethereum "mainnet". References to "smart contracts" and related Ethereum-specific terms can be readily generalised and applied to other blockchains.

It is not necessary to assume that the public database consists of a single database — pre-existing bridging solutions between multiple Ethereum chains [44] would allow a public database to span multiple Ethereum instances, allowing the inclusion of low-fee and highly scalable proof-of-authority (PoA) chains. Furthermore, inter-protocol solutions [20, 21, 22] utilising an intermediary chain are showing progress and could allow for inclusion of multiple, disparate chains.

6.1.1. Requirements Analysis

Selecting a public database (i.e., blockchain) is a complex choice, involving more than a simple technical-requirements analysis, as used for a relatively static technology such as a web server, and being more akin to selecting a long-term strategic business partner. Aspects of the economic and political factors involved in this decision (such as the viability of available consensus mechanisms and governance profiles) are discussed elsewhere. The present section focuses on technological requirements of the public database to determine the base level of required functionality.

The public blockchain must provide data storage and processing for the following features:

- **Account-keeping** — maintaining a tamper-proof ledger of value transfer around the Akropolis system, with the specific goal of providing a public view of fund performance.
- **Gate-keeping** — providing mechanisms to protect users and institutions from malicious activity by non-vetted entities.
- **Staking and voting** — allowing users to participate in decision-making and crowd-sourced processes by providing tamper-proof voting and arbitrarily complex escrow functionality.

Given these requirements, any blockchain used as the public database should possess the following qualities:

- **Turing-complete smart contracts** — future functionality should not be bounded by the lack of general computing capacities.
- **Unbounded storage** — the public database should not impose artificial storage limits that could impede the future development of the platform.
- **Open-source cryptography** — all cryptography should be open source and community tested.
- **Existing tool-sets** — the chain should have an actively maintained ecosystem of third-party and vendor-issued tool-sets. Examples include: block explorers, open-source development tools (testing

DRAFT

and deployment suites, static analysis, UI tooling, etc.) and analysis tools.

The following sections provide additional details regarding the above-mentioned process.

6.1.2. Account-keeping

In its simplest form, the public database can be viewed as an account-keeping mechanism that tracks the allocation of funds in the Akropolis platform. As seen in Figure 4, this (somewhat simplified) overview involves the following objects:

- **Account** — a native account object on the underlying blockchain (e.g., an externally-owned account on Ethereum). It is expected that a user will control multiple accounts.
- **Wallet** — a smart contract providing functionality necessary to delegate funds to FMs/PMs and manage tokenised assets.
- **Delegate** — an object that manages funds delegated from a user wallet (PMs and FMs would fall into this category).
- **Asset** — a tokenised asset.

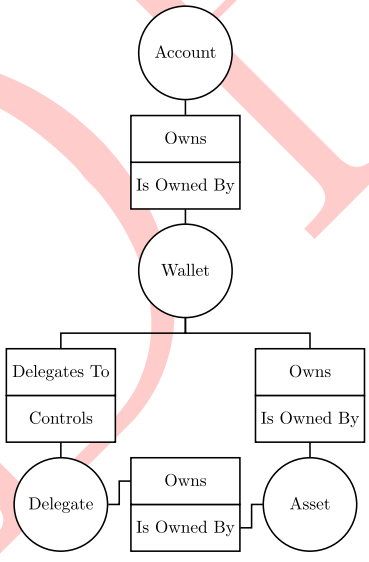

Figure 4. ORM: Overview

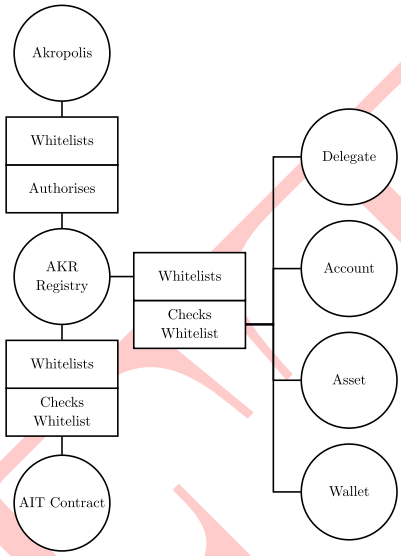

Figure 5. ORM: White-listing

6.1.3. Gate-keeping

To maintain a security and compliance, funds represented by AITs are only transferable to individuals and institutions that have been vetted/KYC'd by Akropolis. Authorisation will be automated by the use of white-lists maintained by Akropolis. Figure 5 illustrates the entities involved in these gate-keeping interactions. New entities appearing in the figure include:

- **Akropolis** — an authorised individual (account) or group of individuals (multi-signature account) that is directly under the control of the Akropolis Foundation.
- **AKR Registry** — a smart contract maintaining a mapping of addresses (externally-owned and smart contract addresses) to their white-list state. In its simplest form, the white-list state would be boolean, though this may become more complex in future iterations.
- **AIT Contract** — the smart contract that maintains the source-of-truth for AIT balances. This contract will need to refer to the AKR Registry for each token transfer.

6.1.4. Staking

As described in Section 3, reports issued by delegates can be issued with a stake as part of the IAP. Bad actions can result in forfeiture of the stake. This process is illustrated in Figure 5, which introduces the following entities:

- **Report** — information published by a delegate (with an optional stake) which contains clear and concise statements about verifiable truths.
- **Dispute** — a challenge to one or more statements in a report.
- **Whistleblower** — a generic term for any entity that contests a report and therefore creates

DRAFT

a dispute. A whistleblower does not need to be a white-listed account and may be anonymous.

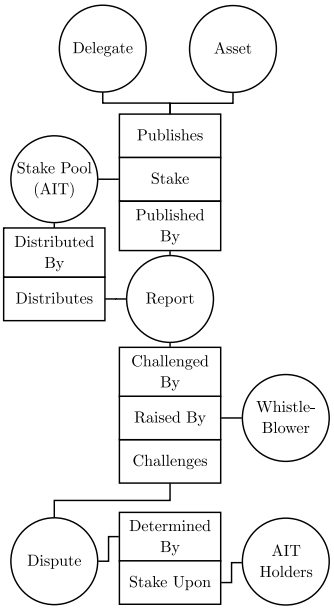

FIGURE 6. ORM: Staking

6.2. PRIVATE DATABASE

The initial requirements of a centralised Akropolis Foundation do not mandate that the private database involves a blockchain; in the current technological landscape it may be more efficient to implement a "traditional" database (e.g., PostgreSQL [45]).

The private database must store the following:

(1) Links between pseudonymous account addresses and personally-identifiable information.
(2) Personally-identifiable information collected during the use of Akropolis services.
(3) Identity documents collected during onboarding process.
(4) Sensitive corporate information.

It is not anticipated that the structure of the private database will be novel. Accordingly, it is not necessary to present additional information here.

6.3. SUMMARY

The Akropolis platform will employ both traditional and blockchain data bases to achieve the combination of privacy and transparency required of a portable, reliable pension service provider. The ratio between public and private computing and storage structures will vary according to the functional requirements of a given service and the extent to which decentralised governance and accountability protocols can be implemented. Functionality offered by the Ethereum blockchain provides the initial template for what is achievable with public blockchain databases, though these capabilities will no doubt evolve as the underlying blockchain technologies advance.

7. ENTERPRISE INSTANCES

The present paper has presented the Akropolis system as a singular, public-facing platform. However, an enterprise version of the platform, which can be deployed on various private, permissioned blockchains, will also be released. The purpose of such a system is to provide large PFs with the option to incorporate the improvements offered by the Akropolis platform into their own private and protected corporate networks. Existing pension industry infrastructure and processes are likely to impose realistic constraints on the capacity of industry participants to transition to new systems. The Akropolis enterprise solution aims to provide a bridge that allows existing industry participants to engage with the Akropolis platform, and benefit from new service features, whilst retaining familiar levels of control over internal infrastructure and processes. The enterprise solution will reduce friction between PFs and FMs by allowing both parties to benefit from the vetting practices, reputation systems and incentive structures that Akropolis provides, whilst ensuring no commercially-sensitive information leaves the organisation.

Instances of the Akropolis enterprise solution will provide direct functionality between FMs, PFs and asset tokenisers. Private instances will also connect to the Akropolis core system (with read-only functionality) to utilise the reputation and vetting registrars of the core system. AKTs and AITs may be present in any given enterprise system but their use is not mandatory and their functionality may be altered:

- **AIT** — the fiat-to-AIT (and vice-versa) conversion provided by Akropolis will not be required for investments between PFs and FMs in enterprise instances. Instead, the managing entity of the instance would ensure the ledger is updated with regards to capital flows between organisational units within, and external to, the given entities. Thus, Akropolis will not be required to act as a "middleman" for each transaction on enterprise networks.
- **AKT** — functionality will match that of the public instance (e.g., used for staking and fee payment, if required). AKT can be "forwarded" to an enterprise instance using a bridging mechanism [44].

Assets in an enterprise environment may be issued internally, or they may be transferred from the global public Akropolis system (akin to AKT) to allow asset trading inside the enterprise environment. Thus, it will be possible to directly trade asset tokens (such as gold [46] or fiat currencies [47]) within the enterprise environment.

The user interface supplied for enterprise instances would be tailored to suit the needs of enterprise clients.

DRAFT

Features such as reporting, performance analysis, and integration to existing corporate authentication structures, will be included.

The underlying blockchain for enterprise instances of Akropolis will initially derive their design/functionality features from the Ethereum blockchain, to ensure compatibility with the initial implementation of the public Akropolis platform. Due to the private nature of the enterprise solution, the corresponding chains will likely require a permissioned node discovery protocol and an altered consensus mechanism to that of the standard Ethereum ETHash Proof of Work algorithm. Quorum [48] is a likely candidate. Such chains will enable processing of the Ethereum smart contracts already developed for the core public Akropolis platform, whilst facilitating the private and permissioned needs of a corporate pension fund.

Enterprise instances will allow Akropolis to engage with existing pension industry participants whilst generating revenue streams to facilitate future developmental ambitions. With regard to Akropolis' long-term objectives, the enterprise instances will provide a bridge that allows Akropolis to navigate existing constraints, imposed by legacy pension systems and processes, whilst building partnerships to aid the realisation of Akropolis' larger goals.

8. Privacy

Any public blockchain-enabled system must deal with the serious issue of privacy on a public ledger. The Akropolis platform boasts transparency and accountability for interactions between users, PMs, FMs, and tokenised assets. However, the platform must also satisfy stringent requirements for user privacy. It is imperative that the dichotomy between transparency and privacy is managed effectively within this system.

The present section outlines the privacy model of the system, describes eminently-feasible methods of implementing such a model in the current technological landscape (along with limitations), and discusses ways in which emerging technologies may provide more interesting/robust solutions in the long-term.

8.1. User Privacy

Information generated while using the Akropolis platform can be categorized into three broad categories:

- **Confidential** — information that should never be publicly released, such as passports, identification documents, passwords, and commercially-sensitive information.
- **Personal** — personally-identifiable information which may only be released to a third-party with the permission of the user/organisation. For example, account balances, personally-identifiable transactions and contact information.
- **Public** — information that should be publicly available; e.g., non-personally-identifiable transactions and public announcements.

Confidential information should never be released and must therefore be stored in a private database exclusively accessible by the Akropolis Foundation (as discussed in the Private Database section). Public information is naturally public, however, specific privacy limitations still apply (see the GDPR section for GDPR considerations). Personal information is private by default but can be revealed to a subset of individuals/entities at will. This is addressed by a simplistic pseudonymous scheme described in the following section.

8.1.1. Pseudonymous Transactions

To allow personal information to be private-until-disclosed, Akropolis intends to implement a pseudonymous account/address scheme. In this scheme, all transactions exist on the public Ethereum ledger, yet the link between Ethereum account(s) and the individual who owns them (the user's wallet) is known only to the private Akropolis Foundation, the user and whomever they wish to disclose this link to. The initial scheme works simply by linking a wallet to a private seed which is used to generate new Ethereum private keys in each transaction. The wallet therefore consists of an arbitrary number of underlying Ethereum addresses.

Schemes in which user wallets are comprised of multiple underlying addresses exist naturally in unspent transaction output (UTXO) ledgers such as Bitcoin [8]. Often wallets in UTXO blockchains intentionally create new addresses with each transaction to aide anonymity through obscurity of addresses in underlying blockchain layer. This technique is not without issues. Data analysis strategies such as address clustering [49, 50] can be used to group addresses back to singular identities in some cases. This particular strategy is only applicable to UTXO-based ledgers. However, it is anticipated that other forms of analysis (such as timing analysis) may be performed to partially reconstruct user's wallets from the underlying Ethereum accounts.

Due to the trust which must be placed upon the Akropolis Foundation to meet regulatory requirements (e.g., KYC and vetting), the platform is afforded some extra functionality that can avoid such analysis techniques and would otherwise be difficult to obtain in a fully trustless environment like Bitcoin. Specifically:

Private entry and exit from AIT — issuance and redemption of AIT is handled by Akropolis, who maintain a private mapping of accounts to user identities. This means that no third-party exchanges are involved, localising the trust requirements to Akropolis.

Obscured inter-account transactions — consider the case where a user, U, has revealed their primary account address, a_1^U, to a third party, T. If U decides they do not wish to disclose further transactions to T, U could transfer their funds into an another account a_2^U. Unfortunately, this transfer would be visible to T who could

DRAFT

then link a_2^U to U. To remove this public link between the two accounts, Akropolis can offer a "private transfer" from one wallet to another, obfuscating not only the "to" address, but also the time and amount of transfer. This would allow U to transfer the funds via Akropolis, leaving no trace for T and trusting no other party than Akropolis. This is not dissimilar to a standard cryptocurrency tumbler.

8.1.2. GDPR

The General Data Protection Regulation (GDPR) act [51] becomes active in May 2018 and Akropolis will undoubtedly need to adhere to its requirements. As such, Akropolis is designed GDPR-native, avoiding the costs of dedicating resources and budget towards migrating legacy systems [52].

Akropolis satisfies GDPR Article 25 [51], "data protection by design and default", by ensuring that the highest level of privacy is enabled out-of-the-box and that encryption and decryption are handled locally (following the European Union Agency for Network and Information Security's specification [53]). On-chain data is minimised to reduce user risk and overhead. Also mentioned in Article 25 and Recital 28 [51], on-chain data is made pseudonymous to reduce risks to and protect the rights of users. Data portability (Article 20 [51]) is enabled through the use of blockchain — transactions on-chain are open to the public and may be translated and ported to another system without any action required of Akropolis.

A significant point of contention around GDPR requirements is Article 17 [51], the "right to erasure" ("right to be forgotten"). The contention arises in that the erasure of a single record from a blockchain ledger will necessarily destroy the integrity of the ledger — data can be "removed" from the current Ethereum state trie, however, a record of its presence remains preserved within the blockchain's history. Furthermore, irrespective of the integrity of the ledger, once data has been published to a public network (such as the Ethereum network), seeking a guarantee of erasure from an anonymous, decentralised network of computers is infeasible, if not impossible. Other projects in the blockchain space are working actively on this problem [54, 55] and Akropolis will continue to adapt and iterate as the GDPR implications for blockchain become apparent. Regardless, Akropolis does not publish personal information to the blockchain — all transactions published are done so directly by the user, at their discretion.

8.2. Credential Management

Given that there are two separate data storage and processing mechanisms used in Akropolis (see the Data Model section), there are two distinct scenarios in which a user may manage their credentials:

- **Off-chain information** — information stored by Akropolis will be centrally managed, therefore traditional credential management solutions apply, such as password authentication with multiple factors (2FA) and password recovery through a proof-of-identity submission to Akropolis.
- **On-chain information** — ownership of an account on a blockchain is generally [13] indicated by the possession of the private key corresponding to that address. Therefore maintaining knowledge of that private key is critical to maintaining access to that account. The following section details this further.

8.2.1. Cryptographic Key Management

To reduce the burden on users of managing multiple private keys, Akropolis envisages the use of a system that derives keys from a seed recoverable from a mnemonic phrase [57]. Such phrases are commonly used in hardware [58, 59] and software [60, 61] wallets. Using such a system allows a user to, in effect, derive a limitless number of keys from a single phrase, without the risk that an opponent can feasibly imply a link between any of the addresses.

A reasonable scenario exists in which a user completely loses access to their private keys, therefore losing the ability to transact their AIT and make other on-chain transactions. Such a scenario would be dire, especially if it resulted in the loss of a users entire pension savings. Fortunately, there are methods to mitigate the consequences of a user losing their private keys, as discussed in the Key/Asset Recovery section.

8.3. Future Privacy Solutions

The design proposed to obscure identities from the underlying public blockchain transactions was opted-for in the initial implementation due to its simplicity. It is envisaged that this approach will serve as an intermediary privacy measure whilst more-advanced techniques, capable of provably maintaining privacy at the blockchain level, are developed and tested.

Recent homomorphic encryption techniques appear to be good candidates for ensuring user's transactional privacy at the blockchain level. Grin [16], which is in active development, leverages the homomorphic property of elliptic curve keys under addition to verify fully encrypted transactions in UTXO systems. This system allows complete secrecy of the underlying values being transferred. Similarly, zk-S(N/T)ARKS are being developed for Ethereum, in particular the Ethereum-focused framework ZoKrates [62] aims to simplify the creation of zero-knowledge systems for use on the Ethereum blockchain. Methodologies such as these, once proven, could be used to provably mask user transaction data and replace the simplistic scheme currently proposed.

[13] This is exactly the case for Ethereum [9], Quorum [48] and Lisk [56].

DRAFT

Before concluding this section, some comments are offered regarding the fact that homomorphic encryption schemes are useful for anonymously providing aggregate data. When users opt-in to monetise their data (see the Akropolis Platform Data section), it is plausible that aggregated private information may be of value. Homomorphic encryption is one means of providing aggregated data privately. For example, an external entity may wish to know how many properties in China are owned (in part or fully) by non-Chinese investors/participants. The participants could individually encrypt their totals and send the information to the external agent, who performs addition on the individual encrypted values. Once finished, a decryption key held (potentially in part) by the Akropolis Foundation could decrypt the final value, thereby ensuring that only information about the aggregate value is received by the external entity, whilst individual users' data remains private.

9. Future Directions

The previous sections described multiple current and future technologies that may be integrated into the Akropolis platform. The present section adds some additional points and highlights some important features that new technologies will bring to the Akropolis platform.

The Akropolis platform utilises AITs, which abstractly represent an independent stable coin. In the initial implementation, this will likely be an Akropolis equivalent of Tether [47]. However, in the future, Akropolis may incorporate an independent, proven, algorithmic stable coin,[14] such as MakerDAO's Dai [63], or develop its own version of an algorithmic stable coin if present coins are deemed unsuitable. Adopting an independent stable coin would alleviate the need for tokenising multiple distinct fiat currencies.

As discussed in the Governance section, Akropolis aims to gradually decentralise its core components, to the extent that regulatory and practical considerations permit. It is envisaged that a DAO-like governing entity will (in part or fully) eventually replace the role of the Akropolis Foundation. Based on existing research, it appears feasible that the initial steps towards decentralisation could utilise DAO-governed Token Curated Lists to partially decentralise the onboarding process of FMs. The overall decentralised picture is heavily dependent on future progress in decentralised governance models and will ultimately be subject to the needs and requirements of platform users.

Finally, as discussed in the Privacy section, Akropolis aims to improve the blockchain layer's privacy by incorporating future advancements in privacy-preserving methodologies. Privacy functionality and features will become increasingly important as the system transitions to a more decentralised state (which necessarily increases the dependence on underlying blockchains for data storage). The transition to a fully-decentralised pension system is dependent on the capacity of privacy-preserving technologies to facilitate such a system whilst maintaining user privacy.

10. Conclusion

The dire state of the global pension industry looms large as a major economic issue for the coming years. A global discrepancy between pension assets held and existing liabilities presents a significant economic challenge both for individuals and the wider global economy. Trends such as increased life expectancies, decreased voluntary contributions, and reduced ratios of workers to retirees all exacerbate the stresses on the pension industry. The systemic issues plaguing the pension sector are intricate and the complexity of addressing these challenges should not be understated. Yet action must be taken if the economy is to avoid a pension-induced global financial crisis.

Any solution to the pension crisis must support the current pension ecosystem, to protect upcoming retirees, whilst also meeting the needs of an aging population and facilitating a global inter-generational transition to a new, economically sustainable system. This presents a complex, interrelated set of demands and constraints for any candidate pension framework. A new pension protocol must also recognize that workplaces and legislative agendas are changing. The workforce is being increasingly atomized and the tendency towards freelancing and a sharing/gig economy has eroded traditional mechanisms for building pension savings. Furthermore, to re-assign responsibility for the forthcoming challenges, states are increasingly liberalising pensions and shifting the burden of funding retirement onto the individual. Thus, the modern worker requires a pension system capable of functioning alongside the atomization imposed on workers by both the modern state and workplace.

The pension industry also suffers from systemic issues relating to poor visibility around fund management, unnecessarily complicated (or hidden) fee structures, portability limitations, and compliance regulations which, at times, are enforced using outdated methodologies. Furthermore, misaligned incentive structures between pension investors, the funds to which they contribute, and the fund managers overseeing the underlying assets, further strain existing pension systems and erode the benefits returned to pensioners.

The Akropolis platform aims to unify a number of recent technological advancements to develop and implement a long-term sustainable solution to the numerous challenges plaguing the pension industry. Akropolis seeks to facilitate the transition from existing pension structures to an atomized, individualised pension protocol capable of satisfying the needs of modern workers. The Akropolis

[14] A coin that is not 1-to-1 backed with a collateralised asset, but instead either algorithmically bound to a collateralised volatile token or has some algorithmic adjustable supply.

DRAFT

platform will deliver a portable pension infrastructure capable of supporting the modern worker along their individual (global) journey in an environment beholden to changing legislative demands and workplace conditions. Fundamentally, the platform aims to leverage the transparency, automaticity, and auditability of decentralized ledgers to provide new tools that balance the competing demands of workers, Pension Funds, and Fund Managers, whilst delivering the flexibility, accountability, and regulatory compliance required of a pension service. Akropolis is a global platform and will connect everyday users with a range of experienced pension funds, products and services. Importantly, the Akropolis platform incorporates game-theoretic incentive structures to mitigate against excessive fees (traditionally borne by users in the pension industry) while simultaneously fostering new levels of transparency.

Akropolis will act as a single source of pension truth for the individual, collating their existing pension products, together with new pension products, collectively under a single account tied to the individual's identity. The tokenisation of pension assets and products will enable new ways for individuals to engage with their holdings and new ways for Pension Funds and Fund Managers to engage with clients. New classes of services are possible, ranging from the monetisation of user's data (should they opt-in), to the direct marketing and delivery of relevant, related pension products, through to the delivery of decentralised pension platforms with in-built accountability, transparency and governance protocols.

The utilisation of blockchain technologies is not a cure-all for the pension industry, yet it is clear that these developing technologies offer new solutions to the challenges faced by the sector. Akropolis is partnering with leading experts in the pension industry and leading blockchain projects to tackle the global pension crisis as a community. The goal of the Akropolis project is to develop a transparent, accountable and portable pension infrastructure that can deliver pension services that meet the needs of the modern workforce. Overcoming the challenges in existing pension structures is a non-trivial task. Yet Akropolis believes that leveraging new decentralised technologies, to empower the community to come together and tackle the pension problem, offers the best hope for both rectifying existing systemic failures and building a sustainable future.

Appendix A. Glossary and Acronyms

- **AKR**: Akropolis.
- **AKropolis external Token (AKT)**: A fixed-supply token whose value is subject to market forces. AKTs can be used for onboarding and platform access, to purchase services on the platform and in some staking processes.
- **Akropolis Internal Token (AIT)**: A stable token used within the Akropolis platform. Users (individual or institutional) obtain AITs when they transfer funds to the system. The AITs may be used to purchase pension products, access services or for staking purposes. A stable token is required to serve as an internal bookkeeping device and to remove volatility risks associated with staking mechanisms (which would otherwise undermine the staking process).
- **Akropolis Council**: An elected body of curators that oversees the functionality of decentralised components of the Akropolis platform. The Council has some authority to work with and alongside the DAO.
- **Akropolis Foundation**: Centralised body that oversees the operation and functioning of the Akropolis platform. The incorporation of decentralised elements within the platform will see the Foundation replaced by a DAO (in-part or fully, subject to regulatory constraints and functional objectives).
- **Asset Tokenisers**: Entities that hold assets, either directly or through verifiable third parties, whilst minting and distributing tokens which represent a share of the held asset. Asset tokenisers are centralized entities that provide a source of truth to the blockchain layer (through the minting of tokens) and as such are key actors in the trust model of Akropolis.
- **Asset Tokenisation**: Process of creating digital representation of assets, suitable for representing assets on a blockchain.
- **DAO**: Decentralised Autonomous Organisation.
- **Developers**: Community members who contribute to the Akropolis platform, building extended/advanced services for pension users.
- **EVM**: Ethereum Virtual Machine.
- **Fund Managers (FMs)**: Institutional entities that purchase or acquire assets on behalf of users and/or PFs. They must undergo stringent vetting processes to obtain access to the Akropolis platform and must regularly report on the assets under their management.
- **FUM**: Funds Under Management.
- **GDP**: Gross Domestic Product.
- **GDPR**: General Data Protection Regulation.

DRAFT

- **Incentivised Accountability Protocol (IAP)**: A protocol for incentivising good behaviour (e.g., transparency and accountability) by actors on the Akropolis platform. An IAP typically requires that entities releasing information to the platform also stake AITs as part of the information-releasing process. The staked tokens serve as a bounty to incentivise agents external to the staking entity to verify the validity of the information. Staking entities that release valid information are rewarded with reputation points.
- **Individual User (or user)**: A singular, non-institutional individual who uses the Akropolis platform to manage their pension savings. When discussing elements on the blockchain, a user refers to a singular identity which is mapped to a collection of public keys via a generating seed.
- **KYC**: Know Your Client.
- **ORM**: Object-Relational Mapping.
- **Pension Funds (PFs)**: Institutional entities that may (or may not) currently exist in the pension industry. These institutional funds act similarly to individual users on the Akropolis platform but control the pension products of multiple/many individuals.
- **PoS**: Proof of Stake (consensus mechanism).
- **PoW**: Proof of Work (consensus mechanism).
- **UTXO**: Unspent Transaction Output.

Appendix B. User Journey and Basic Options

Aspects of the user journey and basic options/functions are described below.

(1) **Registration** — Users sign up with an email and password. This initial interaction with the Akropolis platform incorporates a concise explanation of basic system features. Users are not initially burdened with blockchain specific actions like an account (keys) generation or transaction signing. Registration does not require but instead allows users to explore the application and gradually build up the trust needed to submit to a full screening process.

(2) **Verification** — Users may upgrade their basic (initial) account to unlock investment options by uploading appropriate identification documents and certificates. The three categories of accounts are thus:
   - *Basic Level* — The default level, showcases the application/platform before a user is ready to create a full investment level account.
   - *Investment Compliant* — Available after identification documents are supplied.
   - *Pension Fund Compliant* — Relevant for institutional participants.

(3) **Feed data from legacy pension funds** — Users may import data from legacy pension fund providers, thereby collating all their pension/savings information in a single place. Functionality will be similar to Pensions Dashboard [64].

(4) **Saving Account Creation** — Users may create a new pot or transfer an existing savings account from a different pension fund. New savings pots may be assigned as pensions savings (which imposes certain regulatory demands, such as time-locking requirements, and avails privileges such as tax relief) or as unrestricted savings (which act as a standard investment account).

(5) **Saving Pot Configuration** — There will be three different modes of savings management:
   - *Self-managed* — The user is responsible for asset selection and trading. There are no management and performance fees. Recommended for advanced users with investment experience.
   - *Advised* — The user has control over, and responsibility for, their investments but receives personalised suggestions/advice regarding their current savings, risk level and investment horizons. Acting on the advice is straight forward, requiring users to click on an agree/decline button to trigger automatic execution (in some cases). Advisors may be ranked according to their past performance (as stored on-chain) and can charge fees for their service.
   - *Pension Fund Operated* — The user delegates investment responsibilities to an institutional pension fund. The fund is responsible for all investment decisions and may collect a fee based on performance or volume under custody.

(6) **Defining Contribution** — Users may define an initial contribution and/or commit to periodic contributions to be debited from their account. Options for assigning employer contributions will also be available.

(7) **Assets trading** — Users with self-managed portfolios are responsible for managing trades, otherwise trading activities are outsourced to a pension fund. A user may submit a buy/sell bid stating the desired price and wait for a counterparty to settle the deal.

(8) **Investment monitoring** — Users can monitor the value of savings pot and obtain information about investment performance and fess incurred. Options for executing portfolio stress-testing will be available.

DRAFT

(9) **Third-party add-ons** — Pension funds and users may add tools and services provided by third party developers and software studios. Application producers may need to obtain a licence by staking AKTs. All applicants will undergo a verification/vetting process before being available to users. Developers may collect fees for application usage.
(10) **Benefits Payments** — Users can individualise their benefit payment structures, subject to regulatory requirements.

Appendix C. Technical Architecture

C.1. Overview

To serve the long-term needs of the pension market, the Akropolis platform must adopt a number of key design principles to ensure it is resilient, fault tolerant, flexible, and relevant in an evolving technological landscape. Inevitably this will involve new blockchain architectures, oracles and third-party components that emerge and replace obsolete technologies. Furthermore, it is critical to create a platform architecture that can adapt and respond to new quantum resistant cryptographic security requirements, as appropriate. Given the immutable nature of smart contracts, these issues have to be carefully considered.

C.2. Akropolis High Level Architecture Components

The high-level architectural components of the Akropolis platform are shown in Figure 7. Web and mobile applications

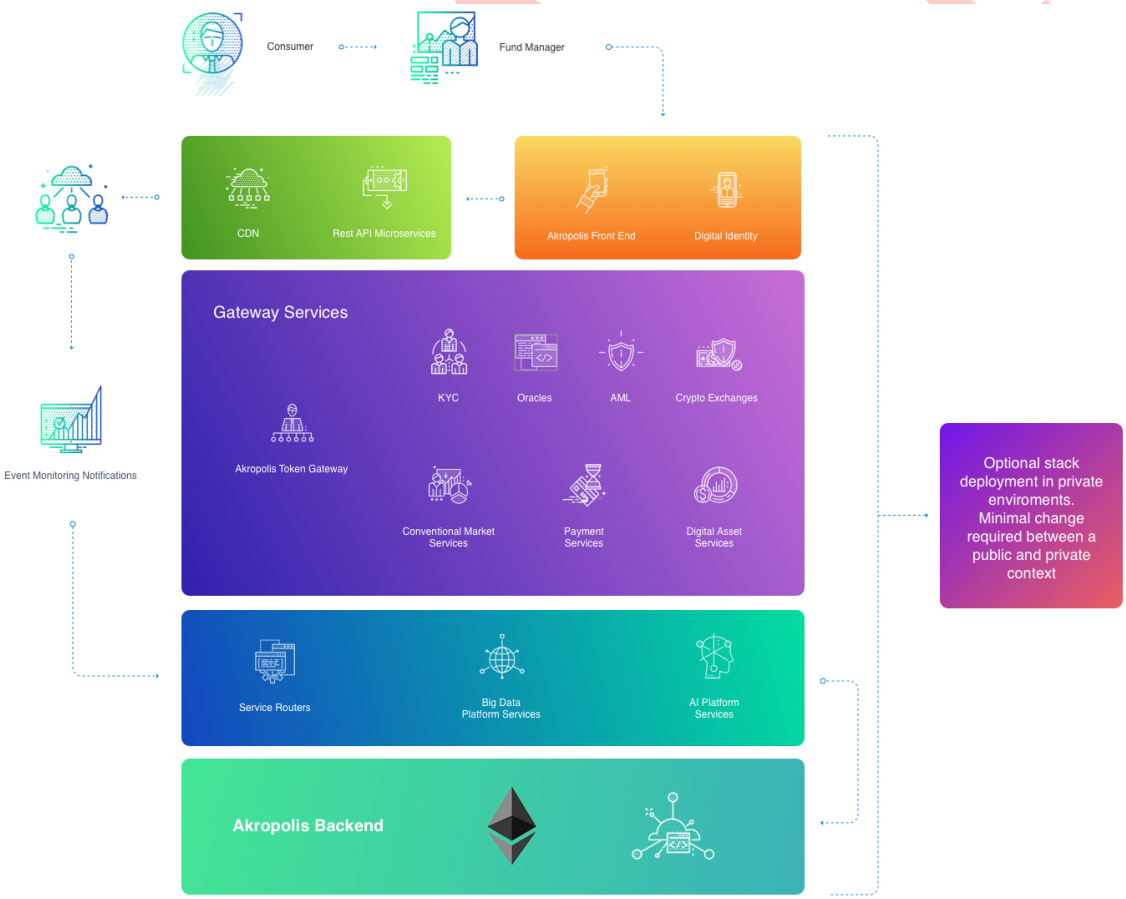

Figure 7. Backend Architecture

will be produced, both relying on the REST API exposed by Akropolis backend microservices along with the requisite wallet and private key support. These applications will be secured with multiple layers of authentication. Design for UI/UX and specific architecture choices for the applications will derive from the business case and users' needs.

C.3. Core Architectural Components

C.3.1. Blockchain and Smart Contracts

Institutional users may prefer to engage with a private blockchain solution for a variety of reasons, whilst the public chain will function in a more decentralised manner. The Akropolis platform will be protocol agnostic. As such, Akropolis will represent a network of public and private blockchains, with Ethereum being the primary protocol initially, followed by other blockchains as the platform evolves.

The ratio of centralised to decentralised capabilities is anticipated to evolve with time, reflecting both general changes in inter-generational saving patterns and the pursuit of transparency and accountability gains that may be achieved by replacing a pension fund activity with smart contracts. Subject to marketplace capabilities and transaction costs, Akropolis may seek to develop its own blockchain. This could provide cost advantages and enable more tightly integrated smart contract and protocol capabilities. Ultimately the platform will engage with multiple blockchains and as the number of blockchain protocols increases, the platform will need to flexibly manage a diverse range of smart contracts and their blockchain interactions.

The platform's core smart contract components act as the mediator of logic and validates the implementation of allocation actions. The initial version smart contract will be written in Solidity, a Turing-complete language that possesses sufficient flexibility to implement the required logic. Akropolis may also use other blockchains such as Adjoint.io's uplink which contains a non-Turing-complete financial scripting language for some security sensitive transactions. To evolve smart contracts and meet future requirements, a "Factory model" will be used in which administrative contracts manage the introduction of new smart contract capabilities.

C.3.2. Oracle Services

Blockchain smart contracts cannot directly retrieve external data, necessitating intermediary services referred to as Oracles. Third party oracle services are agents that typically work by finding and verifying the required external data and then submitting or pushing this information into a target smart contract on the blockchain. An example of desired external data is financial asset price feed information. Oracle services will be required to provide users with up-to-date information regarding fund performance and asset pricing. Asset tokenisation provides new ways for asset holders to interact with oracle services and access blockchain-external data.

C.4. Architecture Principles and Design Considerations

C.4.1. Resilience, Scalability and Performance

Blockchain networks are typically highly fault tolerant and resilient. However, they don't scale well when time sensitive transactions are involved, given the inherent nature of consensus algorithms and numerous resource constraints of each participant. Consequently, for Akropolis capabilities that require scalable, time sensitive transactions or data feeds, such as asset pricing, a combination of high-speed exchange gateways and data oracles will be adopted. In the case of private or permissioned blockchains, this is addressed through a combination of CDN delivered shared assets and highly elastic and fault tolerant infrastructures for selected participants or clusters thereof, as shown in Figure 8.

For key parts of the above core infrastructure, where the solution has to scale across dispersed geographies, an auto-scaling topology will be implemented allowing for transaction execution and data storage to dynamically respond to, and recover from, performance bottlenecks and faults. Containerised, stateless and non-snowflake design patterns are crucial to achieve resilience, scalability and performance objectives (for example, in the integration and gateway bridging services context). This is demonstrated in the above figure, with a Kubernetes orchestrated container application workload for a private-chain deployment.

C.4.2. Security, APIs and Micro-services

Secure, scalable and efficient microservices are an important part of the Akropolis service-oriented backbone. These microservices are critical to ensure that the end-to-end platform can operate seamlessly both within its own network and between networks and other third parties. This microservices architecture pattern is shown in Figure 9.

The backend microservices plays the role of primary coordinator of business logic on the Akropolis platform andserves the following functions:

- Implement identification and authorization, working in conjunction with the smart contracts.
- Handle usage flows and logic for the Assets.
- Receive the events raised by blockchains from the monitoring micro-service.

There will be a RESTful web service for handling requests to the backend micro-service application layer.

Where applicable, to satisfy various KYC and AML requirements, the management of digital identities, associated validation and access management will be performed using highly secure, end-to-end encryption mechanisms and

DRAFT

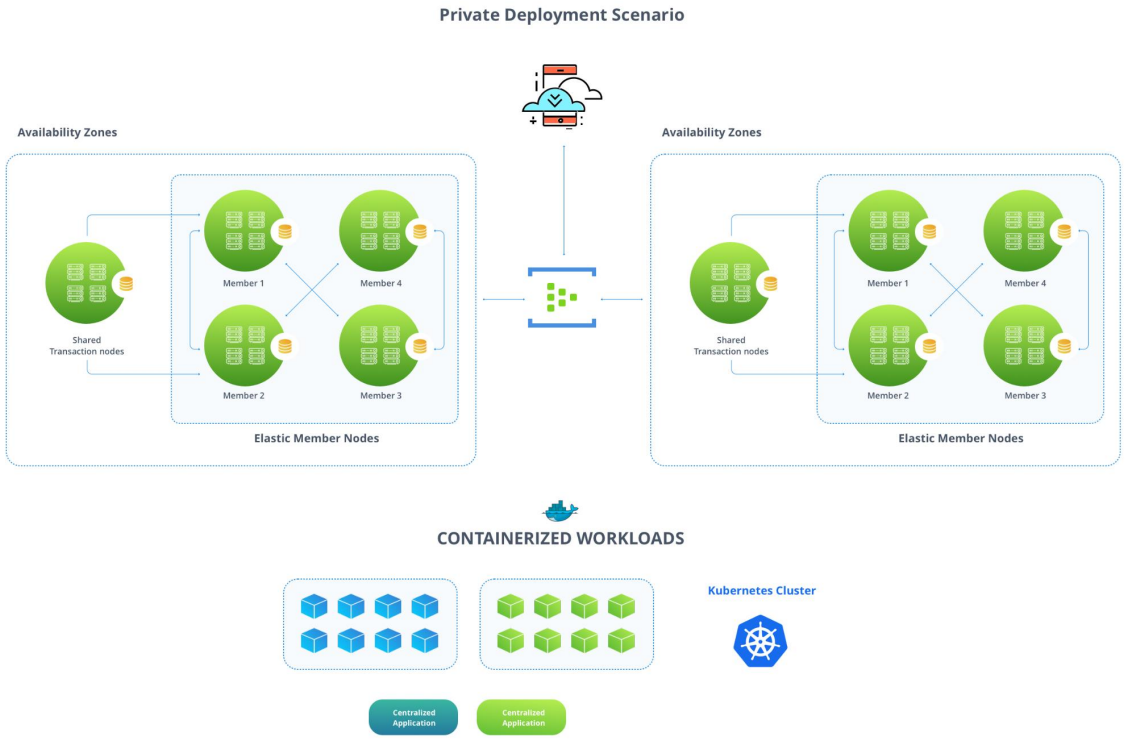

FIGURE 8. Private Deployment Scenario

multi-factor authentication methods. As existing cryptographic security algorithms gradually become obsolete (e.g., RSA and AES) and emerging quantum resistant ones mature (e.g., Ring-LWE and Merkle Hash Trees) Akropolis will adapt in turn.

C.4.3. Data Platform

Fundamental to the Akropolis data platform is the requirement to retain a wide variety of data such as asset information, fund data, oracle-provided information, blockchain and user events occurring throughout the platform, as well as broader platform related analytical data. The implementation must address various information and reporting needs as well as provide the ability to detect anomalies and help prevent malicious usage within the Akropolis platform.

Given the variety of data that must be collected and managed with different data processing requirements, a hybrid data architecture stack will be adopted and collectively referred to as the "Akropolis Data Platform." This data architecture will span blockchain storage, a highly available big data platform and other distributed storage technologies accessed through a supporting microservices layer. The high-level data architecture pattern is illustrated in Figure 10.

C.4.4. Third Party Products, Platforms and Integrations

To provide the highest possible levels of transparency, the platform will:

- Publish approved exchange APIs to guard against the malfunction or hijacking of the Akropolis APIs themselves.
- Publish summary statistics of activity on the platform, such as asset level operation matrices.
- Employ access tokens to pay fees to operate PoA contracts and keep them alive. These can only be generated by locking AKT into the access token contract.

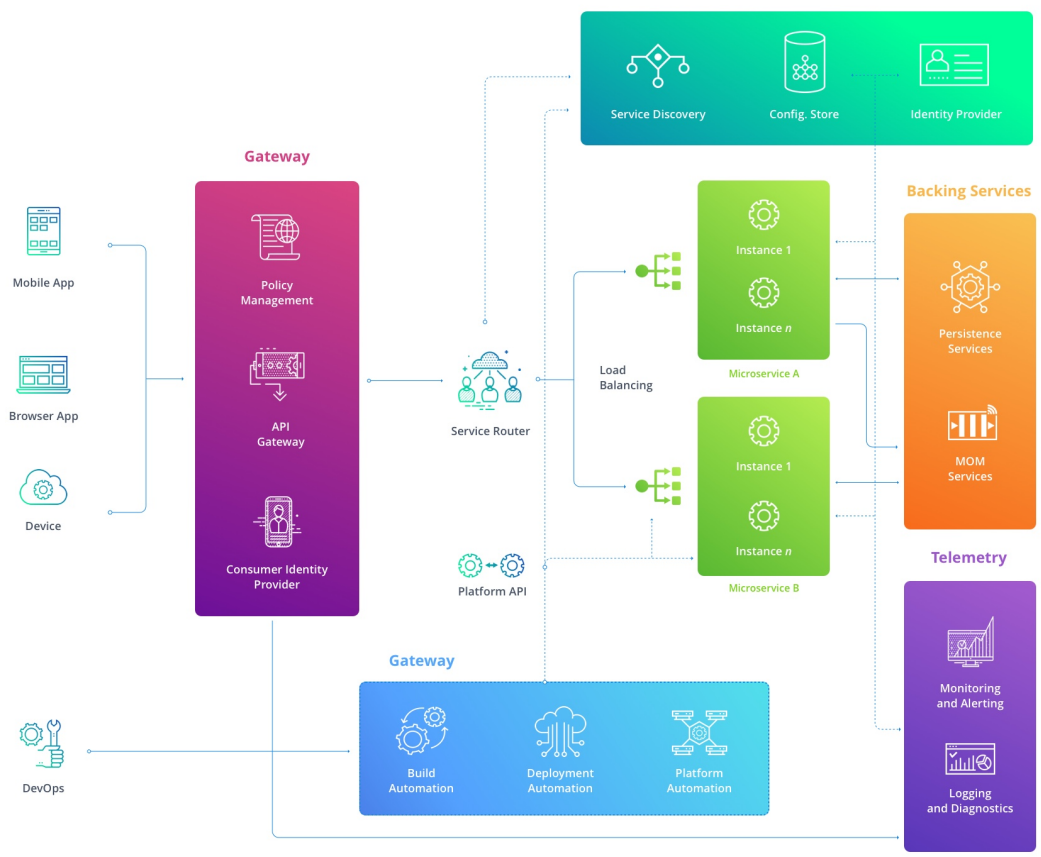

FIGURE 9. Micro-services

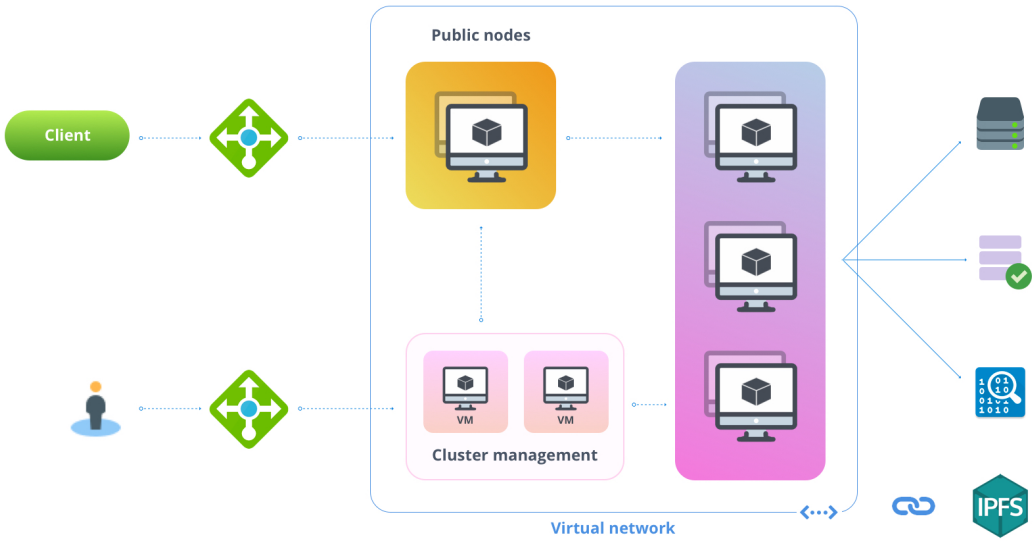

FIGURE 10. Architecture

References

[1] Alex Zhavoronkov. Longevity expectations in the pension fund, insurance, and employee benefits industries. *Psychology Research and Behavior Management*, page 27, January 2015. *DOI:*10.2147/prbm.s75440.

[2] Global Pension Statistics - OECD, 2017, Available: http://www.oecd.org/finance/private-pensions/globalpensionstatistics.htm. Accessed on March 2018.

[3] Laurence J. Kotlikoff and Scott Burns. *The Coming Generational Storm: What You Need to Know about America's Economic Future*. The MIT Press, 2004. *ISBN:*0262112868.

[4] We'll Live to 100 - How Can We Afford It? Technical report, World Economic Forum, May 2017. Available: http://www3.weforum.org/docs/WEF_White_Paper_We_Will_Live_to_100.pdf.

[5] Mark O'Byrne. Pensions and Debt Time Bomb In UK: £1 Trillion Crisis Looms. September 2017, Available: http://www.marketoracle.co.uk/Article60291.html.

[6] Attracta Mooney. US faces crisis as pension funding hole hits $3.85tn. *Financial Times*, May 2017. Available: https://www.ft.com/content/f2891b34-3705-11e7-99bd-13beb0903fa3.

[7] Richard Dyson. The £1 trillion pension crisis facing 11m (and they're the lucky ones. *The Telegraph*, 2016. Available: https://www.telegraph.co.uk/pensions-retirement/news/the-1-trillion-pension-crisis-facing-11m-and-theyre-the-lucky-on/.

[8] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available: https://bitcoin.org/bitcoin.pdf.

[9] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014. Available: http://gavwood.com/paper.pdf.

[10] Raiden. The Raiden Network. Website, Available: https://raiden.network/101.html. Accessed March 12, 2018.

[11] Joseph Poon Vitalik Buterin. Plasma: Scalable Autonomous Smart Contracts. August 2017, Available: https://plasma.io/plasma.pdf.

[12] Ethereum. Github: Sharding FAQ. Website, Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ. Accessed March 12, 2018.

[13] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. *Preprint:*1710.09437v2.

[14] Ameer Rosic. What is Ethereum Casper Protocol? Crash Course. blockgeeks, 2017, Available: https://blockgeeks.com/guides/ethereum-casper/.

[15] Guy Zyskind, Oz Nathan, and Alex Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *Preprint:*1506.03471v1.

[16] Introduction to MimbleWimble and Grin. Website, Available: https://github.com/mimblewimble/grin/blob/master/doc/intro.md. Accessed March 12, 2018.

[17] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*. ACM Press, 1988. *DOI:*10.1145/62212.62222.

[18] Eli Ben-Sasson Alessandro Chiesa Christina Garman Mathew Green Ian Miers Eran Tromer Madars Vizra. Zerocash: Decentralized anonymous payments from bitcoin (extended version). May 2014, Available: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[19] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive, Report 2018/046, 2018. https://eprint.iacr.org/2018/046.

[20] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. 2017, Available: https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf.

[21] Mathew Spoke Nuco Engineering Team. Aion: The third-generation blockchain network. July 2017, Available: https://aion.network/downloads/aion.network_technical-introduction_en.pdf.

[22] Jae Kwon Ethan Buchman. Cosmos: A network of distributed ledgers. 2017, Available: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md.

[23] Eos.io : Technical white paper v2. Github, Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md. (visited on March 2018).

[24] Cardano settlement layer documentation. Website, Available: https://cardanodocs.com/introduction/. (visted March 2018).

[25] Sergio Lerner. Rsk, November 2015, Available: https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf.

[26] Nick Szabo. Micropayments and Mental Transaction Costs. 2001. Accessed March 27, 2018, Available: https://www.researchgate.net/publication/2401801_Micropayments_and_Mental_Transaction_Costs.

[27] Christian Lundkvist Rouven Heck Joel Torstensson Zac Mitton Michael Sena. Uport: A platform for self-sovereign identity. UPort, 2017, Available: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.

[28] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979. Available: https://dl.acm.org/citation.cfm?id=359176.

[29] Tenzorum: Key Management Protocols for the Decentralized Web. Website, Available: https://tenzorum.org/. Accessed March 12, 2018.

[30] Akropolis Sigma Prime. An incentivised accountability protocol for decentralised marketplaces. *In preparation*, 2018.

[31] Jack Peterson Joseph Krug Micah Zoltu Austin Williams Stephanie Alexander. Augur: A decentralized oracle and prediction market platform. February 2018, Available: http://augur.link/augur.pdf.

[32] Arpad E. Elo. *Logistic Probability as a Rating Basis, in The Rating of Chessplayers, Past & Present.* Bronx NY 10453: ISHI Press International, 2008. *ISBN:*978-0-923891-27-5.

[33] Peter Vessenes. The DAO Is Almost Totally Apathetic: It Should Stay That Way. Website, May 2016, Available: http://vessenes.com/the-dao-is-almost-totally-apathetic-it-should-stay-that-way/. Accessed March 16, 2018.

[34] DAOstack. Decentralized Governance Matters. Website, February 2018. Accessed March 16, 2018.

[35] World Economic Forum. Realizing the Potential of Blockchain, June 2017, Available: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf. Accessed March 16, 2018.

[36] Henry M. Kim, Marek Laskowski, and Ning Nan. A first step in the co-evolution of blockchain and ontologies: Towards engineering an ontology of governance at the blockchain protocol level. *Preprint:*1801.02027v1.

[37] Nic Carter. A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors. Master's thesis, University of Edinburgh Business School, 2017. Available: https://coinmetrics.io/papers/dissertation.pdf.

DRAFT

[38] DAOstack. The Operating System for DAOs, October 2017. Accessed March 16, 2018.
[39] Mike Goldin. Token-curated registries 1.0, September 2017, Available: https://docs.google.com/document/d/1BWWC__-Kmso9b7yCI_R7ysoGFIT9D_sfjH3axQsmB6E/edit. Accessed March 16, 2018.
[40] James Young Mike Goldin, Ameen Soleimani. The adchain registry, May 2017, Available: https://adtoken.com/uploads/white-paper.pdf. Accessed March 16, 2017.
[41] Alexander Khoriaty Matus Lestan, Joe Urgo. district0x network - a cooperative of decentralized marketplaces and communities., September 2017, Available: https://district0x.io/docs/district0x-whitepaper.pdf. Accessed March 16, 2018.
[42] O. Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, 2007. *ISBN:*9781139430234.
[43] Karl Floersch. Learning solidity part 2: Commit-reveal voting, 2017, Available: https://karl.tech/learning-solidity-part-2-voting/.
[44] Parity Technologies. parity-bridge source code repository, Available: https://github.com/paritytech/parity-bridge. Accessed March 16, 2018.
[45] PostgreSQL. Website, Available: https://www.postgresql.org/. Accessed March 20, 2018.
[46] Anthony C. Eufemio Kai C. Chng Shaun Djie. Digix's whitepaper: The gold standard in crypto-assets. 2016. Available: https://dgx.io/whitepaper.pdf.
[47] Tether.to. Tether: Fiat currencies on the bitcoin blockchain. 2014. Available: http://www.the-blockchain.com/docs/Tether%20Whitepaper.pdf.
[48] JP Morgan Chase. Quorum whitepaper v0.1, 2016, Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf. Accessed March 15, 2018.
[49] Sean Foley, Jonathan R. Karlsen, and Talis J. PutniÅĘs. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? January 2018, Available: https://ssrn.com/abstract=3102645.
[50] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. *Preprint:*1107.4524v2.
[51] THE EUROPEAN PARLIAMENT and THE COUNCIL OF THE EUROPEAN UNION. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), 2016, Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
[52] Chris Babel. The high costs of gdpr compliance, November 2017, Available: https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263? Accessed March 15, 2018.
[53] The European Union Agency for Network and Information Security (ENISA). Privacy and data protection by design, January 2015, Available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. Accessed March 15, 2018.
[54] Pillar Project A.G. Simplify GDPR Compliance. Website, Available: https://pillarproject.io/gdpr/. Accessed March 12, 2018.
[55] BCDiploma. Whitepaper v2.1, January 2018, Available: https://www.bcdiploma.com/img/BCD-WhitePaper_last.pdf. Accessed March 15, 2018.
[56] Lisk. The lisk protocol - security, Available: https://lisk.io/documentation/the-lisk-protocol/security. Accessed March 15, 2018.
[57] Aaron Voisine Sean Bowe Marek Palatinus, Pavol Rusnak. Mnemonic code for generating deterministic keys, March 2013, Available: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki. Accessed March 18, 2018.
[58] Satoshi Labs. Trezor developers guide - cryptography, Available: https://doc.satoshilabs.com/trezor-tech/cryptography.html. Accessed March 15, 2018.
[59] Ledger. On which wallet can I restore my wallet if I lose my Ledger device?, Available: https://support.ledgerwallet.com/hc/en-us/articles/115005297709-On-which-wallet-can-I-restore-my-wallet-if-I-lose-my-Ledger-device-. Accessed March 15, 2018.
[60] Parity. Backing up and restoring, Available: https://wiki.parity.io/Backing-up-&-Restoring.html. Accessed March 14, 2018.
[61] Mycrypto, Available: https://mycrypto.com. Accessed March 15, 2018.
[62] Jacob Eberhardt. ZoKrates: A toolbox for zkSNARKS on Ethereum. Github, Available: https://github.com/JacobEberhardt. Accessed March 20, 2018.
[63] Maker: Reference Implementation of the decentralized DAI Stablecoin issuance system. Website, Available: https://makerdao.com/purple/. Accessed on March 20, 2018.
[64] Pensions Dashboard. Prototype project, Available: https://pensionsdashboardproject.uk/. Accessed March 18, 2018.

DRAFT