Kweli - Pan-African Self-Sovereign Identity

25 Jan 2020

Published by the Identity Working Group of the African Digital Asset Framework

Authors

Eddie J. Kago	Vibranium ID
Marvin Coleby	Raise and Lead - African Digital Asset Foundation
Melissa Powell	Pocmi
Kenroy George	Cari

Editors and Reviewers

Monique Morrow	Humanized Internet
Kaliya Identity Woman	Internet Identity Workshop
Dr Salma Abbasi	eWorldwide Group
Dr Shelby Solomon Darnell	Vibranium ID
Pelle Braendgaard	uPort
Dr Willy Mutunga	Office of the Former Chief Justice, Kenya
Wanjiku Karanja	Law Lab Africa
Martin Mbaya	EnAdIn
Myra Manawar	Telenor
Yele Bademosi	Binance

Table of Contents

Abstract

Objective of this paper:

The need for a Pan-African SSID: The connection between digital identity, self-sovereign identity, and the opportunity for Africa.

A Pan-African decentralized digital identity can support economic, social and cultural trade between the continent and its diaspora. This paper proposes a framework for a *mobile-first* identity that can connect a digital network of hundreds of millions of people of African descent. This digital network can create economic prosperity and cultural progress for a significant part of the global population. To make this possible, there is an urgent need for a Pan-African version of decentralized identity framework. This is because new developments in artificial intelligence and distributed ledger technologies will power the Internet's decentralized infrastructure for these digital networks.

Fundamental to this infrastructure will be a new kind of identity protocol that empowers individuals and institutions with their sovereignty to create and share their own digital identities. We argue that there is both an opportunity and urgency to build a Pan-African self-sovereign digital identity. This paper presents the patterns for the opportunity, the reasons for the urgency and a conceptual framework for a Pan-African self-sovereign identity. It is important to distinguish that by **self-sovereign**, we do not imply a replacement to state issued identity or that individuals self-issue civic credentials. Self-sovereign in this paper is used in the sense that individuals determine when and for what, their identifying credentials are used in interactions. This paper respects the role of governments and institutions as issuers of identities and the need for decentralized identity to enable individuals to manage their identities and verifiable credentials (data attached to their profiles).

A Pan-African self-sovereign identity will need both a conceptual framework and technical architecture that both aim to create digital networks for the continent and its diaspora. This paper forms the conceptual framework. It will be followed by the release of a technical paper and open source code for communities of engineers, entrepreneurs and regulators to create Pan-African digital identity systems.

Introducing Kweli

A Pan-African *self-sovereign* digital identity ("Pan-African SSI") can support economic, social and cultural trade between the continent and its diaspora. This paper proposes an open source code for a Pan-African identity called **Kweli**. Kweli is a Kiswahili term that denotes that something is true, the basis of trust. Kweli is an effort by the Identity Working Group of the African Digital Asset Framework to propose an identity infrastructure rooted in the Web of Trust[1] for African *peoples*. Kweli is the first technological standard supported by the African Digital Asset Framework ("**ADAF**"), an open source platform that aims to create transnational standards for digital assets and distributed ledger technologies. The first iterations of Kweli are built in partnership with a group of organizations and with Vibranium ID, a Kenyan-based identity company and Steward of the Sovrin network.

Kweli is an open-source codebase that people, companies and governments can use to create secure digital identity applications and systems with the security of distributed ledger technologies. Kweli's infrastructure will be built around two major components:

1) **Distributed Ledger Database** - Kweli is built on Hyperledger Indy, an open-source framework for self-sovereign identity rooted on a distributed ledger database.
2) **Pan-African** - Kweli's infrastructure is built to support Pan-African trade and natively encodes national and regional protocols, rules and legislations throughout Pan-African communities both on the continent and in the diaspora.

Kweli's objective is to support Pan-African trade across the continent and its diaspora. It is specifically built to meet the social objectives set by organizations like the African Union, Caribbean Community and the United Nations. The initial version of Kweli's open sourced codebase is still under development and will be released in the second quarter of 2020.

The immediate objective of Kweli 1.0 is to support trade under the African Continental Free Trade Area Agreement. This version will be released with a ready-built open source codebase. The codebase will contain standardized schemas and documentation that aim to extend the rights for freedom of movement afforded to *all* Africans[2] under the African Union's constitution. Users will be able to digitize personal or corporate credentials and verify their right to freedom of movement under the rules of the African Union.

Kweli is both an **idea** and **technological standard**. This paper explains the idea. Kweli **as the idea** to create a new understanding of identity[3]: a Pan-African *self-sovereign* digital identity where *every* African, regardless of their geographic origin, can seamlessly engage in commercial activity on the African continent. This concept is a natural evolution of the

[1] "Rebooting the Web-Of-Trust." Accessed January 25, 2020. https://www.weboftrust.info/.
[2] "Full Version - African Digital Asset Framework." Accessed January 25, 2020. http://adaf.io/ADAF-Full-Version-2018.pdf.
[3] The earliest example of a borderless "Pan-African" identity was best articulated by The Honourable Marcus Mosiah Garvey's movement called the United Negro's Improvement Association and Communities League ("**UNIA**"). The UNIA stood to create a borderless Pan-African government and its protocols and structure was contained across a series of foundational documents - a constitution and by-laws. Under the constitution, all people of African descent could become members of the UNIA, and could be distributed a UNIA passport.

cultural, economic and philosophical underpinnings of the Pan-African movement. Pan-Africanism stands to politically, economically and socially unite *all* peoples of African descent, *regardless of their geographic origin*. These rights are extended to *all Africans* under the African Union's constitution, and the African Continental Free Trade Agreement is built under the African Union's constitution. Therefore the African Union grants *all Africans* the legal right to freely move and trade on the continent.

Kweli stands for the idea that every *African* person may choose to create, hold and maintain their own identity - and if they do - it will grant them the **right** and **access** to economic, social and cultural activity in Africa, one of the fastest growing continents in the world. The future of trade is rapidly digitizing and there is an urgent need to create identity infrastructure built by Africans, for Africans to engage in this trade. At the same time, there is an opportunity to accelerate Pan-African trade with digital tools for commerce - with identity being a fundamental tool.

Kweli provides a guiding technical framework for defining standardized schemas and credential definitions to support digital trade across Pan-African countries and people. This paper explains Kweli as both an idea and technology throughout four sections. The first sections of the paper focus on both defining a Pan-African identity and arguing its necessity. The last sections outline technical details for Kweli's first iteration and use cases for its first pilots.

Section 1 describes the concept of a Pan-African self-sovereign identity. This section focuses on two major terms relied on throughout the paper: (1) Self-sovereign identities ("**SSI**"); and (2) a Pan-African digital identity. The first parts of this section describe the principal elements of a Pan-African SSI. With SSI, users hold lifetime portable digital identity credentials for different interactions they have in the real world. Parties that seek to ascertain the veracity of credentials presented by an individual do not need to contact the issuer of the credential but can examine proofs by referring to the decentralized ledger that defines formats of credentials.

The paper further argues that a Pan-African identity refers to two major groups of people: (1) nationals, residents and citizens of countries that are Member States of the African Union ("**AU**") and/or Caribbean Community ("**CARICOM**"); and (2) diaspora groups, people and organizations that include, but not limited to, economic migrants, descendants of the Trans-Atlantic slave trade, refugees and people that are generally of African descent. This includes a diverse group of people that may not, or have already, traced their genetic origins to the African continent. This section explains that a Pan-African self-sovereign identity like Kweli can form the infrastructure that connects diverse groups of *Africans* across the world to engage in global trade and commerce. Identity is fundamental to engaging in trade - and there is an unprecedented opportunity to create a truly Pan-African identity. But, there is also an urgent need to create it. The next section argues that there is **both** an **urgency** and an **opportunity** to create a Pan-African self-sovereign digital identity.

Section 2 makes an argument for a tool like Kweli. It argues that a Pan-African SSI can create a fairer identity system for a significant number of the world population and encourage economic, social and cultural trade between them. Africans will soon form more than half of

the world's population[4]. This section first presents a necessary **urgency** to build new infrastructure for African nationals, citizens and residents **both on the continent and diaspora**. The Internet infrastructure is rapidly transforming to store data on distributed ledgers and similar databases. With trade happening online, this means that personal identities in the near future will be digital, with ownership held by the user, and compatible with other web services without necessarily being issued by them.

These rapid technological developments are happening in an environment where identity customs, systems and infrastructure for Pan-African communities have been grossly interrupted by events like the Trans-Atlantic slave trade, Scramble for Africa and colonialist practices. This is exacerbated by still-developing identity infrastructure in many nation states throughout Pan-African countries and communities. There is an urgent need for a Pan-African self-sovereign identity, because without one, Africans around the world will not be able to participate in an increasingly digital world.

The last parts of Section 2 describe why Kweli as a Pan-African SSI is an unprecedented **opportunity** to create new identity infrastructure that accelerates *Pan-African trade*. The new infrastructure for the Internet ("**Web 3.0**") will be digital and decentralized. Web 3.0 architecture will make possible an inconceivable revolution in how people interact with applications built on the Internet. New models for governance, decentralized financial products ("**DeFI**") and political organization will be incredibly flexible. Any engineer can pick up documentation and build new applications that are built to solve problems in their diverse communities. Africans around the world will use these new technologies in Web 3.0 to adapt services that capture the incredible diversity of Pan-African communities around the world. This will open new corridors for economic, social and cultural trade across these communities in the diaspora and on the continent. Fundamental to any of these applications on Web 3.0 **will be** access to a self-sovereign identity. There is an opportunity to create an open-sourced standard for building Pan-African self-sovereign identities. That standard needs to be built by Africans, for Africans, and should aim to quantifiably increase Pan-African trade. Kweli aims to fill this gap.

Section 3 sets out kinds of use cases for Kweli in a Pan-African context. This section contains real examples of how tools built using the Kweli standard can automate trade and facilitate economic and commercial activity across the continent.

The last section, Section 4, provides a framework for understanding Kweli's technological standard for Pan-African self-sovereign identities. Kweli is built on the Sovrin Network and integrates data schemas that enable users to verify credentials for corporations and persons. Kweli provides an open-source codebase, meaning that on its release communities of engineers, designers and regulators can build applications using the Kweli framework, as well as contribute code. Over time Kweli will grow into a network and infrastructure that can be plugged into existing application databases and/or be used to build entirely new kinds of services and applications on the Internet.

---

[4] People of African descent will form over half of the world's population by 2050. https://qz.com/africa/1016790/more-than-half-of-the-worlds-population-growth-will-be-in-africa-by-2050/

The African Union grants **every** African the right to freely engage in commercial activity on the continent of Africa. This right exists, but as long as civil identity systems are fragmented and paper-based, it will be difficult to actualize this right. Kweli is both an idea and technological standard that aims to actualize this right by providing an initial infrastructure for Pan-African self-sovereign identities.

Kweli's vision is simple - to support a world where any African can freely trade across the continent in the click of a button. It is up to all of us to build this world. Kweli is an example of one of the stepping stones necessary to build this world.

Kweli's first versions in 2020 will focus on a standard for credential verification for **both** persons and corporations on the Sovrin Network. Subsequent versions will include documentation that enables businesses to simplify cross-border trade with automated document processing and filing. This project envisions a world where Kenyan, Nigerian, Bahamian and African-American businesses can engage in a commercial transaction at the click of a button.

Section 1:
What is a Pan-African Self-Sovereign Identity?

Section Summary

Pan-African **self-sovereign identity** is a digitally registered version of a person's (individual or corporate) identity maintained on a decentralized database that can verify its relationship with a Pan-African community or jurisdiction either through incorporation or residency.

This paper proposes the first framework and standard for Kweli - which is specifically a **Pan-African** digital identity built on a distributed ledger network. Kweli is made up of three fundamental components: (1) Pan-African identity; (2) digital identities; and (3) Self-sovereign identity protocols on distributed ledger networks.

The combination of these three components creates a **unique** understanding of what a Pan-African identity is. Pan-African identities already exist, and so do self-sovereign identity protocols on distributed ledger networks. The combination of these two to create a Pan-African self-sovereign identity is a natural step in the evolution of **Pan-African trade** using digital tools. Until now, a Pan-African self-sovereign identity did not exist.

This section lays out the fundamental aspects of Kweli as a Pan-African Self-Sovereign Identity ("**Pan-African SSI**") across three parts:

1. Pan-African identity;
2. Digital identity;
3. Self-sovereign identity.

Definition 1: Pan-African Identity

Fundamental to Pan-African self-sovereign identity will be to understand what it means to be **African** - and what it means to hold a **Pan-African identity.** This definition of "African" has always evolved, and will evolve as this project grows. For Version 1, we propose a clear definition of what it means to be African:

Any person of African descent that can politically, socially or culturally trace their origins to the African continent, regardless of their geographic origin or residence.

This broad definition that guides the philosophy, objectives and visions of Kweli. For the purposes of creating the network and technology, the Kweli network Version 1 must rely on definable and verifiable identities. Kweli therefore proposes that an African can include two major groups of people:

1. **African Union residents** - people that are nationals, citizens, residents or habitually inhabit, any of the fifty-five (55) African countries that form part of the African Union (AU) membership;
2. **Diaspora** - members of the diaspora, including peoples that voluntarily (e.g. economic migration) or are forcibly displaced (e.g. refugees, Trans-Atlantic slave trade). This includes communities of people throughout the world, in the Americas, Asia, Caribbean, Europe and Africa.

A **Pan-African identity** therefore includes **both** people of African descent that were born on the continent of Africa **as well as** those that were not born on the continent of Africa. This is a simple, yet difficult, definition of what it means to be *African*. It is a simple truth that there are hundreds of millions of people of direct African descent and genetic lineage, that are born and raised outside of the African continent. They are members of the diaspora, and equally entitled to any economic benefits entitled to Africans on the continent, according to the AU's constitution. However simple this concept, historical environmental and political circumstances that have impacted people of African descent directly have made a 'Pan-African' identity a difficult concept to understand.

There is a strong resurgence of the philosophy of Pan-Africanism and pride in a global community of *Africans* across the continent and diaspora. In entertainment, signs like the Black Panther movie and revival of reggae music and Rastafarian beliefs are reviving a sense of what it means to be Pan-African. In politics, leaders across the African and Caribbean are initiating programs. In government, countries like Ghana are launching initiatives, for example the 2019 Year of Return initiative, that support the unification of the diaspora with the continent. A sense of a Pan-African identity is growing and evolving around the same time as distinct evolution in the tools for digital identity infrastructure available through the Internet. A Pan-African SSI is a well-timed natural step in **both** the evolution of Pan-African ideals and Internet-based identity infrastructure.

This paper refers to this evolution in identity infrastructure from a **digital** identity in Web 2.0 to a **self sovereign** identity in Web 3.0. As such, there are two distinct evolutions in a Pan-African identity in a digital world: a **digital** and **self-sovereign** one.

A Pan-African **digital identity** is a digitally registered version of a person or corporation's identity on a centralized database. This includes what we traditionally recognize as digital identity - Facebook profiles, bank accounts, biometric and electronic passports. These identities are usually digitally imprinted on centralized databases and not directly controlled by the identity's owner.

A Pan-African **self sovereign identity** is a digitally registered version of a person (individual or corporate) identity maintained on a decentralized database that can verify its relationship with a Pan-African community or jurisdiction either through incorporation or residency.

In order to further define a Pan-African SSI, this section describes the evolution of digital identity infrastructure from a centralized digital ("**Web 2.0**") to a decentralized *self-sovereign* ("**Web 3.0**") architecture. Applications built on both these layers of the Internet enable people and companies to directly engage in social, cultural and economic activities around the world. However, digital identities in the Web 2.0 layer failed to create robust and accessible identity frameworks for people both on the continent and diaspora. The result is that millions of people remain without identity documents on the continent, cross-border trade is restricted and government identity systems are slow and inefficient.

The same cannot happen in Web 3.0. Web 2.0 failed Pan-African communities and a Pan-African SSI is a necessary and natural step in the evolution of Pan-African identities.

To better understand this argument, it is first important to understand how digital identity currently works, in light of the first versions of the Internet, Web 1.0 and Web 2.0.

Definition 2: Digital Identity

Identity is complex. Persons, individuals and corporations derive their identity through interaction with other persons, individuals and corporations. Communities can attest to verify credentials and recognize identities in order to grant or restrict services. Any one of these persons, individuals or corporations can possess a range of different kinds of credentials that make up their identity. A graduate student can have a driver's license, a passport, diplomas, their student identification card and one or more Facebook accounts.

Each of these different proofs of credentials make up a single identity that acts as an interface between that student and the worlds and societies they are a part of. The ability to verify that student's credentials could determine whether an employer will hire them. The employer needs to ***trust*** that these credentials exist.

Identity is trust. The easier it is to verify identity through credentials, the more access to benefits like cross-border trade and public services. For example, a citizen with a valid national identity card could be legally entitled to national health insurance, or to a vote in their constituency.

Credential verification depends on documents that attest or prove an identity. Persons, individuals and corporations rely on physical and digital proofs to verify identity. The relevance of **digital identities** is growing proportionate to the acceleration of economic

activity across the Internet in Web 2.0. As people increasingly adopted the Internet and its associated functionalities like online commerce, social networking and financial services, billions of people created their own digital identities to access essential services over the internet. Despite this growth, Web 2.0 was not designed to create an identity layer for persons, individuals and corporations. It never incorporated a true identity layer - Web 2.0 protocols were designed primarily to communicate between machines. Even without this infrastructure, digital identities still needed to be created and maintained for the people to access economies through the Internet.

Today, anyone can create instances of digital identities across multiple applications to access digital services. For example, one Google Account and Apple Identity can be used to access a wide range of applications, services and digital tools (Federated Identity). Similarly a person, individual or corporation can subscribe for services across multiple platforms using multiple emails that need to be verified each time. Since Web 2.0 was not necessarily built to facilitate digital identities, peoples' digital identities have become bytes of data that are owned by the platforms and companies that provide services. An email and password for Google Account, Facebook and Apple may create a seamless user experience, but many applications create a digital imprint of its users and maintain that data to generate new products and services.

Web 2.0 digital identities compromise personal data ownership and safety. A myriad of complicated privacy policies and end user agreements create a broken identity infrastructure for Web 2.0. Any person, individual or corporation's identity on Web 2.0 is vulnerable to:

- Identity theft as a result of poorly implemented verification mechanisms;
- Privacy breaches due to lack of clear guidelines to guarantee the privacy of data held by websites and applications;
- Centralized control of personal data in vulnerable servers or private companies;
- Lack of ownership, since applications and companies can restrict a profile's access to data or services.

Increased digital trade is forcing a necessary upgrade for identity infrastructure. The Internet is rapidly growing from a centralized Web 2.0 to a decentralized infrastructure (Web 3.0). With it is a need for a new kind of digital identity for Pan-African communities. The evolution of digitally managed identities has grown in distinct phases.

The Evolution of Digital Identities

Digital identities are changing. They first began as centralized digital imprints of individual or corporate instances in the real world stored on centralized servers held by private companies and governments. Digital identities are transforming into **natively digital** identities that are stored on **decentralized servers** and securely created and held by their owners. These new versions are digital identities called **self-sovereign** identities.

The evolution of digital identities occurred over four major phases[5]:

[5] The Path to Self-sovereign Identity
http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Web	Phase	Description
Web 2.0	Centralized identity	***Administered control by a single authority or hierarchy.*** Systems of governance where digital identities are created, controlled, denied or destroyed by a single entity, corporation, government or other centralized institution or group of institutions.
Web 2.0	Federated identity	***Administrative control by multiple, federated authorities.*** The ability for a single user to navigate multiple websites and digital databases with a single identity.
Web 2.0	User-centric identity	***Individual or administrative control across multiple authorities without requiring a federation.*** Identities tied to particular users that can be used to access websites and connect with other users and their digital identities.
Web 3.0	Self-sovereign identity	***Individual control across any number of authorities***. User controls their own identity and identity is not tied to any particular website, restricted to any state or authority. User can see when, how, and for what reasons their identity has been accessed. Their identity can store financial, educational and personal information that is private and must be *consensually* shared with authorities.

Governments throughout the world acted quickly to create versions of digital identity in Web 2.0 with varying levels of success[6]. The first three phases of online digital identities on Web 2.0 suffered from major shortcomings:

1. **Fraud -** the probability of fraud in digital identities is high, especially as people establish online relationships for business across borders and in person;
2. **Scale -** during these three phases, digital identities depend on a group of authorities or a single authority. Rooted trust in a central point of failure increases costs/liability for the central authority (e.g. government) administering the identity.

[6] See Appendix III for descriptions of identity systems in countries like Jamaica, Estonia and Nigeria.

3. **Rigidity -** existing online identities are limited in their ability to provide users access to services, and their fixed technological schemas make it difficult to access a variety of interoperable services within a single nation-state, or multiple states;
4. **Privacy -** online identities are centralized in large databases with shared identifiers (e.g. browser cookies), allowing for personal data to be accumulated and shared without the users' consent or knowledge (e.g. Facebook's Cambridge Analytica scandal). Further, there exists the risk of correlation of ones online activity.
5. **Consent -** online identities are vulnerable to being followed and traced by third parties without users' consent.

This version of digital identity on Web 2.0 especially failed Pan-African communities and identities. Millions of Africans are still unable to access basic digital services because of broken identity infrastructure in their countries and communities.

Upgraded identity infrastructure in Web 3.0 can fix these shortcomings of Pan-African digital identities in Web 2.0.

The birth of Bitcoin in 2009 introduced a trustless electronic protocol for digital assets like currencies and identities. That trusteless protocol is usually referred to as "**blockchain**", or, distributed ledger technologies ("**DLTs**"). DLTs are a revolutionary technology for the fourth major phase on the evolution of digital identities. DLTs represent a major upgrade to the Internet, transforming it into a global digital network of value. This digital network will represent a new phase of the Internet's development, that can create digital economic inclusion for hundreds of millions of people.

Self-sovereign identities reliant on a blockchain protocol can help avoid many of the Web 2.0 identity challenges described above and drive efficiency, trust, privacy and consent for digital identities. The major differentiating factors between the first three phases of centralized identities and the fourth phase, self-sovereign identity, are the following:

1. **Decentralized** - decentralized identities (that is, identities that do not depend on a single central authority to manage them), have historically been difficult because identities were largely pooled in centralized databases and directories. Centralized parties managed these databases, making these identities vulnerable to the will of a sole central authority;
2. **Blockchain -** identification data for a self-sovereign identity can be stored on a distributed ledger (blockchain), which ***does not*** rely on a central directory of identities. Therefore, people can use blockchain-based self-sovereign identities to securely and privately prove things about themselves with a verifiable credential.

Self-sovereign identities (SSI) on blockchain infrastructure carry the potential to herald an entirely new phase of digital identities. In this phase, governments, educational institutions, financial services, citizens, peers and *peoples* can securely, privately and efficiently interact online. World conflicts and the inability of centralized state controlled passport-identity systems to scale to citizens and users has created a large gap in the world, where over 1

billion people still do not have any formal identity[7]. 78% of those people live in Sub-Saharan Africa and Asia.

The opportunity for these identities carry significant potential for the cultural, geopolitical and economic makeup of *peoples* of African descent around the world. This paper proposes a standard for a *Pan-African Self-Sovereign Identity* system. Section 2 presents a case for why Kweli as a Pan-African self-sovereign identity framework is necessary, urgent and **possible.**

Web 2.0 Digital Identities Failed to Cater for Pan-African Communities

Despite the impact of the utility enabled by Web 2.0 being felt world over, a significant portion of the world population has not been able to derive benefits relevant to their contexts. On the surface, Africa has majorly benefited from open access to information owing to the spread of internet connectivity and associated online platforms especially through mobile phones. However, some pressing needs facing Africans cannot be addressed extensively with prevailing Web 2.0 architectures. These remain a stumbling block to access to the myriad opportunities that abound for Africans on the continent and for people of African descent (***peoples***) in the diaspora.

For instance, e-commerce websites are designed with a shipping option at checkout that requires a customer to provide a street address. It becomes a challenge to the customer who is required to fill in such a detail since most towns and cities in African countries are not designed with home addresses. To the merchant, it becomes a nightmare establishing where to deliver goods bought. Further, until recently, payments for most e-commerce applications were only possible through credit and debit cards locking out a majority of Africans who lacked a bank account. Emergence of mobile money enabled direct payments from the phone with the only requirement for use being a registered SIM card.

Additional challenges include;

- Access to a majority of web-based systems requiring an internet connection, yet a significant part of the continent does not have reliable internet connectivity.
- The design of most digital solutions being computer-first yet a majority of Africans access the internet through mobile phones.
- Web 2.0 users are prone to fraud due to poorly architected online identity systems.
- Predatory jargon in *Terms of Use* agreements leading to exploitation of user data of most *peoples.*
- Application areas for web-IDs being few for Afro-specific contexts; extensibility is not provided by design.

In light of the challenges that Pan-African people continue to face in their use of existing digital identity systems, there lies a need to design an identity architecture that ensures ***peoples*** derive the most utility from the internet going forward. Such an architecture would be centred around the human ensuring mobile-first access, ease of data portability, clear terms of use, offline access, and ability to directly manage one's personal data.

---

[7] "Counting the uncounted: 1.1 billion people without IDs." Accessed January 25, 2020. https://blogs.worldbank.org/digital-development/counting-uncounted-11-billion-people-without-ids.

The first two generations of the web have been key in bringing humanity closer. However, challenges in guaranteeing user privacy and universal access of personal digital identity data require robust measures that evolve continuously to solve the challenges presented. Interactions over the internet could have a better user experience if identity systems would allow portability of personal identity profiles using standard data formats with minimal barriers to accessing and managing one's personal identity.

As internet standards advance and user needs evolve, the emerging phase of the Internet, Web 3.0 (also the decentralized web) shows possibility of a human-centred internet where transactions and communication between a person and other persons or internet services happen directly without going through an intermediary. Secure peer-to-peer commerce and similar interactions can happen efficiently. This is a feature not available by design in the preceding generations of the World Wide Web (Web 1.0 and Web 2.0). Constraints in their infrastructure imply that authentication on web services is easened through open standards like OAuth which allow people to access websites using accounts from other websites without revealing passwords to the third party website.

With access to a majority of websites being through User-centric identities, accessing services previously pegged on authenticating with the disabled email ID becomes increasingly difficult. Despite being efficient in enabling people to access multiple websites with one account, the inherent risk is being "locked-out" from the internet if an identity provider, say Gmail disables your account. For instance if you forget your TikTok account password and the account was created through a Gmail account, chances are high that you may lose your TikTok account completely. Additionally, retrieving personal data like memes and messages would entail hoops over legal agreements, a scenario that would be magnitudes tougher in jurisdictions with weak data protection laws. Considering that a significant number of countries in the **AU** and **CARICOM** are yet to institute data protection regulations, this leaves millions of people vulnerable.

NIIMS in Kenya and NIDS in Jamaica have faced implementation setbacks where stakeholders observed that interference with privacy laws caused public outcry hence losing citizens' goodwill. This shows that when designing national digital identity systems, existing laws may need to be revisited and updated to support a digital world and redefine privacy. Additionally, there was a lack of proper education of citizens to get buy in, and lack of overall understanding of such a system by associated officials. The approach used to introduce the national identity systems attempted to force citizens in some cases rather than through civic education on what a national digital ID could actually do for the people.

It may be necessary to make enrollment to emerging government digital ID optional. This would provide room for unenrolled citizens to observe associated benefits and once people see the benefits that early adopters have, enrollment will grow gradually as the norm for everyone.

Definition 3: Self-Sovereign Identity

The rise of Web 3.0 has allowed for decentralized data systems that are open, accessible and secure. Emergence of distributed ledger technologies backed by strong cryptography has been encouraging for the future of data privacy and data sharing in the 21st century.

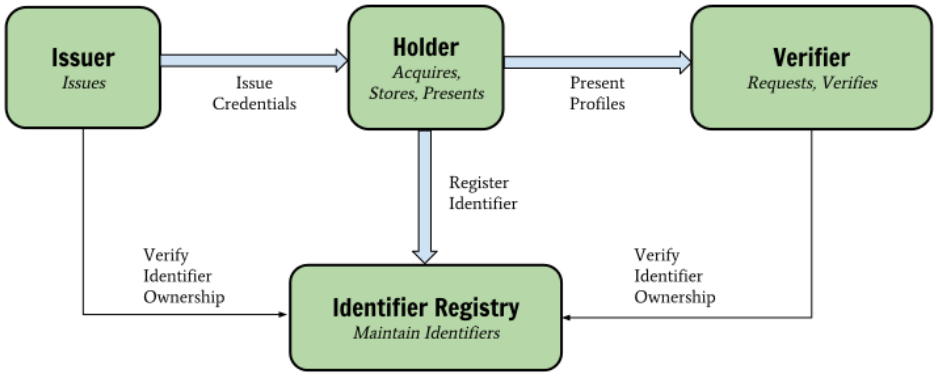
Fundamental to the success of Web 3.0 will be the use of self-sovereign digital identities. These are new software protocols that can redefine online activity for people, by allowing people to assert control over their own identities. A self-sovereign identity is lifetime portable digital identity based on verifiable claims tied to a person's existence. It implies **attributes** of a person's identity that cannot be taken from them. The attributes may be tied to an **attestation** which may be revoked but the identity in itself remains.

Self-sovereign identity (SSI) extends identity to other uses by using verifiable attestations, implemented using the W3C **Verifiable Credentials** data model[8], to prove things about oneself. SSI uses verifiable, trustworthy credentials used autonomously by the identity owner. Interactions between the user, her credentials and the world is through a secure wallet. Relationships established when presenting the digital claims as credentials are represented by identifiers defined by the W3C **Decentralized Identifiers** standard[9]. While credentials can be revoked individually, the identity owner still controls her identity wallet and all other credentials she has collected. Say, a work permit issued by a legal authority may expire but it does not imply that the professional expertise of its holder becomes void.

Verifiable Claims and their Relationships[10]

An SSI network consists of Credential Issuers, Credential Holders and Credential Verifiers where the three roles act as peers. Any person or organization can play any or all of the roles, creating a decentralized system for the exchange of trustworthy digital credentials.

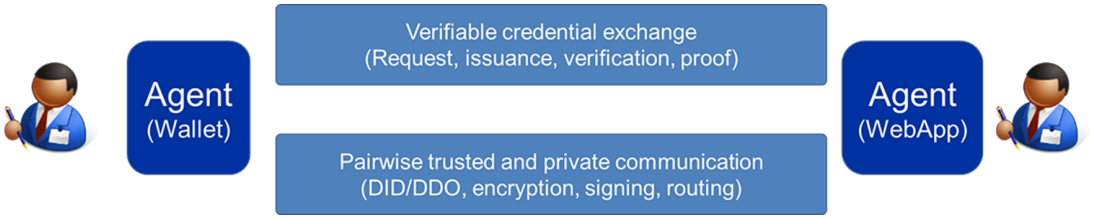
a) Credential Issuers determine what credentials to issue, what the credential means, and defines how to validate the information they put in the credential.
b) Credential Holders determine what credentials they need and which ones they will employ in daily interactions to prove things about themselves.
c) Credential Verifiers determine what credentials to accept and which issuers to trust.



A self-sovereign identity anchored on a blockchain or a similar Decentralized Ledger Technology applies a new identifier called a Decentralized Identifier (DID). A DID is an identifier for verifiable decentralized digital identity. DIDs are URLs that relate a DID subject

[8] "Verifiable Credentials Data Model 1.0." Accessed January 25, 2020. https://www.w3.org/TR/vc-data-model/.
[9] "Decentralized Identifiers (DIDs) v1.0." Accessed January 25, 2020. https://www.w3.org/TR/did-core/.
[10] "A Verifiable Credentials Primer:" https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/verifiable-credentials-primer.md

to means for trustable interactions with that subject by way of a DID document. A DID is globally unique, resolvable with high availability, and cryptographically verifiable. The DID resolves to a DID Document (DDO) that is stored on the ledger. DID documents are simple documents that describe how to use that specific DID. A person can have multiple DIDs representing relationships they have with entities and persons who would also have unique DIDs to establish a connection and enable exchange of credentials.



How SSI works[11]

One of the core benefits of blockchain-based infrastructure for self-sovereign identities is the ability to *verify* identity and its associated data in a decentralized and encrypted database. This means that the verifying party does not need to depend on a centralized repository of data to verify an identity, education credential or financial information tied to a peer's identity.

The central properties of self-sovereign identities includes the following:

1. **Persistent** - identities are owned by the person that creates them and can form the infrastructure for how the user verifiably and securely accesses multiple digital environments to prove information about themselves across the internet;
2. **Peer-to-Peer** - users can use their self-sovereign identities to *securely* interact directly with each other and verify data between themselves online, without the need for a centralized authority;
3. **Privacy** - users control their identity and how information within it is shared with other peers, groups, organizations or states.
4. **Portability** - users can interact with a variety of online and offline systems to gain access to resources.

[11] Self-sovereign Identity - The Good, The Bad and The Ugly
https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly

What is a Pan-African Self-Sovereign Identity?

There are currently one billion[12] people around the globe who do not have any form of identification. Of those with ID, there are 3.4 billion[13] who have difficulty participating in the digital economy. This has an effect on the gender balance: women in low-income nations are more at risk of not having ID compared to men.[14]

By 2050, half of the world's population will be of African descent. However, the current infrastructure for digital identity systems in many African states is still severely underdeveloped. This could mean that by 2050, more than half of the world's population could have a poorly constructed digital identity.

There is an **urgent** need to include those populations into a protected, secure and digital environment to prevent this. In doing so, we could be building entirely new identity protocols for half of the world's population. With this, we could be opening up significant opportunities for economic, social and cultural exchange across hundreds of millions of people. In order to achieve this, there is an urgent need to create and release an **open source** framework to build a Pan-African self-sovereign identity standard.

Introducing Kweli, Pan-African Self-Sovereign Identity Framework

Kweli is a community framework for creating and implementing self-sovereign Pan-African identities into existing or new applications on the Internet. Kweli is built to facilitate the secure creation and storage of self-sovereign digital identities that enable people of African descent to engage in seamless trade across the Internet.

Kweli's vision is simple - to support a world where any African can trade freely across the continent at the click of a button. This project envisions a world where Kenyan, Nigerian, Bahamian and African-American businesses can engage in a commercial transaction at the click of a button while based in distributed geographies. In order for that button to exist, there needs to be an easily accessible digital interface that integrates a secure standard for Pan-African self-sovereign identities.

The first versions of Kweli will focus on verifying compliant credentials for individuals and corporations in the Caribbean and in Africa. The open source protocol will power a new generation of interfaces and applications with two primary benefits for Pan-African trade:

1) Access to assets on distributed ledger networks; and
2) Automated compliance throughout Pan-African jurisdictions.

---

[12] "Digital identification: A key to inclusive growth - McKinsey." Accessed January 25, 2020. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx.

[13] "Global Digital Report 2018 - We Are Social." Accessed January 25, 2020. https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018.

[14] "Global Financial Inclusion (Global Findex) Database - World Bank" Accessed January 25, 2020. https://datacatalog.worldbank.org/dataset/global-financial-inclusion-global-findex-database.

Benefit	Reason	Example
Access to distributed ledger networks	Kweli is built on the Sovrin Network, a deployment of the Hyperledger Indy Network that supports DIDs and Verifiable Credentials. This means that applications built using the Kweli Network will be able to access assets, data and transactions made on other blockchains like Ethereum due to interoperability supported by W3C Verifiable Credentials and DID open standards. This empowers Kweli applications with access to a wide number of applications built with multiple blockchains. As DLT technology becomes more sophisticated, users will be able to exchange data across multiple DLT networks and their chains.	Initial pilots on the Kweli network involve defining schemas for limited companies, hosted on a network using the Stellar DLT protocol. Future tests and implementation will be done on Ethereum blockchain.
Pan-African compliance	Kweli encodes laws and regulatory standards from countries across Pan-African countries like The Bahamas, Algeria, Kenya, Nigeria, Jamaica and Antigua. This means that any Kweli integration and application will inherit automated compliance across multiple jurisdictions. This will ease trade between said countries.	A digital platform for trading securities integrates Kweli identity into its application. Kweli's protocols uses standards for know-your-client verification across The Bahamas, Jamaica, Nigeria and Kenya. Users of the digital platform can compliantly trade securities and automate the verification of their KYC data without cumbersome paperwork and government intervention.

Kweli's objective is to facilitate digital trade between hundreds of millions of people, countries and companies of African descent across both the African Union member states and its diaspora peoples. This is directly in line with the constitution of organizations like the African Union, which exists to increase trade that guarantees better living conditions for both African nation-states and people of African descent[15].

[15] "CONSTITUTIVE ACT OF THE AFRICAN UNION." Accessed January 25, 2020. https://au.int/sites/default/files/pages/34873-file-constitutiveact_en.pdf.

Kweli is made up of two primary **layers**:

1. **Protocol Layer** - open-source software standards that maintain a cryptographically secure and distributed database of identities and transactions. These standards are built with smart contracts that embed privacy policies and data protection rules. This layer constitutes an identity metasystem.[16]
2. **Application Layer** - This entails context specific mobile-first identity applications built on top of the identity metasystem. Users can upload and maintain verifiable identity documents and credentials.

Together, these layers can create an easy to use experience for millions of people to independently control the creation, maintenance and sharing of a secure digital identity. The result is a significant upgrade to existing identity infrastructure for the continent and people of African descent. Where the old identity infrastructure for Pan-African digital identities is (at best) centralized, fragmented, insecure and paper-based, Kweli's standard for Pan-African self-sovereign identities is secure, decentralized, interoperable and digital.

[16] "THE IDENTITY METASYSTEM – Kim Cameron's Identity Weblog." Accessed January 25, 2020. https://www.identityblog.com/?p=355.

Section 2:
Why do we need a Pan-African SSI like Kweli?

Pan-African digital self-sovereign identities are a natural step in the evolution of Pan-African trade. This was first proposed by the African Digital Asset Foundation ("**ADAF**") in a 2018 research paper titled *"Peoples-Driven Standards for Distributed Pan-African Identities"*. The authors of the paper analyzed the legal tools for Pan-African trade and regional trade patterns set by the African Union ("**AU**") alongside the evolution of disruptive distributed ledger network technologies.

The paper concluded that the future of Pan-African trade will be where the continent and its diaspora around the world will rely on distributed ledger network protocols and applications that allow them to seamlessly trade assets, verify digital identities and engage in the exchange of business transactions. Together with the tools for regional trade in the AU, the result would be the creation of entirely **digital economies** and platforms for trade **among the continent and its diaspora.** The paper referred to these digital economies as **Distributed Pan-African Economies** ("**DPAs**"). The paper also proposed that fundamental to the creation of these DPAs would be a Pan-African self-sovereign identity that would allow any individual or corporation to access these applications and protocols - and therefore access global markets for digital trade in the DPAs.

The result would be the creation of innovative and new business models in a digital age. The paper referred to these new exchange of political, economic, social and cultural between the continent and its diaspora. The next step in Pan-African trade will be the creation of **Distributed Pan-African Economies** ("**DPAs**"). The ADAF paper looked at evolutions on trade agreements around the world and in the African Union ("**AU**") alongside the growth in distributed ledger network technologies.

A Pan-African SSI can create the necessary infrastructure to grow Pan-African trade between the continent and among the diaspora. In this Section 2 of this paper, we propose that the first use case for a Pan-African SSI should be an application that facilitates freedom of movement of goods, services and labour. The objective of this first use case is to support Pan-African trade together with the protocols and rights that ***already*** exist for Pan-African communities under the AU's *Protocol on the Free Movement of Persons, Right of Residence and Right of Establishment* ("**Free Movement Protocol**").

The Free Movement Protocol provides members of Pan-African communities with the right to move freely across AU countries. It is a **fundamental** protocol to the opportunity for Pan-African trade. However, the shortcomings of existing identity infrastructure will restrict its performance, and therefore the movement of people, goods and services for Pan-African trade.

A Pan-African SSI is a necessary infrastructure upgrade and can integrate rights from the the Free Movement Protocol. There is **both** an opportunity and an urgent need to create this infrastructure to support Pan-African trade. The urgency lies in creating upgraded infrastructure to support the Free Movement Protocol. The opportunity lies in easing freedom

of movement and supporting Pan-African trade through the African Continental Free Trade Agreement ("**AfCFTA**"). The AfCFTA is being launched alongside the Fourth Industrial Revolution ("**4IR**") and rapid technological developments towards a Web 3.0 infrastructure.

The AfCFTA **requires** a decentralized digital identity infrastructure to support it and Pan-African trade. At the same time, this is an opportunity to leapfrog broken infrastructure and create a truly **Pan-African** identity system for peoples of African descent everywhere.

It is an urgent upgrade to existing identity infrastructure

The shortcomings of Web 2.0 digital identities will limit the Free Movement Protocol, AfCFTA and Pan-African trade. Web 2.0 infrastructure failed Pan-African communities. There is an urgent need to upgrade this identity infrastructure. The existing infrastructure actively creates disconnected communities of people with similar backgrounds and histories. For example, people in the Caribbean are originally descendants of West African communities and tribes. These lineages are scientifically verifiable. Under this definition, communities of Caribbean people ***should*** be afforded the right to move and trade across the African continent, since the AU's tools and AfCFTA aim to support trade across **both** the continent and **peoples** of Africa. However, countries across the continent, the Caribbean and Americas still manage poorly built disconnected identity infrastructures. A Pan-African SSI can **connect** these identity infrastructures and people. Applications built using a Pan-African digital identity protocol could lower the costs of extending the rights for Pan-African trade in the AfCFTA both across the continent and its diaspora.

The effect of these disconnected identity systems is the restricted flow of goods, services and labor across Pan-African communities. These systems will limit the potential for the AfCFTA and Free Movement Protocol to create economic prosperity and extend rights to hundreds of millions of people across the world. To build new infrastructure, we need to understand the existing one. This existing infrastructure is made up of three components:

Component	Description
Paper-based	People and entities prove their identities using primarily paper-based systems. This form of record-keeping is highly susceptible to fraud and breaches to data security.
Fragmented	Driver licenses, land titles, education certificates, bank cards, awards and passports are distributed pieces of data that are assigned to people and entities by disconnected private and government sector actors.
Centralized	Identities are distributed, controlled and recorded by a single entity. This is an unscalable model, since it makes a users' identity dependent on a single entity.

A paper-based, fragmented and centralized identity infrastructure suffers from poor data *retention* and *protection*. This is especially problematic for Pan-African communities, given the unique development of the continent and its peoples' *his*tories and *her*stories. The continent and its diaspora are a complex community of identities with ancient tribal histories

and diasporic migrants that were severely disrupted by events like the Scramble for Africa, European colonialism and the Trans-Atlantic Slave Trade.

The combination of both a data-deficient identity system with complex Pan-African communities makes it harder to conduct cross-border trade, for societies to maintain their cultural histories, and for governments to distribute social services. This existing identity infrastructure erects preventable economic, social and cultural obstacles for people and entities across Pan-African communities. The end result of this existing identity infrastructure is to restrict the potential for Pan-African trade.

This paper argues that a Pan-African SSI can support trade with an upgraded identity infrastructure. Where the existing identity infrastructure is paper-based, fragmented and centralized, a Pan-African SSI is built to be digital, connected and self-sovereign. Most importantly, a Pan-African SSI is built *for* Africans *by* Africans. This **data-driven upgrade** can increase Pan-African trade, maintain important histories and connect hundreds of millions of peoples and businesses.

This upgraded infrastructure is made up of three components:

Component	**Description**
Digital	Records related to identities stored in digital environments that can be created, maintained and accessed by anyone with access to a mobile device or Internet connection.
Connected	A user maintains an account that acts as a digital wallet for various forms of data related to identities.
Decentralized	Transactions associated with the identity data are recorded and maintained on a scalable decentralized ledger. This enables self-sovereignty, since no single entity controls the maintenance or creation of transactions and identities.

A digital, connected and self-sovereign Pan-African identity can connect hundreds of millions of people in an interoperable digital economy. In order to achieve this major digital upgrade, this identity framework must be created and maintained in an open source environment (e.g. Github repository) by people, companies and governments. Open source code bases typically require the creation and maintenance of consensually created standards that can be made to function across multiple systems, frameworks and programming languages. Together with an open source framework, the properties of a Pan-African SSI can create very necessary interoperability between nation-states, businesses, people and governments across Pan-African communities.

Interoperability is a *necessary* precursor to a Pan-African SSI to support economic trade between the continent and its diaspora. Today, identity systems are highly centralized databases where rules are set and accepted by governments and other institutions. Tomorrow, communities of companies, governments and peoples can create, accept and share digital identities.

Interoperability means that a user of a Pan-African SSI can create, maintain and share a self-sovereign identity that can be accepted and verified across multiple systems such as government services, borders, websites and applications. Fragmented and paper-based identity infrastructure have erected real barriers to trade across the continent and its diaspora. Organizations like the AU, CARICOM and agreements like the AfCFTA are a set of legal protocols that aim to ease those barriers with a fundamental policy tool: the movement of labor, goods and services. However, many countries within these trading blocs maintain poor identity infrastructure which maintain the barriers to increased trade between them. These barriers are therefore persistent impediments to economic independence for people across Africa and its diaspora across the Americas, Caribbean and Europe.

The shortcomings of existing identity infrastructure represent an *urgent need* to build an upgrade to our identity infrastructure. This urgent need is also an **opportunity** to leapfrog existing infrastructure and accelerate Pan-African trade in line with the AfCFTA.

There is an opportunity to accelerate Pan-African trade through the African Continental Free Trade Area Agreement

A Pan-African SSI can support the AfCFTA by easing the movement of people, goods and services across borders. The Pan-African SSI's Protocol Layer will need to incorporate the rules and rights for the freedom of movement alongside the AfCFTA. Rights for free movement already exist to support the AfCFTA, they include the (1) *Protocol on the Free Movement of Persons, Right of Residence and Right of Establishment* ("**Free Movement Protocol**")[17] and (2) the African Union Passport project ("**AU Passport**"). Together, these agreements create a strong legal framework for the seamless movement of goods and services across Pan-African borders. They are **fundamental** to the opportunity of Pan-African trade. However, there is a clear gap between the AfCFTA and the rights provided for in the Free Movement Protocol.

At the AfCFTA signing in Kigali, the Movement Protocol was the least supported text signed by AU member states. For a true intra-continental market, all member states of the AU would need to sign the Movement Protocol and commit to its roadmap to ease border restrictions for Africans. The AfCFTA Agreement was originally signed with 50 states present alongside two other legal instruments: *Kigali Declaration* ("**Declaration**") and the Movement Protocol. The central AfCFTA text was signed by 40 states, the Declaration by 44 states and the Movement Protocol by only 30 states. AfCFTA's economic impact will be limited without cross-continental consensus on border restrictions. More than half of the signatories that did not sign the Movement Protocol were Francophone countries, as of March 2018.

There is a need for movement protocol infrastructure that allows countries and *peoples* of diverse backgrounds to customize their own identity solutions without compromising regional movement. The intention for a Pan-African SSI is to integrate the rights and principles for the AU Passport and Free Movement Protocol into its open source codebase. The result is an

[17] "Original Free Movement protocol - African Union." Accessed January 25, 2020. https://au.int/sites/default/files/newsevents/workingdocuments/33023-wd-pa20330_e_original_free_movement_protocol.pdf.

open sourced codebase that people, companies and governments can use to create identity applications and systems that are **natively** built to support Pan-African trade.

The AfCFTA entered into force on May 30, 2019, creating one of the largest trade blocks since the creation of the World Trade Organization ("**WTO**"). Its primary objective is to create a "single market for goods, services, facilitated by movements of persons" to deepen economic integration across the continent and her diaspora[18]. The AfCFTA is a suite of protocols and policies that, together, create an institutional framework to accelerate Pan-African trade in two phases. Phase I creates a framework for the trade of goods and services. Phase 2 is a framework of policies for investment, competition and intellectual property. Freedom of movement is **fundamental** to both phases, and the Free Movement Protocol contains a set of existing rights available to nationals across the AU.

The AU passport provides nationals across the AU with a passport to travel across AU Member States. However, the AU Passport project is a new identity system based on a weak identity infrastructure. We previously summarized the limitations of that infrastructure above. These limitations actively maintain barriers to Pan-African trade. The AU passport could recreate existing **closed** identity infrastructure with **fragmented** systems. A Pan-African SSI is an **open** identity infrastructure that can **connect** people, businesses and governments across borders. There is a clear opportunity to build a Pan-African SSI that directly supports the growth of Pan-African trade with the AfCFTA, using the rights for free movement in existing instruments like the Free Movement Protocol. A Pan-African SSI can integrate and extend the rights under the Free Movement Protocol.

An interoperable Pan-African SSI is a fundamental piece of infrastructure to connect the rights provided for in the Free Movement Protocol with the AfCFTA.

Implementation of the Pan-African SSI

The rules and rights provided for in the Free Movement Protocol can be directly integrated into the Protocol Layer of the Pan-African SSI. The Protocol Layer will be open sourced with a set of development tools for communities of people, governments and companies to continue developing the codebase and creating new applications. The Application Layer can use elements of the Protocol Layer to both build **new** applications or integrate them into existing systems. These new systems can take the form of government-sanctioned identity systems and passports, digital identity applications and digital lockers.

Applications that integrate elements of the Protocol Layer will therefore extend the rights of the AfCFTA and Free Movement Protocol through their own Application Layer offerings to

[18] The AfCFTA specifically mentions that its aim is to accelerate Pan African trade in line with the AU's Agenda 2063. Both Agenda 2063 and the AU's constitutive charters are fundamentally driven by the objective to unite the *Pan*-African diaspora across both the continent and the world. The AfCFTA, however, specifically provides that it is open to accelerate trade between Member States of the African Union. This would initially read that diaspora members are excluded. For the purposes of this paper, we assume that the AfCFTA's goals are to create a single continental market for trade and goods that creates economic prosperity for both those nation states ***and*** Africa's diaspora. See *Popular Version - Agenda 2063 at 1* (https://au.int/sites/default/files/documents/33126-doc-03_popular_version.pdf) and AfCFTA at Article 3, General Objectives.

users. Each of these kinds of applications will need to require strong collaboration between both the private and public sectors across Pan-African communities world over.

The result of a successful implementation of a Pan-African SSI could mean an interoperable framework of identities, financial applications and trade across borders. Most importantly, it could ease free trade across borders and accelerate the free movement of goods, services and labour.

Roadblocks to a Pan-African SSI

Public sector groups like governments and regional groups are central to a successful implementation of a Pan-African SSI. A foreseeable roadblock to a Pan-African SSI is the potential for its rejection by existing nation-state governments. Integrating a new identity infrastructure is a significant undertaking that may require burdensome resources that states may not be able to equally share or commit to. In addition, freedom of movement, goods and services is a highly political issue that is interpreted differently by various governments, parties and states. The end result is often stalled agreements and documents with low levels of ratification, such as the Free Movement Protocol. These geopolitical and financial realities present serious obstacles to a Pan-African SSI.

Without widespread government acceptance, a Pan-African identity infrastructure will be difficult to implement. The most probable implementation would initially begin in the private sector among communities of users, companies and policy institutions.

An open source identity framework can provide a solution to these roadblocks. Open source codebases can be built on by any entity, including governments. Governments and policymakers could openly participate in the drafting, improvement and creation of a Pan-African digital identity system. This open process would contribute to perceptions of transparency among populations and their nation-states, increasing the chances for a government-sanctioned implementation of Pan-African SSI. In addition, successful private sector implementation can create quantifiable economic prosperity for industries and people. This could further motivate governments to adopt and use the Pan-African SSI.

In Section 2, this paper argues **why** there is both an opportunity and an urgent need to create identity infrastructure that supports Pan-African trade. The use of digital applications built with this infrastructure can integrate **and extend** existing rights and protocols under regional governments and bodies of legislation. For example, the rights under the Free Movement Protocol could be extended to passport holders of any African state, or member of the diaspora. A successful implementation could extend the objectives for increased Pan-African trade under the AfCFTA. The AfCFTA aims to create a Pan-African market for the free movement of goods, services and labour. This paper proposes why this Pan-African trade market will need a Pan-African SSI. The next section presents a use case for a Pan-African SSI in the trade sector. The name of this implementation is **Kweli**.

Section 3:

Kweli in Action

The anchor technical implementation of ADAF's Pan-African identity framework is a registry for exchange of verifiable credentials defined by the AU Movement Protocol. This would be a public registry containing templates (schemas) for credentials as per the Movement Protocol. Such schemas define how organizations and companies are to be registered in the member states of the African Continental Free Trade Area. The registry shall be served on a platform which creates a network of verified organizations enabling trusted business transactions, supporting trade between parties in different jurisdictions within the AfCFTA region.

Kweli is the anchor implementation of ADAF's Pan-African SSI framework. Kweli is a Kiswahili term that denotes that something is true. Kweli is aimed at promoting commerce within the AfCFTA region by enabling individuals to manage aspects relating to their identities with ease. Kweli is built to promote a supportive environment for businesses to transact within the continental trade area.

Below are scenarios describing typical experiences of businesspeople when transacting across borders on the continent. Each case is described in its current state and how things would be improved with adoption of Kweli or a Kweli inspired Pan-African SSI approach.

Scenario 1: Meet Mariam

Mariam is a 38 year old Congolese citizen who currently splits her year between DRC and France. She owns and runs a fruit produce business across Democratic Republic of the Congo (DRC), Republic of the Congo, Gabon, and Cameroon. This requires frequent travel between each location for new contract negotiations and to oversee large shipments with very time-sensitive cargo on the line. After much discussion with a friend in Nigeria, she decides that exporting some of her indigineous fruits to Nigeria would be a great move for her business. She contacted a Nigerian supermarket chain with 30 locations and they have agreed to meet to discuss her supplying them with guava and longan.

In order for Mariam to get her goods from DRC to Nigeria, she requires an entry visa. A business visa requires her to fulfill the following conditions:

1. A passport valid for at least 6 months.
2. Completed visa application form.
3. Two recent passport size photographs.
4. A Letter of Invitation from a company/host in Nigeria accepting immigration responsibility.
5. Submit evidence of sufficient funds.
6. Nigeria Immigration Service Visa Payment Receipt and Visa Acknowledgement Receipt

Mariam decides she needs to travel to Nigeria to oversee her investment, she needs to apply for a business visa prior to leaving. Mariam provides the consulate with all necessary paperwork, including a letter from Mariam stating the purpose of her visit and leaving her passport with them. While she is waiting to receive her visa, she gets an invitation from an associate to speak at a conference in Miami about her business and get introduced to potential distributors across the US. Unfortunately, she is unable to take advantage of this opportunity given her passport is sitting at the Nigerian consulate awaiting her visa.

While completing all these steps Mariam must decide if she will also be physically setting up shop in Nigeria. That is whether or not she decides to export to an existing establishment or if she will be physically present in Nigeria to conduct business herself.

Mariam will need to present the following documentation to Nigerian immigration authorities at minimum in order to obtain a temporary work permit if she decided to be present in Nigeria to conduct business:

1. Passport with at least 6 months validity.
2. Printed copy of completed application form for visitors pass.
3. Two recent passport size photographs.
4. Copy of a Letter of Approval from Comptroller General, Nigeria Immigration Service

As an aside, for this process in almost all developed countries, Mariam would also need to submit a signed statement from the bank verifying she has enough funds to cover her entire trip and declare the source of her funds.

In the off-chance she needs to stay in Nigeria longer than 6 months, she would need to present the following:

1. Passport with at least 6 months validity.
2. Completed visa form in **quadruplicate** with four recent passport photographs.
3. Four copies of a letter of Expatriate Quota Approval from Ministry of Interior.
4. Four copies of credentials, certificates and curriculum vitae, all vetted by a relevant official of the Nigerian High Commission/Embassy (English Certified translated copy where applicable).
5. Four copies of offer Letter of Employment.
6. Four copies of Letter of Acceptance of employment, signed by an expatriate.
7. Nigeria Immigration Service Visa Payment Receipt and Visa Acknowledgement Receipt.

In order for Mariam to pay for her Nigerian business visa while outside of Nigeria, she has to do the following:

1. Make her payment in US Dollars where she will be redirected to an approved payment platform to complete her application.
2. She will then take her visa payment receipts, passport and other documents to the Nigerian Embassy in Congo on her slated interview date for her Visa.

Upon entry, she is required to submit a valid passport at the border point. When she gets to Nigeria, her textiles supplier requires payment by MPESA, mobile money from Kenya. For

Mariam to access mobile money, she has to purchase a local SIM card. Acquiring a SIM card requires her to submit her national ID card or passport.

At each step, Mariam has to fulfill some requirements to access an essential service or entry access. This is done through different forms of her identity attested by documents such as her identity card, temporary visa or business permit and even her mobile number. She finds herself submitting more information than necessary about herself to access essential services. For example, she only needs to prove she is a legal citizen or resident to buy a SIM card yet by submitting her identity card, she gives details she would otherwise keep private like her date of birth and residence address. Each step or organisation has different requirements and in the unfortunate situation she does not have a required item, she likely encounters opportunistic agents soliciting bribes, and in an effort to avoid inconveniences she incurs unplanned costs.

In order to get the process going Mariam must first understand her options to do so legally. She contacts the Congolese trade commission to help her get moving on the idea. They send her the General Export Procedures and Documentation (See Appendix II) to review and prepare. Stipulations in these documents would also have been information submitted for immigration purposes; or should be considered alongside the timing of immigration processes[19].

Additionally there are import requirements into Nigeria relating to documents submitted to immigration. The main requirement is the e-Form “M” which is processed through an authorized dealer bank irrespective of the value and whether or not payment is involved. The process to obtain an e-form is long and complex, creating a serious barrier to trade for Mariam. For the full list of requirements including other necessary documents that are also duplicated in other processes, see Appendix.

At the end of the process Mariam loses countless hours up to possibly months due to inefficiencies in the current papertrail processes. She also releases unnecessary information about herself and her business that can be used to open a bank account or obtain a visa, only to buy a sim card. Let us take a look at how a self-sovereign digital identity could help to make identity verification processes more efficient and more secure.

Mariam after using Kweli

With the current system, Mariam leaves multiple pieces of her identity in the hands of several agencies. In the case of her original documents when required to be submitted, they can be lost without recourse. Additionally, a delay in the processing of one agencies could mean a delay in processing with other agencies, which in some cases could lead to the loss of a contract.

Mariam’s situation can be alleviated with a self-sovereign identity at numerous points. In Mariam’s case, she would be able to digitally and instantly prove she is who she claims to be. Applying for a visa would be close to seamless, given her travel and finance data is tied to her verified digital identity, and she could easily give the consulate access to it. This

[19] For example, Mariam would need to obtain licenses for different control agencies, fee payments and verification certificates. A list of the documents she would require are provided in the Appendix I to this paper.

verified digital identity could also facilitate multiple applications at the same time and allow movement while the visa is being processed. This could mean shorter verification times and subsequently a more efficient governing immigration body.

The identities she acquires based on her real world interactions are issued by an authority; an identity provider. In most cases, the identity provider is a centralized entity. A centrally issued identity bears inherent challenges in practice. Ascertaining authenticity of an identity or identity document across regulatory domains requires several steps to prove. Additionally, it becomes tough to replace a person's issued identity in the event of loss or damage due to legal steps one must fulfill. While some of the forms of identity Mariam may hold may be digital such as her email address or mobile number, they are similarly limited since the issuing authority is central.

However, Web 3.0 presents with it technologies that provide the possibility to issue an authentic and functional self-asserted identity. A self-sovereign identity reliant on an identity blockchain protocol would allow Mariam to create personas as per her interactions and subsequently choose who to share her identity information with. An ADAF Self Sovereign Identity model would rely on a portable, always available, secure mobile-first identity wallet. A mobile first SSI model would be appropriate considering the widespread use of mobile phones and a mobile first digital approach in Africa. McKinsey estimates 636 million smartphone connections in 2022 according to their Africa report in 2018.

Mariam presents an excellent example of what application of a Pan-African SSI can achieve, built to support freedom of movement for people, goods and services within the world's largest free trade area: African Continental Free Trade Area. Breaking down the essential credentials Mariam needs to run her cross-border business and to prove her identity includes her passport, academic and professional requirements, proof of business incorporation and good standing, and up to date financial history.

Here is how Mariam's life would be different were a Pan-African SSI involved:

1. The need to visit an embassy everytime you need a visa would not be necessary unless in special cases. Embassies would support secure e-submission of documents and issue approval (visa) directly to the digital identity platform. An embassy can verify your ID, travel history and financial requirements all on the blockchain without revealing exact details of yourself and you leaving a long papertrail. All this information can also be re-verified in person with a border agent upon arrival. Using zero-knowledge proofs, embassy authorities and border agents can set the criteria needed and return with simple yes/no answers to each.
2. Her business registration will be available for easy verification on the blockchain. With this, she can also get the necessary licenses and inspections done by trusted entities who will issue her operating credentials.
3. Mariam can have both her import credentials for Nigeria and her export credentials for DRC on the blockchain, significantly reducing the paperwork she has to carry around on her trips. This significantly increases the chances of large supermarkets carrying her produce by providing assurances of the safety of her products. Preparing her waybill would be a lot easier and all documents can be tracked by herself and the logistics company at every step of the way.

a. Government would easily track the quantity and types of products crossing their borders. They can easily ascertain from whom an item came from in the event of a public health issue.
b. This allows countries to better plan food security projects with this newly available data. Farmers would be able to track inputs and demand better prices for their produce. Sellers can easily verify the details and solve a major value-chain problem plaguing many countries experiencing major trade imbalances.

By housing information that often requires verified submissions within an SSI system that is broadly accepted, Mariam will avoid costs associated with constantly verifying the same documents, she will no longer have the inability to submit to multiple agencies at the same time, and she will be able to release only the absolute necessary information to each agency rather than additional unnecessary information that happens to be on a document proving other information.
It is important to note that a member of the African diaspora (Pan-Caribbean) would likely go through the same woes as Mariam.

Scenario 2

Let's take an example where cross border movement of goods and individuals includes a process less cumbersome regarding immigration and more painstaking for the trade of goods even with a free trade agreement in place.

Meet Shiro

Shiro runs a fish export business from Mozambique where her fish is harvested and processed to be sold in Botswana and Chad. Her business requires formal registration to operate in her country. She also requires health approvals from food and public health inspectors. For Shiro to transport her cargo to markets in Chad and Botswana, she must have business permits allowing her cargo to move across borders.

The entire process to enable her get formal registration up to the point where she is able to export to her customers across Africa requires a lot of manhours and could run up to months before she gets to run her business smoothly. Not to mention acquisition of legal compliance documents in respective jurisdictions and asks for bribes she may be compelled to, to facilitate her transactions.

However, Shiro's hassles in moving her cargo across borders within Africa are lessened when she transacts under the African Continental Free Trade Agreement, especially with the support of the Movement Protocol. AfCFTA enables her to trade freely with member states of the trade area while the Movement Protocol allows her to move across borders within the AU with minimal restrictions.

Pan-African SSI (**Kweli**) would ease the process that Shiro goes through to register her business and operate it under the AfCFTA. On a local instance of Kweli in her home-country of Mozambique, Shiro enrols for an SSI backed user profile. She uses her newly registered

account to access services on connected Kweli registry instances in other countries within the African Union. Through a webservice relying on Kweli, she identifies herself and registers her business in the requisite section on the web-portal she accessed. Once registered, the registration credentials for her business are stored in her account profile. With a Kweli backed business account, Shiro is able to apply for licenses she may need and permits she would require to trade within the AfCFTA block.

Atomically, her experience would be as follows:

1. Shiro signs up on Kweli for a new user account.
2. Her Verinym DID is created and stored on her Kweli interoperable wallet.
3. Shiro selects her business type from provided options on a Kweli instance and registers her business. She receives a business registration certificate to prove legal existence. This is stored in a new Business Profile.
4. She applies for a Fishing license, Food Safety license and an Export license, which are stored alongside the business registration certificate in her Business' Profile.
5. Shiro requests for an AfCFTA Trade Permit, issued after qualification of having the prior documents (Business Certificate and appropriate licenses).
6. Shiro's fish trading business is finally legally registered and approved to transact within the Trade Area.
7. If she needs to expand her business to another line of product, say importing Gum Arabic from South Sudan, she only needs to request for import licenses and related appropriate permits.

A Kweli based web application as suggested in Shiro's case where within trade sector, (using the Freedom of Movement Protocol, a set of rights for movements as long as credentials are verified) would be considered for the first implementation given the current framework to accept such a system. Gradual movement to a system that works for personal identity, supporting User Decentralized Identity for Shiro, Mariam and millions in the diaspora and the continent would follow.

Characteristics of a Pan-African SSI

What is it about decentralized identities that makes it such a compelling case for adoption? Here, we look at some of the most prominent ones. Tying many of our important daily interactions to an SSI removes a lot of the inconvenience we shrug off currently but are unnecessary and repetitive. Life is already hard; SSI helps to make it easier. Imagine the time saved and the previously-missed opportunities you can now take advantage of.

Convenience
Being able to have one source of trust that you can take with you wherever you go will significantly reduce the amount of time spent waiting in lines. As explained in both cases with Mariam and Shiro, the number of trips you needed moving between organizations in order to procure documents to prove who you are will be a thing of the past.

Single source of truth to avoid reverifying
With a SSI, now, neither Mariam nor Shiro have to go through the process of re-documenting, requesting and picking up copies of credentials from the governing body, finding an agent to notarize their identifying information and submitting multiple copies to the authority. The aim is to have their credentials already verified by a source trusted by government agencies, so that as soon as the information is needed it can be presented at her convenience, showing only the necessary information for each particular authority.

Interoperability
Once you become part of the self-sovereign identity ecosystem, you have the option to move seamlessly through different providers sharing only the necessary information while not having to go through a constant process of reverifying and preparing the same documentation over and over again.

Persistence: lifelong credentials
We already have all of the credentials in a Pan-African SSI. These credentials provide data points that could also be applied commercially. In some cases only a few pieces of the information within these credentials need to be updated regularly. Yet currently, the entire document will need to be updated and in some cases kept with the older version for reference. Having a blockchain based SSI allows an ease of maintaining lifelong information alongside those that need to be regularly updated.

The five key credentials to Self Sovereign Digital Identity include information within these documents:

1. Passport (individual KYC)
2. CV, academic and professional requirements (professional validity)
3. Proof of business (Incorporation, good standing)
4. Financial statements (Validity, proof of sufficient funds and money management)
5. DNA verifiability (for quota preference)

The table below shows information that needs regular updates and general reasons for updates within these documents.

Document	Does any information change with time?	Is it currently updated regularly?	Reason for Update	Is it necessary to keep the original information each time the document is updated?
Passport	Yes	No (10 years apart)	Appearance changes (photo), limited space for immigration stamps, Criminal record introduced	Yes (Travel and visa history required for most new visa applications)
CV	Yes	Yes	Obtaining additional credentials	Yes
Proof of Business	No	No	Only if no longer in business	Yes
Financial Statements	Yes	Yes	Changes in financial management	Yes
DNA	No	No		

It is clear that changing the entire document each time is unnecessary and having a place that manages **all** historical data gives a better view of a person's character. A Pan-African SSI facilitates lifelong credentials allowing authorities to make better judgement with full view of history while still allowing necessary sections to be updated. A system could be implemented that allows automatic access to certain information for specific institutions disabling the user from hiding important information needed to make a decision.

The next section takes a deeper look into a potential technical framework to facilitate solutions for Shiro, Mariam and the diaspora.

Section 4:

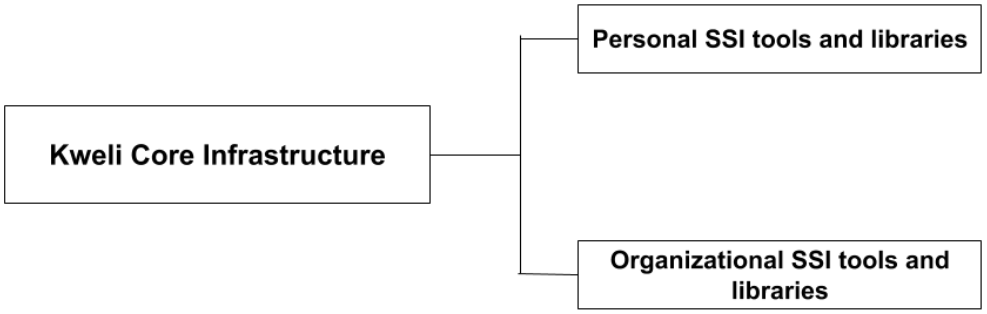
Implementing a Pan-African Identity Infrastructure

A Pan-African digital identity solution should support interoperability across digital systems and enable online to offline connection. The African Digital Assets Framework proposes a Pan-African identity ecosystem that entails individuals acquiring decentralized identities embodied by SSI in a way that supports; person to person interactions, person to business interactions and business to business interactions. In such an identity ecosystem, peer to peer transactions would thrive and commerce across the African Continental Free Trade Area (AfCFTA) would grow.

A decentralized Pan-African identity ecosystem based on a blockchain, would allow individuals access to their own records in a transparent manner with persistence. Such would provide for a continuous record of an individual's profile on/off ledger hence enabling proofs for requirements like Know-Your-Customer and Anti-Money-Laundering checks, hence improved financial access and better chances for economic opportunity.

Open standards for Pan-African Decentralized ID

To create a functional technical framework for personal decentralized identity and organizational SSI, Kweli implements open standards and seeks to collaborate with active organizations like the W3C and the Decentralized Identity Foundation. The result would be a robust decentralized identity infrastructure on which services and tools will be built.



SSI Relationships in Kweli

Guidelines for a Pan-African Decentralized Identity Infrastructure

We propose an Ubuntu guided approach with the following features by design when designing solutions for Pan-African SSI.

Guideline	Description
Self-sovereign ownership	A Pan-African decentralized ID infrastructure should allow user control over how their credentials are managed.
Openness	A Pan-African decentralized ID infrastructure should support community involvement with an open-source approach.
Interoperability	A Pan-African decentralized ID infrastructure ought to be built on open standards of information exchange.
Accountability	A Pan-African decentralized ID infrastructure should be clear on terms of use and clearly define responsibilities of parties involved.
Transparency	A Pan-African decentralized ID infrastructure should embody clear mechanisms of governance built and communicated in a decentralized manner.
Guardianship	A Pan-African decentralized ID infrastructure should provide mechanisms to support management of credentials for individuals facing restrictions on managing their identity credentials.
Longevity	A Pan-African decentralized ID infrastructure should support lifetime persistence of identity credentials issued and managed.
Decentralized	A Pan-African decentralized ID infrastructure should ensure identities are not managed centrally.
Inclusive	A Pan-African decentralized ID infrastructure should provide for all individuals seeking a Pan-African ID the ability to create one regardless of political or socio-economic classification.
Pan-African	A Pan-African decentralized ID infrastructure should be at its root Pan-African in the sense that people of African origin within Africa and in the diaspora can uniquely create a decentralized digital ID.
Security	A Pan-African decentralized digital ID infrastructure should embody best software security practices to guarantee safety of data and trust in issued IDs.
Privacy	A Pan-African decentralized ID infrastructure should adopt a privacy first approach, in the sense of privacy by design.

Interactions within the Kweli Identity Infrastructure

As earlier described, Kweli provides a registry supporting exchange of verifiable credentials as required by the AU Movement Protocol. Kweli will provide a public registry that will define schemas for credentials defined by protocols and annexes of the AfCFTA for organizations and companies in member-states to use for transactions across borders. Kweli's registry shall be served on a platform which creates a network of verified organizations enabling trusted business transactions, supporting trade between parties in different jurisdictions in the AfCFTA block.

The registry would hold;

- Licensing schemas.
- Business Registration schemas.
- Regulatory Permits schemas.

As a functional Pan-African identity infrastructure Kweli proposes including the various interactions between persons to persons, persons to institutions and institutions to institutions.

1. Government Axis: Nation-State to Nation-State interaction.
2. Organization Axis: Corporate to Corporate (including agencies) interaction.
3. *Peoples* Axis*:* Person to Person interaction.

These interactions underpin day to day transactions that people are involved with. As such, the design of Kweli supports:

1. Management of personal credentials and associated data. This entails a person having agency over data related to their health, property or academic records.
2. Intra-African trade: Know Your Customer (KYC) and Anti-money Laundering (AML) checks for e-commerce and funds transfer. Services providing KYC/AML would be built on top of the Kweli network as decentralized by design.
3. Intra-African travel: ID and Passport verification at border entry points. A state issued Passport document backed by SSI would reduce unnecessary checks and support e-commerce amongst AU citizens.

The steps to onboarding on the Kweli registry would include:

1. User enrolls on Kweli backed service and have SSI credentials on their wallet.
2. User invokes actions based on the Protocol on Trade in Goods and the Protocol on Trade in Services to register a new business entity.
3. A new business is registered and the corresponding documents are sent to the business wallet.

Kweli Systems Overview

Kweli is structured as a Verifiable Organizations Network defined by credentials about organizations and businesses being provided for assertion. This could either be self asserted or asserted by an authority and the credential provided for in a public ledger where anyone can refer for verified business entities. These proofs are done in such a way that a third party is not necessary due to the concept of zero-knowledge proofs (ZKPs).

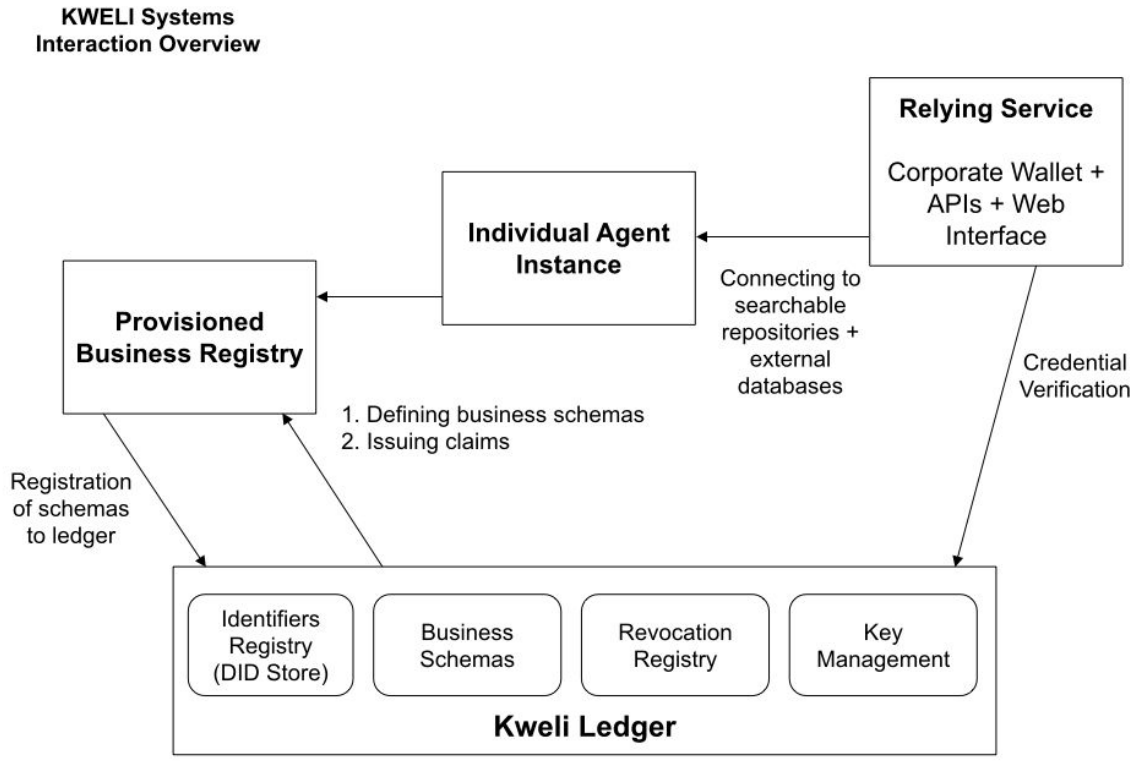
Kweli is built on Hyperledger Indy blockchain framework utilizing the Sovrin network. Indy functions as a public permissioned blockchain in that records published on the ledger are available publicly for anyone to audit but the network nodes that ensure consensus of transactions are governed by the Sovrin Foundation. Therefore, only authorized entities serve as nodes with each node holding a copy of the ledger. Records can be audited in a transparent way by stakeholders while maintaining integrity of records since only authorized entities can commit.

Stewards validate identity transactions to assure consistency about what is written on the ledger and in what order. Consensus across the nodes is maintained by a Byzantine fault tolerant algorithm. To avoid correlation of one's user profile, the system allows for an individual to have unique identifiers for connections made when transacting with other actors within the Kweli ecosystem.

These identifiers, called Decentralized Identifiers (DIDs) are a way to identify things, people or organizations over the decentralized internet while preserving privacy and not tying the user to an identity provider. For example, when interacting with a certificate issuing authority like a university, a unique DID is created for the interaction between you and the university. When presenting the degree certificate to an employer, the university creates a unique DID connection with the employer. Relying web services reference the shared ledger to ascertain credibility of DID Documents (DID Docs).

Kweli is provisioned on a decentralized ledger network on which credential definitions are publicly available for reference. Verifiers and issuers can query the network for proofs regarding a credential to ascertain or issue it. Alongside the network, is a screening interface for businesses to check credentials they require to operate within the African Continental Free Trade Area (AfCFTA). Such credentials include licenses, permits and business registration certificates as required by the AfCFTA agreement. An implementation of the Kweli Business Registry should allow for people to search through to check businesses registered within the trade area.

Other web based services and applications can be built to interact with the ledger as Agents, through individually provisioned APIs and software development kits (SDKs).



Kweli Infrastructure Overview

Choice of blockchain protocol

Hyperledger Indy was preferred for building Kweli since Indy is so far the most advanced blockchain based identity protocol in terms of implemented applications, community of developers and the extensibility provided by Sovrin.
Other identity protocols we explored include uPort on Ethereum[20] and Veres One[21].

[20] "uPort: A Platform for Self-Sovereign Identity - Blockchain Lab." Accessed January 25, 2020. http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf.
[21] "Summary - Veres One." Accessed January 25, 2020. https://veres.one/summary/.

Conclusion

Having introduced the need for a digital Pan-African identity system, the foundational work remains in ensuring a stable infrastructure which supports services to be built on top. To support international interoperability, Kweli will continue embodying open internet identity standards.

For widespread adoption of Kweli and increased applicable domains for Afro-centric enterprises and institutions, continuous user education must be a priority. User awareness shall be conducted through blog and news articles, guides with industry specific use-case summaries, guides to get started as well as audio and visual content to be distributed freely for public access.

This can only be achieved through collective community ownership by industry practitioners, early adopters and educators alike. For Kweli to become a reality and achieve practical applicability, the community around it should leverage strong partnerships with forward looking institutions in the public and private sector and development institutions whose missions align with Kweli. It is going to take a village.

References

African Union, *Draft Protocol to the Treaty Establishing the African Economic Community Relating to Free Movement of Persons, Right of Residence and Right of Establishment,* accessed at link.

African Union, *Constitutive Act of the African Union,* accessed at link.

African Digital Asset Framework, "*Peoples-Driven Standards for Distributed Pan-African Economies*", accessed at link.

Blockchain TNO, "Self-Sovereign Identity - The Good, The Bad, and the Ugly", accessed at link.

Equal Times, "Africa's Invisible Millions Survive without Identity Documents", accessed at link.

Federal Government of Nigeria, Immigration Portal and Visa Guidelines, accessed at link.

Identity, "The Identity Metasystem - Kim Cameron's Identity Weblog", accessed at link.

Kweli's Github Repo, access at link.

Life with Alacrity, "The Path to Self-Sovereign Identity", accessed at link.

McKinsey Institute, "Digital Identification: A Key to Inclusive Growth", accessed at link.

Mckinsey Institute, "The Trillion Dollar-Prize: Plugging Government Revenue Leaks with Advanced Analytics,", accessed at link.

Quartz Africa, "People of African Descent will Form Half of the World's Population by 2050", accessed at link.

United Negro Improvement Association and Communities League, Constitution, accessed at link.

We are Social, "Global Digital Report 2018", accessed at link.

W3, "Verifiable Credentials DAta Model 1.0: Expressing Verifiable Information on the Web", accessed at link.

W3, "Decentralized Identifies (DIDs), v1.0", accessed at link.

Web of Trust, "Web of Trust: General Information", accessed at link.

Web of Trust, "Github: A Verifiable Credentials Primer", accessed at link.

World Bank, "Blog: Global Identification Challenge", accessed at link.

World Bank, "Blog: Counting the Uncounted - 1.1 Billion People without ID's", accessed at link.

World Bank, "Data Set: Global Financial Inclusion - Global Findex Database", accessed at link.

Appendix

Appendix I - E-Form Application Process

- The initial validity period of an approved e-Form "M" for general merchandise shall be 180 days, which may be extended for 180 days by the Authorized Dealer Bank. For capital goods, the initial validity of an approved e-Form "M" shall be 365 days subject to a maximum extension of another 365days. However, any subsequent request for subsequent revalidation of e-Form "M" shall be forwarded to the Director Trade and Exchange Department, Central Bank of Nigeria, for consideration.
- The relevant pro-forma invoice (which shall have a validity period of three months) shall carry a proper description of the goods to be imported to facilitate price verification viz;
- e-Form M shall be valid for importation only after registration by the Nigeria Customs Service (NCS). Consequently, Authorized Dealer Banks are to confirm registration of the e-Form M before proceeding with other import processes.
- Documents in respect of each import transaction shall carry the name of the product, country of origin, specifications, date of manufacture, batch or lot number, Standards to which the goods have been produced (e.g. NIS, British Standards - PD. ISO, IES, DIN, etc).
- All goods to be imported into the country shall be labeled in ENGLISH in addition to any other language of transaction; otherwise the goods shall be confiscated.
- The following procedure shall be adopted for payments for:
    a. Letters of credit transactions: where the transactions involve issuance of Certificate of Capital Importation (CCI) and or supplier's credit, all negotiating documents and or shipping documents (as may be applicable), must be routed from the Beneficiary/Supplier through his/her bank to the correspondence bank of the issuing bank and thereafter to the issuing bank. For the avoidance of doubt, on no account must banks endorse or pay on documents which do not comply with the routing outlined Above.
    b. For Bills for Collection transactions and Unconfirmed Letters of Credit, documents must come to the issuing bank either directly from the supplier's bank or through the offshore correspondent of the issuing bank.
    c. For 'Not Valid' for foreign exchange transactions (which do not require foreign exchange transfer), the supplier should forward the documents directly to the applicant bank that validates the e-Form M.

If we look further at the example with Mariam we can identify some credentials that she had to use multiple times to get what she required on her journey to selling her goods and functioning in general in Nigeria. These credentials would all need to be reverified each time she was submitting them, even if submitting to the same authority. These are the credentials Mariam was required to produce multiple times, the information within them and the level of necessity of that information, and the process of verifying them each time.

Document	Need for Verification		Times verified	Process to Verify	Is there a cost to verify documents?	Submitted to the same authority more than once	Is all the information in the document required for purpose?		Information on Document duplicated on other required documents
	Yes	*No*					*Yes*	*No*	
Visa Application Form		No	5			2		No	Date of Birth, Full Name, Places travelled in last 10 years, Place of birth, Occupation, Place of work, Address of Home and of Work, Nationality, Issue and Expiration date of Passport and Visas, Credentials, Prevailing institution of Credentials, Contact information
Pictures	Yes		5	Notarization	Yes	2			
Letter of Approval From controller General, NIS	Yes		5	Copies to be notarized		2			
Expatriate Quota Approval	Yes		4	Copies to be notarized					
Passport		No	4			2		No	Date of Birth, Full Name, Places travelled in last 10 years, Place of birth, Occupation, Nationality, Issue and Expiration date of Passport and Visas

Business Incorporation	Yes		4	Copies to be notarized	Yes	2		No	Business Name, Date of Registration, Full name
Credentials	Yes		4	Copies to be notarized	Yes	2			Full Name, Prevailing Institution
Curriculum Vitae		No	4			2			Credentials, Prevailing institution of Credentials, Business Name, Full Name, Contact Information, Occupation
Certificate of Export	Yes		2	Copies to be notarized		2			Business Name, Full Name, Contact Information, Occupation, Bank Authorization and information
E-Form “M”	Yes		5						Full Name, Address, Bank Authorization and information.

Formalities and procedures for obtaining different licenses

- Obtaining the different licenses required.
- Subscribe to an export license, then validate the license after paying the OCC control fees at the approved commercial bank or at the Central Bank of Congo.
- Obtaining the Verification Certificate for Export (CVE), after checking the product batch ready for export from the Congolese Control Authority (OCC)

Required documents:

- a letter of request ;
- Sales contract or pro forma invoice ;
- List of the batch of products ready for export ;
- Business license;
- Quality certificate;
- Authorization from the Ministry concerned (case of various products and species protected Certificate CITES).

Formalities and procedures for obtaining different licenses

- Application forms

- Purchase and sales license for specific products.

Formalities and export clearance procedures

- BTR or Waybill entry into system before arrival of shipment at port
- Registering the goods to be exported in the register C148
- Acceptance and processing of the EX declaration and attachments (originals and copies)
- Release warrant

Responsibles	**Actions**	**Documents**
One-stop Shop Authority	Sending requests through the One-stop Shop system	Application forms
Administration of Economy	Evaluation of request and creation of purchase and sales licenses for specific products	Purchase and sales license for specific products
Administration of Agriculture, Fisheries and Breeding via animal and vegetal Quarantine department	Evaluation of request and creation of phytosanitary certificates and export license for agricultural products	Phytosanitary certificate and export license
Administration of Culture and arts	Evaluation of request and creation of export license of piece of art	Export license of piece of art
Administration of environment and wildlife	Evaluation of request and creation of logging permit, logs quota attribution and validation of sales contracts	Logging permit, logs quota attribution and validation of sales contracts
Administration of health through the channel of international quarantine	Evaluation of request and creation of export license of cosmetics, pharmaceuticals, narcotics and soporific	Export license of cosmetics, pharmaceuticals, narcotics and soporific
Administration of mines	Evaluation of request and license of mining products	Export license of mining products
Administration of hydrocarbons	Evaluation of request and creation of export license of oil products	Export license of oil products

Appendix II - Formalities and export clearance procedures

Responsibles	**Actions**	**Documents**
Dealer Sales Department/Declarer	The dealer's sales department or declarer enters the BTR or waybill in the computer system dealer before the arrival of the shipment at the port.	● BTR ● Waybill
Dealer	● Pointing the shipment at the port entrance ; ● Updating data on the dotted packages ; ● Weighing and storage of the consignment	
DGDA-Support	● Support in customs or authorized facilities based on report of pointing jointly signed by the Customs and the representative of the exporter of the goods to be exported ; ● Sealing or putting in declaratory signs of the goods ; ● Entering the report of pointing.	Pointing report
	● Registering the goods to be exported in the register C148	Register C148
Declarer	Inputting the EX customs declaration for export in similar conditions with declarations for import	EX declaration and attachments (originals and copies)
Dealer	● Billing transit at Port ; ● Integrating transit cost in the liquidation report	
DGDA – One-stop Shop	● Acceptance and processing the EX export declaration in similar way as the import declaration	● EX declaration and attachments (originals and copies)
	● Liquidation after checking as per the criteria of selectivity (OCC, OGEFREM, dealer and other department)	● Liquidation report
	● Payment of taxes and rights due	● Liquidation report

	● Edition of the release warrant to allow export of goods .	● Release warrant

Office Border/Inside for direct export

Steps	**Boarding**	
Responsible (Role)	Actions	Document
Forwarding agent	Input in the customs computer network : ● Of BL ; ● Of the boarding instruction	BL, Boarding instruction
Dealer	● Retrieval of the boarding Instruction of the forwarding agent validated by the customs authority, OCC and OGEFREM ; ● Processing the boarding instruction in the Stevedoring invoice sent to Shipping Agent ; ● Checking and loading the shipment ; ● Updating the database on the shipment boarded ; ● Editing the list of the boarding sheet ; ● Sending the boarding signal to different partners.	List and boarding sheet
Shipping Agent	● Retrieval of BL in the customs computer network ; ● Electronic transmission of BL signed to Forwarding Agent (optical pencil or scanning) ; ● Establishing electronically the manifest considering the shipments really loaded ; ● Electronic transmission of the manifest made.	
Customs-OCC-OGEFREM-Dealer	● Retrieving electronic manifest ; ● Auditing their data.	
	● Transfering the electronic signal to the One-stop Shop to confirm the real need of port facilities ; ● Issuing a checking certificate on export by OCC.	Checking certificate on export

Import requirements into Nigeria

- Any person intending to import physical goods into Nigeria shall in the first instance process e-Form "M" through any Authorized dealer bank irrespective of the value and whether or not payment is involved;
- The initial validity period of an approved e-Form "M" for general merchandise shall be 180 days, which may be extended for 180 days by the Authorized Dealer Bank. For capital goods, the initial validity of an approved e-Form "M" shall be 365 days subject to a maximum extension of another 365days. However, any subsequent request for subsequent revalidation of e-Form "M" shall be forwarded to the Director Trade and Exchange Department, Central Bank of Nigeria, for consideration.
- Supporting documents shall be clearly marked "Valid For Forex/Not Valid for Forex" as appropriate i.e. depending on whether or not foreign exchange remittance would be involved.
- All applications for goods subject to Destination Inspection shall carry the " BA" code, while those exempted shall include "CB" in the prefix of the numbering system of the e-Form "M". Payments for goods exempted from Destination Inspection under the Scheme, would not be carried out in the Foreign Exchange Market, without prior approval from the Central Bank of Nigeria. The list of goods exempted from Destination Inspection shall be as approved by the Honourable Minister of Finance and the approval shall be a pre-condition for the completion of e-Form M exempted from Destination Inspection.
- The e-Form M and the relevant pro-forma invoice (which shall have a validity period of three months) shall carry a proper description of the goods to be imported to facilitate price verification viz;
    a. Generic product name, i.e. product type, category;
    b. Mark or brand name of the product where applicable;
    c. Model name and or model or reference number. where applicable;
    d. Description of the quality, grade, specification, capacity, size, performance etc.
    e. Quantity and packaging and/or packing.
- e-Form M shall be valid for importation only after registration by the Nigeria Customs Service (NCS). Consequently, Authorized Dealer Banks are to confirm registration of the e-Form M before proceeding with other import processes.
- Documents in respect of each import transaction shall carry the name of the product, country of origin, specifications, date of manufacture, batch or lot number, Standards to which the goods have been produced (e.g. NIS, British Standards - PD. ISO, etc).
- All goods to be imported into the country shall be labeled in ENGLISH in addition to any other language of transaction; otherwise the goods shall be confiscated.
- Where import items such as food, drinks, cosmetics, drugs, medical devices, chemicals, etc. are regulated for health or environmental reasons, they shall carry EXPIRY dates or the shelf life (minimum of half shelf life at the time of importation) and specify the active ingredients, where applicable.
- Electrical appliances (fluorescent lamps, electric bulbs, electric irons and ties, etc) shall carry information on life performance while cables shall carry information on the ratings.

- All electronic equipment and instruments shall carry:
    a. Instruction Manual;
    b. Safety information and/or safety signs;
    c. A guarantee/warranty of at least six months.
- Any false or fraudulent misrepresentation of facts will result in delays and/or impoundment/seizures.
- Importation of products not properly labeled shall automatically qualify for seizure and destruction without warning, and subject to prosecution.
- All imports into the country shall be accompanied by the following documents:
    a. Combined Certificate of Value and Origin (CCVO), and shall contain the following information:
        1. e-Form "M" no.
        2. Adequate description of goods
        3. Port of destination (The actual port shall be specified e.g. Tin Can, Apapa, Kano, Onne, etc.)
        4. Shipment identification, date of shipment, Country of Origin, Country of supply
    b. Final/Commercial Invoice
    c. Packing list
    d. Shipped/ Clean on Board Bill of Lading/Airway bill/Way bill/Road Way bill
    e. Manufacturer's Certificate of production, the Phytosanitary Certificate or Chemical Analysis Report, which shall state standards, where applicable, should be made available.
    f. Laboratory test certificates for chemicals, foods, beverages, pharmaceuticals, electrical appliances and other regulated products, where applicable.
- The following procedure shall be adopted for payments for:
    a. Letters of credit transactions: where the transactions involve issuance of Certificate of Capital Importation (CCI) and or supplier's credit, all negotiating documents and or shipping documents (as may be applicable), must be routed from the Beneficiary/Supplier through his/her bank to the correspondence bank of the issuing bank and thereafter to the issuing bank. For the avoidance of doubt, on no account must banks endorse or pay on documents which do not comply with the routing outlined Above.
    b. For Bills for Collection transactions and Unconfirmed Letters of Credit, documents must come to the issuing bank either directly from the supplier's bank or through the offshore correspondent of the issuing bank.
    c. For 'Not Valid' for foreign exchange transactions (which do not require foreign exchange transfer), the supplier should forward the documents directly to the applicant bank that validates the e-Form M.
- For transactions with Post Landing charges, a retention fee of 5 – 15% of the project cost as agreed between the importer and the overseas supplier shall be indicated on both the Contract Agreement and the Pro-forma invoice which shall form part of the supporting documents for the registration of relevant e-Form M. In addition,
    a. the stated fee shall not be remitted until a satisfactory evaluation of the project has been undertaken by the Industrial Inspectorate Department of the Federal Ministry of Industry

b. The Authorized Dealer Bank shall forward to the Nigeria Customs Service (NCS), Federal Ministry of Industry (Industrial Inspectorate Department) and the Central Bank of Nigeria , Trade and Exchange Department copies of the Contract Agreement and Pro-forma invoice of such projects for monitoring purposes.
c. The Nigeria Customs Service shall take cognizance of the value of shipment and Post Landing charges as would have been indicated on the Pre Arrival Assessment Report (PAAR)
d. The Industrial Inspectorate Department, Federal Ministry of Industry shall thereafter carry out an evaluation of the project and advise the Central Bank of Nigeria accordingly
e. On receipt of the report of the evaluation from the Federal Ministry of Industry (Industrial Inspectorate Department), the Central Bank of Nigeria shall advise the NCS on the issuance of the PAAR in respect of the retained value and the Authorized Dealer Bank advised to remit same to the beneficiary.

- Buying Commission: The percentage of buying commission to be paid to agents or confirming house acting as intermediary between importers and exporters is a maximum of 2% of the FOB value of the consignment, where applicable.

https://www.customs.gov.ng/Guidelines/Destination_Inspection/guidelines.php

Appendix III - Attempts by Governments to build nationwide ID systems

Name	Short Description	Structure	Regulatory Environment
Kenya: **National Integrated Identity Management System (NIIMS)**	The National Integrated Identity Management System, or Huduma Namba, started as a mandatory registration for all citizens and registered foreign residents.	Each member is given a unique identifier "to create a single source of personal information" [22] when interacting with multiple departments within the government including national identification cards, work permits, and passports.	A pilot program was started on 15th February, 2019 in 15 counties across Kenya and all citizens were given 45 days for biometric registration.
Nigeria: **National Electronic Identity (e-ID) Card**	Each person is given a National Identity Card with a SmartCard built-in giving the user access to multiple "applets" including payments (EMV) and travel (ICAO).	National Identification Number (NIN) is issued by the National Identity Management Commission (NIMC).	NINs are assigned to all Nigerians and legal residents of all ages but the National e-IDs are issued only to Nigerians and legal residents over 16 registered into the National Identity System.
Jamaica: **National Identification and Registration (NIDS)**	With NIDS, Jamaican citizens and legal residents only require one ID to access government and private sector services.	National Identification Number (NIN) is issued by the National Identity and Registration Authority (NIRA).	NINs are assigned to all citizens of Jamaica, lawful residents, and persons residing for a period of six or more months.
Estonia: **e-Estonia**	98% of all Estonians have enrolled for an e-Estonia ID-card, Mobile-ID, or Smart-ID. They also have an e-Residency program for non-Estonia citizens to access the EU business environment.	IDs are assigned by a collection of public and private Estonian organizations.	All citizens and legal residents are encouraged to signup for a digital ID and they also make provisions for non-citizens to apply for virtual residency.
Australia: **myGovID**	The Digital Transformation Agency of Australia introduced myGovID to allow citizens to easily interact with government services.	myGovID and other digital ID providers are run by the Australian Taxation Office. The digital ID program is built as a federation.	All citizens and legal residents are encouraged to sign up for a digital identity.

[22] https://www.cio.co.ke/niims-mandatory-registration-huduma-namba-explained/