Overview

Cognida™ delivers trusted blockchain solutions that address the increasingly complex information sharing challenges that enterprises face by allowing them to incorporate decentralized blockchain security features into their existing systems for external and internal sharing of data.

The Cognida Network™ and its open source platform enable enterprises to more securely manage connected devices, systems and shared information using blockchain agnostic technology.

Cognida's Service Interfaces secure digital assets on the network, enabling enterprise IT administrators to enforce their security policies and establish trusted connected relationships, owning and controlling their data, even when sharing with service providers and third parties.

Enterprises can leverage Cognida's Service Network Interface to connect to trusted service networks where they can administer third-party cloud services from a single interface, enabling administrators to manage privacy, access, and security of their data on remote systems through a unified platform.

As enterprises adopt new distributed technologies, the data landscape is evolving away from centralized services maintained behind corporate firewalls to a complex distributed landscape. This trend has corporate data scattered across devices and services outside the enterprises' administrative control.

The decentralized features of blockchain offer solutions for enterprises to regain control in this distributed data landscape. To onboard these solutions, the gap between enterprises and blockchains must be bridged so that the blockchains' integrity is not altered and organizations can retain and administer service relationships with trusted service providers.

The Cognida Platform, which has been developed by Windmill Enterprise, solves these disconnects by enabling enterprises to benefit from the advantages of existing blockchain technology to address their growing security and privacy challenges. The Cognida Platform will be released to the open source Cognida Foundation at the launch of the Cognida Service Network.

1. The Technology of Cognida

1.1 Addressing the Enterprise Blockchain Disconnect

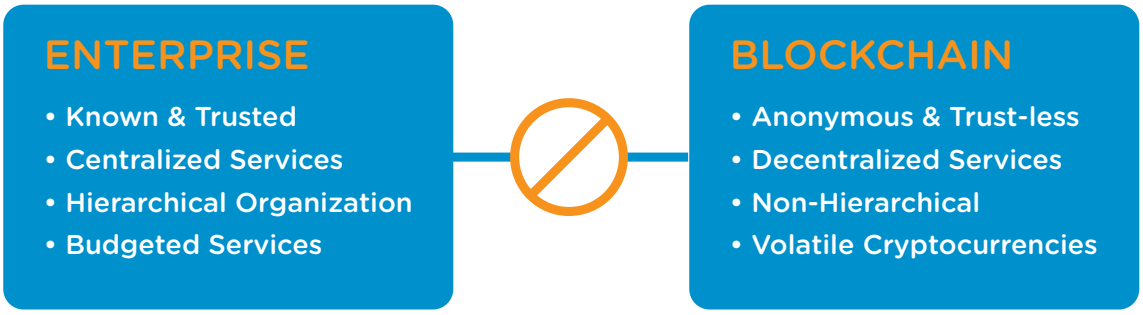

fig. 1: Enterprise Blockchain Sector Disconnect

Enterprise IT and security managers are beginning to show interest in blockchain technologies, but the plethora of solutions to choose from is daunting. Additionally, blockchain technology presents barriers to adoption with enterprise customers due to the vast cultural differences between enterprise security and blockchain communities, and the advanced skills required for education and development.

Enterprises on the verge of embracing the technologies face these issues:

1. Blockchains are inherently anonymous and their transactions are performed in a trustless manner which is incongruent with enterprise security policies which require known and trusted services and transactions on their network.
2. Services and ledger data are decentralized and distributed across anonymous locations. Enterprise security traditionally uses centralized security with equipment located in known locations.
3. Enterprise security administration is done in a hierarchical fashion. Administrators and managers have varying levels of access and control within the enterprise. Blockchain security is not natively hierarchical. While existing smart contract technologies address some of these challenges, they are difficult to map to complex security policies found within enterprises.

1.2 Cognida Platform Core Features

The Cognida Platform solves these crucial issues through its native core capabilities:

Blockchain Agnostic

- Enterprises will not have to choose one blockchain with the built-in compatibilities
- Cognida delivers standardized security APIs for interaction with multiple blockchains
- Blockchain portability allows migration between blockchains or the ability to utilize multiple blockchains
- Built-in optimized interoperability allows best possible utilizations of different blockchains

Distributed Permissions

- Removes a single point of failure by using distributed blockchains that have immutable properties
- Allows multiple stakeholders the capability of interacting and retrieving data

Trusted relationships

- Ledger data is anonymized and unreadable outside trusted stakeholders

Secure Interaction with Service Providers

- Enables third-party services to address volatile cryptocurrencies associated with Blockchains to offer predictable cost structures
- Single-payment interface across multiple vendors and services

Familiar Administration Functionality

- Supports administration hierarchies common in enterprises
- Delivers extensive permission and access controls critical to securing cloud services
- Enables enterprise to manage permissions more efficiently across all remote locations

1.3 Blockchain Services

The Cognida open-source platform provides blockchain API libraries that map to enterprise services, including:

1. API translation services and App2BC integration
2. API proxy services (access toggling agents to communicate with users)
3. Authentication (verifying devices and individuals within an enterprise)
4. Authorization (granting access to only the permissioned devices and instances)
5. Encryption (added security on hashes, permissions, and queries within the network)
6. Decryption (interpretation of encrypted signals and data within the network)
7. Data integrity (verifying the data obtained by a query has not been tampered with)
8. Subscription services (real-time feedback and alerts of devices synced to the Cognida Platform)

1.4 Cognida Agent Core

The Cognida Agent Core is a flexible compute architecture that can run on servers, PCs, tablets, and other devices. It offers a flexible programming environment that is script-based and template driven. Scripts executed on an agent can perform native protocol transactions on local devices, databases, and services. Templates are used to format and translate native data and messages into a common shareable format, enabling diverse and distributed devices and services to communicate using a common information protocol.

The Cognida Agent Core is used across the Cognida Platform to establish customized Service Interfaces. Agents are registered within an enterprise as a trusted node on the network using public/private keys. Digitally signed transactions authenticate the agent when communicating with administration messaging systems and shared data services.

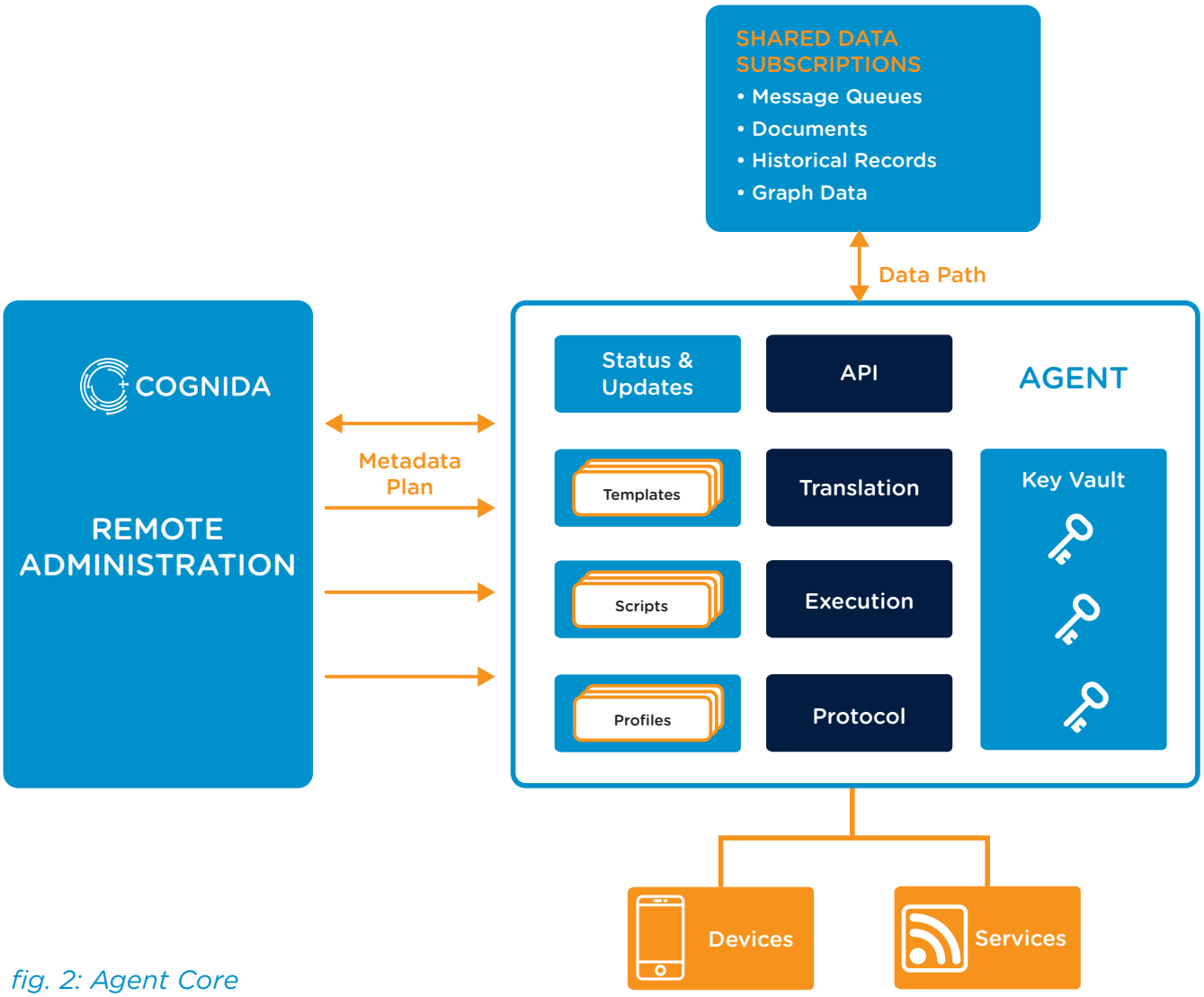

fig. 2: Agent Core

1.5 Cognida Service Interface

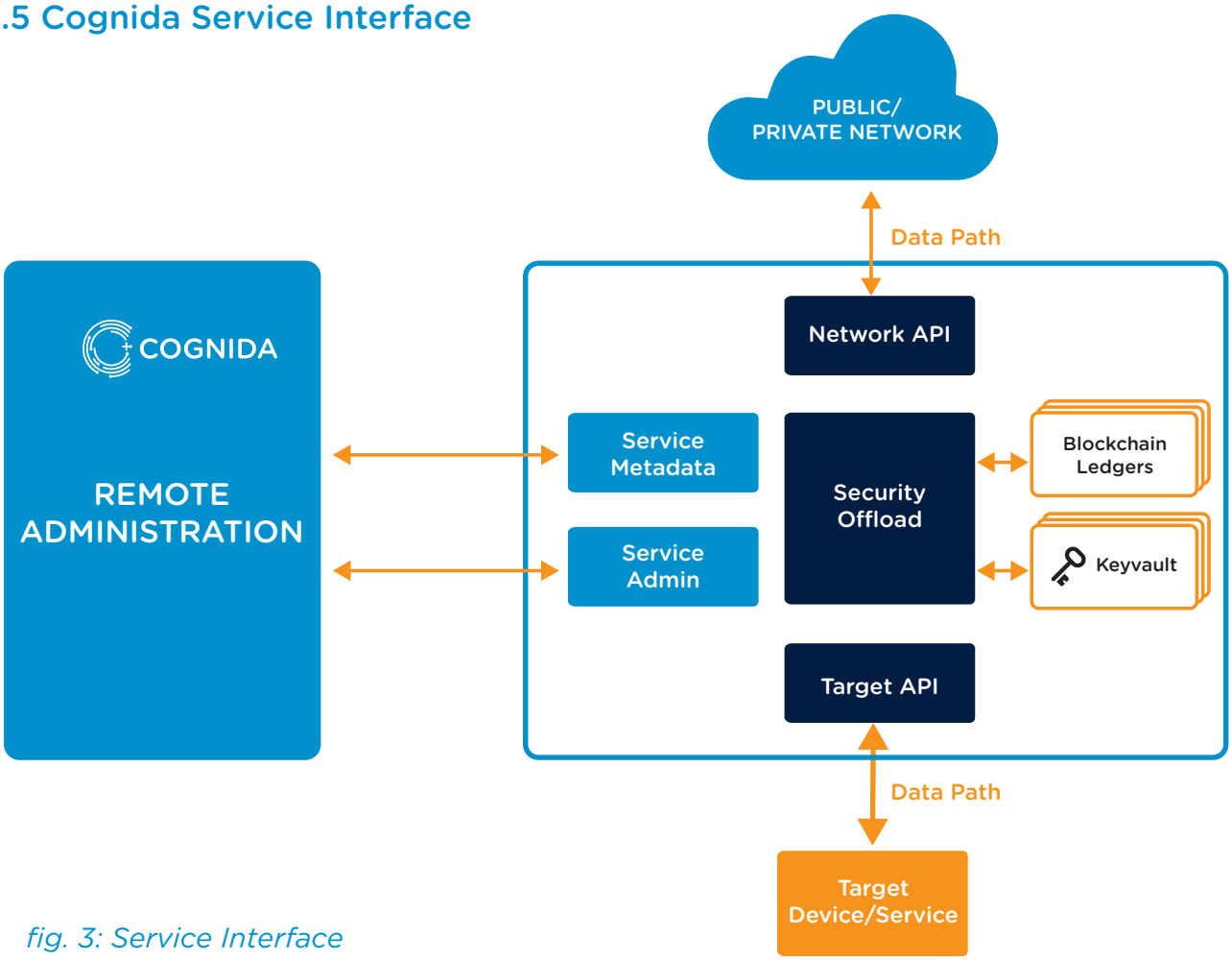

fig. 3: Service Interface

The Cognida Agent Core establishes the heart of the Cognida Service Interface. It utilizes its translation capabilities to connect to a public or private network API and transform API operations to a target device or service. The Service Interface offloads security operations, utilizing public/private key encryption/decryption and a suite of blockchain scripts that maintain and/or read local blockchain ledgers. Blockchain ledgers can be used to perform authorization and data integrity functions.

The remote administration capabilities enable administrators to remotely enforce security policies and manage service relationships on enterprise assets, cloud services, and remote devices or systems.

1.6 Subscription Services

This establishes a flexible security tool with applications ranging from securing legacy systems to enforcing access permission, data privacy, and security policies on cloud and SaaS services.

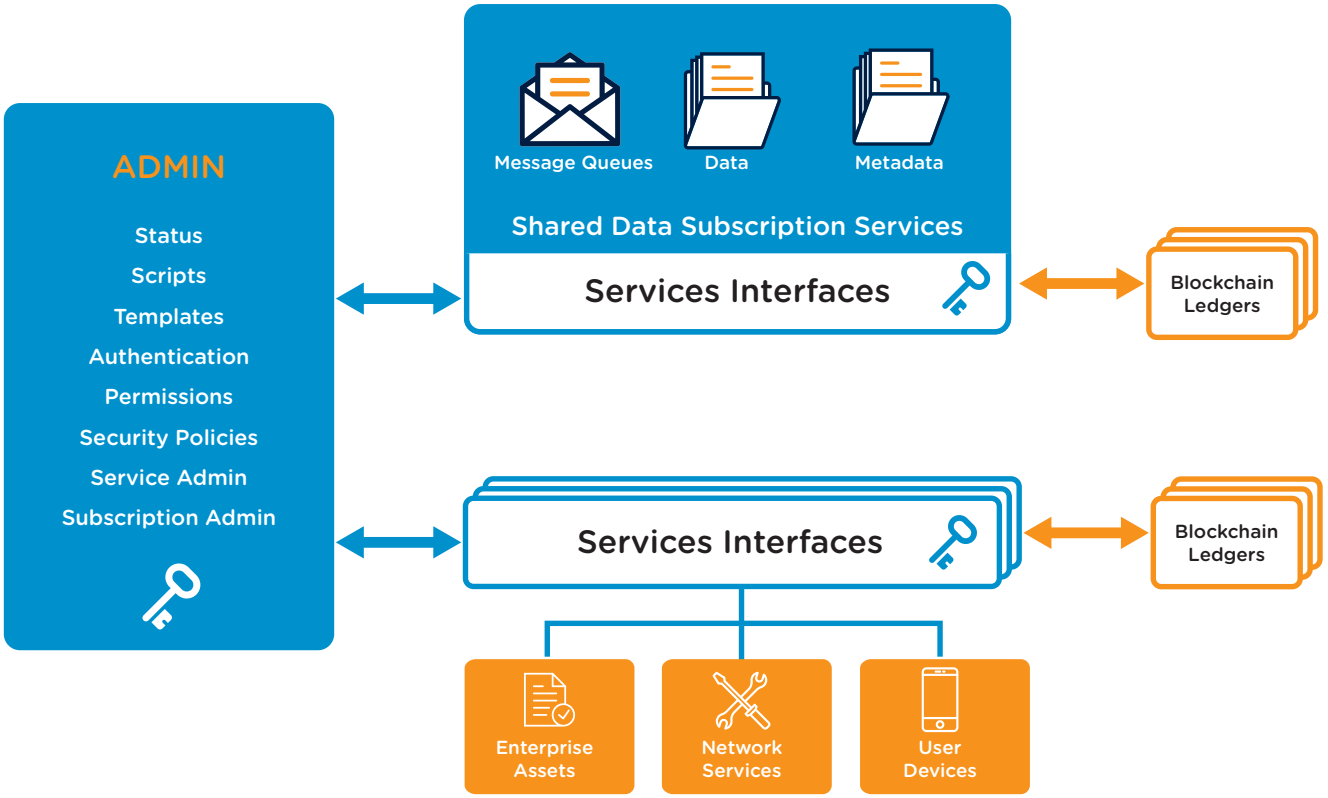

fig. 4: Subscription Services

The Cognida Platform comes with a flexible subscription services module. It incorporates the Cognida Service Interface, which offloads authorization, authentication, and security operations and connects to document databases and messaging services on a common API. The Admin Service feature offers a familiar interface through which subscriptions and subscription access can be administered with a hierarchy like those found within an enterprise organization.

Cognida's template-driven subscription architecture utilizes templates to profile access operations to data and messaging services. This offers a flexible set of tools that dynamically filters access on a subscription ID basis. This approach enables diverse systems, applications and devices to share messages, data and metadata using a common language.

1.7 Securing Enterprise Assets

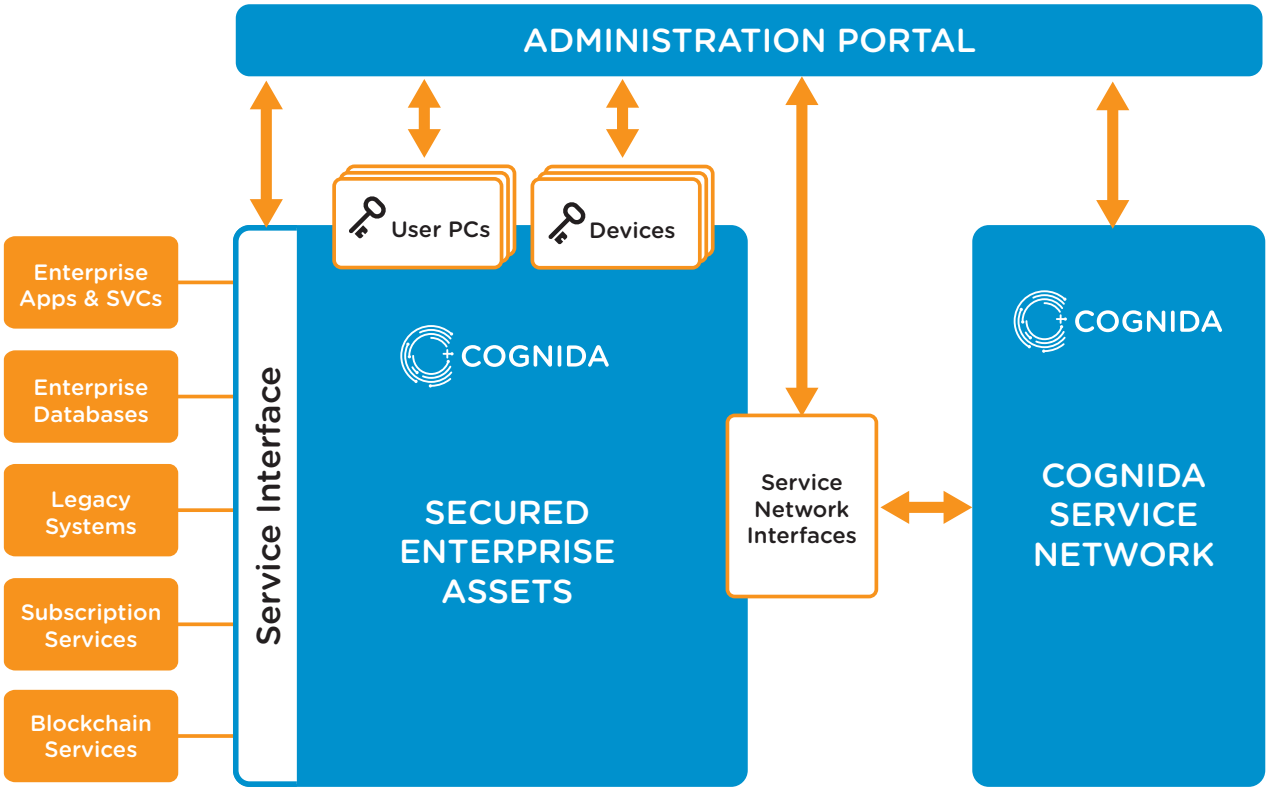

Fig. 5: Securing Enterprise Assets

Cognida's open source library offers tools for enterprises to administer public/ private keys within their organization to secure devices and user accounts on devices. The Cognida Service Interface can be deployed on existing applications and services that utilize distributed Blockchain ledgers to offload key based authentication and authorization functions, as well as performing any encryption/ decryption and blockchain-based data integrity operations.

These tools enable enterprises to integrate the Cognida Platform into their existing enterprise services with minimal disruption. Enterprises can choose to incorporate Cognida in an incremental fashion rather than an entire migration. The incorporation of Cognida subscription services offers flexible data sharing services across diverse systems within the enterprise and in the cloud, providing enterprise admins the ability to manage what is shared and with whom, both within and outside their organization.

1.8 Cognida Service Network

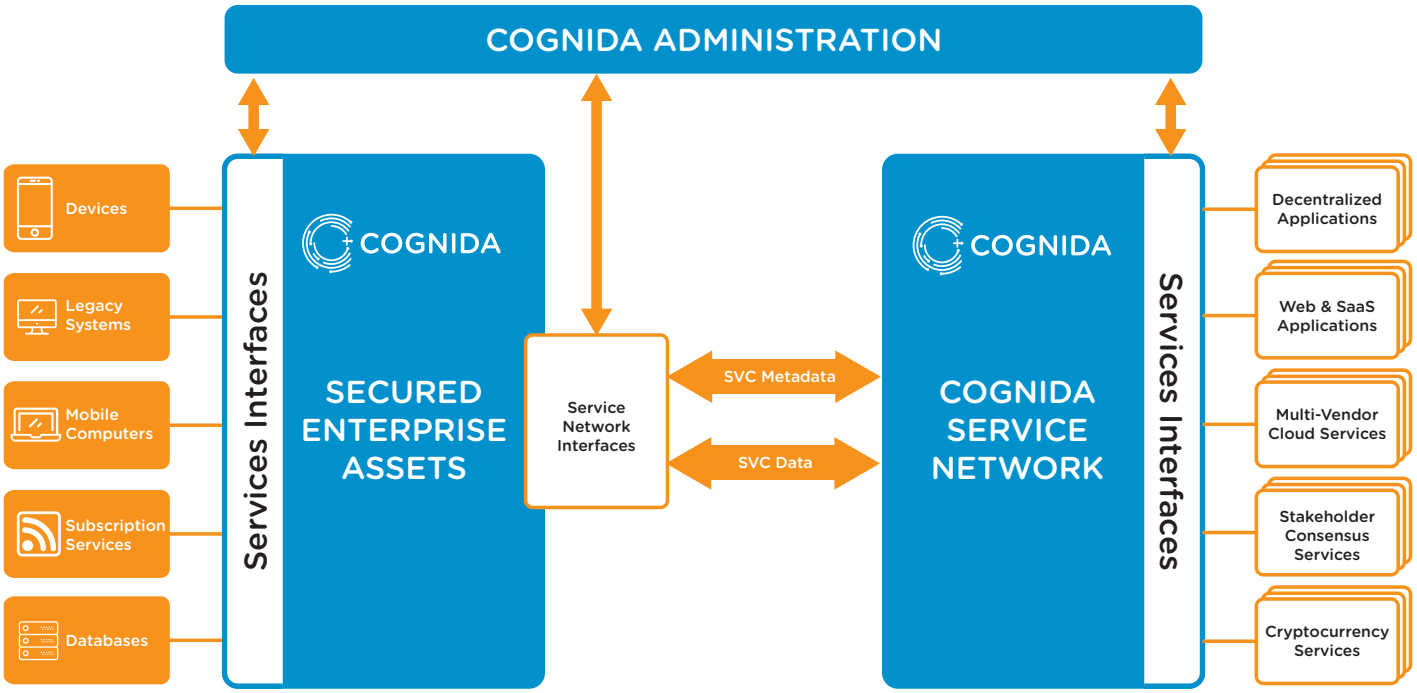

Fig. 6: Cognida Service Network

The Cognida Platform secures enterprise assets and provides a Service Interface into a network of trusted vendors. This reverses the conventional "terms of services" contracts that vendors require customers to sign. This approach enables enterprise administrators to enforce their service policies with Cognida Service Network Vendors including managing access to subscription data, enterprise assets and enforcing data persistence/deletion policies. This allows the Cognida Platform to provide solutions that are streamlined to comply with emerging regulatory policies such as the General Data Protection Regulation (GDPR), which came into effect in the EU in May 2018 and impacts all companies doing business with any company or individual in the EU.

1.9 Flexible Device Authentication

While the Cognida Agent provides public/private key generation for the device, there is not a singular solution that fits all needs, so it is adaptive to the environment's requirements. A great platform is not a rigid system and the Cognida team's extensive experience has observed that creating an adaptive system is a competitive advantage. In some cases, an IT administrator wants to assign identity by having physical access, two-factor authentication, biometric security, or another solution. The Cognida Platform provides a flexible integration solution for authentication, as methodology varies widely across enterprise organizations.

The Cognida Agent Core checks in with the Enterprise Administration Service on a regular basis to relay online status, fault conditions, and security risks. These communications are also used to update the device, including sending remote messages to reset, re-initialize, or disable a device. If a device is not responsive or considered a risk by policy, its permissions can be disabled on the network.

Security Policies can be highly configured, and while basic configurations are available, many administrators will use the provided tools and scripting capabilities to adapt to their needs. Some of the most common functionalities that may be used include:

- Combining user and device authentication to gain access to enterprise networks based on their imposed password policies and allowing secondary authentication like biometric data.
- The ability to detect tampering on device with scripts and issuing notifications. Some examples are multiple failed password attempts, GPS location reporting, and lapse of responsiveness.
- Any breach set by the Administrative level configurations can trigger events. Events include the revoking of the devices permissions on platform or temporarily locking specific classes of devices in the case of a broad breach.

2. COG Token

The Cognida Foundation will issue the COG cryptocurrency to provide a single cryptocurrency payment method for enterprise customers to utilize to pay for settlement services. This offers several advantages:

1. COG cryptocurrency is based on the value of the Cognida Network and Platform to members and customers.
2. The native currency makes it possible to create more predictable and stable cost structures.
3. The COG cryptocurrency is the currency that supports ongoing services offered by the Foundation, including Settlement Network oversight, open source development, and administration.
4. Utilization of COG cryptocurrency to a fund paid into by Settlement Providers provides the Foundation with tools to trigger release of these funds to customer accounts if a service provider fails to deliver on contractual agreements.

2.1 Token Details

The Cognida token is an ERC20 token with a maximum supply of 550 million. The Cognida token facilitates the Settlement function between providers of services to create a unified token. Cognida's Settlement Engine manages exchange to other tokens or currencies needed to facilitate the use of the platform.

Meta-data from the Enterprise security services provides Cognida security related transaction data so COG Tokens stored in a COG wallet can be transferred into the appropriate cryptocurrency accounts to ensure sufficient coins are present to support ongoing transactions. Third-party service providers will charge their own fees for services, and these will be added to the enterprise's projected and ultimate cost in COG Tokens.

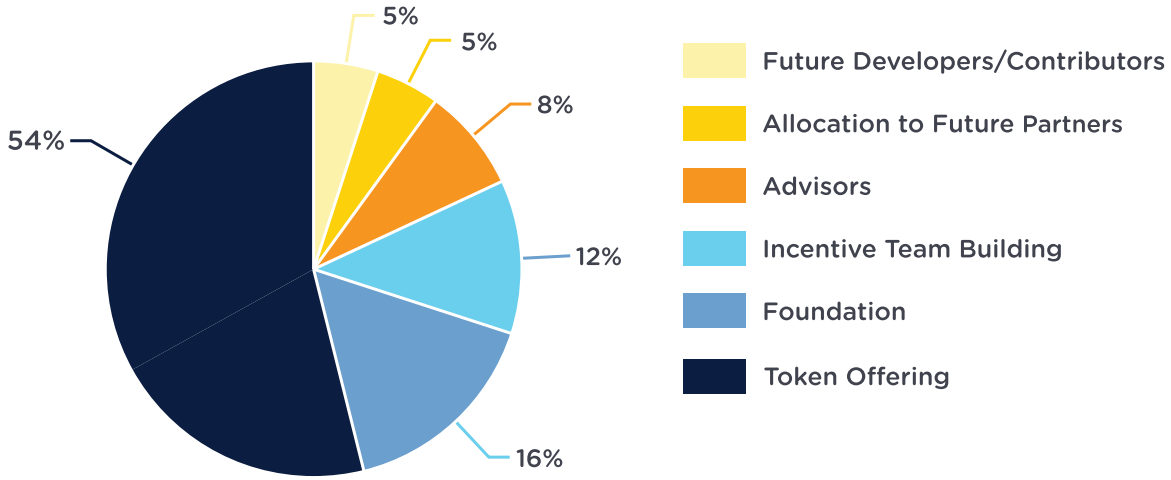

Fig. 7: Token Allocation

3. Cognida Open Source Foundation

The Cognida Open Source Foundation will be a US-based non-profit. Its role will include oversight of ongoing community development of the Cognida Platform, as well as administration of the Cognida Network.

3.1 Cognida Platform Community Development

Foundation members will jointly oversee ongoing enhancements of the platform. This will involve membership voting to issue proposals for new projects and selection of developers. COG coins will be the method of compensation for ongoing development.

Primary development enhancements include:

1. API libraries for new blockchains
2. New security services
3. Open source decentralized applications
4. Administration tools

3.2 Cognida Service Network

The Foundation will provide oversight and administration of the Cognida Service Network. Its roles include:

1. Recruitment of service vendors
2. Oversight and enforcement of service network policies

Service network connection and transaction fees will provide the Foundation with funds for these ongoing services.

4. About Windmill Enterprise

Windmill Enterprise, Inc is a Delaware 'C' corporation co-founded by Michael Hathaway of Information Xchange, Inc, and Bing Byington of CareConnex. Bringing the technology and capabilities of their two companies together unites decades of technology and know-how that addresses information access security in the Industrial IoT sectors.

Windmill Enterprise has transformed an existing token-secured information sharing and access platform into the blockchain agnostic Cognida platform. In addition, Windmill is developing the first Cognida enterprise application, providing HIPAA compliant information management and access services to the clinical trials market sector.

Following the launch of the Cognida Network, Windmill Enterprise will be an ongoing platform contributor and member of the Foundation required to pay the network of service providers in tokens native to the open-source network for interaction. Beyond participation with the Cognida Foundation and development community,

As a founding member, Windmill Enterprise will bring new customers and market sectors into the platform and encourage new enterprises to manage their data universe with blockchain powered data integrity solutions.

Windmill will also operate on a continuing basis as an integration and development contributor to guide enterprise clients in their implementation of Cognida.

4.1 Blockchain Technology Integration and Partnerships

Windmill has a growing list of technology partners that it is incorporating under a single enterprise framework. In addition, Windmill is integrating key cross-chain technologies into its platform. The Windmill framework offers enterprise software developers a menu of technologies to incorporate into their application. This is done transparently through the application. Windmill will offer a single token as currency for services. Any token transactions required by Windmill partners will be settled transparent to the application.

Technologies currently identified for integration into the Windmill platform:

- Rivetz Intl is a formal Windmill technology partner. Rivetz's Trusted Execution Environment (TEE) takes advantage of security hardware being integrated into mobile processors. This provides a vault for private keys that cannot be accessed by applications. TEE brings an entirely new level of device authentication that secures data transactions and validates data at the source.
- Factom offers cross chain transaction services that supports document security and authentication.
- Wanchain operates a private, consensus based Blockchain platform that addresses the needs of enterprises and financial institutions. Wanchain connects to multiple blockchain platforms to facilitate cross-chain token exchanges.

4.2 Development Partners

Information Xchange (IX) www.ixot.net
Information IX's core technology, Tensor-Connect, evolved out of decades of connecting devices and systems to the internet in demanding industrial environments. Tensor-Connect enforces ownership of data using a tokenized security system enabling parameter level access permissions to be enforced across the Enterprise, Cloud and Internet connected devices.

CareConnex www.caretrendsconnex.com
CareConnex is an FDA Medical Device Data System "MDDS" with 10+ years of transferring, storing, converting, formatting, displaying, and integrating patient data from medical devices in hospital ICUs, EDs, General Surgical departments, and Homecare sectors.

Rivetz www.rivetzintl.com
Rivetz Trusted Execution Environment ("TEE") should be thought of as a private "vault" inside your device's hardware – but instead of software (like apps and iOS/Android), it's already built into your device (the hardware). Inside of this vault, everything is isolated which makes it an ideal location to store private keys needed for blockchain transactions. Furthermore, the Rivetz app will take a snapshot
of your device's health and store it on their distributed network. The Rivetz app will verify the user's device identity and health status by comparing the device's current health snapshot to the one they have on file. Rivetz has an infrastructure that will record the details of all riveted transactions. Each transaction will have proof that the device that authorized the transaction was in compliance with the
requirements set by the user.

5. Windmill Team

5.1 Leadership Team

Michael Hathaway, Co-Founder, Technology and Managing Director

Michael Hathaway's career has placed him in the vortex of multiple electronic revolutions. In his early career, he worked with pioneers in electronic music and digital audio. After developing a line of affordable digital audio products at Lexicon (acquired by Harmon Industries), he transitioned to the networking sector. He was a technical contributor during the early days of Ethernet and ATM network switches, culminating in developing the first gigabit capable Internet packet forwarding engine for a DARPA project while working at BBN. He was a founder and executive at the pioneering terabit Internet router startup, Ironbridge Networks, and CTO at network processor startup Agere (acquired by Lucent Micro).

Since 2003, after a short stint working with Venture Capitalists, Michael set his sights on developing a signaling and messaging layer to facilitate secure transactions over the public Internet. After 10 years of applying his architecture principals across multiple consulting projects, he founded Information Xchange (IX) and developed the Tensor-Connect platform based on his architectural principles. This lightweight information management platform assigns tokens to users and software applications, providing parameter level access permissions to Internet accessible data. This technology is the core of applications in Industrial IoT and agriculture sectors. With blockchain now reaching a level of maturity to support enterprise applications, he is spearheading the incorporation of blockchain into Tensor- Connect. He believes the incorporation

Bing Byington, Co-Founder, Strategy and Operations Director

Bing Byington is a serial entrepreneur creating businesses in the mobile wireless, digital imaging and healthcare sectors. The famous words "Some people see things as they are and ask 'why'? Others see things as they should be and ask 'why not?'" initially led him into the very early days of the cellular phone industry. He became the CEO and a principal of a consortium of seven Mobile/Cellular licenses in the US and two internationally and sold his business to George Soros and the predecessor companies to Verizon and AT&T Mobile. In his next venture, he built industry leading digital imaging software for early generation digital cameras.

The benefits and cost savings for consumers and photographers were obvious to him. As the digital photography market matured, the company's solutions became mainstream and utilized for events, weddings, school photos, and government IDs. The business was sold to Kodak. Bing is currently Executive Chairman of CareConnex, integrating patient data from hospital ICUs and emergency wards, beyond the hospital walls into EMRs, lowering re-admissions and supporting "aging in place." These healthcare, wireless, and technology experiences have led him to his clear understanding of the need to utilize protocols layered on top of a blockchain to create platforms to deliver enterprise solutions for a variety of industries.

Wayne Lawler, Founding Partner, Customer and Enterprise Relations Director

Wayne Lawler is an accomplished executive with more than 30 years of leadership management roles in the technology, software, hardware and semiconductor fields working at IBM, Dell, Flextronics, HP Enterprise, Applied Materials, and Information Xchange. Wayne's guidance has repeatedly resulted in revenue growth multiples, business transformation success, and successful timely product launches. Key roles include: Sales & Business Development, Global Account Management, Program Management, New Product Development, Supply Chain Management Operations & Procurement, Customer/Supplier Business & Relationships Management, and Software Development Contracts Management.

Wayne graduated from Duke University with a Master of Business Administration from the Fuqua School of Business and from Michigan State University with a degree in Supply Chain Management from the Eli Broad College of Business.

Frank Fernandez, Partner, Director of Finance

Frank Fernandez has been managing and advising multi-billion-dollar institutional private equity portfolios for more than 20 years. More recently, he has been utilizing this experience to serve as an advisor to blockchain projects such as Cognida, Hatch Crypto and Vault Wallet. He founded Gateway Private Capital ("GPC") in 2004 to advise large institutional investors and assist with the management of their private equity portfolios. Since 2008, he also has served on the Investment Committee for Keystone National Group, a private equity and private credit fund manager with over $1 billion under management. Frank previously was the founding member and Senior Portfolio Manager of the Alternative Investments Asset Class at the $100 billion Florida State Board of Administration.

During his six years at the Board, Frank managed a private equity portfolio with over $6 billion of committed capital, including a $1 billion direct investment program and a $1 billion co-investment program. He was a member of more than 20 advisory committees, for funds at Carlyle Group, Apollo, among others and from 2000 - 2004 served as the Vice- Chairman of the Institutional Limited Partners Association. After receiving an MBA in finance from Tulane University's Freeman School of Business and a BS in engineering from Tulane's School of Engineering, Frank began his career in New York at Kidder Peabody & Co. in the investment banking.

department and then moved to Smith Barney in Chicago. A former officer in the U.S. Army, he has also served as a member of the Advisory Board of the Robert Toigo Foundation.

Josh Jones, Chief Marketing Officer

Josh Jones is a global corporate and marketing strategist who specializes in growth expansion strategies, branding, communication, marketing technology and measurement and go-to-market initiatives. Prior to joining Cognida in 2018, he led B2B initiatives and marketing for Oh My Green. His 14+ year background allows for complex understanding and improvement of revenue growth and service levels across pre-sales, negotiation, and product and service delivery. Notable is his in-depth insight and application of customer experience and outreach programming, where his efforts focus on acquisition and conversion.

Josh's greatest strengths are his creativity, leadership, and entrepreneurship. As the Founder and President of Dine on Demand, a food technology company, he produced organic growth and sold the company in 2016 to Zula Food. He then served within the role of VP, Sales and Marketing for Zula Food, where he led national expansion efforts. He thrives on challenges, particularly those that expand the company's reach through deployment of digital marketing solutions that create an insight-driven culture. Josh is recognized as a volunteer for multiple industry organizations, including serving as VP for the Restaurant Marketing and Delivery (RMDA) Board.

Lead Developers and Architects

Jon Saperia, Enterprise Architect

Formally a Harvard Enterprise and Software Architect who has a system architecture background in network management and enterprise platforms, Jon Sapiera also has extensive experience in encryption and authentication technologies for large commercial networks and enterprise networks. In addition, Jon has proven success managing software development teams on large scale projects, maintaining deliverable schedules and budgets. He has held architect positions at Digital Equipment Corp, IronBridge Networks, Ohia Networks, Ambient University, and Harvard University.

Michael Anderson, Software Architect

Harnessing a strong dedication to reducing technology miscommunication in the workplace and creating scalable technology solutions that enhance business development and performance, Michael Anderson has always enjoyed supporting and managing broad spectrums of technology for companies in multiple stages of growth. His career includes roles as Senior Software Engineer, Technology Consultant, and Business Analyst for Commercial and Industrial Customers, System integrators, OEMs and Software Application Developers.

He was an early architect and platform developer and CTO at EnergyIX (now IXOT) where he co-architected the core software which enables Operational Technologies (OT), emerging Machine to Machine (M2M) and IoT technologies to share information and connectivity with Cloud and Enterprise applications while addressing security and data privacy challenges facing commercial and industrial customers.

Nick Etson, Enterprise Development and Integration and Software Architect

An avid technology enthusiast with a tenured background in software development and technology, Nick Etson's varied skill set of technical know-how comes from his experience working in multiple sectors of business over the past ten years, most recently integrating API's into multiple blockchains.

Beginning his career in the aerospace industry, Nick spent six years mastering the roles of UNIX systems administrator, network administrator, and software developer for Swales Aerospace. During this time, Nick architected crucial enterprise infrastructure such as e-mail, HTTP, and DNS servers.

Nick's software related projects at Swales Aerospace ranged from developing accounting and task planning applications to niche subjects such as finite element analysis engineering software, 3D graphics programming and electrical engineering/embedded systems development for spacecraft ground support equipment. Most recently, Nick led a software development team for a start-up company focused on streamlining conferencing and collaboration solutions and integrating enterprise solutions into several blockchains.

Advisors

Dustin Byington, Former President, Wanchain

Dustin graduated from Columbia University in 2007 and went to work at Goldman Sachs one year before the financial collapse. Watching the banking meltdown from the inside, Dustin came to the realization that the problems were systemic and that solutions would need to come from outside the existing system. Embarking on a journey of financial entrepreneurship, Dustin received his MBA from the University of Michigan and co-founded multiple companies within the blockchain space: Satoshi Talent, Tendermint, Stokens Venture Capital, and the Austin Blockchain Collective that now has more than 100 members. He most recently served as President of Wanchain where he helped fuel it's meteoric growth to a $1 billion market cap in less than 7 months. He is presently CEO of his new start-up that is focused on security tokens.

Steve Sprague, CEO, Founder Rivetz

Steven is one of the principal industry evangelists for the application of trusted computing technology. Steven served as President and CEO for 14 years at Wave before transitioning to the board of directors. A popular speaker on cybersecurity and trusted computing, Steven has a strong technical foundation in the principles, capabilities, and business models of incorporating trusted hardware into everyday computing and is skilled at translating these concepts into layman's terms. He is founder and CEO of Rivetz, a decentralized & hardware-based cybersecurity ecosystem. Rivetz provides the core infrastructure for cybersecurity and seeks to fully enable the hundreds of millions of devices that have security already built-in.

Oliver Birch, Vice President Wanchain

Oliver Birch graduated from Lancaster University with a BA (Hons) Philosophy, Politics and Economics. He is passionate about innovation and planning, creating and managing large projects within Clinical Trials. Oliver first got into the crypto space in 2011, researching and writing academic papers at university about the rise of bitcoin.

Currently, Oliver is working as a Senior Project Manager for MeDiNova Research Spain (with an established parent company in London, UK). Oliver helped set up the MeDiNova network in Spain and is actively helping with the company expansion. MeDiNova is a Site Management Organization (SMO) with a network of 34 Investigator Sites. Its principal aim is to conduct clinical trials for pharmaceutical companies. MeDiNova is a leading SMO in recruiting large numbers of subjects within a short time frame, providing high quality clinical trial data and maintaining high subject retention rates. He is also the Global Community Lead for Wanchain.