strategyworks

TECHNOLOGY-ENABLED CREDENTIALS FOR YOUNG PEOPLE IN AFRICA

A STUDY COMMISSIONED BY THE MASTERCARD FOUNDATION

ALEX GRECH AIAZE MITHA

AUGUST 2018

Contents

Acknowledgements

This study includes insights from structured interviews[1] with experts with linkages to Africa and young people and a hands-on involvement in the credentials and technology sector, including the blockchain.

We are grateful for the contribution of the following colleagues who also reviewed the final report:

- Shailee Adinolfi – VP Account Management and Marketing at BanQu
- Dr Borhene Chakroun – Chief of Section, Youth Literacy & Skills Development, UNESCO
- Amelia Diaz – International Trade Centre (ITC)
- Tricia Martinez – CEO Wala & Director Dala Foundation
- Renita Nabisubi – FSD Uganda
- Dr. Bitange Ndemo – Chairman of the Blockchain Task Force in Kenya
- Vivian Onano – Social Entrepreneur, Global Youth Ambassador at Water Aid, Women Deliver Young Leader and Youth Advisor to the UN Women Civil Society Advisory Group
- Maria Perdomo – Global Specialist, Youth Finance at UNCDF
- Professor Mario Scerri – Professor of Economics, Institute for Economic Research on Innovation, South Africa
- Dr Balaji Venkataraman – Director of Knowledge Management, Commonwealth of Learning, with expertise in Information and Communication Technology applied to rural development

We worked closely with the Mastercard project manager, Dr Olga Morawczynski. We are very grateful for her support, feedback and insights throughout the course of this project.

Dr Alex Grech, University of Malta and Commonwealth Centre for Connected Learning Foundation

Aiasze Mitha, Amarante Consulting

(1) The interview questions are included as *Annex 1* to this report

Executive Summary

Digital technologies offer opportunities and challenges for skills development and recognition globally. Africa, within this context, is no different to the global landscape.

Credentials mean different things to different stakeholders – from those who issue them to those who receive them to those who use them at some later stage, such as employers. In this study, we differentiate between academic, TVET, micro and reputation credentials. Most African nation states continue to have one-stop-shop, education systems in place that lead to an academic pathway, when the skills needed by the labour markets that may offer employment to young people may not necessarily be best served by academia. Before engaging in any discussion on the appropriateness of tech-enabled credentials, **it is vital to determine the right credentials needed by the specific labour market sectors in specific target countries**: in this study, after consultation with the Mastercard Foundation we focused on Kenya, Rwanda, South Africa and Ghana.

There are no major infrastructure barriers in the target countries which would prevent the deployment of tech-enabled credentials in Africa. However, such initiatives must add value to the end user by improving the chances of young people in securing gainful employment: technology cannot be dropped in socio-cultural, political and economic silos - otherwise, they risk being perceived as a fad. The Africa unemployment context challenges many established education and labour market norms: traditional credentials may not necessarily be the currency to kickstart the labour market or new recruitment, for the matter. Recruitment outside cities tends to rely on trust credentials and informal references, built from real life social networks and social relations as opposed to the advice of recruitment agencies or CVs on LinkedIn ('my tribe is my social network').

The immediate opportunities point towards tech-enabled credentials that recognise the accumulation of a variety of skills secured during the lifelong learning journey. Although formal learning pathways remain primarily locked in the one-size-fits-all model leading to academic achievement, the quick wins are likely to be the recognition of skills acquired through TVET and informal learning. The jobs available for young people are not those necessarily requiring academic credentials, but work-based skills such as plumbers, and labourers. The sectors that are currently contributing to new job creation are agriculture, transportation and education. In the case of agriculture, vacancies are as likely to be in rural agricultural areas as they are in cities. Within this context, the valorisation of skills through visible credential systems (including skills gained through informal and non-formal learning in 'narrow areas') and the recognition of motivational or so-called 'social capital' credentials (including those acquired through unorthodox or online means) will contribute towards trust and the personal reputation of the job-seeker - and are therefore likely to be appreciated by employers.

African higher education and TVET institutions have to mitigate similar challenges to those encountered by overseas counterparts – loss of certificates, fraud, administration costs etc. The digitization of learning credentials alone will only partly mitigate these risks: while such solutions may contribute to institutional administrative efficiencies and brand management, they will not necessarily lead to the self-sovereignty of young people seeking increased access to employment. The emerging use case studies using blockchain for the notarization of certificates holds significant promise.

This study identifies **a tangible opportunity for African youth to gain access to a fourth generation of qualifications frameworks though the creation of a set of strategic pilots around technology-enabled credentials that use blockchain technologies for notarization.** The core social value principles of blockchain technology are particularly appropriate as a potential value-added to young people in Africa trying to secure gainful employment: Self-Sovereignty and Identity; Trust; Transparency and Provenance; Immutability and Disintermediation.

There are many challenges to navigate and tech-enabled credentials and the systems that support them need to be simple to understand, solve existing problems and clearly add value to the issuing institutions, learners and employers. Identifying stakeholders interested in the potential of tech-enabled credentials requires an inquisitive approach as opposed to generalisations and assumptions. Public sector employment continues to drive employment in city contexts, but change is often dependent on identifying individuals in key positions who may act as advocates for new technologies; private sector employers include multinational firms as much as sole traders and the formal domestic labour market or enterprises; informal companies often contribute to rural livelihoods, including craft associations, artisans etc. Employers' needs for credentials in these sub-sectors will vary greatly. Selecting the right people in the right industries for pilots will be key. The insertion of technology features in the accreditation of skills acquired through TVET and in sectors such as agriculture may help mitigate negative perceptions of young people in securing such skills and applying them to sectors which may not appear as attractive as the service industry.

This study proposes five hypotheses as recommendations for tangible pilots that may fast-track the take-up of tech-enabled credentials by young people in Africa, and in turn increase their chances of securing gainful employment. They include: levering on the existing Mastercard Scholars Program to issue co-branded Foundation and participating university credentials which are notarized using the Blockcerts open standard; issuing secure immutable TVET credentials; the development of verifiable professional certifications for independent professionals; the recognition of reference letters and ratings as valid social collateral by notarizing certificates on the blockchain; and the use of the blockchain to develop a system for the crowd-based validation of skills.

Much depends on the willingness of the Foundation to lead experimental projects and partner up with governments, actors in the labour markets, intermediaries and experts. With the exception of the first hypothesis, all research and early use case studies point to the need for the Foundation to engage with Government in the target country at the outset as the key stakeholder to fast-track sustainable change through workable pilots in economic sectors that are perceived to be driving job creation. The Foundation would also need to reach out to employers' associations that can also support a set of pilots in these specific economic sectors on the basis that they can contribute to economic development. Strategically, identifying pilots that can be built around an economic sector will secure the attention of both government and the labour market, even if the latter is deeply mistrustful of government.

We believe that the Foundation is ideally placed to lever on its reputation in Africa and meets the goals of its strategy by facilitating tech-enabled certification initiatives in target countries. Specifically, it has the ability to: a) interact with senior officials in governments with authority and purpose; b) facilitate access to funding of initiatives around tech-enabled credentials that can contribute to meeting the needs of target economic sectors and c) put its proprietary networks to good use, by securing partnerships with various stakeholders in technology, education, TVET and the labour market; and engaging experts already working with use case studies in the blockchain credentials space.

Acronyms and Abbreviations

AWS	Amazon Web Services
CEN	European Committee for Standardisation
CPD	Continuing Professional Development
DAO	Distributed Autonomous Organization
DLT	Distributed Ledger Technologies
GDPR	Global Data Protection Regulation
IPFS	InterPlanetary File System
ISO	International Standardisation Organization
FINTECH	Fusion of Finance and Technology
MOOC	Massively Open Online Course
NGO	Non-Governmental Organization
P2P	Peer to Peer
PKI	Public Key Infrastructure
TVET	Technical and Vocational Education and Training
UNCDF	United Nations Capital Development Fund
UNESCO	United Nations Educational Scientific and Cultural Organization

Glossary

For the purposes of this study, we use the following definitions:

Authenticity means the degree to which the genuineness and undisputed origin of a digital certificate and the data therein can be verified and have not been forged. Within a blockchain context, this involves the process of proving the counterparty identities and the existence of assets via private / public keys.

Badge means a symbol or indicator of an accomplishment, competency, skill or quality. It is similar to the paper certificates one receives upon school graduation, participation in an event or successful completion of a course. A digital badge is an image file and can be easily shared. Moreover, a digital badge contains within its code hidden, encrypted data with information on its owner, its origin, the criteria required to earn it and a link to the documentation that confirms it was successfully earned. Thus, the performance task, criteria and evidence all become accessible to educators, employers and others who may want to understand more about a student, candidate employee or volunteer.

Bitcoin means a cryptocurrency and a digital payment system invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto. It was released as open-source software in 2009. The system is peer-to-peer, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a blockchain. Since the system works without a central repository or single administrator, bitcoin is called the first decentralised digital currency. Besides being created as a reward for mining, bitcoin can be exchanged for other currencies, products, and services in legal or black markets. The invention of the Blockchain for bitcoin made it the first digital currency to solve the double spending problem, without the use of a trusted authority or central server.

Blockchain means a distributed ledger or database that maintains a continuously growing list of transaction records with various protections against tampering and revision. It is collectively built and maintained by every party that uses it. It is made up of a number of entries, called blocks, which are composed of the data being stored. These blocks are transmitted to the partners in the distributed ledger so they can be verified by unaffiliated parties. Each block contains a hash code that identifies the block that immediately preceded it, making the blocks sequential and chaining them together - hence the term 'Blockchain'. In terms of size, Bitcoin is the largest blockchain and in terms of the popular vernacular is automatically associated as being 'the Blockchain'. In practice, there are other blockchains, such as the Ethereum blockchain, as well as public and private blockchains. All blockchains have a digital currency of some kind associated with them.

Blockchain Software means a broad class of systems also known as distributed ledger technology (blockchain) which enable ledgers (records of activity) to be cryptographically distributed across a diffuse network of nodes (such as personal computers or servers), cutting out the need for a central ledger keeper and effectively delegating that task to the users of the ledger. Rather than a single party keeping a record of all of the transactions that happen within a given system, a blockchain shares the task of logging and recording those transactions amongst the people making them, with the underlying technology verifying that all users are keeping matching records. The technology effectively solves the problem of 'trust' across networks as it enables complete strangers to complete transactions without risk of the participating parties defaulting or failing to pay.

Certificate means an official document, issued by an awarding body, which records achievements of an individual following an assessment against a predefined standard. Certificate can be interchangeably referred to as diploma or title.

Certification (of learning outcomes) means the process of formally validating knowledge, know-how and / or competences acquired by an individual following a standard assessment procedure.

Consensus mechanism means a method of authenticating and validating a value or transaction on a blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any Blockchain or distributed ledger.

Credential means an electronic or paper-based representation of accredited learning outcomes (a set of knowledge, skills and / or competences) acquired or demonstrated by an individual after completing a formal, informal and / or non-formal learning process.

Cryptocurrency means a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin and Ether are the best-known examples.

Cryptography means the process of enforcing the authentication and cryptographic validation of transaction integrity via quorum structures and confirmation via code without the need to trust or rely on a centralized authority.

Cryptographic signature means a method to mathematically validate the owner of a piece of data beyond any doubt if the user has kept the private key to sign the transaction safe.

Digital Badge means a clickable graphic that contains an online record of 1) an achievement; 2) the work required for the achievement; 3) evidence of such work; and 4) information about the organization, individual or entity that issued the badge.

Digitization means the conversion of information into a digital form that can be used by the internet, mobile phones and all other tools that collect, store, analyse and share information digitally.

Digital Signature means binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message. It is similar to an electronic "fingerprint". In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature (eSignature).

Distributed ledger means a digital record of ownership that differs from traditional database technology, since there is no central administrator or central data storage; instead, the ledger is replicated among many different nodes in a peer-to-peer network virtual private network, and each transaction is uniquely signed with a private key.

Ethereum means a decentralised platform that runs smart contracts. Developed as a custom-built blockchain with shared global infrastructure, that can move value around and represent the ownership of property. Every node (computer) in the network runs an operating system called Ethereum Virtual Machine (EVM). EVM understands and executes the software written in Ethereum specific programming language. The software/apps executed by Ethereum Virtual Machine are called 'smart contracts.

Europass means an EU initiative which aims to help people make their skills and qualifications clearly and easily understood in Europe, thus facilitating the mobility of both learners and workers. The Europass documents have been designed in such a way as to help people chronicle their skills and competences in a coherent manner, whether they are planning to enrol in an education or training programme, looking for a job, or getting

Formal Learning means learning that occurs in an organised and structured environment (such as in an education or training institution) and is explicitly designated as learning (in terms of objectives, time or resources). Formal learning is intentional from the learner's point of view. It typically leads to certification.

Hash Functions mean an application programming interface creates, through a process called hashing, a unique key or digital fingerprint for each file. Cryptographic hashes, such

as the SHA256 computational algorithm, ensure that any alteration to transaction input — even the most minuscule change — results in a different hash value being computed, which indicates potentially compromised transaction input.

Immutability means unchangeability. An **immutable** object (unchangeable object) is an object whose state cannot be modified after it is created. Blockchain data cannot in practice be easily changed because it is continually replicated across many different locations and Organizations. Blockchains are tamper-evident. Attempts to change it in one location will be interpreted as fraudulent and an attack on integrity by other participants and will be rejected.

Informal learning means learning resulting from daily activities related to work, family or leisure. It is not organised or structured in terms of objectives, time or learning support. Informal learning is in most cases unintentional from the learner's perspective. Informal learning outcomes may be validated and certified.

Interledger protocol means a protocol that connects legacy ledgers of the past with the distributed ledgers of the future.

Interoperability means exchangeability between a range of products, or similar products from several different providers, or even better past and future revisions of the same product. Interoperability may be developed post-facto, as a special measure between two products, while excluding others, by using open standards. When a vendor is forced to adapt its system to a dominant system that is not based on open standards, it provides not interoperability but compatibility.

Ledger means an append-only record store, where records are immutable and may hold more general information than financial records.

Lifelong learning means all learning activity undertaken throughout life, which results in improving knowledge, know-how, skills, competences and/or qualifications for personal, social and/or professional reasons.

Merkle tree means multi-signature; an authentication function that allows a group of users to sign a single document with more than one private key.

Micro-credential means a term that encompasses various forms of credential, including 'nano-degrees', 'micro-masters credentials', certificates, badges licences and endorsements. They focus on modules of learning much smaller than those covered in conventional academic awards, which often allow learners to complete the requisite work over a shorter period. In their most developed form, micro-credentials represent more than mere recognition of smaller modules of learning. They form part of a digital credentialing ecosystem made possible by digital communication technologies establishing networks of interest through which people can share information about what ta learner knows and can do.

Network Protocols mean the formal standards and policies comprised of rules, procedures and formats that define communication between two or more devices over a network. Network protocols govern the end-to-end processes of timely, secure and managed data or network communication.

Node means members or systems of a consensus network; a server that holds a replicated copy of the ledger can have varying roles: to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a VM instance.

Non-formal learning means learning embedded in planned activities not explicitly designated as learning (in terms of learning objectives, learning, time or learning support). Non-formal learning is intentional from the learner's point of view. Non-formal learning outcomes may be validated and may lead to certification.

Open Standard means a non-proprietary protocol or specification that has been developed in a collaborative process and is published for free use by any interested party. Open standards tend to be governed by an organization that is open to all who wish to

join, facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

Participant means an actor who can access the ledger: read records or add records to.

Peer means an actor that shares responsibility for maintaining the identity and integrity of the ledger.

Peer to peer (P2) network means an architecture of computers or networks that shares tasks, work, or files between peers. Peers are partners in the network with equal privileges and powers in the environment. In a P2P network, each computer or user is called a "node" and collectively they comprise a P2P network of nodes. The P2P network in the Blockchain consists of a series of computers and servers that each act as a node in the network. A blockchain network can be either permissioned or permissionless.

Permissioned means a private network in which users set rules about access, the consensus mechanism, governance, participation etc. Permissioned networks are limited to participants within a given business network. On permissioned Blockchains, participants are allowed to view only the transactions relevant to them.

Permissionless means a network that is open to any participant, and where transactions are verified against the pre-existing rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous. Bitcoin is the most familiar example of a permissionless network.

Permissioned Ledger means a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler that the consensus process used by unpermissioned ledgers. Permissioned block chains provide highly-verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than a permissionless ledger.

Portability means the ability to share and translate credentials from one context to another and to represent them in different combinations for different audiences.

Privacy means ensuring that only the receiver intended can read the message. The field of computing cryptography addresses many security and privacy issues of distributed consensus through the use of mathematical formulas for specific secure communication requirements within the context of any application-to-application communications.

Private Blockchain means a blockchain with constrained read/write access alongside a consensus algorithm which allows only a preselected group of people to contribute and maintain the integrity of the blockchain. A private blockchain may also refer to a blockchain operated by a private entity or consortium, with no or limited access by other parties, and typically with a small number (tens or hundreds) of processing nodes operating the blockchain. In this context, compared to public blockchains, technical optimisations may be used to improve the latency and throughput of the blockchain, and BFT consensus mechanisms may be used to provide stronger guarantees about the completion of transactions.

Private Key means an encryption key uniquely linked to the owner and known only to the parties exchanged in a transaction; it is secretly held in a digital wallet.

Professional Standard means a public statement that describes the professional knowledge, professional practice and professional engagement required of someone working in a professional capacity.

Public Blockchain means a network in which anyone can participate by reading data, submitting transactions, and participating in the validation process. A public blockchain is operated as a public peer-to-peer system. Parties are usually identified by pseudonymous

public/private keys, and a form of Nakamoto consensus is typically used to allow a large number (thousands) of processing nodes to operate the blockchain.

Public Key means the public address where other wallets send transaction values.

Public Key Infrastructure (PKI) means a secure data transmission and authentication system that uses public key cryptography.

Qualification means a proxy for the different types of learning acquired by an individual using learning outcomes. It is a formal acknowledgement of a successful completion of a course, including meeting its designated learning outcomes. Terms typically used for qualifications include degrees and certificates. Completion of a long-term course leads to a macro-qualification. For example, a traditional degree typically requires three years of a full-time study or the equivalent; courses of between one and three years might culminate in the award of a diploma. Completion of a shorter course can lead to a more restricted from of qualification, increasingly referred to as a micro-credential.

Scalability means the capability to cope and perform an increasing throughput and maintain or even increase its level of performance or efficiency when tested by larger operational demands. Latency is the delay in transaction processing

Security or Distributed ledger security means the process for protecting and safeguarding business and personal data, as well as transaction information. The validation of the results should be correct under non-Byzantine failures; also includes integrity (an assurance to the receiving node that a message received has not been altered in any way) and nonrepudiation (a mechanism to prove that the sending node really sent this

Smart Contracts mean applications that run on a custom-built blockchain, exactly as programmed and without any possibility of downtime, censorship, fraud or third-party interference.

Tokenisation means the process of replacing sensitive data with unique identification symbols that retain all essential information about the data without compromising its security.

Technical and Vocational Education and Training (TVET) means the acquisition of knowledge and skills for the world of work.

Recognition means all learning activity undertaken through life, which results in improving knowledge, know-how, skills, competences and/or qualifications for personal, social and/or professional reasons.

Skill means the ability to apply knowledge and use know-how to compete tasks and solve problems.

Validation means confirmation by a competent body that learning outcomes (knowledge, skills and/or competences) acquired by an individual in a formal, non-formal or informal setting have been assessed against predefined criteria and are compliant with the requirements of a validation standard. Validation typically leads to certification.

Verification means the process to check the authenticity of a digital certificate.

Wallet means the store for the information necessary to transact bitcoins. While wallets are often described as a place to hold or store bitcoins, due to the nature of the system, bitcoins are inseparable from the Blockchain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bitcoin holdings" and allows one to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys.

1 Purpose and Objectives of this Study

The MasterCard Foundation ('The Foundation') commissioned this exploratory study as a primer to determine the relevance of tech-enabled credentials for young people in Africa as a means of social empowerment. By the latter, we primarily mean an increase in personal social capital which may help young people secure dignified and fulfilling employment or follow an entrepreneurship pathway.

There are a number of pre-requisites to this study:

1. Any recommendations are to be in line with the strategies articulated in the Mastercard Foundation Strategy: 2018-2030 *Young Africa Works*[2].
2. The Foundation's interest extends beyond academic credentials to: work-performance credentials secured from formal TVET training programmes; credentials gained from memberships of professional associations; and informal credentials which may contribute to the holder's social capital: the latter may also be recognized on online social platforms such as LinkedIn, Uber and Little Cab. This is a particularly important differentiator, which resulted in us developing a bespoke, 'wider' definition of what constitutes a credential for the purpose of this study.
3. The geography of focus is sub-Saharan Africa. After an initial wave of desk research and discussions with the Foundation, we proposed four countries where we would conduct local research: Kenya, Rwanda, South Africa and Ghana.
4. While the analysis explored a wide array of technical options, the study places a significant focus on emerging blockchain-enabled solutions, with a view of integrating these solutions into a broader digital credentials ecosystem, since these offer material advantages over other technical solutions.

The report has been structured to facilitate a quick read, with tabulations and tables employed to facilitate this process. The annexes at the end of the report are primarily technical in nature but are essential in providing detail and empirical evidence on issues discussed during the course of this study.

In the case of readers with no previous knowledge of blockchain technologies, we strongly recommend that *Annex 4* is read before the report.

(2) The following strategies inform the Foundation's Goals: Design Country-Specific Strategies; Empower Young Women; Work with African Organizations; Use Technology to Drive Impact and Scale; Share Evidence-Based Knowledge; and Innovation.

2 Approach

This study was developed organically, using available literature, proprietary market intelligence, a set of interviews with experts and stakeholders with an interest in the African youth and education sector and our own hands-on experience with relevant use case studies.

As initial ideas emerged from the first wave of interviews and use cases in other countries, we triangulated our hypotheses with a second set of interviews (sometimes with the same interviewer) and further research.

Figure 1 provides an overview of our approach.

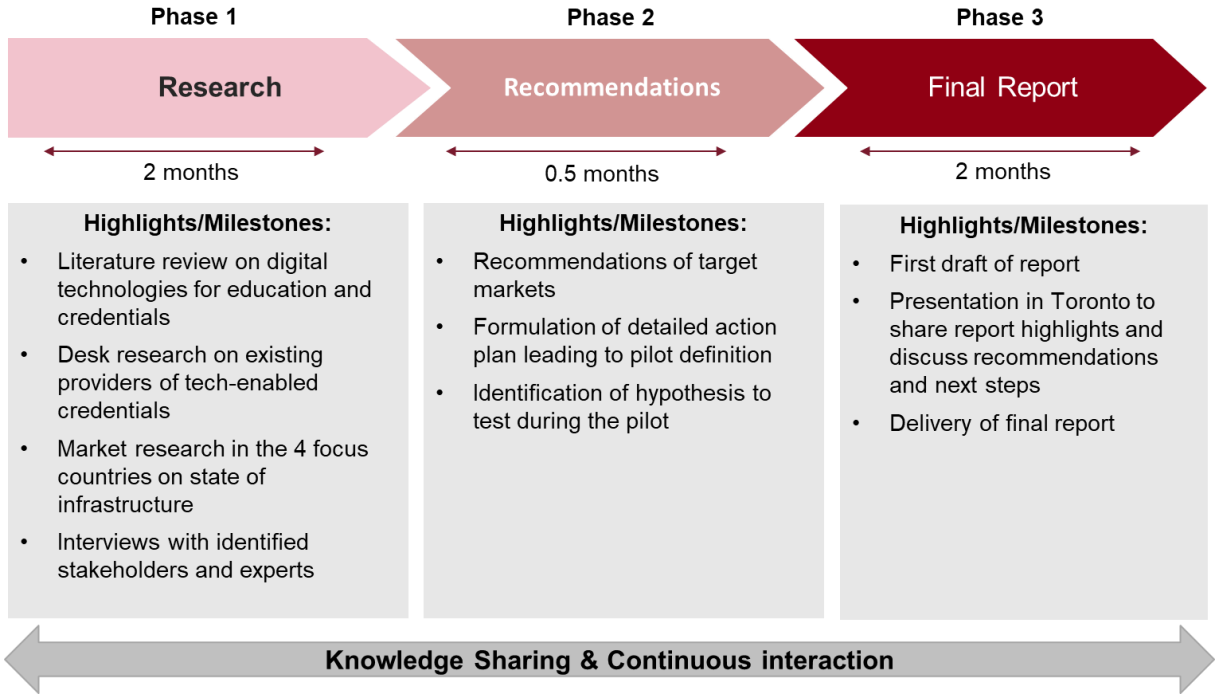


Figure 1: Overview of Approach

3 Credentials and Youth Employment in Africa

3.1 An Introduction to Credentials

The literature on what constitute credentials is extensive, and constantly being updated, not least because of the significant opportunities that digital technologies bring to the recognition of skills and qualifications.

Typically, credentials tend to be categorised within the taxonomy of formal learning; informal learning; and non-formal learning (see *Figure 2*)

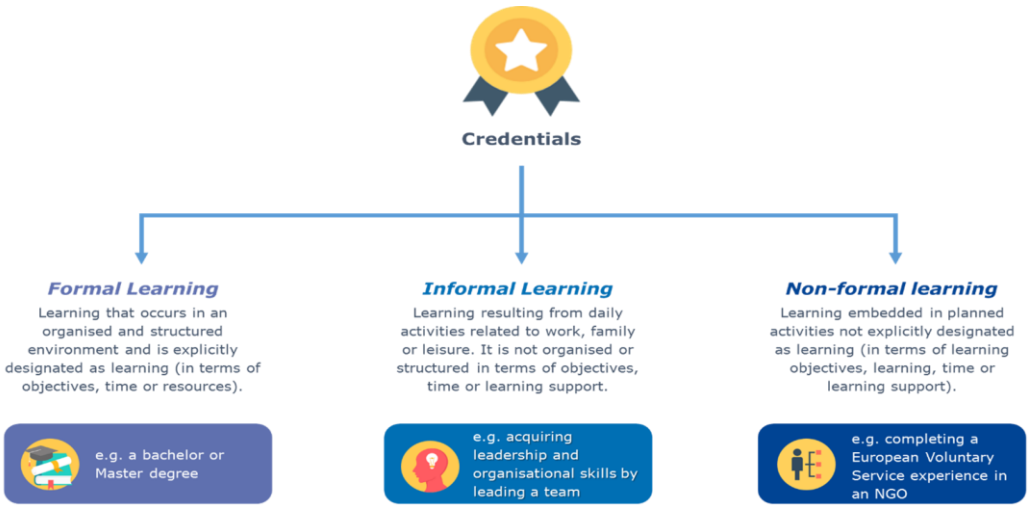


Figure 2: Taxonomy of Credentials

This study approaches credentials within a wider, more inclusive context than the academic context, to include the recognition of TVET, skills and more personal attributes and skill sets related to identity and experience.

A credential is a **statement** issued by one party (the issuer) to another party (the recipient) describing the recipient's **qualities**.

Credentials are used for the purpose of **proving to a third party** that the holder **qualifies for something**.

In this report, we distinguish between five distinct types of credentials (see *Figure 3* overleaf):

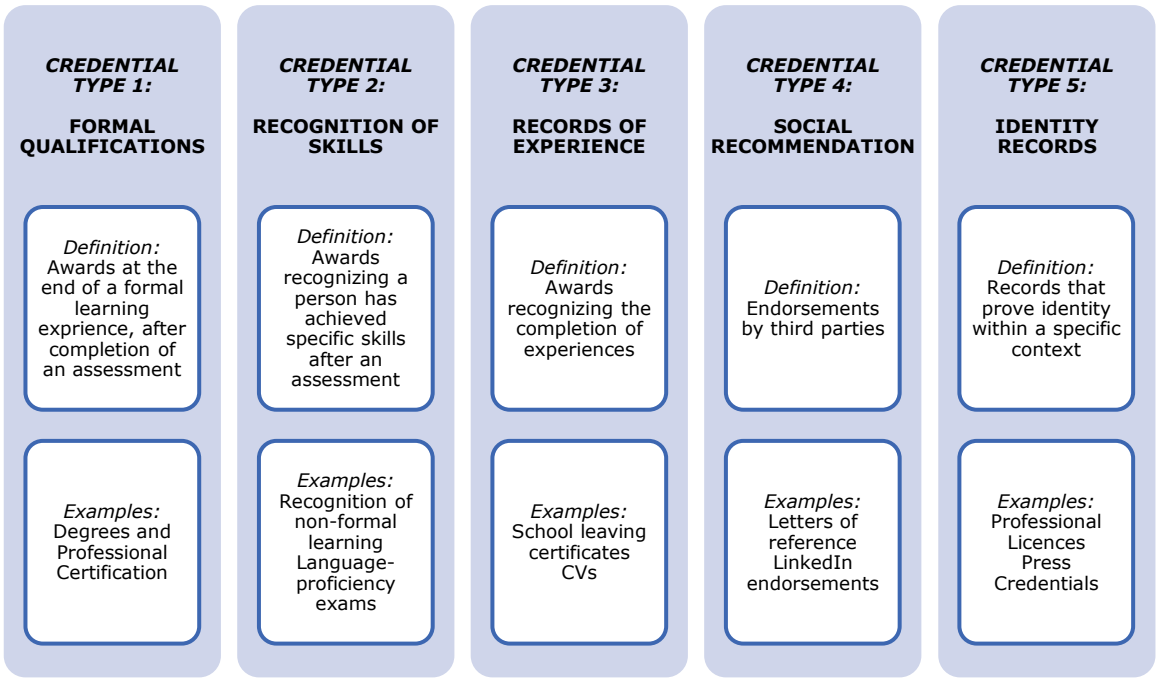


Figure 3: Five Types of Credentials

To further illustrate the differences between these types of credentials:

- A degree is a ***formal qualification*** from a **university** to a **graduate** describing that they have **achieved expertise in a subject** (e.g. medicine). This credential can be used to prove to another **educational institution** that the holder qualifies for admittance into a **doctoral degree programme**;
- A job-reference is a ***social recommendation*** from an **employer** to a **previous employee** describing their **job performance and attitude**. This credential can be used to prove to a **recruiter** that the person qualifies for a **job**;
- A medical licence is an ***identity*** from a **medical chamber** to a **doctor** describing that they have the required **medical knowledge, skills and conduct**. This credential can be used to prove to a **patient** that the holder is qualified to **practice medicine**

To determine the relevance of tech-enabled credentials in specific contexts, it is important to engage with the concept of the digital credentials ecosystem, made up of a set of stakeholders, their functions and the artefacts they use (see *Figure 4* and *Table 1*):

Figure 4: Key Functions in A Digital Credentials Ecosystem (adapted from Chakroun & Keevy, 2018)

FUNCTION	TYPICAL STAKEHOLDERS	ARTEFACTS
USE	Students, Recruitment Agencies, Citizens, Employers, Professional Associations, Immigration Services	Academic Record, Transcript, Digital Badge, Qualification
PROVIDE	Academic and VET institutions, Digital Platforms	Awards, Student Account, IT Platform, Digital Badge, Data sets, Repository
AWARD	Institutions, Faculty Vendors, Suppliers, Online communities	Awards, Credentials
QUALITY-ASSURE	Ministries, Qualifications Authorities, Sectoral Bodies, Governments and Government Agencies, Standards Bodies	Policies, Guidelines
EVALUATE	Quality Assurance Agencies (such as ENIC-NARIC Network), For-profit undertakings, Association for International Credential Evaluation Professionals (TAICEP)	Transcripts, Evaluations
VERIFY	Verifiers (Non-Profit), Qualifications Agencies, Government Departments	Verification Certificates
CONVENE	UNESCO, World Bank, OECD, European Commission, African Development Bank, Governments (and Government Agencies), GDN	Minutes, Conventions, Conference Proceedings

Table 1: Functions, Stakeholders and Artefacts in a Digital Credentials Ecosystem

The ecosystem is very much dependent on the range of tools and technologies available at any given time. **A cursory review of the functions, for instance, reveals a number of activities associated with the production of a 'credential' that are likely to be disrupted by fast-developing technology.**

These activities include: the award of Qualifications; Licensing and Accreditation; Management of Student Records and Learning Achievements; Intellectual property management and Payments for services.

Technology-enabled credentials are currently very much associated with the disruptive potential of the blockchain. *Annex 4* includes a primer on the blockchain, one of the emerging technologies for digital credentials. It also includes a synthesis of **the core social value principles of blockchain technology, which are particularly appropriate as a potential value-added to young people in Africa trying to secure gainful employment.** It is the combination of the core principles of Self-Sovereignty and Identity, Trust, Transparency and Provenance, Immutability and Disintermediation that makes the blockchain such a compelling proposition for stakeholders, and young learners in particular.

This introductory section to credentials therefore must be read in conjunction with *Annexes 3, 4 and 5*. *Annex 3* proposes a framework for credentials. *Annex 5* includes an analysis of the different architectures available regarding their scope and functionality and their impact on the mobility of learners, security and participation.

3.2 Overview of the Credentials Landscape in Africa

The following is a high-level analysis of the different categories of credentials associated with sets of credential providers:

3.2.1 Formal Learning Qualifications

3.2.1.1 Degrees by Accredited Academic Institutions

Feedback received from interviews with experts indicates that the most relevant credentials in Africa remain the ones delivered by formal academic institutions, in that they are the most broadly accepted by employers. In each market, a central authority is in charge of accrediting institutions[3] in that it assesses, accredits and awards charters to both public and private learning institutions as a confirmation that they are meeting prescribed standards of academic excellence established by the same central authority. These standards are important in that interested stakeholders recognize qualifications or awards if they are issued as credentials from accredited and recognized institutions.

In some cases, as in the case of recognition and equation of qualifications, the qualification must be certified by an Advocate and Commissioner for Oath or an Advocate and Notary Public or the issuing institution. The verification process by which the Advocate or Notary will be able to attest the legitimacy of the credential remains questionable. Certificates tend to be mostly paper-based and anecdotal evidence shows that they are often scanned and stored by students as a PDF file on their computer at the risk of losing them. Re-issuance of certificates is a lengthy and costly process and is cumbersome for all parties involved but also generates revenue for institutions.

3.2.1.2 Certificates issued by employers and NGOs

It is common practice in Africa for employers like Nestle or MaRS to provide on the job training to farmers and other professionals on techniques such as how to grow organic crops, use non-chemical pesticides, use specific machinery etc. These training programmes do not always result in the issuance of a formal certificate of achievement or the recognition of skills secured through participation in the course, yet they are particularly valuable to the learner and important to potential employers. There have reportedly been attempts on the part of Nestle to formalize these certificates in West Africa.

At the other end of the spectrum, NGOs like Save the Children and governmental and inter-governmental organizations such as the UN, USAID, GIZ are also concerned with the well-being of adolescents and are attempting to provide them with skills that will contribute to meaningful employment or entrepreneurship pathways. Training may be provided on site or via online learning using schemes such as GIZ's Global Platform 21[4].

Their main focus revolves around youth employability skills, entrepreneurship and vocational training and they are already working with governments, labour, technical and vocational education and trainings, employment offices, online job sites, youth associations and other Organizations. In our interviews, NGO representatives described the need to track the progress and development of adolescents and their learning journeys in a manner that creates trust and measures achievements, and identified significant gaps in this area.

---

(3) In South Africa, providers of education and training must apply for accreditation with an Education and Training Quality Assurance (ETQA) body under the South African Qualifications Authority (SAQA). Kenya has a Commission for University Education.

(4) See https://qc21.giz.de/ibt/var/app/wp342P/1522/

3.2.2 Recognition of Skills

3.2.2.1 Skill-Certificates from Training Organizations

TVET and other semi-formal training institutions deliver training in areas as diverse as Project Management (PMP) and Quality Management (Six Sigma): such training courses are particularly sought after in Africa. Credentials are typically delivered in a paper format and a downloadable electronic format, with a specific credential number that any potential employer can easily verify against the issuing institution's database.

These types of training are typically administered by a global brand through a franchise network, sometimes also involving further sub-franchisees. Each brand has its own set of accreditation and quality criteria for monitoring franchisees, some of which are more stringent than others.

It would be invaluable for the learner to be able to manage all these in one single place from one ''overlay'' interface.

3.2.2.2 Badges and Skills Awards

Badges and other skills awards are gradually being recognised, albeit more often in 'city' and higher education contexts. Open badges in particular are visual digital tokens of achievements, affiliation or some other trust relationship which can be shared across the web. They represent a more detailed picture than a curriculum vitae or resume' in that they can be presented in ever-changing combinations, creating a constantly evolving picture of a person's lifelong learning.

In 2017, IBM announced "IBM Digital - Nation Africa", which provides a cloud-based learning platform designed to provide free skills development programs for up to 25 million African youths over five years, enabling digital competence and nurturing innovation in Africa. A key part of the initiative is a range of freely available self-assessment tests to track the progress of individuals, together with industry recognized 'Open Badges' aligned to digital competencies. The badges can then be shared with prospective employers.

3.2.2.3 Records of Experience

- **School-leaving certificates**
  - In the majority of cases school-leaving certificates are issued in a paper format and, unless issued by an accredited and recognized institution, will in most cases require certification by an Advocate or a Notary. The verification process is lengthy and imperfect and very vulnerable to fraud and other misrepresentations.

- **Training-course certificates of participation**
  - There is an awareness in target countries that unless a certificate is issued for the completion of a training course, the end user will see little value in the participation of the learner in the exercise. Typical training course certificates often only certify participation without necessarily looking into skills or learning outcomes.

3.2.2.4 Social Recommendations

- **References**

From the feedback gathered in interviews, professional references do not appear to carry a lot of weight unless they are verifiable – that is that the working relationship with the referring party can be established with certainty and the validity and integrity of the referral can also be established. In general, that reference check is done by directly contacting the referee via a formal interview, probably as a way of mitigating the risk of fraud.

References are inevitably linked with CVs and resumes. Digitization of references and other lists of achievements can contribute to the integrity and veracity of the resume.

— Social-Recommendation Platforms

Social recommendation platforms such as review sites, directory sites, local vertical sites and local search portals are in their infancy in Africa and therefore not widespread or universally recognized as playing a key role in employment decisions. However, there is an opportunity to use social recommendation platforms on the quality of service delivered by solopreneurs and trades people such as carpenters, plumbers, hair salons etc. In these areas, social reputation is a driving factor for supplier selection. The challenge remains in validating recommendations since the risks of tampering are high.

— Gig Economy Reviews and Rankings

There are a number of 'Uber-like' companies in Africa, from Safe Bodas to Little Cab, Mondo Ride, Safemotos and Taxify. Additionally, gig-economy platforms like Amazon's Mechanical Turk and upwork.com are making significant inroads into the continent. A core component of each of these platforms is that each job completed results in a rating. Good ratings are essential to be awarded more 'gigs' within the platform. Each of these platforms have economic incentives to keep the rating information locked within the platform – they therefore do not allow for export of these ratings from the platforms or for the creation of profiles harvested from a number of different platforms.

The most significant challenge is that all of these platforms seek to lock users within the taxonomy of the platform, so inevitably portability of credentials is challenging or impossible without entering into a direct relationship with the owner of the platform. Some digital lenders in Kenya are starting to look at Uber ratings as a way to make a credit decision for Uber drivers, most likely for its psychometric value.

At face value, the more formal /academic / training type of credentials appear to be more useful or acceptable to employers – and hence more suitable for investigation for tech-enabled credential deployment.

The corollary is that 'social capital' or experiential credentials could well become a reinforcement of oral credentials, and particularly relevant for employers in more rural contexts. Moreover, a driver with impeccable Uber credentials may be just as useful in a city context as in a rural context. Some interviewees opined that employers in cities are more likely to look for academic credentials as opposed to craft associations, artisans and those operating in informal economies. Within an 'Africa scenario', adult learning and literacy programs for young people and rural communities tend to be run by volunteers and NGOs working 'on the ground', as opposed to governments or academic or VET institutions. It is equally likely that these NGOs are not necessarily digitally-literate or immediately responsive to the affordances of technology.

3.3 Youth Unemployment and Credentials

This section explores the challenges of youth unemployment in Africa and how digital credentials may help address some of the issues.

Africa has more people aged below 25 years old than anywhere in the world. According to a recent World Bank report, about 20% of Africa's population is between 15 and 24, and in Sub-Saharan Africa, about 67% of the population is under the age of 25. It is also estimated by United Nation's International Labour Organization (ILO) that by 2030, 42% if the world's population between 15 and 24 will be African and by 2100, 50% of the world youth will be African according to Africa Ahead. Currently, the Youth unemployment rate in Africa is around 12%, and on the increase, with young people accounting for 60% of all Africans unemployed. According to African Centre for Economic Transformation, half of the nearly 10M yearly graduates are unable to find gainful employment. There are high disparities from one country to another, but the numbers are staggering.

There are several, well-documented factors that contribute to youth unemployment in Africa: skills mismatch, inadequate entrepreneurship training, corruption and fraud, lack of access to capital, digital divide, and a lack of stable quality job opportunities are some examples that are frequently cited. Skills mismatch seems to be a salient factor within the context of this study: there are obvious gaps between the skills young people acquire and the jobs that are available in the market. For instance, most job opportunities are currently found in agriculture or in the informal sector or even in apprenticeships such as plumbing, carpentering, electrical repairing: these are areas that do not traditionally attract young people; these skills are also not acquired traditional, one size fits all, monolithic, formal education systems.

The majority of interviewees believe that there is a need for a paradigm shift from traditional education systems with achievement at higher education as the contributory factor to secure employment towards a valorisation of the lifelong learning journey, within which a variety of stakeholders (including NGOs, private sector training institutions, TVET centres and others) may contribute to the learning pathway of the individual. In today's scenario, this remains a radical proposition, a repositioning from institutional learning to ecosystem-based learning. One innovation in the education sector could be to involve the private sector in curricula development (including technical vocational education), as suggested by the World Economic Forum's 2016 ''Action Agenda for Africa's Competitiveness'' so as to ensure that the skills acquired by young people correspond to the reality and needs of the labour market. A university degree may not necessarily lead to the employment of a young person seeking to work in tourism; training in customer service, food preparation or transportation services might be. Acquiring these skills is a necessity; being able to demonstrate and leverage these to gainful employment remains challenging.

We need to distinguish between urban areas and rural areas, as the economic fabric differs considerably and the type of credentials that would be pertinent to capture as well. In urban areas, it is likely that social credential platforms like LinkedIn that provide professional references and confirm one's employment experience or platforms like Uber might carry more weight with employers. In rural areas, any private sector organization or community platform or any NGO delivering vocational training that is relevant to the needs in that rural community will provide useful validation of the skills that have been acquired by learners and allowing these organizations to contribute to the track record of the learner will be immensely valuable. It is expected that by 2050, 50% of Africa youth will live in rural areas where agriculture is predominant, which in turn means that focusing on agriculture as a potential employer is key.

This is where technology-based credentials can start to mitigate youth unemployment: by supporting a digital credentialing system that is more inclusive, reaches beyond the traditional academic sector, and allows for a greater diversity of stakeholders to contribute in a trusted manner to the learning records, the Foundation can contribute to recognition of a wider range and typology of qualifications, that are in turn more in line with the skills required by the labour market.

To illustrate the type of new stakeholders that could be engaged in this process, and recognise their specific needs:

- Sarah joined a work-based learning programme supported by an NGO during which she was trained in the technique of using a certain type of non-harmful, non-chemical pesticide in a specific agricultural value chain. She now seeks employment in a different value chain and needs to demonstrate that the skills that she has acquired in her current role can be applied in different context. One way to do that would be to produce a letter from the NGO that confirms and validates the training that she has received. To this, she could add a letter from her employer. These would take time to obtain and could possibly be questioned by receiving parties. If Sarah goes to another potential employer, she would need to produce the same documents and repeat the same

validation cycle. A tech-enabled credential platform in which participating parties can trust the content of the database would solve that issue and allow Sarah to freely apply to multiple jobs and produce proof of her achievements and skills.

— John is seeking employment in a transportation company in the capital city and is relying on his ability to demonstrate his quality (as attested by his rating) as an Uber driver to find a job. In that particular case, the Uber rating as produced directly from the Uber app would likely bear more weight than any written recommendation. Similarly, the ability to display trusted references, whether from a social recommendation platform such as LinkedIn or directly obtained from the referees, will add more efficiency to the process.

1. **Different industries will most likely look for different qualifications and thus give weight to different types of skills when assessing individuals for a potential job.** It would therefore be sensible to first identify industries that are generating massive employment for youth and then contextualize the digitization of credentials in the specific context of these industries in order to maximize impact. Such an approach would also likely be favoured by Governments, whose priorities it is to generate more job opportunities.
2. **The distinction between rural and urban contexts is important**, as there are likely already established social practices that impact both the inherent value and technical quality of the credentials that are in use.
3. **Technology-enabled credentials need to recognize these social norms if they are to provide additional benefits to the current state of play.** They must contribute both to matters of relevance (the right skills, for the right market opportunity) and efficiency (time, cost, effort). Efficiency is an inherent quality of well-designed digital platforms. Relevance will be a function of localization and contextualization of the approach, which will involve the build-out of a rich ecosystem of local contributors.

3.4 Technology-enabled Credentials for Youth Unemployment

Within the context of this study, **technology-enabled credentials are synonymous with blockchain credentials: automatically-verifiable, secure credentials notarized on the blockchain that are immutable and as a direct consequence prevent fraud[5], lead to self-sovereignty, and solve a number of issues relating to identity, trust, transparency and provenance and disintermediation.**

Blockchain credentials are tamper-proof, revocable, user-held and independently-verifiable. Any institution can issue a digital credential (in any format) to a learner and register the hash of that credential on a blockchain. The learner can hold the credential themselves on their own device or in an online wallet. Any person wishing to check the authenticity can simply compare the hash of the document against the entry on the chain.

(5) The blockchain is used to cryptographically seal a record of the credential when it is created so that third parties can be absolutely certain that a record has not been altered since being issued. Once a credential is recorded on the blockchain it cannot be altered, faked or spoofed. The credential information provided is used to create a series of numbers (a hash) that represent that information, which is notarized and stored on the blockchain. Whenever someone goes to verify a credential the stored series of numbers are checked against what the credential information it generates today to ensure they are the same. No private or personal information is stored on the Blockchain – just the series of numbers mathematically derived from the credential information which is in turn used to verify that the content displayed matches the original record.

3.4.1 Technology infrastructure is not a barrier to the deployment of tech-enabled credentials in Africa

The digitization of the economy and society promises to bring dividends, spur innovation, generate efficiencies and improve the quality of services to a wide range of sustainable areas, including agriculture, education, health, infrastructure and the environment (World Bank, 2016). At the same time, digitization raises important policy challenges, including privacy, security, consumer protection, competition, taxation, new skills, cross-border and international delivery of education and training, and new forms of credentialing (Chakroun & Keevy, 2018).

The first hurdle to overcome when considering technology-enabled credentials in the Africa context is the 'readiness' of the technology infrastructure in target countries.

Internet and mobile infrastructure are developing rapidly in sub-Saharan Africa. By 2020, half of the population will have a mobile connection and there will be 500 million smartphones, with most people accessing the internet via their mobile phone at acceptable speeds. Most countries are also rolling out biometric ID systems that will establish a robust baseline for identity verification.

Annex 3 in this study provides a review of infrastructure readiness in the four target countries for this study.

Table 2 below summarizes how the proposed pilot countries compare in terms of their readiness:

	Kenya	**South Africa**	**Rwanda**	**Ghana**
Population	50m	57m	13m	29m
Mobile penetration (unique mobile subscribers as % of population)	56%	67%	51%*	67%
*GSMA mobile connectivity score***	48.44	62.87	43.05	50.69
Access to Internet (internet users as % of population)	86%	54%	30%	35%
Via mobile (as % of internet users)	92%	94%	90%	91%
Breadth of national Blockchain initiatives	Broad	Focused	Broad	Focused
Thriving blockchain tech scene	Yes	Yes	Yes	Yes
Robustness of National ID System	Good	Good	Very good	Good
Proposed Priority Level	**1**	**1**	**3**	**2**

Table 2: Snapshot of Infrastructure Readiness in Target Countries

* Estimate

** Average of mobile infrastructure score, affordability of devices and services score, and consumer readiness score based on GSMA analysis

On the basis of this analysis, **we do not see any significant infrastructure barriers in any of the four target countries to prevent the Mastercard Foundation from considering projects involving technology-enabled credentials.**

When is a Credential high-quality enough to help with unemployment?

When recruiting, the majority of employers conduct some testing procedures to ascertain the knowledge, skills and experience of potential recruits. Thus, with the exception of regulatory barriers for protected professions, a lack of credentials is only a barrier to employment if the employer considers the cost of verifying a person's knowledge, skills and experience too high to be economically feasible.

Thus, for a tech-enabled credential to have sufficient quality to help its holder gain employment, *it would need to:*

- Describe the qualities of the holder which are of **relevance and interest to the employer**, and
- Be **cheaper to verify in terms of the authenticity of the credential and its claims** than for employers to conduct their own test.

The following section discusses how educational credential technologies can improve the chances for young African people to secure meaningful employment.

3.4.2 Stackable Credentials for Employment Pathways

According to the World Economic Forum, employers across Africa identify inadequately skilled workforces as a major constraint to their businesses, including 41% of all firms in Tanzania, 30% in Kenya, 9% in South Africa and 6% in Nigeria. This pattern is forecast to get worse in the future: in South Africa alone, 39% of core skills required across occupations will be wholly different by 2020. Currently trending professions on the continent include the creative industries, food technologists, 3D designers, data centre workers and care, education and health workers. Many of these jobs are becoming increasingly dependent on the use of digital technologies (World Economic Forum, 2017).

Creating a pipeline for future jobs requires systems which will allow for lifelong acquisition of skills, particularly in STEM subjects, and which allow for persons to combine customised combinations of skills, to meet emerging job needs.

Technology can enable credentials to be more **stackable**, **transparent** and **transferable**. Therefore, their promotion could help youth unemployment by allowing for:

- The definition of jobs in terms of discrete skills which need to be obtained, thus allowing persons to understand what life and educational experiences they need to obtain to access these jobs;
- Young people to combine a mixture of credentials from different formal and non-formal sources, thus building up evidence of suitability for a job even if such suitability comes from a non-traditional pathway.

3.4.3 Facilitating the sharing of Job Experience

In Africa, where many people are employed in the informal economy, interviewees pointed to the need to move away from an over-emphasis on formal diplomas and qualifications and towards an emphasis on skills development, and the corresponding need to facilitate recognition.

Levering on Yang (2015), such a new paradigm includes the shifts from:

- A centralised and state-controlled system to a decentralised, regulated, coordinated and partnership-based system;
- A formal educational system to a system integrating the diversity of formal, non-formal and informal pathways;
- School-based training to skills development pathways based on apprenticeships which may have been acquired formally or non-formally in the community;
- A knowledge-based national certification framework to a framework which recognises and validates all types of skills and work experiences.

While some argue that such a shift also entails a movement away from diplomas and certificates, it can also be argued that one of the many barriers to shifting towards such a paradigm is in establishing a trusted system to describe skills.

Tech-enabled credentials can help guarantee the **identity of the issuer**, as well as allow for credentials to be **self-verifiable** and **collectable** by the issuer. Thus, by allowing young persons to obtain credentials that have comparable quality to formal diplomas, despite coming from different educational pathways, young people would be able to make their learning more visible to potential employers.

Additionally, tech-enabled credentials would allow for much of the verification conducted by employers to become automated, increasing the likelihood that they would accept such credentials.

3.4.4 Improving Mobility

According to the African Union, international migrants in Africa increased from nearly 13.2 million in 2008 to about 15.9 million in 2014. International migrants tend to face additional challenges to finding meaningful employment, including different languages, cultures, employment markets and qualification standards. Employment rates of international migrants range from 39% in Nigeria to 82% in Ghana.

Within this scenario of increased mobility from one African country to another, credentials remain important – not just for a job search but also to meet the requirement of nation-state accreditation systems before the granting of work permits, residence permits etc. The administrative implications for governments and quality assurance organisations are significant. The recognition and validation of TVET credentials as opposed to standard academic credentials is challenging, not least because TVET and apprenticeship systems are very different to those prevalent in HE. The recognition of work-based learning and skills acquired via non-formal and informal learning routes is similarly complex.

In transnational contexts, it is common for the party using the credential to verify job-seeker skills to have difficulty in understanding the value of a credential secured from a third country, particularly when it comes to establishing parity with credential norms in the recipient country.

In this context, it is prudent to assume that the deployment of technology and tech-enabled credentials can help improve the **transparency, traceability** and **recognisability** of the claims made by employment seekers. Specifically, tech-enabled credentials might be:

- Automatically translated or issued in multiple languages;
- Linked to the underlying standards which governed their issue;
- Linked to underlying supporting documentation explaining how they awarded.

3.4.5 Improving Resilience to Political and Social Upheaval

Multiple sources including the Word Bank and United Nations contend that Africa has for decades seen the highest number of conflicts of any region[6]. Conflicts often lead to mass displacement of persons, destruction of infrastructure and records, and re-organization of governmental systems and borders.

In such environments, it is extremely difficult to ensure the longevity of databases of credentials, or of physical credentials issued to users. Without these documents it is often impossible for a person to access certain parts of the labour market without having their experience reconstructed in a time-consuming forensic process, or without them having to redo exams or parts of their education (Loo, 2016).

Tech-enabled credentials offer the promise of **immutability**, that is, indestructible digital credentials, which can be accessed from anywhere (i.e. not carried on one's person), which can even survive major disasters and conflicts. Here, the potential of the blockchain as an enabling technology is significant.

3.4.6 Reducing Fraud

There are several primary types of international credentials fraud. First is the tampering or fabrication of documents from legitimate institutions. Another is of the diploma mill variety, passing off diplomas or transcripts purchased from bogus institutions. A close variant is representing as 'educationally significant credentials' summer or semester programs that are little more than vacations (Tobenkin, 2011). While it is hard to come by exact statistics on credential fraud in Africa, interviews with all stakeholders, as well as ancillary evidence from news-reports indicate that it is widespread.

In cases of wide-spread credential fraud, it is not unusual for employers to block applications from entire regions, institutions or classes of credential, due to the difficulty and resources required to determine their authenticity.

Technology-enabled credentials can be **immutable, traceable, self-sovereign** and **allow for the verification of the identity of the issuer.** This addresses the issue of fraud from two perspectives:

- Institutions issuing credentials can be audited and accredited, and then issued credentials evidencing such accreditation, thus combating the problem of fake institutions. Furthermore, public databases of accredited institutions backed up by these credentials can aid in the transparency of such processes;

- Credentials issued from legitimate institutions can be rendered **tamper-proof** through the application of technologies such as the blockchain to ensure to employers that the credential presented was actually the one issued.

3.4.7 Increasing Transparency

HR management is traditionally based on three key principles: merit-based recruitment and promotion; tenure of employment to protect the independence of public servants from undue political influence; and a standardised framework of pay and conditions (World Bank, 2013). Corruption can affect all aspects of HR management processes, with favouritism and nepotism and abuse of authority in areas of recruitment, training, promotion and transfer identified as major risk areas. This is rendered possible by

(6) Sources include: https://www.un.org/pga/70/wp-content/uploads/sites/10/2016/01/Conflict-and-violence-in-the-21st-century-Current-trends-as-observed-in-empirical-research-and-statistics-Mr.-Alexandre-Marc-Chief-Specialist-Fragility-Conflict-and-Violence-World-Bank-Group.pdf; and http://siteresources.worldbank.org/EXTCPR/Resources/407739-1267651559887/Violent_Conflict_Dataset_combined.pdf

unchecked discretionary power, lack of integrity, accountability, checks and balances and transparency in the overall administration of HR services.

In many countries, corruption and nepotism severely limit the job-prospects of young people who do not have access to social capital which may be transformed into contacts etc. For example, studies in Ghana show that 80% of bank sector employees interviewed obtained their employment through personal contacts and networks as opposed to some basis of merit (Nyukorong, 2014).

Tech-enabled credentials are easily **shareable** and easily **recognisable** in particular by computer systems. While, they cannot completely reduce fraud and nepotism, automatic screening of credentials by software, using transparent auditable methods can significantly reduce corruption in recruitment processes, and thus improve access chances of certain groups.

3.4.8 Improving Discoverability

According to the majority of our interviewees, despite the overt excess supply over demand, employers across Africa still have trouble finding the right talent to fill jobs. Tech-enabled credentials are easy to **share**, in particular on profile sites such as LinkedIn or via e-portfolio platforms. Giving young people the chance to publicly share job-experience, academic accomplishments, skills and recommendations from others gives them a way to be discovered directly by recruiters and connect to job opportunities they might not otherwise have been aware.

3.5 Strategic Considerations for Foundation in potential engagement with Technology-enabled Credentials & Youth Employment

The lack of jobs and long-term employment for African youth over-rides the discourse on credentials and technology. Despite the many physical and economic challenges and a lack of skills credentials, people continue to move across borders in search of gainful employment: youth labour market supply inevitably exceeds demand in Africa.

NEVERTHELESS, WE BELIEVE THAT THIS IS THE RIGHT TIME FOR THE FOUNDATION TO CONSIDER PARTICIPATING IN THE TECHNOLOGY-ENABLED CREDENTIALS SECTOR AS A MEANS OF EMPOWERING YOUNG PEOPLE:

- **Digitizing, securing and validating credentials are vital processes in a citizen's lifelong learning journey**, and particularly in ensuring that academic, TVET, professional, informal and non-formal learning credentials can be recognized, secured, stored and shared by the learner, without the need to rely on intermediaries, including the issuing institution.

- **Blockchain technology is already in a state of maturity to be deployed in high-profile credentials projects around the world**[7]. The Foundation has ready access to the lessons learnt and the opportunities identified in these cases, and specifically the know-how an eco-system of policy-makers, government officials, technology suppliers, consultants and funding bodies associated with these projects.

- **Platforms that support technology-enabled credentials can be rapidly scaled up**. Examples from Kenya and UNCDF already provide a reward-based system for

(7) See Grech and Camilleri (2017)

learners to select apprenticeships and trainings that will result in higher chances of getting a job, match job seekers and employers based on keyword searches in the credential database etc.) These existing programmes could be impacted extremely positively through the digitization of credentials.

— Government, Education Institutions, Learners and Employers are the constituted stakeholders in the tech-enabled credential space: in practice, these **stakeholder groupings will need to be deconstructed down to individual actor level if the Foundation is to make any headway with pioneering technology-enabled credential projects in Africa.** However, through its high-profile pioneering work in the region, its existing relationships and its proprietary networks, we believe that the Foundation is already in an excellent position to identify key people who can overtly or proactively support pilots in the region, if these projects can demonstrate tangible benefits to young people.

— We believe that **strategic communications campaigns** will be essential to inform, 'educate' and engage target stakeholders and decision-makers in target markets. These initiatives may be both formal and interpersonal. Campaigns around key positive impact of technology-enabled credentials could include: the empowerment of young learners through self-sovereign, secure blockchain credentials; how these can quickly become the 'norm' for the recognition of skills secured by young people in Africa; how the mass take-up of mobile technologies and related infrastructure has already paved the way for uptake by target users; how blockchain credentials can help solve perennial institution issues with credentials' tampering and fraud etc.

— **Key people in the Ministries for Education (and some other ministries) in target countries can 'make or break' any future inroad into technology, and particularly in starting meaningful discussions on the blockchain.** And if the vision is to build a broader platform around e-learning and tokenized models, then the Central Bank will probably play a key role as well. There is a broader government movement around electronic identity to get all IDs related to government services under a single identity management system (taxes, pensions, voter registration etc.). There are already many blockchain initiatives in payments, land registry, identity, movable property transfers etc. From our experience, we suggest that while education is not necessarily at the top of African government priorities list, policy-makers and other decision-makers quickly understand the practicality of engaging with technology-enabled credentials once the value-added to stakeholders is communicated clearly.

— **Distributed Ledger Technologies (DLT) and disintermediation may not necessarily be welcomed by all jurisdictions in Africa.** Much will depend on particular nation-state agendas: for instance, we were advised that the relatively recent changes in the political landscape in South Africa mean that the new regime would be very receptive to the fundamental principles of tech-enabled credentials, including their social value proposition.

— **Widespread adoption of any records-based system requires standards, agreements and regulatory frameworks as well as systems for interoperability.** While various forms of student qualification data, especially in tertiary education have been somewhat harmonised and standardised in regions such as Europe over the years, in the case of Africa, there are reams of other data which still have no common format or standard. At lower levels of education, not even school leaving certificates have yet to be harmonised or standardised.

— **When it comes to discussions about blockchain, there are trade-offs between open and closed standards, but data portability and operability and minimum lock-in with suppliers is desirable**. The Foundation's strategy implies that we want young people to be able to take and verify their data anywhere in the world, by any

system – in which case open standards are a must. The discussion on which data needs to be portable and where it should be stored would need discussion with stakeholders in key target countries.

— We suggest that **the Foundation should 'start small'**: to find a set of use cases with willing institutions and lever on tech-enabled credentials to solve the challenges of the use case, create a demonstration effect and then rapidly scale.

The next section provides more detail on the rationale for these strategic considerations.

4 Supplementary Findings

This section includes **supplementary findings** that may impact the Foundation's decision to engage or otherwise in projects relating to tech-enabled credentials in Africa, and specifically to the blockchain.

The findings are tabulated below as four, inter-connected themes: *Governance; Technology & Infrastructure; Education & Credentials* and *Blockchain*.

GOVERNANCE	
1. **Governments are expected to lead, sponsor and facilitate innovation in the tech-enabled credentials sector**	— There is a consensus among all interviewees that Government will need to be engaged early on by the Mastercard Foundation if it wishes to make an impact with tech-enabled credentials. Indeed, Government is involved in many aspects of credentialing - from identity management to the accreditation and recognition of learning institutions. — Moreover, the emergence of the blockchain as a disruptive technology provides an unprecedented opportunity to leapfrog embedded / legacy technologies in target countries, and address a number of socio-economic issues in addition to the creation of jobs. Unsurprisingly, many governments in Africa are looking closely at blockchain applications as 'likely to impact future national strategies'. Some have already established Task Forces to drive national blockchain experiments.
2. **Regulation still has to catch up with decentralized technologies**	— Target countries are paying attention to credentials policies and qualification systems but there is a mismatch between policy attention and the implementation of workable regulatory measures. While the South African Qualifications Authority is running a verification network for credentials in the country as a means of reforming the entire certification system, others are much slower in reforming their qualification systems. — There is a consensus among public officers that credentials are a reference for the recruitment of young people who are trying to enter the job market; and that there is a need to redefine those skills and learning outcomes that merit credentialing and hence 'recognition' by stakeholders in the labour market. — South Africa's Qualifications Authority is running a verification network of credentials. In southern regions, the data on qualification frameworks indicates that the regional framework is not operating. There is the intention at policy levels to implement drastic changes, but these are often associated with the need to secure funding: there is a gap between central directions and expectations and actual implementation. — As far as regulation of the blockchain and crypto space are concerned, regulators tend to make a useful distinction

	between blockchain as a technology and cryptocurrencies as an underlying asset. — Some regulators (such as those in South Africa) have adopted an open position to provide a clear signal that there is no intention to shut down or discourage innovation before understanding the emerging technology landscape better. Regulators in Kenya, Ghana and Rwanda are taking an equally progressive approach. However, a deeper understanding of cryptocurrencies and blockchain as the enabling technology is still required in many key government positions to ensure adequate regulation of that space.
3. **Large elements of the credential ecosystem are ungoverned and unregulated**	— Private certifications, as well as education offered by NGOs, foreign governments and inter-governmental organizations are commonplace across the continent. These typically operate with little supervision or regulation from governments. — Many of these systems use a 'charter model' of educational provision, with several levels of decentralization between the designers of curricula and tests, and those actual administering these curricula and tests. Therefore, there is often very little visibility as to who specifically stands behind many of these credentials. — Several platforms which offer credentials, in particular various forms of social recommendation and gig-economy platforms, effectively lock users into the platforms, and offer little to no value to users outside the walls of the platform. They rarely interact or connect with wider credential ecosystems. Yet it is inevitable that they are trusted and valued within specific contexts in Africa, and the Foundation should investigate opportunities for partnering up with high-profile platforms should the opportunity arise.
TECHNOLOGY & INFRASTRUCTURE	
4. **Most target countries have technology which is ready for tech-enabled credentials**	— Despite concerns that many young people in African countries do not possess a smart phone[8], this does not appear to be the case in the target countries. In fact, the number of smartphones in Sub-Saharan Africa is on the rise and is expected to reach 500 million by 2020. In the target countries, mobile penetration exceeds 50% and internet penetration is in excess of 30%, with most internet users already accessing 3G broadband services via their mobile phones. African consumers are definitely getting ready to participate in the digital economy.
5. **Blockchain applications for education are still in their infancy**	— Currently, the implementations of blockchain technology for education tend to be in pilot stages, although some are moving rapidly to become components of small nation-state systems. Several organizations are in the initial

(8) See Education in Africa 2010, Global Education & Skills Forum (2018) – video accessible at: https://www.youtube.com/watch?v=HkNZbZ7psOM

	stages of pilot-testing award of certificates using a blockchain, while others are accepting blockchain-based cryptocurrency payments. — There continues to be a widening gap between the claims being made about potential distributed ledger technology applications and the actual roll-out of such applications. Anecdotal evidence suggests that a growing number of organizations are 'looking down the wrong end of the telescope' with blockchain technology: instead of bringing their problems to the table and assessing whether blockchain technology might provide solutions, they are bringing blockchain technology to the table and looking for problems to which the technology might be applied. — While the majority of attention is currently directed at Fintech as opposed to education, trust in blockchain technology will migrate from finance to education. Large players will eventually inevitably shift their attention to the opportunities to re-energize and repurpose education. The implications and applications of trying to outsource trust to technology cannot be accurately forecast and may well entail complications and side-effects that we can't currently envisage (Collins, 2017). — The indicators are that most industries and their business models will be impacted by this technology, in the same way as they were impacted and disrupted by the Internet. Industry insiders are talking in three- to five-year increments but blockchain technology implementation may well be a decades-long experiment. — Among the envisaged pilot markets, the only one known to have already had in-depth thinking around the use of blockchain for education is Kenya[9]. There are plans for the publication of a blockchain roadmap this year[10] with concrete proposals which are likely to include the use of blockchain in the education sector. It would be expected that credentials would be high on a priority wish list.
6. **Innovation needs legal and regulatory clarification**	— Africa may not yet have its version of the GDPR, but it is clear that decentralized technologies pose a significant challenge to existing laws and regulations, particularly in the area of data protection. Compliance with African versions of the GDPR will require a specific design and implementation. — In the current GDPR scenario in Europe, most actors seek to build something that is compliant, but they don't know what that means, and their lawyers, when they can afford them, don't know either. Blockchain and GDPR pursue common general goals of users' control on their privacy, data control and security for citizens - and blockchain is

(9) See: http://techtrendske.co.ke/4-organizations-spearheading-blockchain-education-in-kenya/ and https://bitcoinmagazine.com/articles/kenyas-government-task-force-explore-blockchains-land-and-education/

(10) See: https://www.businessdailyafrica.com/corporate/tech/Ndemo-taskforce-Kenya-blockchain-roadmap-ICT/4258474-4323074-gjwgqnz/index.html

	currently the safest and best available way to reach these goals. But the way GPDR requires these goals to be reached make it very difficult for blockchain to comply with these requirements at the moment.
EDUCATION & CREDENTIALS	
7. **Interoperability between national and global credential systems is weak**	— To date, there has not been an efficient national or global system to collect, connect, search and compare up-to-date information about learning outcomes and credentials in a common language or format that can be universally understood and easily accessed. — In Africa, this situation is exacerbated: the lack of information and systems contribute to confusion, lack of trust and uninformed decision-making regarding the recognition of skills and qualifications within and across borders. It also leads to talent loss for economies and employers.
8. **Academic credentials remain the most-valued credentials for both African youth and the first point of reference for employers. Yet much depends on the particular context.**	— The academic certificate remains the recognised social currency in target countries and University degrees remain the 'gold standard' in terms of credentials. The reason for this is that they have a high technical as well as inherent quality (see *Annex 2*). — VET and TVET credentials from reputable colleges are becoming increasingly important for the labour market. There is also likely to be less 'political resistance' to considering alternatives to the traditional paper-based credentialing model in place in the majority of higher education institutions. — Credentials for professional / specialized training (such as PMP and 6Sigma) from reputable centres are also gaining currency. There are also on the job trainings and work-based learning that may translate into some kind of credential (such as Nestle training people on certain machinery, or a type of chemical-free pesticide, or on how to grow organic cocoa). — Social credentials are only currently considered to provide an additional level of 'trust'; interviewees do not believe they will replace academic or VET credentials earned the hard way. However, in the case of jobs in specific sectors or in specific areas – such as in rural areas with agriculture as the predominant employment sector – tech-enabled social credentials are perceived to add a level of comfort to prospective employers.
9. **Tech-enabled credentials must address and mitigate existing problems for issuing institutions,**	— Credentials fraud and corruption are widespread in the region. Existing, sophisticated credential scams may also infiltrate digital solutions. A tech-enabled credential system is still likely to require robust control mechanisms to detect and prevent fraud at the point of contribution. — Loss of certificates remains a problem. Many young people store their credentials as a PDF on their laptop and end up

governments and employers	losing the file and having to pay the institution for re-issuing a certificate. — For trust in technologies, projects must help both employers and aspiring employees have faith in a credential, and specifically in the trustworthiness of the underlying data, without the additional need to seek a third-party letter of reference. — Issues like certification, the interoperability of systems and the ubiquity of standards have to be addressed, including concerns about the certification of work-based learning and for skills such as those needed for jobs in agriculture, which are not normally associated with 'credentials' and formal pathways – let alone tech-enabled credentials. The notarization of TVET and professional credentials and work-based learning on the blockchain can contribute to making them more mainstream and hence acceptable to the labour market.
10. **Interoperability for TVET systems is hard to achieve, although very desirable**	— The academic education pathway is more understandable than the landscape for lifelong learning certification in target countries. There are issues around quality, readability and transparency that challenge the basic premise of interoperability. — What has worked for academic education must now start to work for TVET and informal and non-formal - there has to be more traction here for blockchain. — People who are in traditional apprenticeships will have less understanding than those in TVET - their supervisor may be known, so the certificate may be less important.
11. **The full benefits of blockchain technology and credentials are only achieved through open implementations**[11]	— Only 'fully-open' blockchain implementations can reach the real goals and promise of blockchain in education (see below). By this, we mean solutions for credentials whose fundamental components include: **a) recipient ownership;** **b) vendor independence** and **c) decentralised verification.** — If those aren't all being achieved, using a blockchain is likely to be a waste of effort and resources for the Foundation at this juncture. — Much will also depend on the value that education institutions, governments or even learners (the target users) will attribute to the basic tenets of 'openness', 'vendor independence' and 'learner empowerment' - particularly those related to the value learners will attribute to owning their own digital certificates, as opposed to being perpetually locked in with (albeit trusted) institutions or vendors.

(11) As a yardstick, open solutions tend to be associated with the following: open source; open access; open to innovation (at the edge, not the centre); open security; permissionless; decentralized; uncensored; nobody in control; individual privacy; no patents (which prevent participation); self-sovereign by design; vendor-independent; portable; public good; and future-proof.

	— Although in principle these are very powerful arguments, it is too early to determine whether these are more compelling for target users than, say, proprietary solutions being developed by global brands.
BLOCKCHAIN AND EDUCATION[12]	
12. **Blockchain will likely disrupt the market in student information systems**	— Blockchain technology has significant use cases beyond crypto currencies, whose use cases are beginning to enter the mainstream. Blockchain-based ledgers have the potential to disrupt the key technology that underpins an industry currently worth $2.7 billion[13], and as such will likely disrupt the market as a whole, including that for student information systems. Established companies and start-ups are already seeking to secure early-mover advantage of this space. — Since significant network effects will be achieved through scale, it is likely that within the next few years a handful of powerful technology vendors will gain a foothold over the entire industry.
13. **Vested interests have an interest in locking down blockchain technology and creating standards based around partial implementations.**	— Implementation of the blockchain offers a significant social value proposition. These benefits result directly from the removal of key ledgers from the control of single authorities. — Organizations and companies that have built (or are planning to build) solutions and business models around controlling these ledgers, have a vested interest in resisting implementation. Since they cannot roll back the invention of blockchain technology, many of them are creating 'partial' and hybrid implementations which allow them to retain control of the ledgers, while still offering other advantages of the technology such as cost savings. — Despite the hype, the mention of blockchain technology does not automatically imply a universal trust protocol - it often implies exactly the opposite. To transact anything of value other than tokenisable assets via a blockchain requires additional layers of agents, third parties and auditors – things that just don't square with the trust-free architecture. — Within education, the first implementations are related to a flurry of companies offering to issue certificates linked to a blockchain, but only allowing access to the content of those certificates through proprietary, closed platforms – effectively using the promise of an open system as a foil to creating a closed system.

(12) The conclusions from this point onwards summarise some aspects of developments with blockchain technology that has an impact on education, and tech-enabled credentials in particular. It is primarily based on Grech and Camilleri (2017) and should be read in conjunction with *Annex 4*.

(13) According to Technavio (2017), the Student Information System market is likely to grow to $5.7 billion by 2021.

14. **Public private partnerships are necessary to fully exploit blockchain**	— The interests of the market and the public are not always in alignment when it comes to deployment and application of blockchain technologies in education. Such a situation is usually a textbook case for market regulation. — On the other hand, due to the fact that blockchain technology is so new, and that the potential of the technology is just being discovered, governments should not at the moment 'pick winners' or lock down the technology with excessive regulation. — In Africa, there are already a number of private and public sector actors (tech providers, employers, NGOs focusing on youth employment, government insiders and public servants) that have an interest in promoting blockchain implementations. The only possible model to achieve the full potential of the blockchain in the short term is through a balanced, constructive system of strategic public private partnerships.
15. **Blockchain technology will accelerate the end of a paper-based system for certificates**	— The adoption of digital certificates has been held back by the ease with which they may be forged. The blockchain provides a way for organizations to issue immutable digital certificates which are valid in perpetuity, since their authenticity can be verified against the blockchain. Where certificates are transferred as tokens on a blockchain, even the certificates themselves can be made available in perpetuity. — These advantages over traditional digital certificate systems significantly increase the value proposition of digital certificates and will likely push digital certification into the mainstream.
16. **Blockchain technology removes the need for educational organizations to validate credentials**	— Since certificates issued on the blockchain can be automatically verified, educational organizations will no longer need to commit resources to this task, significantly reducing their administrative load, and practically eliminating the 'after-sales support' they need to provide to learners following the end of courses[14]. However, since many Organizations also offer this service at a profit, it may also mean that institutions will need to adapt their business models accordingly.
17. **Blockchain has the potential to release a wave of innovation around learners' data**	— Learners' data is a critical component of many applications including human resource management systems, e-portfolios and professional social networks. Blockchain technology allows all these systems to automatically validate certificates from any issuer in any (metadata) format.

([14]) Institutions would still have a role in re-issuing certificates if they were lost by the user, or revoking them, e.g. if they were late found to have been obtained by cheating.

	— This ability to store verified claims rather than mere claims, should significantly enhance the usefulness of such systems to their various stakeholders. — We may well imagine applications that: automatically verify CVs and shortlist candidates with appropriate qualifications; and other applications that would automatically place employees into a higher-earnings bracket based on evidence of completed training and professional networks that would use verified professional certificates as the requirement for subscription. — The blockchain may start to address gaps in the labour market by using learners' notarized skills data with the specific needs of employers, automatically recommending training that would result in higher chances of securing employment.
18. **Self-Sovereign Identities have the potential to significantly reduce educational organizations' data management costs**	— European law imposes significant obligations on organizations who act as custodians of personal data, obliging them to control who has access to it within an organization and to ensure its safe storage within the organization. The more people have access to the data, the more complex the management, the higher the costs and the higher the risks of a data breach or abuse. — Self-sovereign identities effectively create a secure identity card which can be held by a student, and which can be biometrically linked to them – allowing the student to identify themselves without actually handing over any data, and without the need to cross data with a database held by the institution. The institution will be able to identify the student without actually holding and retaining their data. — This significantly reduces the administrative overhead, as well as reducing the potential 'footprint' for a data breach or abuse.
19. **Blockchain technology enables much more sophisticated systems for reliably tracking usage of intellectual property**	— Blockchain technology has the potential to revolutionise the management of intellectual property. Depending on the policy choices made, it could be used to increase openness or to close intellectual property. — By publishing hashes of documents onto a blockchain, a person can provide proof of first publication without actually needing to share the document or invention being published. This turns conventional notions of copyright and patent law on their heads, allowing the possibility for a far more restrictive system whereby knowledge could be protected without being shared. — Blockchain technology also allows for detailed and incremental tracking of who has used intellectual property, where and how, and for these to be associated with credit – either in the form of payment or in the form of academic credit. Such systems for intellectual property could, for example, serve as the basis of future journals, or even as the basis for tracking the production

	and re-use of open educational resources. As such, they would be able to significantly incentivise the opening up of education and educational resources.
20. **Educational networks can automate and standardise many of their functions through decentralised autonomous networks**	— A Decentralised Autonomous Organization (DAO) is effectively a community, with its resources organised according to rules agreed in advance and set out in its code (Allen & Overy, 2016). As such, communities which exist for the purpose of creating and transferring those resources against set rules, are ideal candidates for being reimagined as DAOs. — It is foreseeable that decentralised education networks in Africa will eventually consider levering on DAO principles and technologies like the blockchain to operate. institutions. The application of DAOs may: (a) automatically ensure that such awarding of credit or certification always happens according to the same set of criteria in every implementation; (b) ensure that transfer and/or use of these certificates always occurs in accordance with the rules; (c) create a single unified database of awarded certificates; (d) share control of the system between members of the network, with no party having centralised control.
21. **Regulation and Standardisation will might determine the extent and speed of progress**	— Widespread adoption of any records-based system requires standards, agreements and regulatory frameworks as well as systems for interoperability. — While various forms of student qualification data, particularly in tertiary education, may be somewhat harmonised and standardised within a particular country, the notion of standardisation and harmonisation of credentials across African nation will be challenging because of a lack of common formats and standards: this will be particularly the case at lower levels of education, where school leaving certificates have yet to be harmonised or standardised. — Furthermore, the tools that may exist (such as diploma supplements or inter-government agreements) have not been designed with digital records in minds: essential tools do not follow a digital data format or digital metadata standard. — With its ability to store different kinds of records, as well as its ability to automatically establish consensus between parties without a central authority, blockchain can simplify the creation of such standards, but cannot be deployed in a truly pan-European sense without them. — There are trade-offs between open and closed standards, but data portability operability is essential. If we want people to be able to take and verify their data anywhere in the world, by any system, open standards are a must.

22. **Stakeholders are unaware on the social advantages and potential of blockchain technology**	— With practically daily news of major data breaches around the world, adopting digital technologies for record keeping has implied a social contract: increased efficiency and effectiveness at a price: less security, privacy and permanence. In the absence of a better option, many Africans have accepted to surrender their data and personal information to gain access to valuable services such as mobile money services or digital loans. — Properly implemented blockchain technology significantly improves all three of these criteria, allowing digital records to have far fewer unwanted side-effects. — However, educational organizations have little evidence available to prove that blockchain offers a significant value added, either to themselves or to their students. Understanding the potential of blockchain without examples of implementations to point to requires significant knowledge, specialisation and communication skills. — There are immediate opportunities in Kenya and South Africa to open a communication channel with between the Foundation and government authorities, including the blockchain task forces, to identify tangible pilots that can lead to visible net return for key stakeholders. The next section tabulates four concrete hypotheses for such pilots.

5 Key Recommendations

We believe that there are the right conditions for the Foundation to consider entering the tech-enabled credentials sector by supporting a set of high-profile pilots.

When deployed strategically through use cases, we believe that blockchain technology is likely to have a positive impact on credentialing in target sectors - particularly in TVET, informal and non-formal learning - and in the process empower African job-seekers and those who wish to employ them.

5.1 Preparing to engage with Target Stakeholders

Prima facie, the number of stakeholders to engage with on tech-enabled credentials wihtin a lifelong learning context are likely to be numerous, and very much dependent on the specific nation-state for the pilot(s). **Much will depend on the ability of the Foundation, its partners and advisors to activate existing human networks before considering technology and fast-track pilots.**

Different sets of stakeholders in the credentials sector typically have different needs:

- **Education and training providers** need learning data to build new programmes and learning pathways
- **Employers** need data to understand where to find qualified workers
- **Learners and workers** need data to discern which learning pathways are more likely to lead to career opportunities.

To illustrate, *Figure 5* is a cluster of stakeholders who would typically need to be engaged *if* the Foundation were to focus on policy actions in the implementation of tech-enabled credentials in Africa:

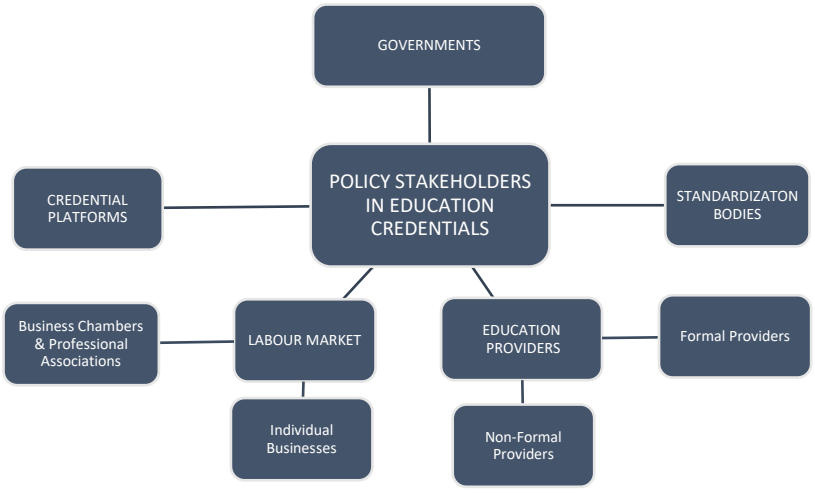


Figure 5: High-Level example of Policy Stakeholders cluster in a Tech-Enabled credentials pilot

To further illustrate - targeting each of these stakeholders comes with trade-offs:

Stakeholder	Impact	Propensity to consider Change
Governments	Systemic – impact due to legislation	Requires, political commitment, a multi-year campaign, typically from a network of stakeholders to generate action.
Standardization Bodies	Systemic – impact due to codifying best practice	Standards can be deployed in a 12-24-month period, and initiated by a multi-country network of stakeholders from industry and government.
Credential Platforms	Depends on reach of the platform	All online social credential platforms with significant reach (such as LinkedIn) are proprietary. The possibility of impacting the operations of these platforms is low, although they *may* adopt widely promoted standards, particularly if sanctioned by Governments or other regulatory bodies.
Businesses: Individual Businesses	Micro	It is not feasible to work with individual businesses on tech or standards for credentials. However, automated services deployed to large numbers of individual businesses for free may lead to the creation of *de facto* standards
Businesses: Business Chambers & Professional Associations	Meso	Actions conducted with these actors can lead to the adoption of practices across entire industry segments simultaneously. Feasibility is likely to depend on proving a value-case to the associations.
Educational Providers	Micro	It is not feasible to work with individual educational providers on tech or standards for credentials. However, automated services deployed to large numbers of individual businesses for free may lead to the creation of de facto standards

Table 3: Typical Stakeholder positioning on tech-enabled credential systems

Nevertheless, there is a sufficient number of 'live' blockchain and credentials use cases (including those that we are currently engaged with) that will provide the Foundation with the requisite know-how to ensure that pilots funded by the Foundation will be successful.

In the remainder of this section, we propose: a framework for action; five hypotheses for consderation by the Foundation as tech-enabled credentials pilots;and a high-level implementation plan.

5.2 Framework for Action

The route to improving youth employability through technology-enabled credentials involves actions that increase the supply of *high-quality* credentials to users.

We have identified **four levers for action** that can help credentials meet stakeholder expectations in terms of high-quality credentials, linked to the underlying features of those credentials:

1. **Accreditation:** this involves methods of guaranteeing the reputation of the issuer of the credentials.
2. **Capacity Building:** this includes investments in Training and Infrastructure
3. **Digitization of Credentials** (Tech-enabled Credentials, and the recognition of micro-credentials)
4. **Standardisation of Credentials**

We are assuming that the Foundation may **wish to engage with any or all of the four levers of action** in order to maximise the potential for positive change through the deployment of tech-enabled credentials in the African region. *Table 4* tabulates options to be considered for the Foundation's initial positioning with pilots:

1	**Work with government and/or industry associations to create accreditation systems for educational organizations, NGOs and businesses, where these do not already exist.**	— Activities related to aspects of a person's learning such that it is electronically documented, authenticated and accessed at any time, and anywhere, shared and amended by the owner or by an authorized body.
2	**Facilitate the creation and maintenance of directories of accredited actors based on public records.**	— 'Actors' may include directories of students, recruitment agencies, employers, professional associations, education and VET institutions etc. as may be required within the context of the target countries. — Tech-enabled credential systems can lead to lifelong learning registers in target countries that recognise informal, professional VET and TVET using blockhain to recognise, certify and verify once skills certification has taken place.
3	**Issue verifiable public-key certificates to all certificate issuers**	— These could include Government e-id schemes or 'Let's Encrypt' style schemes.

4	**Promote national initiatives for digitisation of credentials**	— These could include legislation that defines standards, facilitating interoperability and acceptance both within a nation state or among nation states; and the issuing and acceptance of digital credentials as government.
5	**Create incentives for national, interoperable credential platforms**	— This is a funding function, that could be based on competitive bids for practical solutions.
6	**Create free to use middleware for digital credentials**	— This could encompass both issue and use-cases for verification of credentials.
7	**Create new platforms for CVs and other learning credential collateral**	— Focus on digital credential displays.
8	**Create toolkits for educational institutions**	— Support institutions who do not offer credentials through design and backup credential schemes
9	**Lever on proprietary networks and trusted intermediaries to facilitate quick wins**	— These may include NGOs and social actors working on the ground, youth ambassadors, EdTech and credentials experts and government intermediaries. — NGOs in target countries can help in many ways: providing know-how, securing buy-in from key third parties (governments, institutions & labour market) supporting communication programs to disseminate the potential of tech-enabled credentials and celebrate short-term wins. — Through long-established advocacy norms, NGOs can identify credible partners in target stakeholder groups. Subject to funding, they will be able to provide the requisite resources on the ground to identify, launch, manage and monitor pilots. — Levering on use cases and the expertise of will be important in communicating strategically to key stakeholders such as governments and the labour market.

Table 4: Framework for Action with Tech-Enabled Credentials

5.3 Hypotheses for consideration by the Mastercard Foundation

We are proposing that the Foundation considers the following 5 hypotheses as pilots to be tested by the Mastercard Foundation.

The hypotheses rely on **three key applications of tech-enabled credentials: Education credentials; Accreditation of professional bodies; and Experiential credentials**

HYPOTHESIS 1: Use the existing Mastercard Scholars Program[15] whereby graduates secure immutable credentials which are notarized using the Blockcerts open standard	
Pilot	Lever on the existing Mastercard Scholars Program and use a Blockcerts-based provider to create a Mastercard Foundation digital certificate which is in turn notarized on the blockchain. This certificate is likely to be a new, additional certificate to the (paper-based) certificate issued by the partner institution. Clearly, this hypothesis is dependent on agreements with participating academic institutions in the Mastercard Scholars Program. There is no need for all the institutions to accept to join the pilot: if anything, starting with a handful of organizations will facilitate implementation and engagement with stakeholders. The first set of applications will then serve to attract other institutions to the pilot. The Foundation is in a strong position to control the various components of the pilot because of its existing relatonship with the issuing institutions and possibilities of including its own brand to the digital certification.
Application	Education Credentials
Country	Countries where participating institutions have a presence.
Sector	Academic
Scale	To be determined through exploratory discussions between the Foundation and its academic partners in the Mastercard Scholars Program.
Indicators of Effectiveness	Check employment outcomes 12 months after award.
Indicators of Efficiency	Number of certificates issued with Mastercard Foundation Logo, together with logos of participating university partners. Number of certificates downloaded by students on completion of the Program; activation of private keys etc.
Partners	Participating Universities; Blockcerts provider ready to implement solutions within reasonable timeframes (such as Learning Machine)
Timeframe	6 months to implement, 12 months of impact measurement.

(15) See http://mastercardfdn.org/all/scholars/

HYPOTHESIS 2: Facilitate the notarization of secure immutable TVET credentials	
Pilot	This pilot extends hypothesis 1 in its use of Blockcerts to secure educational credentials issued by TVET training centres and non-formal educational institutions. Award Blockcerts credentials to only half of graduates from the programmes selected in the non-formal sector.
Application	Education Credentials
Country	Kenya
Sector	Agriculture
Indicators of Effectiveness	Check employment outcomes 12 months after award, and compare the status of learners who were awarded Blockcerts credentials with those who were not awarded Blockcerts credentials.
Indicators of Efficiency	Monitor ease of issue with non-formal educational institutions Activation of private keys and number of certificates downloaded by students
Partners	TVET training centres; Blockcerts supplier; University developing on Blockcerts; NGOs like Save the Children; Kenya Blockchain Task Force
Timeframe	6 months to implement, 12 months of impact measurement

HYPOTHESIS 3: Develop verifiable professional certifications to improve employment outcomes for independent professionals	
Pilot	Work with a Professional Association to: (a) secure / notarize accreditation certificates; and (b) create a directory of trusted issuers of professional certificates. The pilot would facilitate verification of identity through a triangulation of sources and different definitions of 'truth'. Educational organizations, including non-formal organizations, would hold wallets of directly issued or reputational credentials. By sharing the wallet, they could prove accreditation, legal status or other aspects of identity. Since each credential is validated, trust in the institution is built gradually. It is possible to set up multi-level accreditation, whereby one institution accredits another, who in turn accredits another. Independent verifiers would apply KYC-tests to the wallets for different validation purposes. 50% of certificates issued to TVET graduates are given a link to accreditation data. All certificates issued to learners have a reference to the accreditation, enabling these to be verified as issued by an accredited organization.
Application	Accreditation of professional bodies
Country	Kenya, South Africa
Sector	TVET - particularly certified trades such as plumbing, electricians, skilled repairs and maintenance (automotive spray-painting etc.)
Scale	A Pilot with one network and all training organizations within the network
Indicators of Effectiveness	Check employment outcomes 12 months after award, and compare.
Indicators of Efficiency	Ease of use for professional networks Reduction in requests to confirm accreditation of members to professional association
Partners	Professional Accreditation bodies; Networks of training providers (e.g. ICT or for ISO standards); Professional network offering CPD; Corporate Training Providers
Timeframe	6 months to implement, 12 months of impact measurement

HYPOTHESIS 4: Recognise value of secured reference letters or ratings by notarizing these on the blockchain	
Pilot	Work with a set of employers or employment platforms to secure either (a) employer reference letters, (b) employer ratings or (c) client ratings/reviews on blockchain at end of employment period.
Application	Experiential Credentials
Country	South Africa
Sector	All gig-based sectors, taxis, construction industry etc.
Scale	Pilot with one employment agency and at least 150 employment references issued.
Indicators of Effectiveness	Compare set of persons who received certified-references vs. those who did not, and check employment outcomes 12 months after issue of certificates.
Indicators of Efficiency	Ease of use for (new) employers and job applicants
Partners	Employment agency working with a) large numbers of candidates & vacancies b) offering short-term positions; FMCG companies such as Nestle or MaRS etc
Timeframe	12 months to implement, 12 months to measure impact

HYPOTHESIS 5: Use blockchain to develop a Reputational System for Crowd-based endorsement and validation of Skills	
Pilot	Work with indorse.io or a similar service to create a crowd-sourced reputational system for the endorsement and validation of skills in a specific sector. Learners would request validation of a specific skill, which would trigger a request for evidence and a corresponding call for validators on the network. Learning is validated once a pre-determined score is received, with the learner's reputation increased with every endorsement. Learners would also be able to validate skill levels lower than their own in a peer review system. The system would include safety checks – for instance, validators not reaching consensus would be penalised.
Application	Experiential Credentials
Country	Kenya
Sector	TVET (Travel and Tourism)
Scale	At least 200 credentials endorsed throughout the platform
Indicators of Effectiveness	Follow up employment outcomes of persons who had the credentials endorsed in the platform after 12 months. If they are employed, follow-up with employers and check if the endorsed credentials had any bearing on the recruitment decisions.
Indicators of Efficiency	Ease of use for (new) employers
Partners	Kenya Blockchain Task Force; Companies in the tourism space (travel agents, hospitality industry, catering industry, transportation industry etc.); Indorse.io etc.
Timeframe	6 months to implement, 12 months to test impact

5.4 Implementation

This high-level Implementation Plan assumes that the Foundation:

— Has an interest in facilitating credential frameworks as a new 'technology' that improves the recognition of different forms of learning, and in the process contributing to the transferability of such recognition, and ultimately the entry and mobility of young African people in the labour market.

— Wishes to move towards the planning, development and implementation of a set of high-impact projects for piloting in one or two initial markets. Pilots may be designed that are country-, region-, and industry-specific; and also consider existing customs, practices and social norms.

— Has an interest in the recognition, accreditation and certification of non-degree qualifications that may in turn be captured and notarized using immutable technologies such as the blockchain; and ideally using open standards.

Table 5 overleaf suggests a set of steps that the Foundation should consider if it wishes to move beyond this report to the implementation of its recommendations.

Should the Foundation decide to participate in the technology-enabled sector, we would be interested in exploring how we may partner up to initiate and project manage the first set of high-profile pilots from concept to delivery.

Specifically, we have significant, hands-on experience with relevant technology-enabled credentials use cases in Europe and the Commonwealth; access to cutting edge research, know-how and experience with blockchain technologies and the Fintech sector; networks in emerging EdTech sector; and a track record of working with high-profile stakeholders, including governments.

1	Determine if one or two hypotheses can be aligned with the Foundation Strategy, and tranformed into high-profile technology-enabled credential pilots in core markets	— We strongly believe that hypothesis 1 and 2 provide the Foundation with a signficant opportunity to kickstart two tech-enabled credentials. We suggest that the first core markets should be Kenya and South Africa, in that they are likely to deliver high-impact pilots.
2	Identify 1 or 2 industries that are creating jobs and economic growth and are a government priority in the target countries	— In Kenya, there were 897,000 jobs created in 2017. The largest contributors were education sector, agriculture, fisheries and manufacturing, with education contributing 20.7% of the total. Government is putting a lot of emphasis on vocational training to produce more technicians and artisans and is also promoting agriculture. A number of private sector organizations and NGOs are also involved in agriculture development. — Education and agriculture seem to be the two most promising sectors for the pilots.
3	Determine if further research is needed on specific economic sectors in Kenya and South Africa which would benefit from the introduction of tech-enabled credentials	— In South Africa, agriculture holds the record in terms of job creation in 2017 with a slowdown in Q1 2018, and with Community & social services (95,000), construction (58,000) and trade (40,000) taking over in terms of net job contributions.
4	Engage with Government	— Irrespective of the market selected, early engagement with government is needed.
5	Speak to employers, academic institutions, youth associations, industry associations, government entities involved with these industries to try and identify a first use case that can be enabled on the blockchain as a proof of concept and that would deliver value for everyone.	— Investigate these industries to understand their recruitment/qualification verification challenges but also develop a clear picture of vocational training or on the job training that they are providing. Understanding which learning institutions are involved in delivering the required skills and how these qualifications / awards are delivered is as important as understanding the challenges that the youth are facing in acquiring, demonstrating and managing these qualifications.
6	Develop a framework for action	— Design a framework to accommodate public /private partnerships, levering on a network of insiders and experts.
7	Identify private sector players for pilot	— Involve technology vendors, NGOs and region ambassadors.
8	Implement the pilot use case and monitor	— As soon as the pilot is in implementation stage, start to monitor for at least 6 months.

Table 5: 12-month Implementation Plan

Figure 6 suggests an example of a phased approach to the implementation of one or more pilots based on the hypotheses proposed in this study.

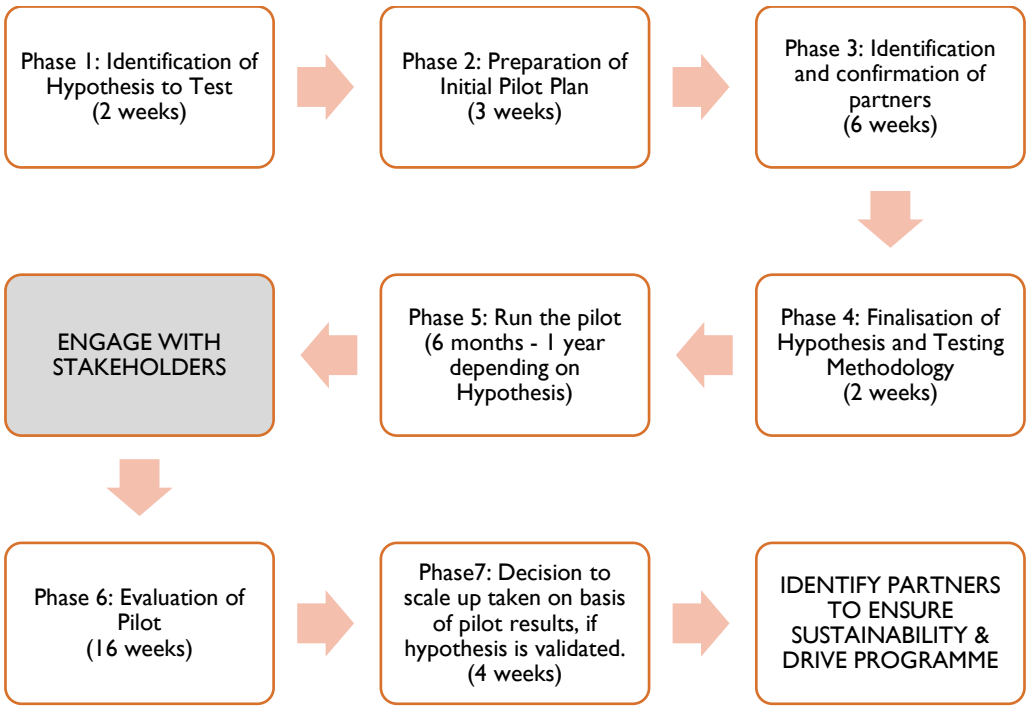


Figure 6: Snapshot of a Phased Timeline

References

African Union Commission (AUC). (2017). Repot on Labour Migration Statistics in Africa in 2015. Addis Ababa, Ethiopia. Retrieved from http://www.ilo.org/wcmsp5/groups/public/---africa/---ro-addis_ababa/documents/publication/wcms_575651.pdf

Allen & Overy (2016). Decentralised Autonomous Organizations. Available at: http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralised%20Autonomous%20Organizations.pdf

Allen, C. (2016). The Path to Self-Sovereign Identity. Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Au, S. (2017). Don't forget what self-sovereign identity system uPort doesn't claim to do. Available at: https://decentralize.today/dont-forget-what-self-sovereign-identity-system-uport-doesn-t-claim-to-do-1f43ca228575

Batchu, Y. (2017). What did #Blockchain bring to the table? Available at: https://blog.unocoin.com/what-did-Blockchain-bring-to-the-table-ded18ef70432

Blockchain Bundesverband (2018). Blockchain, data protection, and the GDPR. Available at: https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf

Byrne, W.I. (2017). What is the Blockchain? Available at: https://medium.com/badge-chain/what-is-Blockchain-5e4498f05c20

Cabrol, M. (2018). Technology is Creating a Human-Centric Economy, and It's Based on Trust. Available at: https://blogs.iadb.org/caribbean-dev-trends/2018/05/30/technology-is-creating-a-human-centric-economy-and-its-based-on-trust/

Carson, B.; Romanelli, G.; Walsh, P.; and Zhumaev, A. (2018) Blockchain beyond the hype: What is the strategic business value? Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Clark Donald (2016). 10 ways blockchain could be used in education. OEB Insights. Available at: https://oeb-insights.com/10-ways-blockchain-could-be-used-in-education/

Collins, A. (2017). Four reasons to question the hype around Blockchain. Available at: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-Blockchain

Domingue, J., (2016). Blockchains and Higher Education. Available at: https://www.slideshare.net/johndomingue/the-potential-of-Blockchain-in-higher-education

Domingue, J. (2017). Education's new kid on the block. Available at: http://www.open.ac.uk/research/main/news/educations-new-kid-block

European Union Blockchain Observatory & Forum (2018). Blockchain innovation in Europe. European Commission. Available at: https://www.eublockchainforum.eu/reports

Feldstein, M. (2017). A Flexible, Interoperable Digital Learning Platform: Are We There Yet? Available at: http://mfeldstein.com/flexible-interoperable-digital-learning-platform-yet

Forde, B. (2017), Using Blockchain to Keep Public Data Public, available at: https://hbr.org/2017/03/using-Blockchain-to-keep-public-data-public

Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. Seville, Spain: Joint Research Centre of the European Commission. Retrieved from https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-education

Griffith, E. (2018). 187 Things the Blockchain is supposed to fix. Available at: https://www.wired.com/story/187-things-the-blockchain-is-supposed-to-fix/

GSMA, The Mobile Economy, Sub-Saharan Africa 2017 available at: https://www.gsma.com/mobileeconomy/sub-saharan-africa-2017/

Gupta, M., (2017). *Blockchain for Dummies*, IBM Limited Edition. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN&

Hall, M. (2016). The Blockchain revolution: will universities use it, or abuse it? Available at: https://www.timeshighereducation.com/blog/Blockchain-revolution-will-universities-use-it-or-abuse-it

Hardjono, H., Lipton, A., Pentland, A. (2018). Towards a Design Philosophy for Interoperable Blockchain Systems. MIT Connection Science. Available at:

https://arxiv.org/pdf/1805.05934.pdf?utm_source=MIT+Technology+Review&utm_campaign=1a3e8b85ea-EMAIL_CAMPAIGN_2018_02_27_COPY_01&utm_medium=email&utm_term=0_997ed6f472-1a3e8b85ea-157729057

Hootsuite, Digital in 2018 (Global) available at: https://hootsuite.com/pages/digital-in-2018 and regional overviews available at: https://www.slideshare.net/wearesocial/digital-in-2018-in-southern-africa-8686590; https://www.slideshare.net/wearesocial/digital-in-2018-in-eastern-africa-part-1-north-86865720 ;http://abidjanvilledurable.com/wp-content/uploads/2018/02/Digital_in_2018_WestAfrica.pdf

IBM (2017). Blockchain basics: Introduction to distributed ledgers. Available at: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html

Jagers, C. (2018). Which blockchain should we use? Available at: https://medium.com/learning-machine-blog/which-blockchain-should-we-use-e2b8667f5805

Jagers, C. (2017a). Blockchain-Based Records and Usability. Available at: https://medium.com/learning-machine-blog/Blockchain-based-records-and-usability-179a4eeaeb6e

Jagers, C. (2017b). Digital Identity and the Blockchain. Available at: https://medium.com/learning-machine-blog/digital-identity-and-the-Blockchain-10de0e7d7734

Keevy, B. and Chakroun, B. (2018). Digitisation of Credentials. Implications for the Recognition of Learning. UNESCO

Lewis, A. (2017). A gentle introduction to self-sovereign identity. Available at: https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M. (2017). UPort. A platform for self-sovereign identity. Available at: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

Mamoria, M. (2017). WTF is the Blockchain? The ultimate 3500-word guide in plain English to understand Blockchain. Available at: https://hackernoon.com/wtf-is-the-Blockchain-1da89ba19348

McArthur, D. (2018). Will Blockchains revolutionize Education? Available at: https://er.educause.edu/articles/2018/5/will-blockchains-revolutionize-education

McKinsey (2016). How Blockchains could change the world. Available at: http://www.mckinsey.com/industries/high-tech/our-insights/how-Blockchains-could-change-the-world

MIT Media Lab (2016). What we learned from designing an academic certificates system on the Blockchain. Available at: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-Blockchain-34ba5874f196

Nakomoto, S. (2013). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

Piscini, E., Guastella, J., Rozman, A. and Nassim, T. (2016). Blockchain: Democratized trust. Distributed ledgers and the future of value. Deloitte University Press. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology/deloitte-uk-tech-trends-2016-blockchain.pdf

Ryan, P. (2017). We need to figure out how to use the Blockchain properly. This is why. Available at: https://www.weforum.org/agenda/2017/06/Blockchain-is-stalling-but-whats-holding-it-up

Russell, J. (2017). Sony wants to digitize education records using the blockchain. Available at: https://techcrunch.com/2017/08/09/sony-education-blockchain

Schmidt, J.P. (2017). Credentials, Reputation, and the Blockchain. Available at: http://er.educause.edu/articles/2017/4/credentials-reputation-and-the-Blockchain

Smolenski, N. (2016). Identity and Digital Self-Sovereignty. A New Paradigm for Sovereignty on the High Seas. Available at: https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3

Smolenski, N. (2017). Blockchain Records for Refugees. Available at: https://medium.com/learning-machine-blog/Blockchain-records-for-refugees-bd27ad6e6da1

Tapscott, D. and Tapscott, A. (2017a). The Blockchain Revolution and Higher Education. Available at: http://er.educause.edu/articles/2017/3/the-Blockchain-revolution-and-higher-education

The Economist Babbage Science & Technology Podcast: Digital Self Sovereignty. Available at: https://soundcloud.com/theeconomist/babbage-send-in-the-microbots?utm_source=soundcloud

University of Nicosia (2017). Self-Verifiable Certificates on the Bitcoin Blockchain https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-Blockchain

Vian, K. (2016). Own Your Achievements: Three Ways Blockchain Tech is Disrupting Education. Available at: https://Blockchainfutureslab.wordpress.com/2016/03/16/own-your-achievements-three-ways-Blockchain-tech-is-disrupting-education

Watterson, A. (2016). The Blockchain for Education: An Introduction. Available at: http://hackeducation.com/2016/04/07/Blockchain-education-guide

World Economic Forum (2015). Deep Shift Technology Tipping Points and Societal Impact. Available at: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf#page=24

World Economic Forum. (2017). The Future of Jobs and Skills in Africa: Preparing the Region for the Fourth Industrial Revolution. Geneva, Switzerland. Retrieved from http://www3.weforum.org/docs/WEF_EGW_FOJ_Africa.pdf

Yang, J. (2015). Recognition, validation and accreditation of non-formal and informal learning in UNESCO member states. Hamburg: UNESCO Inst. for Lifelong Learning. Retrieved from http://unesdoc.unesco.org/images/0023/002326/232656e.pdf

Online Resources

Blockcerts.org

Blockchain.open.ac.uk

Blockchain.mit.edu

Blockchain-lab.org

Blockchainpilots.nl/home-eng

Certificates.media.mit.edu

Community.blockcerts.org

Consensys.net/resources/guides

Consensys.net/academy/resources/

Dci.mit.edu

Ethereum.org

Hyperledger.org

ibm.com/Blockchain

openbadges.org

Videos

ASU GSV Summit, (2017). Trust but Verify: Block Chain – Knowledge as a Currency. Available at: https://www.youtube.com/watch?v=x6TDCTiUO9M

European Blockchain Observatory & Forum Videos. Available at: https://www.eublockchainforum.eu/knowledge

Gupta, V. (2017). European Parliament Blockchain Presentation. Available at: https://www.youtube.com/watch?v=fCYT9KWoldI

IBM Think Academy (2017). Blockchain, how it works. Available at: https://www.youtube.com/watch?v=lD9KAnkZUjU

Perry, R.E. (2017). Blockchain technology: From Hype to Reality. Available at: https://www.youtube.com/watch?v=v--lqndp0V4

Rosic, A. (2017). What is Ethereum? A Simple Explanation Anyone Can Understand. Available at: https://www.youtube.com/watch?v=ptLfwp6JYgk

Rosic, A. (2017). What is a Smart Contract? A Beginner's Guide. Available at: https://www.youtube.com/watch?v=qdoUpGg_DpQ

Stagars, M. (2017) The Blockchain and Us. Available at: https://www.youtube.com/watch?v=2iF73cybTBs

Tapscott, A. (2016) Blockchain Revolution. Talks at Google. Available at: https://www.youtube.com/watch?v=3PdO7zVqOwc

Annex 1: Interview Questions

We used a pre-determined set of interview questions to facilitate a conversation with the interviewees who agreed to form part of this study.

Introductions

- Introduction of Project, and reasons for the Research
- Introduction to the concept of Credentials within context of project.
- Quick explanation of different types of credentials in terms of:
- Formal educational credentials
- From educational institutions
- From professional associations, networks etc
- Credentials from non-formal learning / job-experience
- Reputational credentials
- Identity Credentials

Context of Credentials

- What kind of credentials do employers typically accept?
- What kind of credentials are most valued by employers in country?
- Who are the main issuers of credentials? (per type - also get references)
- Trust & Credentials
- Is there trust in the different kinds of credentials?
- What elements increase or reduce trust?
- How important is 'brand' as an element of trust?
- Are there issues linked to:
- Credential fraud?
- Transparency of credentials?
- Interoperability and recognition of credentials?

Youth Unemployment

- What are the main drivers of youth unemployment?
- Is there a skills gap issue? In which areas is this most prevalent?

— Do young people have a problem making visible education and/or skills received?

— Is there a regional/transnational/international dimension to this?

— Do young people understand the value of different credentials adequately?

Policy Landscape

— Are there any policy initiatives in the area of credentials - for each type of credentials?

— What are the reasons behind this (ask Q irrespective of positive or negative response)

— Which areas would you consider should be next priorities for policy?

Role of Non-Government Actors

— What role do you see for non-government actors (in particular, NGOs, Foundations, Networks, or the private sector) in developing the credentials landscape?

— What would be required for these actors to take on such a role?

— What do you consider an immediate next step forward would be?

Future Scenarios

— What would your vision of a mature credentials eco-system look like? How is this different from today?

— In ideal circumstances, how might this help tackle issues of youth unemployment?

Technology

— What are the main barriers to implementing tech-based digital credential systems? What are the minimum requirements in terms of national infrastructure?

— How mature do the IT systems of contributing stakeholders need to be? Is that often a problem? How do you see that gap being bridged?

— What about technology on the user side? How will they exercise control over their digital identity? What technology do they need?

— Overall, what options / mechanisms do you foresee could help bridge that digital divide? What's the role of public and private sectors in bridging the technology gap?

Annex 2: A Reference Framework for Credentials

Deconstructing Credentials

A credential may have two distinct sets of characteristics, which influence its **Quality**:

1) **Inherent Value**; and

2) **Technical Characteristics**

The more of these characteristics a credential has, the more likely is the credential's **fitness for purpose** and that it will be accepted by third parties.

Inherent Value of Credentials

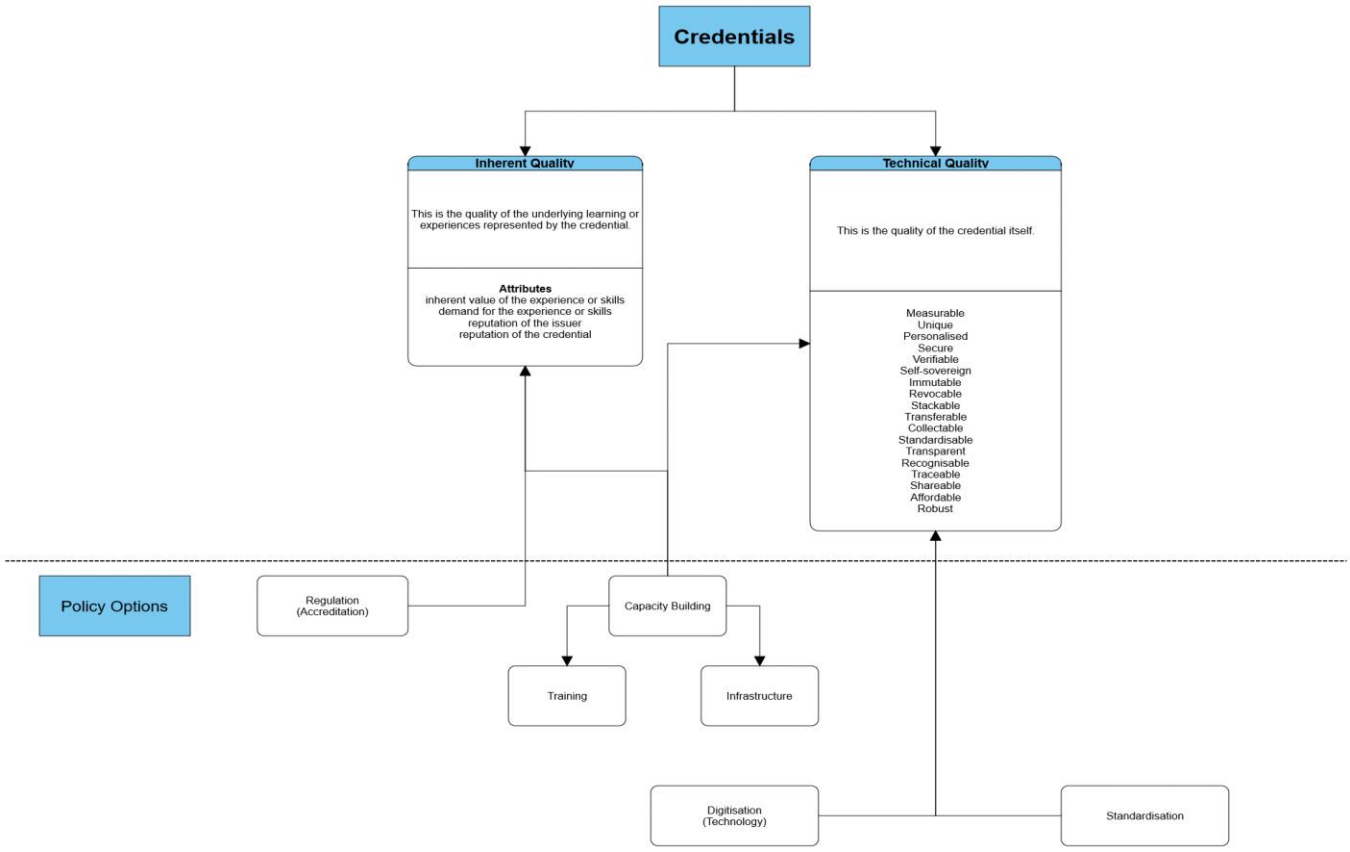
The Inherent Value of credentials are a set of characteristics linked to the **value of the statement** made by credential. The inherent value is in turn is determined by the:

- Reputation of the party issuing the credential;
- Demand for the experience or skills described by the credential;
- The robustness of the assessment process for issuing the credential;
- The reputation or brand equity of the credential itself

Technical Quality of Credentials

The following table tabulates a set of characteristics that also contribute towards a credential's quality – for the purpose of this study, we are describing these as 'technical':

CHARACTERISTIC	DEFINITION *(THE CREDENTIAL SHOULD BE…)*
MEASURABLE	represent an identifiable and measurable experience, skill or fact
UNIQUE	represent a distinct experience, skill or fact, attributable to the holder
PERSONALISED	be attributable to a single, identifiable person
SECURE	not be falsifiable
VERIFIABLE	allow for its authenticity to be verified
SELF-SOVEREIGN	be proof of its statement, in and of itself.
IMMUTABLE	not be changeable
REVOCABLE	be withdrawable
STACKABLE	allow for credentials of the same type to be added together to form a greater whole
TRANSFERABLE	allow for conversion into different credentials
COLLECTABLE	allow for the holder to control and physically possess it
STANDARDISABLE	always be issued with the same characteristics under the same conditions
TRANSPARENT	be backed up by published standards and evidenced
RECOGNISABLE	be available in a language and format that allows for wide use and acceptance;
TRACEABLE	allow for the conditions which led to the issue of the credential to be audited
SHAREABLE	be easily shareable
AFFORDABLE	have low issue and verification costs
ROBUST	be supported by reliable technology


Credentials
Inherent Quality
This is the quality of the underlying learning or experiences represented by the credential.
Attributes
inherent value of the experience or skills
demand for the experience or skills
reputation of the issuer
reputation of the credential
Technical Quality
This is the quality of the credential itself.
Measurable
Unique
Personalised
Secure
Verifiable
Self-sovereign
Immutable
Revocable
Stackable
Transferable
Collectable
Standardisable
Transparent
Recognisable
Traceable
Shareable
Affordable
Robust
Policy Options
Regulation (Accreditation)
Capacity Building
Training
Infrastructure
Digitisation (Technology)
Standardisation

From Paper to Digital Credentials

Paper Certificates

Most records are still issued on paper or other physical formats, although digitisation efforts by governments and industries are proceeding all over the world. There is no 'perfect format' for certificates, with many countries using hybrid-certificates whereby paper certificates are backed up by digital databases. However, the significant limitations of each system clearly show a need for a better, more robust certification technology.

Limitations of Paper Certificates

Paper certificates are still seen in many quarters as being the most secure form of certification, since they are:

- Difficult to forge due to security features built into the certificates themselves;
- Usually held directly by the recipient, who thus as full control over their certificate;
- Relatively easy to store securely for prolonged periods of time, e.g. by keeping them in a safe;
- In a format where they may be presented by the recipient anywhere, to any person for any purpose.

However, paper certificates also have significant disadvantages:

- No certificate is immune from the risk of forgery. Thus, the issuer is obliged to retain a central register of issued certificates that may be used to verify certificate authenticity;
- Certificate registries are single points of failure: while the certificates may remain valid, the ability to verify them is lost;
- Keeping such a register of claims, and answering queries as to the validity of certificates is a manual process, which requires significant human resources;
- Security features in the physical certificate derive exclusively from the difficulty level and expertise required to author the document. The more secure the certificate, the more expensive it is to produce. Single secure certificates such as passports routinely cost €20-€150;
- There are no limitations on the ability of the issuer to fraudulently state the timestamp or other details of the certificate;
- Once issued, there is no way to revoke a certificate without having the owner relinquish control of it;
- If a third-parties need to use the certificates, e.g. to verify claims in CV, they need to read and verify each certificate individually and manually, a significantly time-consuming process.

Digital Certificates

Digital certificates hold many advantages over paper certificates:

— They require far fewer resources to issue, maintain and use, since:
  - The veracity of certificates can be checked against the registry automatically, without human intervention;
  - Where a third party needs to use the certificates, these can be automatically collated, verified and even summarised if they are issued in a standardised for format;
  - The security of the certificate derives from the security of cryptographic protocols, which ensure that the certificate is cheap to produce but extremely expensive to reproduce by anyone except the issuer;

— Certificates can be revoked by the issuer;

— Certain types of issuer-fraud, such as changing the timestamp or changing the certificate serial, can be made impossible depending on the design of the system.

However, digital certificates also have significant disadvantages, namely that:

— Without the use of digital signatures, they are extremely easy to forge;

— Where digital signatures are used, these require the involvement of third-party certificate providers to guarantee the integrity of the transaction;

— These third parties have significant control over every aspect of the certification and verification process, which can be abused;

— In many countries, there is no universally-used open standard for digital signatures, leading to certificates that can only be verified within the context of specific software ecosystems;

— It is easier to destroy electronic records – keeping them safe requires sophisticated, multi-tier backup systems which are prone to failure;

— Should the registry fail, the certificates themselves become worthless since unlike paper certificates, they hold no intrinsic value without the registry;

— Registries of digital certificates are prone to large-scale data-leaks.

Digital Certificates using Blockchain Technology

Blockchain technology is ideal as a new infrastructure to secure, share, and verify learning achievements (Smolenski, 2016). In the case of certifications, a blockchain can keep a list of the issuer and receiver of each certificate, together with the document signature (hash) in a public database (the blockchain) which is identically stored on thousands of computers around the world.

Digital certificates which are thus secured on a blockchain hold significant advantages over 'regular' digital certificates, in that:

— They cannot be forged: it is possible to verify with certainty that the certificate was originally issued by and received by the same persons indicated in the certificate;

— Verification of the certificate can be performed by anyone who has access to the blockchain, with easily available open source software – there is no need for any intermediary parties;

— Since no intermediary parties are required to validate the certificate, the certificate can still be validated even if the organization that issued it no longer exists or no longer has access to the issued record;

— The record of issued and received certificates on a blockchain can only be destroyed if every copy on every computer in the world hosting the software is destroyed;

— The hash is merely a way of creating a 'link' to the original document, which is held by the user. This means that the above mechanism allows for the signature of a document to be published, without needing to publish the document itself, thus preserving the privacy of the documents.

Thus, blockchain certificates have the following advantages:

— **Independence:** the recipient owns the credential, and does not require the issuer or verifying third-party to be involved after receiving the credential;

— **Ownership:** the recipient may prove ownership of the credential;

— **Control:** the recipient has control over how they curate credentials they own. They may choose to associate credentials with an established profile they own, or not;

— **Verifiability:** the credential is verifiable by third parties, like employers, admissions committees, and verification organizations;

— **Permanence:** the credential is a permanent record (subject to the limitations imposed on the original credential)

Opportunities of Tech-Enabled Credentials

How Technology can improve the inherent value of credentials

With digital technology driving change in education, and with alternatives to traditional credentials all directly associated with digitization, it is pertinent to assume that technology will eventually play an important role in improving the inherent quality of credentials. The list below provides some examples of solutions which can raise the quality of each of the characteristics described above:

Characteristic	***Ways Technology can help***
Reputation of the person issuing the credential	Technology can help make **visible** the reputation of the person through any of the following methods: • Allowing for verification of identity of the issuer; • Creating databases of accredited / national issuers; • Allowing issuers to create shared self-sovereign identities whereby they make visible all certifications and accreditations they have received as an issuer; • Creating ranking systems based on social recommendations
Robustness of the assessment process for issuing the credential	Technology can help improve the **security** and **auditability** of the assessment process by: • Providing secure identity verification of test-takers; • Allowing records for each step of the assessment to be kept and to be linked to the certification itself.
Reputation of the credential itself	Tech can help improve the reputation of the credential by: • Allowing for the creation of databases of credentials; • Keeping track of how credentials are used, and by whom they are accepted, and making this available.

How Technology can improve the technical quality of credentials

Technology can play an important role in improving the technical quality of digital credentials, by 'upgrading' the medium:

Characteristic	***Ways Tech can help*** ***Advanced Credentialing technologies such as blockchain and PKI can improve the usability of credentials by creating credentials which:***
Uniqueness & Security	Cannot be copied or forged.
Personal	Can only be used or shared by the intended recipient of the credential
Self-Provability	Can be verified for authenticity without checking with external parties or databases
Immutability	Cannot be edited or destroyed
Revocability	Can be revoked by the issuer
Stackability	Can be linked
Transferability	Can be 'spent' to achieve other credentials
Collectability	Can be fully controlled and securely held by the user
Transparency	Can be linked to the underlying standards on the basis of which they were issued OR the standards can be in-built into the credential itself
Recognisability	Can be issued automatically in multiple languages **and** which Can be automatically read and verified by software
Traceability	Can be linked to the underlying evidence on the basis of which they were issued
Shareability	Cannot be used or shared without the explicit permission of the user for each use
Affordability	Can be issued at high volume with low cost

Standards for Credentials

Prerequisites for standardised credentials

While quality industry credentials are essential to strengthening connections between working and learning, the marketplace is full of so-called "solutions," making it hard for employers, educators and students to understand which credentials have real value. Representatives from more than 10 high-demand industry sectors have identified the attributes of high-value, standards-based, industry credential programs. While this list refers mostly to certifications, a type of industry credential, it is a first step in defining the qualities that make programs valuable to consumers—employers, workers and students.

Quality credential programs have:

- An independent, third-party governing body that operates with impartiality
- A scope statement for the credential that is publicly available
- Current job task analyses or other standards on which a program is based
- A validation process for the job task analysis
- A process for examination development, maintenance and administration
- Eligibility requirements or prerequisites
- Alignment of learning objectives with assessments
- Credential and training that are industry recognized
- A code of Ethics*
- Policies that guide all credentialing decisions, including due process
- Protection of intellectual property, including examination, logos and marks
- Stakeholders that provide ongoing systematic input
- Separation of training from testing*
- Evaluation of program against program performance objectives
- A complaints and appeals process
- Ongoing professional development

Initiatives for Awarding Digital Certificates & Credentials

Open Badges

The OBI (Open Badge Infrastructure) is a set of software tools and specifications to support people and organizations who want to adopt badging. The OBI is the core underlying technical scaffolding for the badge ecosystem.

The OBI supports a multitude of issuers conferring badges into the ecosystem, as well as many displayers and earners using badges to share their competencies and achievements. Anyone can earn badges across many issuers, collect them in one place tied to their

identity, then share them with various websites and audiences (including career sites, social networks or personal portfolios).

The OBI aims to support badge issuing, collection and display. This involves:

- Allowing earners to tie badges to their identity and carry their badges with them wherever they go
- Displaying badges to parties the earner cares about (e.g. employers, college admin, peers)
- Allowing earners to manage collections of badges and control visibility of those collections
- All of this is supported within a framework that is open and decentralized to facilitate badging across sites and sources.

A badge is a special digital certificate comprised of a digital image and some metadata. The data can be baked into the badge, meaning that it is embedded into the image file. The individuals and organizations who issue badges create the badge metadata - which is designed to support verification of badges, so that an earner's badges can be checked for authenticity. The data includes information about:

- What the badge represents
- Who earned it
- Who issued it

Despite offering the world a free-to-use secure digital credentialing system, badges have failed to gain significant update in education. It is postulated that the reason for this is that credentials are, in their essence, classifications or categorizations of persons. They represent distinctions or symbolic boundaries between those who hold a particular credential and those who do not. The value of credentials, therefore, lies largely in their relative scarcity – thus, a technological system that allows anyone to issue similar credentials has limited use for stakeholders in formal education (Olneck, 2015).

Further it is claimed by some that Stakeholders in the high-school-to-college-to-career pipeline understand and value credentials as they exist now, and rarely need or want a new way to understand them (Matthews, 2016).

Let's Encrypt

Let's Encrypt (LE) is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG). While it involves the award of digital security credentials, rather than digital educational credentials, it is included since it is the largest issuer of free secure digital certificates globally.

LE gives people the digital certificates they need in order to enable HTTPS (SSL/TLS) for websites, for free, in the most user-friendly way we can. The key principles behind Let's Encrypt are:

- **Free:** Anyone who owns a domain name can use Let's Encrypt to obtain a trusted certificate at zero cost.
- **Automatic:** Software running on a web server can interact with Let's Encrypt to painlessly obtain a certificate, securely configure it for use, and automatically take care of renewal.

- **Transparent:** All certificates issued or revoked will be publicly recorded and available for anyone to inspect.
- **Open:** The automatic issuance and renewal protocol is published as an open standard that others can adopt.
- **Cooperative:** Much like the underlying Internet protocols themselves, Let's Encrypt is a joint effort to benefit the community, beyond the control of any one organization.

LE has been successful in disrupting the certificate industry, which has been slow in covering the lower-cost end of the market. By addressing the two major barriers inhibiting ubiquitous encryption (cost and complexity required in issuing X.509 certificates), LE has become one of the largest CAs within only one year after its first certificate was issued.

Research shows that LE has been playing a major role in democratizing encryption: LE has been widely used, and mostly by the low-cost share of the market (shared hosting), which would be unlike to deploy the complex and costly X.509 certificates before LE. Once these barriers are eliminated, it enables big hosting providers to issue and deploy certificates for their customers in bulk, thus quickly and automatically enable encryption across a large number of domains.

Blockcerts

Blockcerts is an open standard for building apps that issue and verify blockchain-based official records. These may include certificates for civic records, academic credentials, professional licenses, workforce development, and more.

Blockcerts consists of open-source libraries, tools, and mobile apps enabling a decentralized, standards-based, recipient-centric ecosystem, enabling trustless verification through blockchain technologies.

Blockcerts uses and encourages consolidation on open standards. Blockcerts is committed to self-sovereign identity of all participants and enabling recipient control of their claims through easy-to-use tools such as the certificate wallet (mobile app). Blockcerts is also committed to availability of credentials, without single points of failure.

These open-source repos may be utilized by other research projects and commercial developers. It contains components for creating, issuing, viewing, and verifying certificates across any blockchain. These components form all the parts needed for a complete ecosystem.

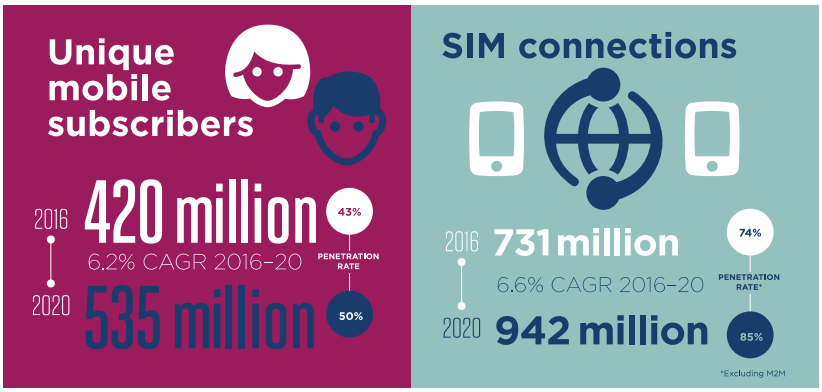
Annex 3: An Overview of Infrastructure and Technology in Africa

This Annex provides a high-level overview of current and projected levels of development of infrastructure in Africa and focuses on three main aspects or components of infrastructure:

1. **Mobile penetration** and more particularly smartphone penetration, as it is relevant to the way citizens will relate to / engage with digital services;
2. **Internet access**, as it is the backbone upon which any digital service will be delivered to its targeted users;
3. **Maturity of the technology scene**, as it ensures that stakeholders participating in new technology-enabled business models will be able to access local providers and expertise to support
4. **Availability of national ID infrastructure**, as any credentialing system will rely on existing ID systems for verification. The section starts with an overall summary of what is happening in the continent before focusing on specific markets that were singled out as possible candidates for a potential pilot.

General state of Infrastructure

At the end of 2016, there were 420 million *unique* mobile subscribers in Sub-Saharan Africa for a total of 731 million mobile subscriptions. This number is projected to grow to half a billion *unique* subscribers by 2020, for a total of nearly 1 billion mobile subscriptions, reaching half of the population and concentrating two thirds of all broadband connections with 3G as the dominant broadband technology. It is therefore expected that by 2020, half the Sub-Saharan African population will be connected via mobile, and the majority of them will be accessing broadband services using their mobile devices.

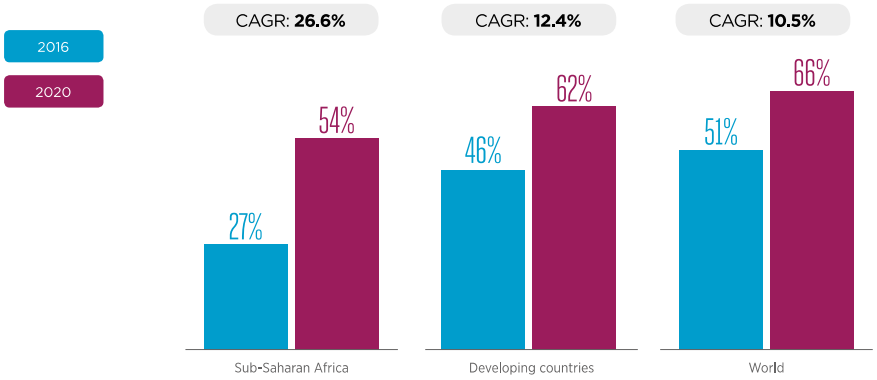


Source: GSMA, The Mobile Economy, 2017

Smartphone penetration has also doubled over the past 2 years to reach over 200 million, accounting for about a quarter of all mobile subscriptions. Smartphone penetration is expected to dramatically increase over the next 3 to 5 years, pushed by the availability of cheaper sub-$100 devices and a growing second-hand market, driving the demand for digital content. As a consequence, data traffic is also projected to grow twelvefold in Africa over the next 5 years, driven mostly by younger, more tech-savvy users.

Smartphone adoption growing

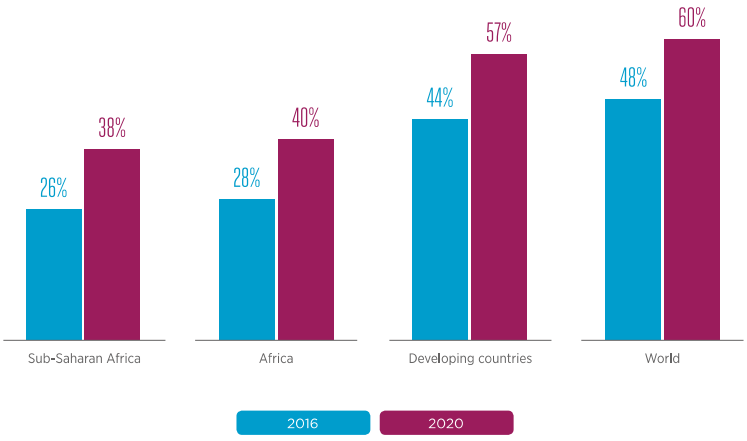
(Percentage of connections)



Source: GSMA, The Mobile Economy, 2017

In most markets, mobile operators are offering smartphone-financing schemes, which will further drive mass adoption of smartphone. They are also rolling out 4G networks, but 3G remains the dominant broadband technology although 4G adoption is on the rise with live 4G networks in 39 countries and about 28% of the population covered. By 2020, there will be 500 million smartphones in Sub-Saharan Africa. In this respect, mobile technology has really brought Africans online, with an additional 155 million subscribers projected to join the mobile internet community, achieving a penetration rate of 38% by the end of 2020.

Mobile internet subscriber penetration

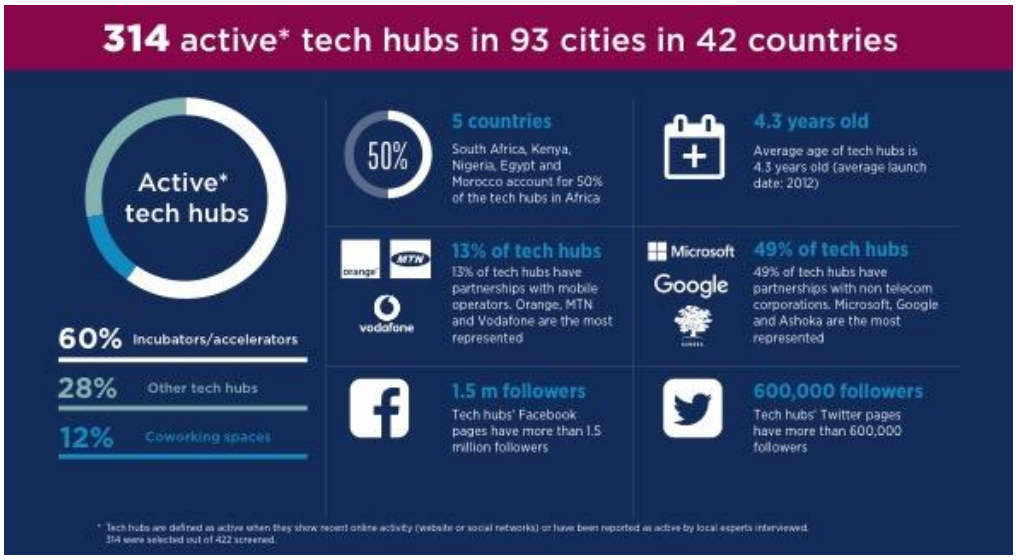


Source: GSMA, The Mobile Economy, 2017

As a matter of fact, mobile is increasingly becoming the platform of choice for creating, distributing and consuming digital services as the tech industry matures. A number of homegrown platforms (IKOKOtv, Buni tv etc.) are closely working with mobile operators to drive affordability, usage and mass-market uptake and about 77 tech start-ups raised around $366.8 million in funding in 2016 alone to drive more digital services on the mobile platform.

Mobile Financial Services have undoubtedly been a driving force behind increased mobile user engagement, with over 280 million registered accounts and countries like Kenya, Uganda and Tanzania leading the way in terms of customer activity and product innovation. More generally, mobile-based innovation continues to attract talents and

funding, and tech hubs have been flourishing over the last few years with 314 tech hubs across Africa as of July 2016.



Source: GSMA, The Mobile Economy, 2017

All in all, it seems that consumer connectivity to the cellular network and to internet is rapidly becoming less of a concern in Africa, and this trend has been confirmed by most interviewees. Challenges that remain are mostly anticipated at stakeholder level (banks, universities, governments etc) whose IT systems and infrastructure are often not at the level that would be required for them to participate in various innovations, leading to delays in technology integration times. It is however noteworthy that the tech scene has been developing rapidly in Africa, resulting in higher levels of awareness and expertise especially in the blockchain space.

It is also interesting to note that a number of innovative business models are currently being discussed by various public and private sector initiatives in support of the UN DGS goals, in particular in the field of education, where the stated goal is to ensure inclusive and equitable education and promote lifelong learning for all. One such initiative is led by the Blockchain Task Force in Kenya, exploring ways to tokenize life-long learning journeys and attempting to influence the trajectory that these journeys may take through a reward mechanism based upon potential job outcomes. Some of these emerging initiatives will be interesting to explore further in the context of digital credentialing in Africa, as they may be relevant to the youth segment.

General state of Infrastructure in Target Markets

In the inception report, we suggested that this research be focused on Kenya, Rwanda, South Africa and Ghana. These countries present certain infrastructure characteristics that make them particularly suitable for further exploration within the context of tech-enabled credentials.

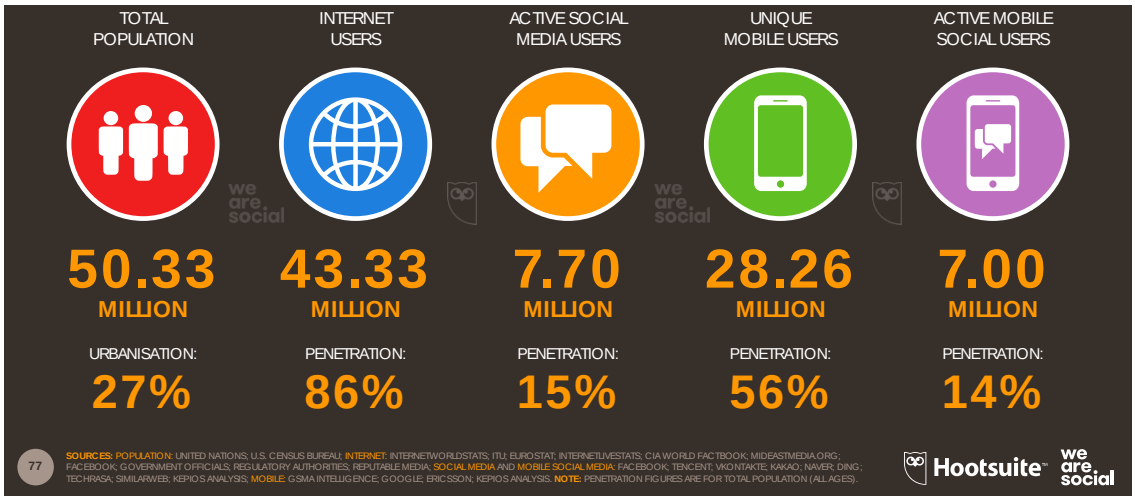
Kenya

More people than ever are connected through their cell phone

In Kenya (population: 50 million), mobile subscriptions have raised to 41 million in 2018 in a market dominated by Safaricom (71.9% market share) followed by Airtel Networks (4.9% market share), according to the Communications Authority of Kenya in its

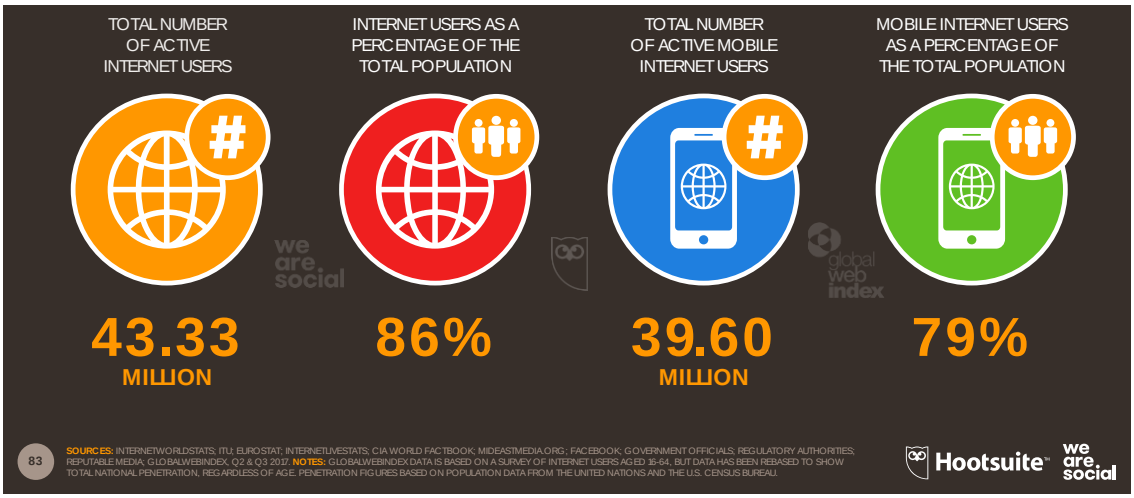
2017/2018 Financial Year report. This translates into 28 million *unique* users, which points to a 56% penetration rate.

At the same time Internet subscriptions have grown by 4.3% to reach 30.8 million subscriptions (for a total of 43 million Internet users), of which mobile data subscriptions represented 99%.



Source: Hootsuite, Digital in 2018 in Eastern Africa

Internet use is heavily mobile



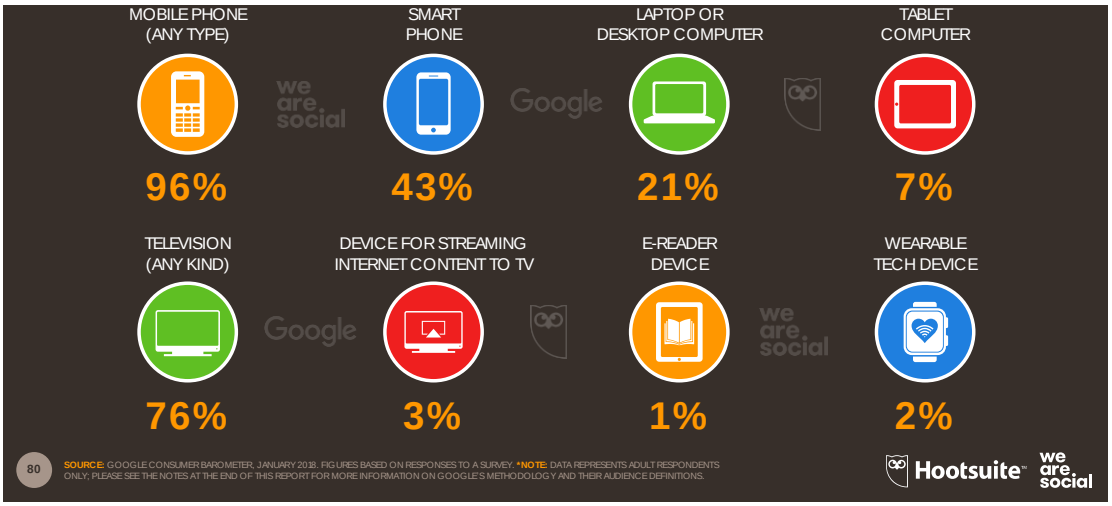
Source: Hootsuite, Digital in 2018 in Eastern Africa

The above chart shows that a large percentage of the population uses Internet and that most Internet users are already accessing the Internet through mobile. In fact, Kenya is now the global leader in share of Internet traffic coming from mobile. This is partly driven by the entry of aggressive smartphone vendors like Transsion, who controls 58% market share of smartphones by volume and is driving the prices down, making smartphones more and more affordable for the masses.

Furthermore, significant improvements in the broadband infrastructure in the country have also propelled the number of broadband subscriptions to 17.6 million.

Feature phones are still more widespread than smartphones

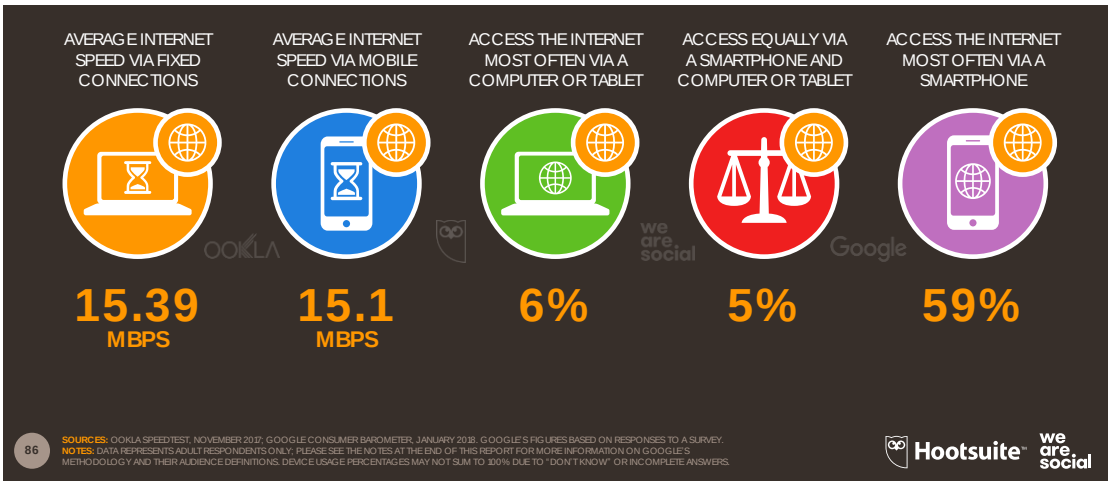
In terms of the share of web traffic by device, the following chart shows that about 96% of web traffic is originated on mobile phones and 43% on smartphones, attesting that feature phones are still more popular in Kenya.



Source: Hootsuite, Digital in 2018 in Eastern Africa

And current data speeds are good enough for digital products consumption

Improvements in mobile infrastructure have allowed users to access the Internet at speeds that are compatible with the consumption of more sophisticated digital content. At the moment, the average Internet speed achievable via mobile connections is comparable to what is available on fixed connections, which encourages further adoption of mobile as a primary channel to access and should support digitally-enabled management of personal credentials.



Source: Hootsuite, Digital in 2018 in Eastern Africa

The tech scene is flourishing in Kenya

Kenya currently has over 27 tech hubs and is a hotbed for mobile tech innovation with Fintech start-ups leading the pack, which got the country the title of 'Silicon Savannah'.

Among the most ambitious projects is the construction of a technology city called Konza City, which will sit on 5,000 acres of land and will become a centre of innovation.

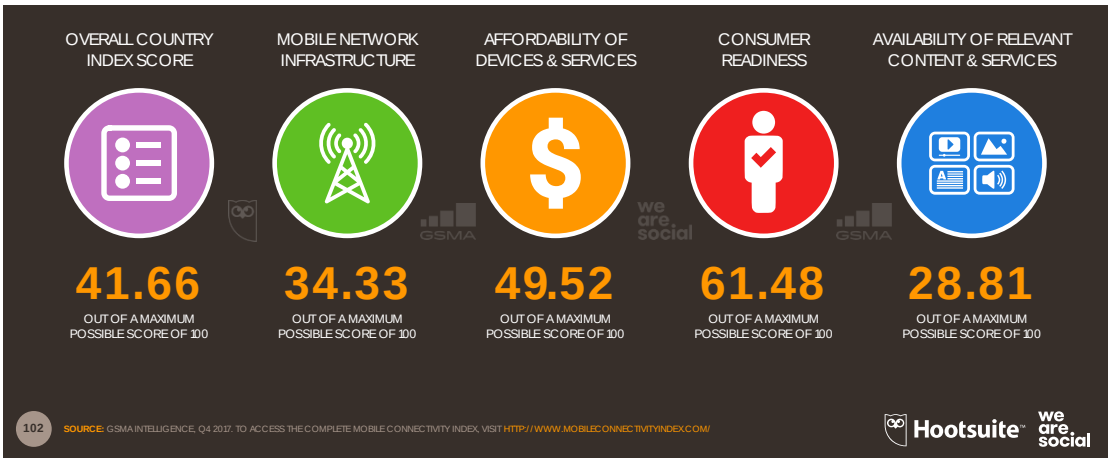
In February of 2018, Kenya also announced the appointment of a Blockchain Task Force to explore the use of Digital Ledger Technologies and Artificial Intelligence with a focus on education, land title registry, single digital identity and overall public service delivery. The Task Force, reporting to the ICT Cabinet is expected to produce a roadmap at the end of May 2018 for further deliberations. In the meantime, Kenya has been hosting a number of blockchain events, including the World Blockchain Summit in March 2018, in a resolute attempt to be at the forefront of blockchain developments in East Africa.

Kenya has also been a land of innovation in the blockchain space. Among some of the many start-ups in the blockchain space are BitHub Africa (Nairobi based blockchain accelerator and advisory firm, creating the best pool of expertise in this area across Africa), BItPesa (B2B money transfer for African businesses), Bitsoko (Android mobile wallet that creates a bridge between mobile money platforms and blockchain tokens), ChamaPesa (the first blockchain based bookkeeping solution for savings groups).

GSMA mobile connectivity assessment for Kenya

The GSMA has established a mobile connectivity index to measure the performance of a number of countries against four key enablers of mobile internet connectivity: infrastructure, affordability, customer readiness and content, These indicators are built through analysis of 38 individual indicators and provide a snapshot of where each country finds itself (https://mobileconnectivityindex.com).

According to this index (see chart below), Kenya achieved an average of 41.7, placing it in the emerging category.



Source: Hootsuite, Digital in 2018 in Eastern Africa

National ID Infrastructure in Kenya

Kenya has several national ID systems in place, and they are extensively used by banks and other Digital Finance providers for the purposes of identifying their customers. For instance, there are currently over 28 million mobile money subscribers in Kenya who are duly identified against official government-issued ID documents (driving license, voter card, ID card). All Kenyans are actually issued a national ID card at the age of 18 however there has been no interoperability between most of these systems, pointing to the lack of a unified registry for each citizen.

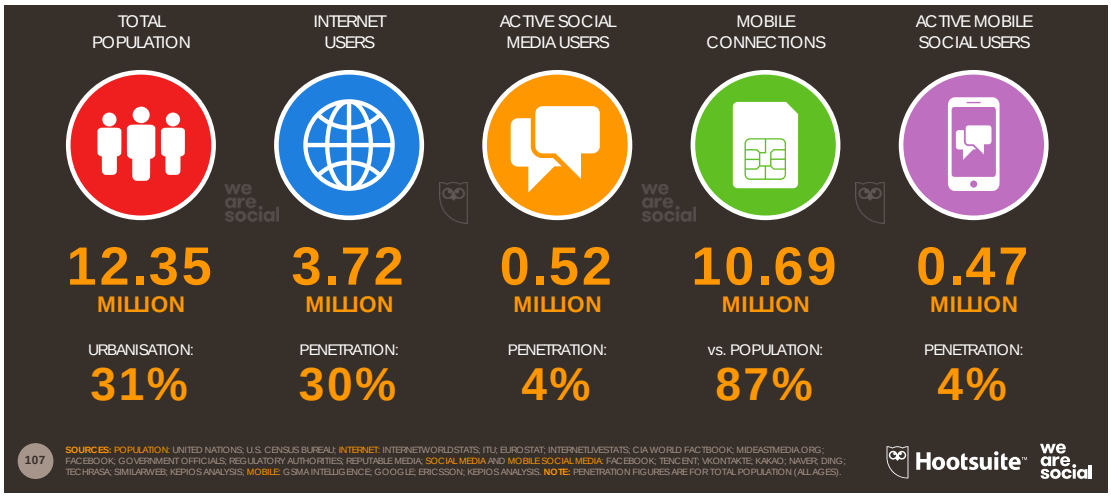
Recently, Kenya's Ministry of Interior has worked on the rollout of a third generation ID card for Kenyans, and all other government documents (driving license, National Hospital Insurance Fund and Kenya Revenue Authority Personal Identification Number) will be integrated with that ID card. This card is expected to be issued in 2019 and will be massively distributed.

The implementation of the smart ID, along with other initiatives surrounding it, is going to establish a new biometric identification system for all citizens of Kenya that can be exploited for broader credentialing purposes as well. In the meantime, current ID systems and processes in place should suffice to provide the required foundation.

Rwanda

A growing mobile penetration

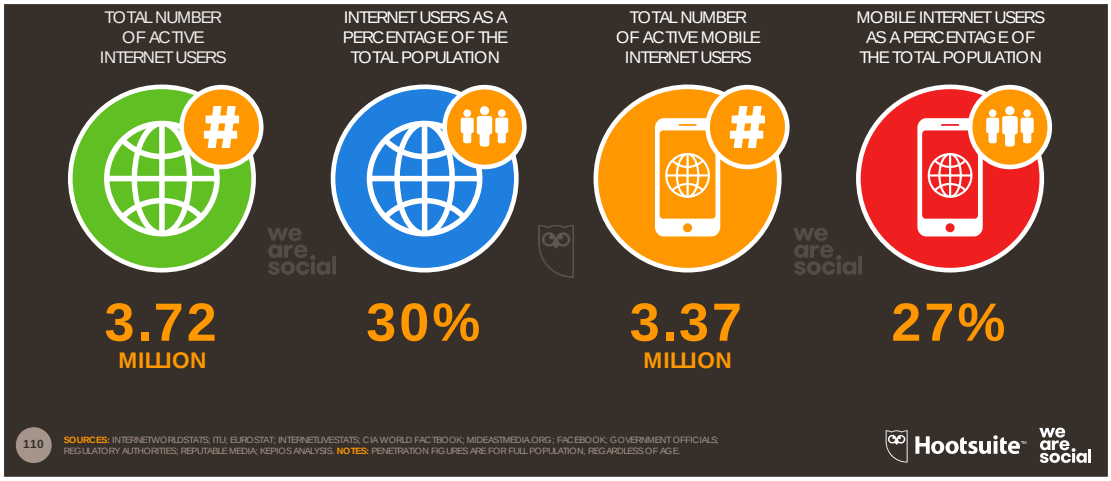
In Rwanda (population: 13 million), mobile penetration has raised to 75.5% at the end of 2017 according to RURA (Rwanda Utilities Regulatory Authority), in a competitive market where MTN holds a 42% market share and Airtel holds a 58% market share, after Airtel's acquisition of TIGO. There are currently around 10 million mobile connections in Rwanda.



Source: Hootsuite, Digital in 2018 in Eastern Africa

Internet use is relatively limited

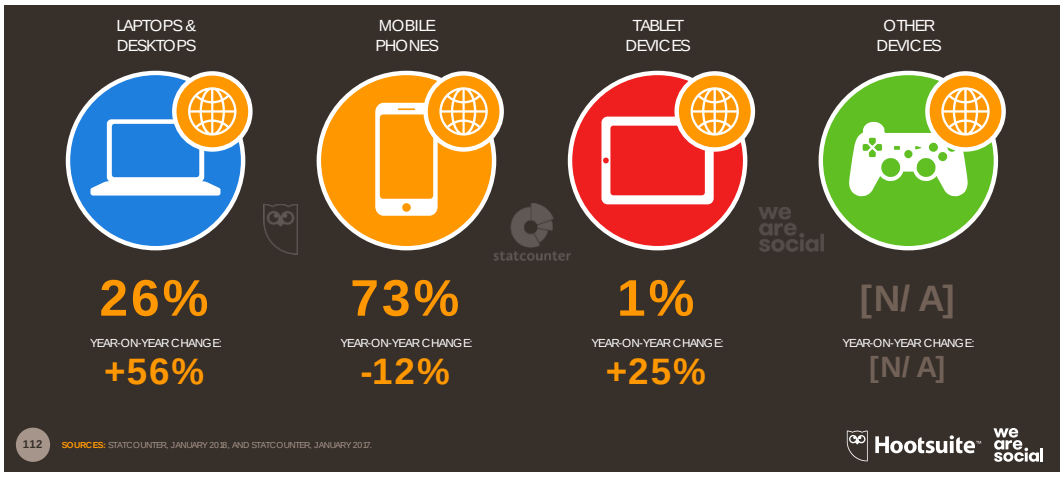
As for Dec 2017, there were 3,7 million Internet users in Rwanda, amounting to 29.8% of the population. However, smartphone penetration is still low, in the range of 10%, most Rwandans not being able to afford smartphones despite the fact that international traders such as Konka Group and Tecno mobile have entered the local market. As a result, the number of mobile Internet users as a percentage of total population is much lower in Rwanda compared to Kenya.



Source: Hootsuite, Digital in 2018 in Eastern Africa

Mobile phones remain the primary channel for Internet access

In terms of the share of web traffic by device, the following chart shows that 73% of internet traffic in Rwanda is currently channelled through mobile phones, confirming low ownership of laptops and desktops. The government of Rwanda has many initiatives to allow university students to own laptops through loans, one of which is called Viziyo and also involves MTN and Bank of Kigali. There are also discussions to push down the price of 1Gb of data below 2% of the average monthly income.



Source: Hootsuite, Digital in 2018 in Eastern Africa

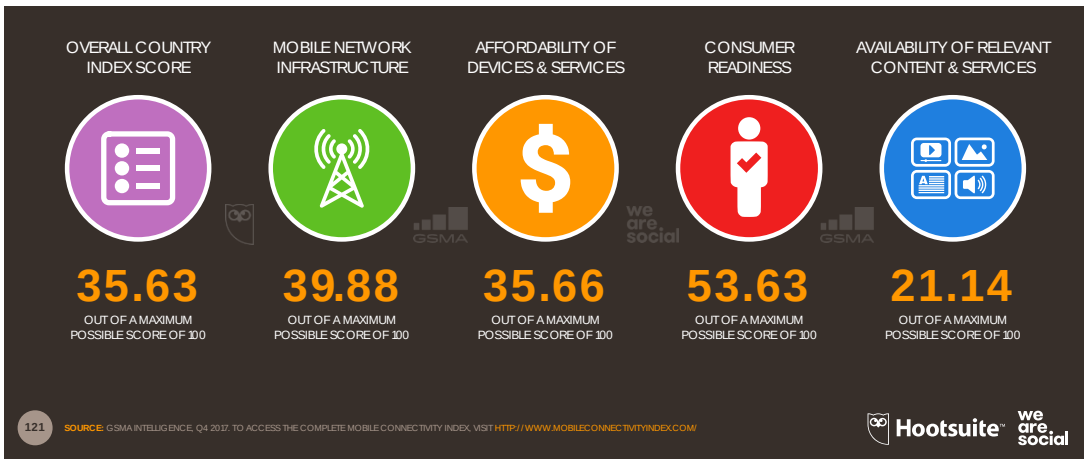
The tech scene in Rwanda

Rwanda has developed a vibrant tech scene, with specific policies encouraging economic development and ease of doing business, and the government investing heavily in creating a knowledge-based economy. Besides, the government has established a $100 million venture fund to create over 100 tech companies valued at over $50 million by 2030. Among the rising tech stars are companies like Safemotos, a local Uber-like service that allows users to hail a safe motorcycle-taxi from their smartphones and Zipline, a company using drones to deliver blood to citizens across the country, delivering over 5,500 units of blood in 2016 and reducing maternal mortality rates.

Rwanda government's Blockchain project, launched in 2017, aims to drive Rwanda's digital transformation and seems to be gaining some momentum. The first phase of the project focused on land registry digitization to enable authenticity of identification and validation of assets. Within this context, The Rwandan government partnered with the Swiss firm WISekey to establish a blockchain / IOT (Internet of Things) centre of excellence. This initiative is gaining momentum, as the government wants to be at the forefront of digital transformation of public services.

GSMA mobile connectivity assessment for Rwanda

Against the GSMA mobile connectivity index, Rwanda fares slightly lower than Kenya, placing it in the emerging category as well.



Source: Hootsuite, Digital in 2018 in Eastern Africa

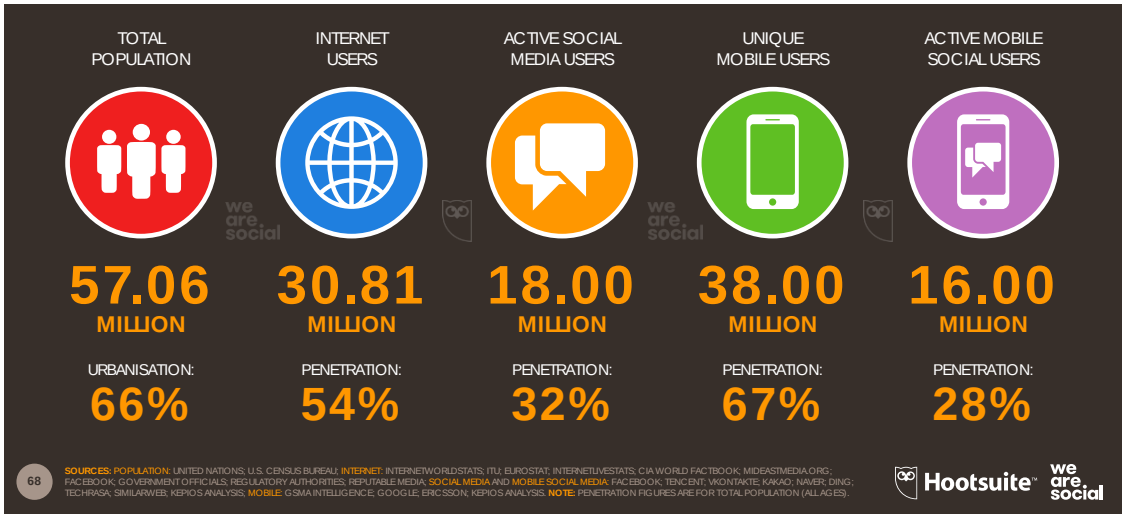
National ID Infrastructure in Rwanda

The identity ecosystem in Rwanda is very mature and is able to support the daily personal identification needs in a Digital economy. The National Identity Agency has already issued a biometric National Identity Card for citizens of 16 years old and above, which builds both on a comprehensive National Population Register (NPR, covering 95% of the population) and a unique National Identity Number (NIN) that one keeps for life. The intention behind the NIN is to provide a unique interface between a unique individual and the government agencies and improve service efficiency.

These developments have been largely facilitated by Rwanda's decentralized administration structure and many government agencies are now linking to the NPR. The cost of the mandatory ID is one of the lowest in Africa (under USD 1) and optional smart IDs are offered at a cost to those who need them. Together with state-of-the-art storage, security, enrolment, identification and online verification services, the above constitutes a robust identification system that can reliably be used by any credentialing project.

South Africa

In South Africa (population: 57 million), unique mobile users and Internet users have both grown by 7% since Jan 2017 to reach 38 million unique mobile users (penetration rate of 67%) and 31 million Internet users (penetration rate of 54%).

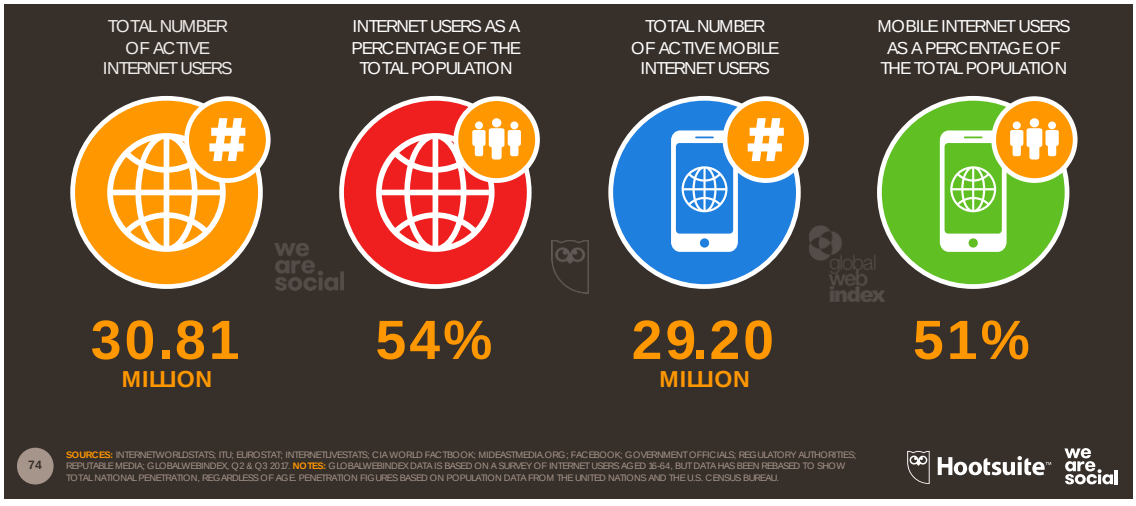


Source: Hootsuite, Digital in 2018 in Southern Africa

During the same time, smartphone penetration has reached 60% penetration of the population, with most users accessing the Internet via a smartphone. This makes South Africa a very exciting market for Fintech leveraging smartphone access to deliver richer digital experiences to their users.

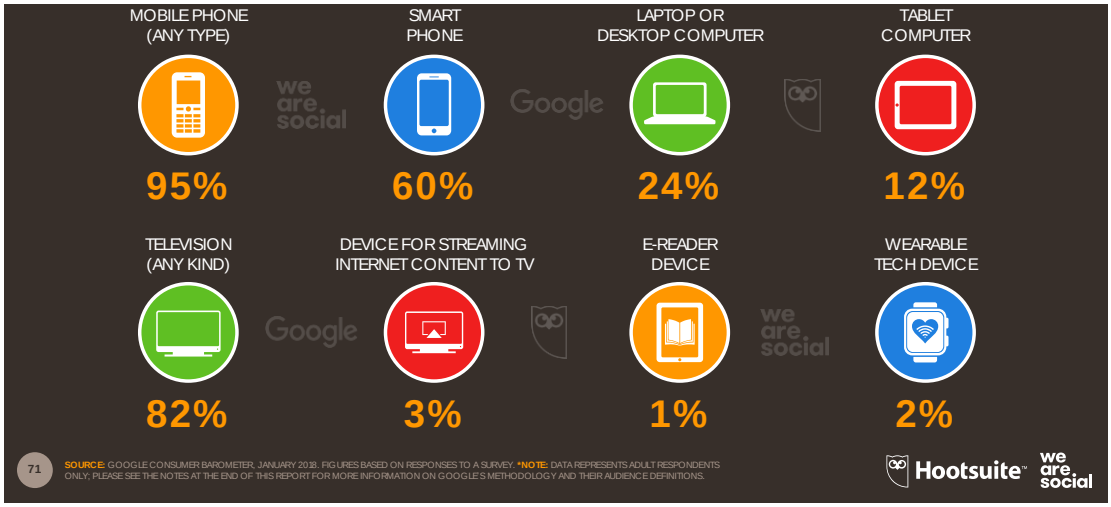
Internet use is mostly mobile

The following chart shows that most Internet users are mobile. In that respect, South Africa fares better than Rwanda.



Feature phones are more widespread than smartphones but the gap is narrowing

In terms of the share of web traffic by device, about 60% of web traffic is originated in smartphones versus 95% on mobile phones. This provides a confirmation of the growing prevalence of smartphones in that particular market. South Africa is also a relatively highly computerized market, with 24% of web traffic originating in laptops or desktops.



Source: Hootsuite, Digital in 2018 in Southern Africa

The tech scene in South Africa

South Africa boasts one of the most advanced tech scenes in Sub-Saharan Africa. Many tech hubs like SmartXchange in Durban and RLabs in Cape Town have set to serve the growing tech industry while two major acceleration programmes also launched in 2017: Startupbootcamp launched a 3-month programme in Cape Town while Google launched its own Accelerator programme to South African start-ups.

In terms of the tech start-up scene, Fintech has taken the front stage with a number of players focusing on enhancing user convenience - such as Walletdoc, Karri, Zapper and SnapScan – and solving a real customer pain point. Last year has also seen a number of developments in the areas of chatbots (with companies like FinChatBot) or robo advisors (with companies like OUTvest and Coreshares) and Insuretech (Click2Sure, Cascade etc.). The tech ecosystem in South Africa is rapidly expanding as more and more venture fund is pouring in. In 2017 alone, venture funding to African start-ups jumped to $195 million and South Africa ranked 2nd in terms of top recipients. As the ecosystem matures, more and more South African start-ups are also nourishing international ambitions.

Indeed, among the most promising South African start-ups, a few set themselves for aggressive expansion across Africa in 2018: Yoco, a start-up integrating card payment and point-of-sale systems is expanding in East and West Africa; Mam Money, enabling the unbanked to transfer money via mobile is expanding into Mozambique Malawi and Kenya; Libryo, providing regulatory information has expanded into 45 countries cross Sub-Saharan Africa; Luno, a Bitcoin platform enabling crypto-trading is also expanding across markets; IOT.nxt is planning to expand into Europe given the relevance of the platform in mature markets.

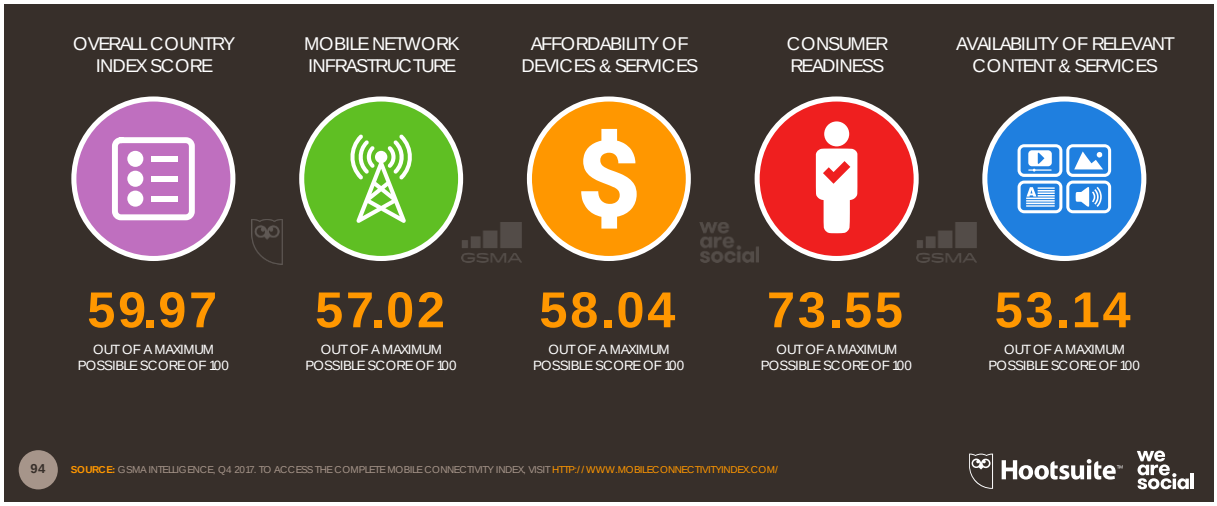
From an investment deal perspective, 2017 also saw one of the biggest acquisitions of a South Africa start-up, with the over $100-million acquisition of GetSmarter. By the end of October 2017, South African start-ups had secured deals valued at around $140 million.

Blockchain as an emerging technology is gathering significant attention in South Africa. In Cape Town, the Blockchain Academy is providing training on cryptocurrencies and blockchain to local start-ups and entrepreneurs and helps businesses revisit their business models through the introduction of blockchain in their operations. The South African Reserve Bank (SARB) also launched a new initiative with Consensys based on enterprise blockchain Quorum. And more blockchain developments are to come, in particular around the crossover between solar energy and Bitcoin mining and projects like UBU, which operate a low cost digital payment system and aim to economically empower lower income South Africans.

Last year (2017) was also a year in which initial coin offerings developed in South Africa, with companies like Augmentors, Prosperiprop, Wala and eKasi bucks launching their ICOs.

GSMA mobile connectivity assessment for South Africa

Against the GSMA mobile connectivity index, South Africa fares the highest of all suggested pilot markets.



Source: Hootsuite, Digital in 2018 in Southern Africa

National ID Infrastructure in South Africa

In South Africa, every citizen above the age of 16 is required to have an ID card. Currently, the ID card has a barcode, a photo and a unique number. That ID card is necessary to obtain a bank account or access financial services or any other formal service.

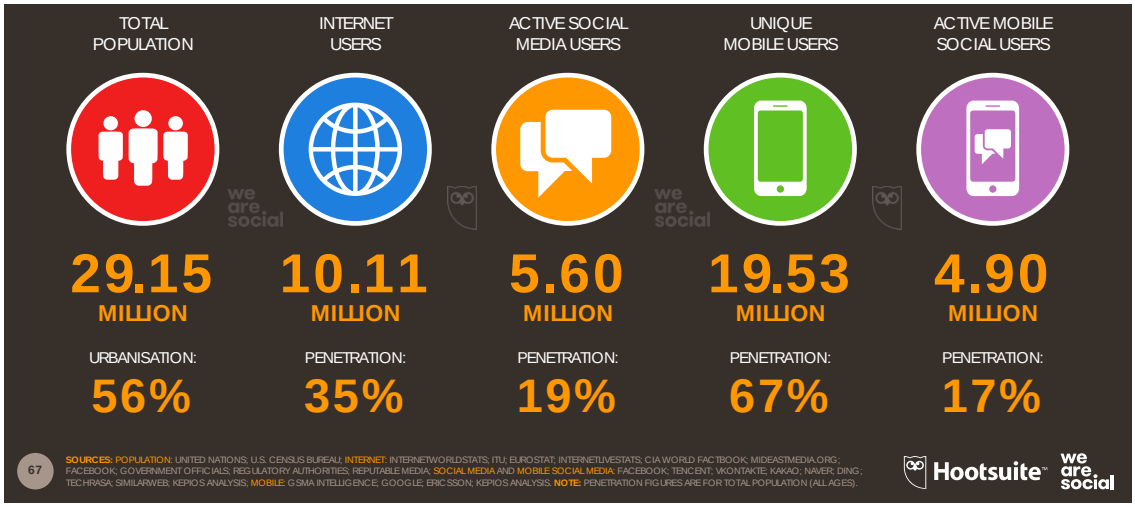
Over the last five years, South Africa has engaged in a modernization effort of its national ID system and has been issuing 10 million smart ID cards in an attempt to replace the 38 million bar-coded ID cards. It is projected that they will all be replaced with smart IDs by 2023. More recently, South Africa also announced the launch of its new Automated Biometric Identification System (ABIS), which will initially integrate with the existing Fingerprint Identification System but will eventually use facial and iris recognition and serve immediately as the new foundation for the National Identification System.

At any rate, the current ID system is robust enough to support a credentialing system.

Ghana

In Ghana (population: 29 million), mobile penetration has soared to reach a total of 34.57 million mobile subscriptions, corresponding to a penetration rate of 119% and a total of almost 20 million unique users.

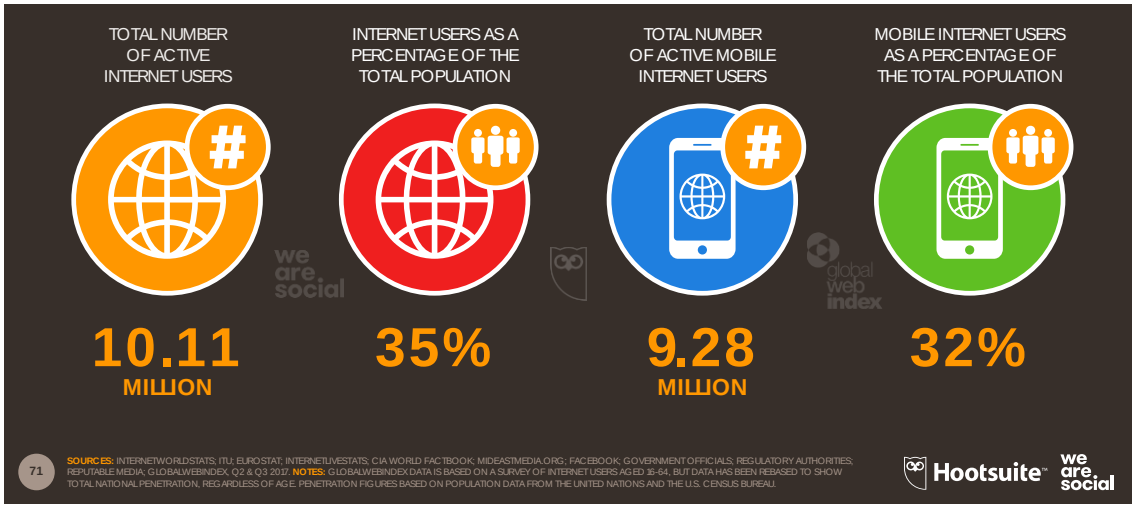
Internet penetration has also increased to reach 35%, with over 10 million Internet users (nearly a third of the country) now having access to the Internet, exceeding the overall penetration rate in Africa that is currently at 34%. This is an increase of 2 million on the figure recorded in January 2017. Ghana is also on the path of a massive social media revolution with 17% of the population being active.



Source: Hootsuite, Digital in 2018 in Western Africa

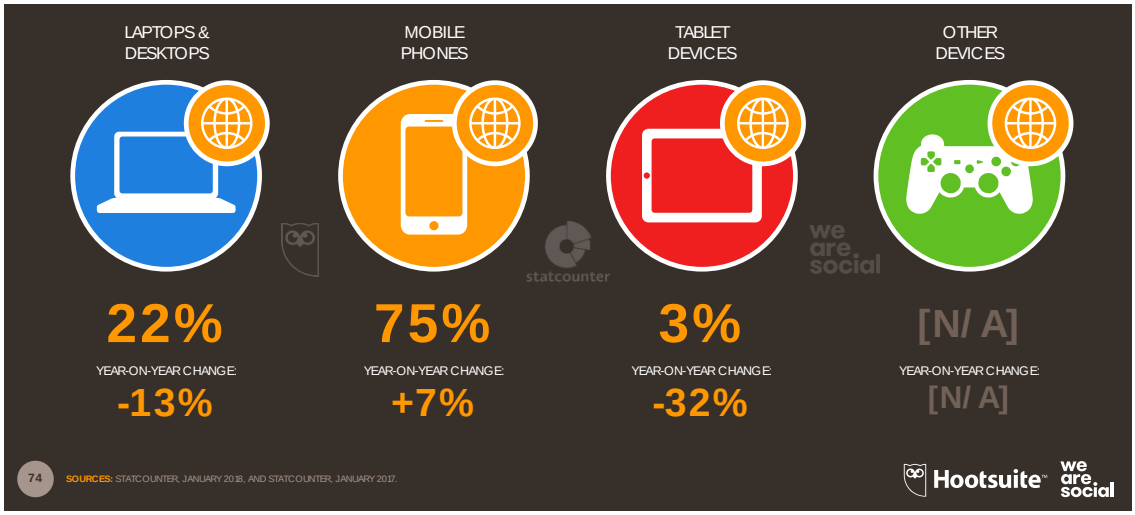
Internet use is mostly mobile

The following chart shows that most Internet users are mobile, similar to the other markets. It is confirming the fact that Africa is becoming a mobile only market, leapfrogging every other technology as we know in mature markets.



Source: Hootsuite, Digital in 2018 in Western Africa

In terms of share of web traffic, it is interesting to note (see chart below) that 75% of Internet traffic is already mobile in 2018. This trend has been significantly growing over the last few years and it is projected that Ghana will become a mobile first country, with most Ghanaians favouring mobile phones over laptops and other devices to access the Internet.

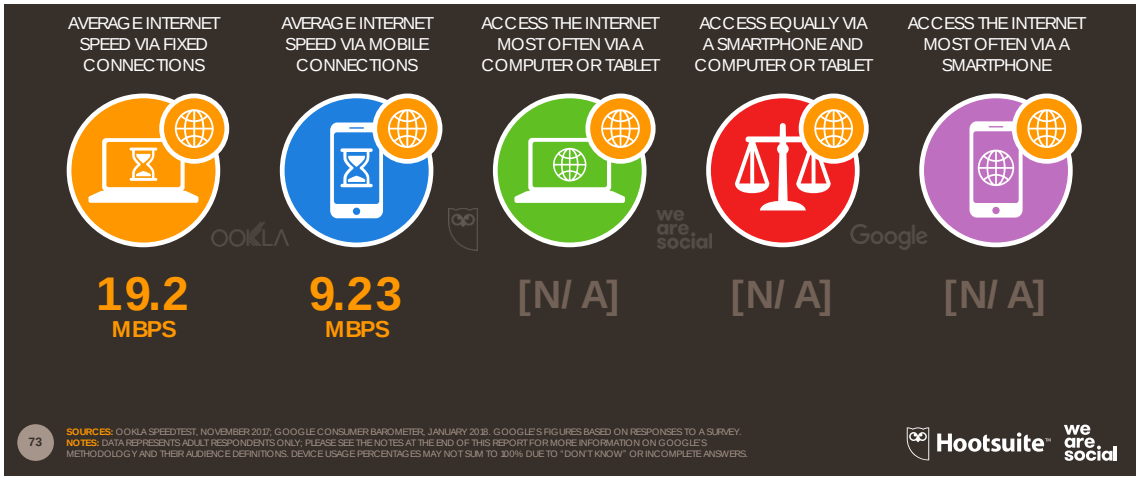


Source: Hootsuite, Digital in 2018 in Western Africa

Smartphone and feature phone usage is becoming popular

Over the last few years, smartphone prices have significantly dropped in Ghana, from USD 219 in 2014 to an average price of USD 65 in 2017. This has really helped increase smartphone penetration in Ghana and will likely continue to boost smartphone usage over the next few years.

Mobile internet speed is acceptable for simple digital content



Source: Hootsuite, Digital in 2018 in Western Africa

Mobile Internet speed has been improving and is at the levels that enable good user experience, particularly considering that most Internet activity is centred on social media.

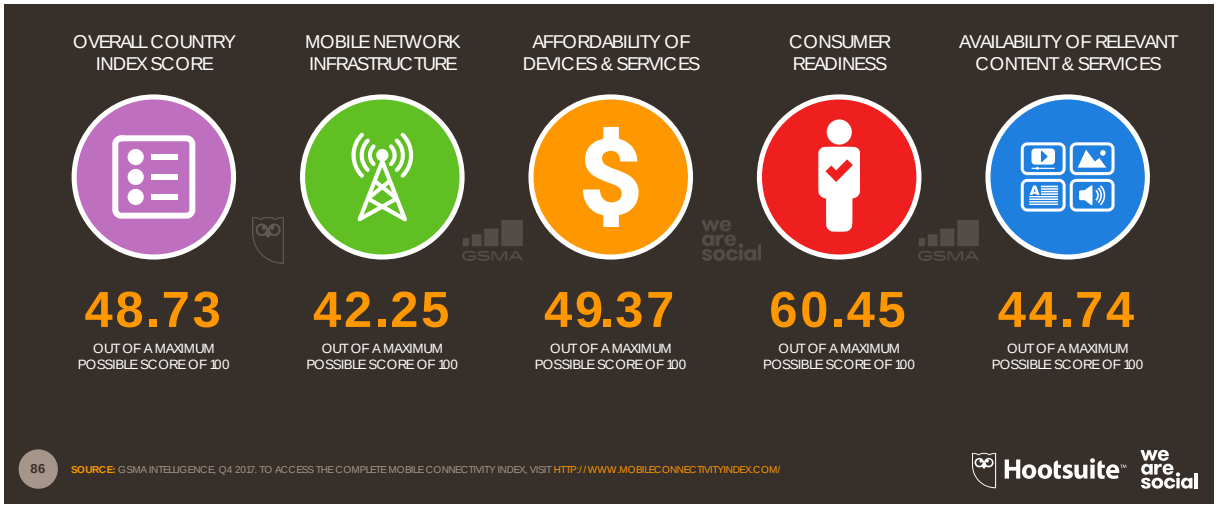
The tech scene in Ghana

The Ghanaian tech industry has flourished over the last few years, and tech innovation has started to reach various sectors like energy, agriculture, banking, healthcare, and transport. Ghana's main incubator, the Meltwater Entrepreneurial School of Technology is regularly hosting events like the Africa technology Summit while start-ups like Farmerline are leveraging analytics and big data to better serve farmers.

In the meantime, the blockchain space has also been developing rapidly to the extent that Ghana Dot Com launched a Blockchain Academy, a professional training program aiming at developing talent pool in the blockchain space. Enthusiastic individuals have organized themselves around a Blockchain Society; start-ups like Bitland are offering land title registry solutions based on blockchain in a country where 90% of agricultural lands are still unregistered with the Land Commission of Ghana; and new companies like Token media are providing marketing solutions to nascent blockchain projects, like already a few clients like PIVX, Komodo, Local World Forwarder and SmartCash, with already more than $40 million raised in token sales. Other start-ups have also emerged in recent years, like BTCGhana, allowing Ghanaians to receive bitcoin remittances directly in their mobile money wallets in Cedis.

GSMA mobile connectivity assessment for Ghana

Against the GSMA mobile connectivity index, Ghana rates fairly high especially on the consumer readiness front. This is clearly an indication of the transition that the country has gone through.



Source: Hootsuite, Digital in 2018 in Western Africa

National ID Infrastructure in Ghana

Ghana is also in the process of reforming its Identity Management System and is planning to issue new cards to citizens over a period of 1 year. There will be 2 types of cards:

1. 2D barcodes: issued to children under 15 years. There are currently 12 million such cards in stock that will be distributed rapidly.
2. Smart ID card for all other citizens: these will meet all international quality standards of a smart card (ICAO, ISO), will include an e-passport profile to allow travel in the ECOWAS region and will be interoperable with telcos and other institutions. It also relies on a Public Key Infrastructure for data protection.

In the meantime, all other forms of identification remain valid (driving licenses, National Health Insurance Cards, baptismal certificates, voters identity card) and are heavily used by financial institutions and mobile money providers to identify their customers. There are currently 12 million active mobile money accounts that have been identified using these valid forms of ID. Current systems and processes can also be used for verification purposes in the credentialing context.

Annex 4: A Primer on the blockchain

This Annex is positioned as a primer on the blockchain for readers with little previous knowledge of the technology, and its potential application in the credentials context. It levers on research and proprietary material, and is meant to be read as a 'stand-alone' annex: inevitably, issues discussed here are also discussed in other parts of the document

In recent years the term 'Blockchain' has almost entered every household, popularized by its native and wildly hyped cryptocurrency Bitcoin, but the underlying technology is frequently misunderstood. This section introduces the describes some of the basic components of the technology[16], and how businesses - and the education sector in particular - may benefit from it. As a relatively recent innovation in computer science, blockchain is a global, cross-industry and disruptive technology which is forecast to fuel the growth of the global economy for the next several decades[17]. It is also a divisive concept in that it challenges stated norms[18].

What is the blockchain?

The following high-level definition provides a quick introduction to the subject:

In its simplest form, a blockchain is a **distributed electronic ledger** that provides a mechanism for a community to record and exchange information.

In this community, each member maintains his or her own copy of the information and all members must validate any updates collectively.

The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form.

Entries are permanent, transparent, and searchable, which makes it possible for community members to view transaction histories in their entirety.

Each update is a new "block" added to the end of a "chain."

A protocol manages how new edits or entries are initiated, validated, recorded, and distributed. With blockchain, cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole.

Unlike databases maintained by a centralized authority that guarantees data integrity through its proven trustworthiness and practices, blockchains are records of transactions that are replicated across many systems (or nodes) and are cryptographically guaranteed to be immutable. In the public blockchain that bitcoin uses, this immutability is guaranteed by cryptographic hash functions and a clever consensus algorithm that requires blockchain miners to solve puzzles; in doing so, they validate blocks of records, which are then accepted into the blockchain (McArthur, 2018).

(16) Also see: https://www.coindesk.com/information/how-does-blockchain-technology-work/

(17) The World Economic Forum (2015) estimates that by 2025 at least 10% of the world's GDP (USD 100 trillion) will be managed via Blockchain technologies, and half of that will be in the form of a crypto-currency.

(18) Turner (2018) identifies '187 things the Blockchain is meant to fix'.

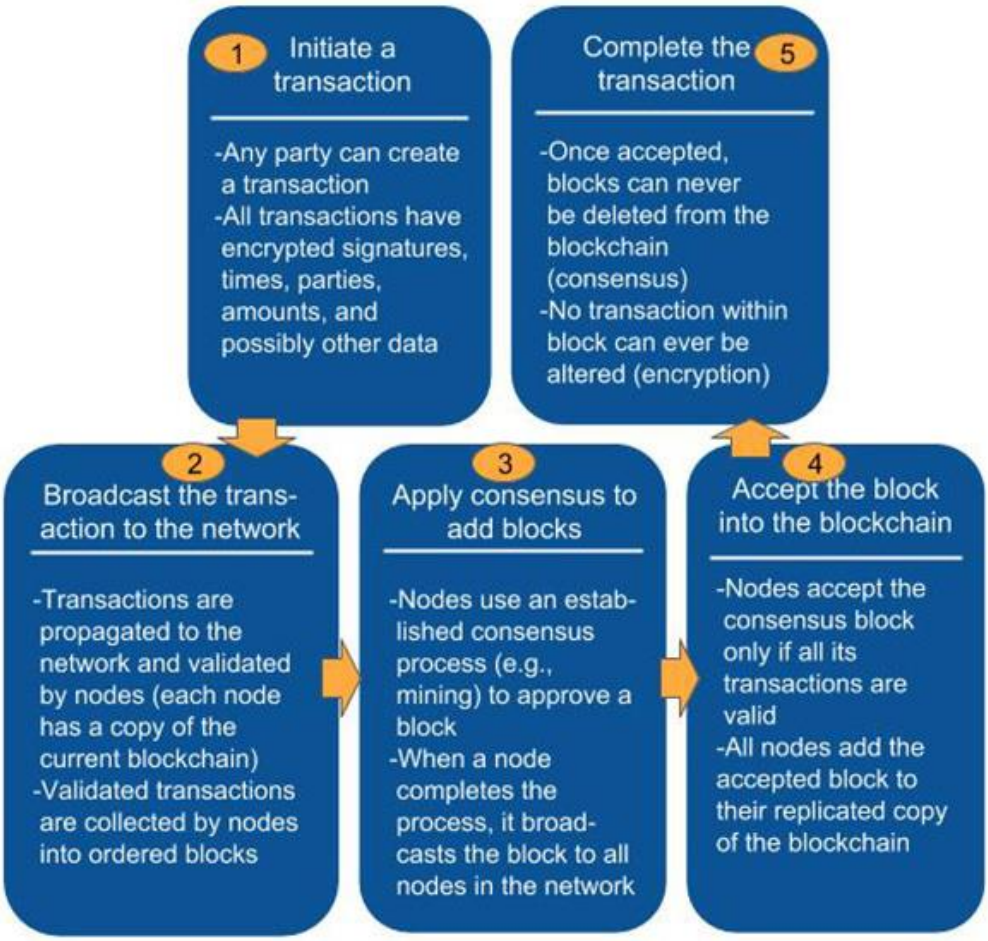


Figure 7: Steps in the Blockchain Approach

Source: McArthur (2018)

The ledger can always be written onto with new information, but the previous information, stored in blocks, cannot be edited or altered. This is achieved by using cryptography to link the content of the newly added block to the previous blocks (each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data) in a way that any change to the previous blocks would also invalidate the data in all the future blocks.

Thus, a well-defined process manages how new entries are initiated, validated, recorded and added as a new 'block' at the end of the 'chain', and that process replaces third-party intermediaries as the keeper of trust between the participants. In that respect, the blockchain contains a true, immutable and verifiable record of each and every transaction ever made between the participants or in the community.

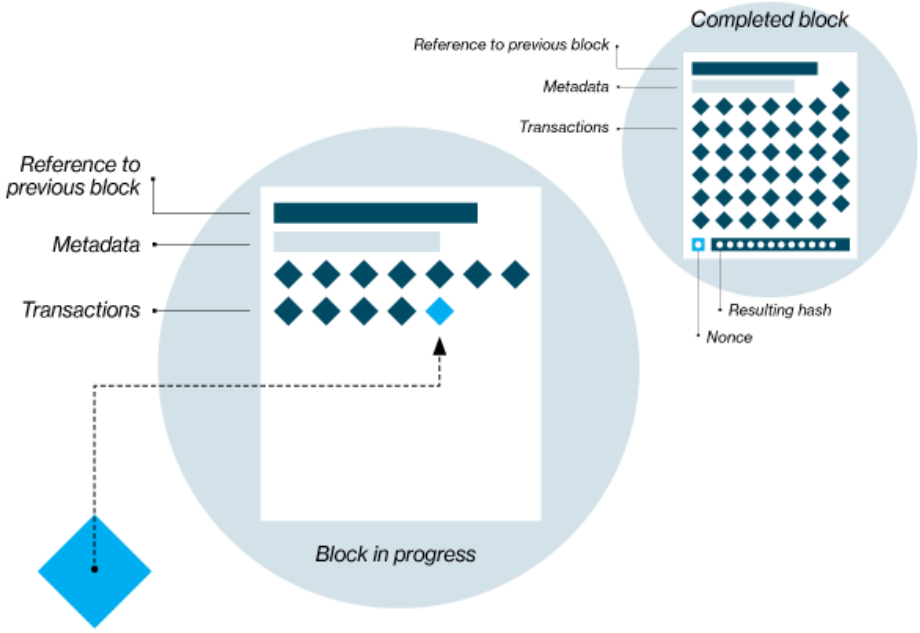


Figure 8: An overview of a blockchain

Source: MIT Technology Review (2018)

Blockchains are consensus-driven: each participant maintains its own copy of the ledger and any updates must be validated collectively. This is achieved by having a subset of participating computers ('miners') compete to solve a labour-intensive mathematical problem to be able to add information to the chain. Once the problem solved, the result (or 'proof of work') must be shared by the first miner to solve the problem with all other computers on the network for them to agree on the solution, hence the 'consensus'. That miner then gets the right to update the ledger with the new entry and all other computers will subsequently update their copies of the ledger accordingly. This ensures that appending data to the ledger remains decentralized and that no single entity can control the information that is on the blockchain.

The information that is stored on the ledger usually represents an asset such as a transaction, a title deed, a contract, an identity, a vote, a medical record or anything that can be represented in digital form.

There have been experiments with blockchains since the early 1990's, but it was only in 2008, with the release of a white paper by an individual or group of individuals operating under the pseudonym of Satoshi Nakamoto that blockchains gained wide adoption. The first well-known blockchain was the Bitcoin blockchain, which is also the name of the first widely used, decentralised cryptocurrency. "Bitcoin" also refers to the network protocol underlying the cryptocurrency. In terms of the popular vernacular, the Bitcoin blockchain is automatically associated with 'the Blockchain' when in practice, there are other blockchains of significant importance, such as the Ethereum blockchain.

Ledgers

Ledgers are tools by which one can determine the owner of an asset at any point in time since they serve as an authoritative list of transfers of the asset in question. For any community using a ledger to determine ownership of a particular asset, all that is required to transfer ownership between two parties is to make an entry in the ledger indicating that this transfer has happened.

This simple concept of keeping an authoritative list of transfers of an asset, enables the systematic transfer and accumulation of capital, and as such has been referred to as the essential technology that makes capitalism possible (Windjum, 1978; Yamey, 1949).

There are many challenges that come with traditional ledgers. The organization that physically owns or controls a public ledger, including the infrastructure in which the ledger is stored, is in a position of significant power and influence. Specifically, the owner of the ledger may:

- Decide whether to record a transaction, which in turn provides this organization with the ability to:
  - Impose conditions for individuals to have their transactions recorded; and
  - Decide on the system of controls to be applied to check accuracy of those transactions
- Modify or delete transactions that are already in the ledger;
- Destroy the ledger entirely or allowing it to be destroyed.

Since under such a system, writing, modifying or deleting a transaction in the ledger also changes the ownership of the object, the person or Organization controlling such ledgers also wields significant influence by effectively controlling who owns what - simply by being the custodian of the list of transactions.

The responsibility of keeping accurate ledgers has traditionally been assigned to a variety of institutions: governments control ownership of land by controlling ledgers of property; banks control the world's monetary system by holding the ledgers for currency; while stock exchanges control large shares of the business world by holding ledgers for business - ownership. Since capitalist societies are built around the concepts of sale and ownership (the transfer and accumulation of capital), there are great responsibilities associated with the custodianship of ledgers.

The corollary is that these institutions may individually or collectively cause significant harm or even social chaos by abusing the trust placed in them to accurately keep and maintain these ledgers. The inference is that these institutions have the power to use or abuse their control over the ledgers and exert significant control over individuals and societies within their immediate remit.

Blockchain as a ledger

The most widely known application of the blockchain has been as a ledger of transactions for cryptocurrencies, providing a record of the provenance and transfer of ownership of a cryptocurrency. To identify who owns an asset, once simply needs to consult the ledger to check who is its most recent owner.

The transactional structure of blockchain protocols in fact facilitates the transfer not only of cryptocurrencies but also of any type of digital asset and addresses a number of market inefficiencies and limitations around costs, delays in executing contracts, taxes, regulations, bureaucracy, involvement of intermediaries and so on.

Levering on Gupta (2017), some of the market frictions that can be alleviated by blockchain include:

1. **Information frictions:**

a. Imperfect information: participants in a transaction don't have access to the same information, resulting in information asymmetry and unfair advantage in favour of one party. Information may also be incorrect, leading to bad decisions and reconciliation delays.

b. Inaccessible information: relevant data is not captured, stored, analysed and shared due to the abundance of information and technical limitations in capturing or even accessing the data.

c. Information risks: hacking and cybercrime are on the rise, creating more concerns around counter-measure costs and brand reputation damage

Blockchain has unique properties that can help reduce these frictions: it shifts the paradigm from information held by a single entity to a shared lifetime history of a digital asset (shared ledger). All participants can have access to transactions and validate identities and ownerships without needing third-party intermediaries, and each participant can be given access to information based upon their roles and access rights (permission) and can transact with other members in confidence that the person they are dealing with is who they claim to be. Unauthorized access is prevented through advanced security measures (cryptography) and transaction validation is performed collectively (consensus).

2. **Interaction frictions:** these are mostly related to the number of intermediaries that is required in business transactions where the degree of separation between parties involved is high.

   Blockchain provides the ability for every participant to operate without the need of an intermediary, whether they are exchanging an asset of sending the shared state of a task that needs to be moved along its life cycle, saving on cost and delays and enabling business decisions to be made according to the pace of each participant.

3. **Innovation frictions:**

a. Institutional inertia: internal processes and legacy systems, compounded with human resistance to change, can affect an Organization's ability to innovate

b. Regulations: regulations, while necessary, can also introduce delays related to compliance and other processes

Blockchain can enable a level of automation that improves business processes, including regulatory processes, and saves the organization time and money while supporting more innovative business models.

Since they are primarily designed to record and preserve transactions, all blockchains have had a cryptocurrency attached to them as the most basic asset transacted in the network and as a way to incentivize contributors to the network by paying them in the network's own cryptocurrency.

The other characteristics of a blockchain such as security, immutability and programmability generally depend on the architecture of the blockchain and the consensus protocol that is being used on that blockchain. These technical characteristics often underpin a broader set of social principles (the 'social value proposition') that also define that very blockchain's social utility and ethos.

Social value proposition of blockchains[19]

Blockchain is often quoted as a technology that has the potential to disrupt a number of industries but it was primarily conceived to deliver social value in response to a number of socio-economic drivers, which are probably as important as the digital technology itself. History shows us that the digital business models that have been the most successful were the ones that best understood people and social factors, like in the case of M-Pesa in the Digital Financial Services Space.

Adapting the core arguments in Byrne (2017), Gupta (2017), Hanson et. al (2017), Morabito (2017) and Piscini et al. (2016), it becomes possible to extract the following social value principles of blockchain technology.

Self-Sovereignty and Identity

The early literature on blockchain makes frequent references to 'self-sovereignty', and the individual's ability to own and control his or her own identity online (Lilic, 2015; Allen, 2016; Smolenski, 2016b) and be the final arbiter of who can access and use their data and personal information. Within an educational context, this would mean empowerment of individual learners to own, manage and share details of their credentials, without the need to call upon the education institution as a trusted intermediary.

This can also be thought of as citizens acquiring significant 'self-authority' over the way personal data and identity is shared online and being able to choose to release all or parts of it in return for access to services they want – *without the need of constant recourse to a third-party intermediary* to validate such data or identity.

> *Identity is… [the basis for] trust and confidence in interactions between the public and government; it is a critical enabler of service delivery, security, privacy, and public safety activities; and it is at the heart of the public administration and most government business processes. How identity information is collected, used, managed, and secured is of critical interest to leaders in the public sector" (Government of Canada)*

Identity is complicated territory for citizens and those who need to verify it: it is the verification of personal attributes, personal history, relationships and/or transactional histories[20]. Digital identity is verging on a human right. Yet there has yet to be a fail-safe method to deal with one of the flaws of the internet - identifying people or machines online[21]. When citizens are obliged to, or agree to divulge their online identity, new problems are created, such as the use of private algorithms to maximise the commercial use of users' personal data on social media. In Africa, there has been many questions raised by the use of digital footprints and personal data collected through smartphone apps in order to assess the credit worthiness of otherwise underserved customers and offer them loans. In markets where customers are less educated about their privacy rights and the appeal of the services being offered is strong enough, the question of whether customers are giving way too much personal information becomes very acute.

---

(19) This section is primarily replicated from Grech and Camilleri (2017).

(20) According to Hanson et. al (2017), the assessment of identity is used to minimise any perceived gap in trust. This gap is proportional to the measure of risk, which reflects the perception of the identity and any potential losses. *The trade-off is often a loss of privacy in exchange for access to high value transactions.* The downside has historically been the loss of privacy where the transaction is asymmetrically of moderate to minimal value to the individual being vetted compared to the risk presented to the other party. In order to verify certain attributes of their identity to complete the transaction they also expose other attributes of their identity they may not wish to disclose. This disclosure places all of their attributes, on that document, at risk of further unwanted disclosure or illegal use.

(21) See https://qz.com/989761/microsoft-msft-thinks-blockchain-tech-could-solve-one-of-the-internets-toughest-problems-digital-identities/

Technology is fundamentally changing our perception of ourselves, and along with it of identity and trust. The cryptography at the core of blockchain technology promises to address identity lacunae and 'wrestle' the ownership and control of personal data back to the individual user. People, businesses and institutions can store their own identity data on their own devices and provide it efficiently to those who need to validate it, without relying on a central repository of identity data and for the amount of time that they so desire. Blockchain technology does not just provide a new way of digitising bits of paper which have an intrinsic value, such as our credentials – it provides us with the means to take control of our identity online and manage it appropriately for further information on the affordances of the Blockchain to credentials and certification).

In its most advanced form, self-sovereignty may eventually depart from the sharing of anything like a permanent "identity," but instead become a system of verifying claims. In other words, rather than soliciting extraneous information, querying parties will instead request only information that is immediately pertinent to the transaction at hand: Is the individual over the age of 18? Did they receive a PhD in Neuroscience from MIT? Are they a citizen of Italy? Once verified satisfactorily, claims can then be retracted by the subject[22].

Trust

An influential UK Government study[23] suggests that trust is a risk judgement between two or more people, Organizations or nations; and that in cyberspace, it is based on two key requirements:

a) **Authentication** – *prove to me that you are who you say you are*;

b) **Authorisation** – *prove to me that you have the permissions necessary to do what you ask.*

If one of the parties is not satisfied with the response, they may still choose to allow the other party to proceed, but they would be incurring risk. However, there is no viable relationship unless the parties trust one another. In this sense, being trustworthy in a society is analogous to being creditworthy.

This basic concept of trust remains unchanged in the digitised world where we have to rely upon many actors, whom we will never meet, to act in good faith and on our behalf: trust is often granted only for a very specific application, within a specific context, and for a set period of time. In a global, digital economy, the challenges of maintaining trust - with the resultant checks and balances – are becoming increasingly expensive, time-consuming, and inefficient[24].

Blockchain technology might provide a viable alternative to the current procedural, Organizational, and technological infrastructure required to create institutionalised trust. The improved trust between stakeholders is associated with *the use of decentralised public ledgers as well as cryptographic algorithms that can guarantee approved transactions cannot be altered after being validated*.

The distributed ledgers contribute to trust by *establishing a fact at a given point in time*, which can then be trusted. They achieve this by automating the three roles of the trusted third-party: a) *validating; b) safe guarding* transactions; and c) then *preserving* them.

(22) See Andreas Antonopolous in the "ADISummit: Self-Sovereign Identity Panel." Available at: https://www.youtube.com/watch?v=DZbyiJqKT8c

(23) Government Office for Science, UK (2016)

Transparency and Provenance

Ease of sharing, visibility and traceability are essential features of a blockchain; they are particularly critical in transactions in which more than one Organization is making entries into the database.

Blockchains enables participants to track the origins of each asset or record and how its ownership has changed over time by linking transactions to an identifier. Without a public identifier, such as a linked document or serial number, blockchain transactions cannot be decoded and tracked. In this way, blockchains—even "public" blockchains—are private by default but can also be used to track transactions of specific individuals over time via linked "off-chain" data.

With Blockchain technology and the underlying cryptography linking every block to the previous ones, the shared ledger provides a single place to determine the ownership of an asset or the completion of a transaction.

Immutability

> An immutable record is an unchangeable record whose state cannot be modified after it is created.

Immutability is interlinked with security, and its classic properties of confidentiality, integrity and availability. Immutability is also about resilience and irreversibility. Blockchain data cannot be easily changed because it is continually replicated across many different locations. With private and public key cryptography as part of blockchain's underlying protocol, transactional security and confidentiality become virtually unassailable.

The immutability of blockchains means that it is essentially impossible for changes to be made once established: this in turn increases confidence in the integrity of the data and reduces the opportunities for fraud. For a transaction on a blockchain to be considered valid, all participants in the transaction must agree on its validity nodes or "peers" running the blockchain protocol must come to consensus on the transaction's validity.

Furthermore, no participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to rectify the error, and both transactions are then visible in the ledger. Blockchain resilience stems from its structure, since it is designed as a distributed network of nodes in which each one of these nodes stores a copy of the entire chain. Hence, when a transaction is verified and approved by the participating nodes, it is virtually impossible for someone to change or alter the transaction's data. Attempts to change data in one location will be interpreted as fraudulent and an attack on integrity by other participants, with the result that it will be rejected.

Disintermediation

By replacing middlemen with mathematics, blockchain also can go some way towards maintaining trust (Piscini et al. 2016). Participants on a blockchain are linked together in a marketplace where they can conduct transactions and transfer ownership of valued assets with each other in a transparent manner and without the assistance or intervention of third-party mediators or intermediaries. A value network operates without a defined central authority.

With blockchain technology, peer-to-peer consensus algorithms transparently record and verify transactions without a third-party - potentially reducing or even eliminating cost, delays, and general complexity. For instance, blockchains can reduce overhead costs when parties trade assets directly with each other, or quickly prove ownership or authorship of information — a task that, is otherwise currently next to impossible without either a central authority or impartial mediator. Greater decentralisation of the internet would place more

control in the hands of the user—or more specifically, the user's devices—instead of relying on clouds platforms operated by the likes of Google or Amazon.

Types of records stored on blockchains

Blockchains are typically used to store records of:

1. Asset transactions
2. Smart contracts
3. Digital signatures and certificates

Asset transactions

Records of assets have been discussed previously. They generally take two forms:

- Money, expressed in units of a currency: each single unit of a currency has the same value as every other unit of the same currency at any one time. Currencies are also intra-convertible at an exchange rate. The most common forms of currencies built on blockchains are Bitcoin and Ether.
- Documentary evidence of ownership rights, known as title deeds. These are commonly used to represent immovable property such as land or intangible property such as intellectual property

Smart contracts

Smart contracts are pieces of code that are stored on a blockchain and facilitate the automation of transactions based on pre-defined business logic: they are designed to self-execute themselves when specific conditions are met, for example 'transfer X to Y if Z occurs', without further involvement of any of the parties involved in the transaction or any other third-party. The promise represented by smart contracts is that once an industry's important digital records are verifiable, a whole new ecosystem of automation can thrive that will produce a new social fabric that enables civic efficiencies, personal mobility, and institutional transformation.

Certificates and digital signatures

In its most essential form, certification is the issue of a statement from one party to another that a certain set of facts are true.

Signatures are proofs that the statement was issued from and to the said parties. Blockchains can be used to either store cryptographic hashes ("digital fingerprints") of the certificates, or to store the claims themselves. Thus, a blockchain can take on the function of a public certificate registry.

Technical characteristics of the blockchain

There are three principal technologies that combine to create a blockchain, and one of these are new. Rather, it is their orchestration and application that is new. These technologies are:

1. Private key cryptography;
2. A distributed network with a shared ledger; and
3. An incentive to service the network's transactions, record-keeping and security.

This section describes some of the characteristics and features of blockchain technology which are pertinent to tech-enabled credentials.

Distributed ledger

A centralized ledger is a single, authoritative list of transaction records. A good example of this is a national land registry, where a central database is stored and executed on a single node. Various regions might share some responsibility vis-a-vis the central registry and capture data for their respective jurisdictions in order to populate the central database, but all of that ultimately results in a central database of national land information and if the central server goes down, its database becomes inaccessible.

Decentralization completely removes that central authority by:

1. Allowing several participants to retain a copy of the entire ledger
2. Defining how changes or updates are made to the ledger through consensus from the participants who have copies
3. Every change is recorded in each copy of the ledger, thus making each copy equally authoritative (Peters & Panayi, 2016)

The implication of such a distributed system is that the network can only go down if all of its nodes go down, making it virtually always available.

Cryptography and hashing

The blockchain protocol protects data stored in the ledger from fraudulent manipulation by ensuring that each block contains a cryptographic hash of the previous block. A hash is a short code of defined length that acts like a digital fingerprint for a document or asset. It is usually produced using a hash generator and produces the same output (the hash) if the input string is identical. Any small alteration in the input string would result in a totally different hash ID. A hashing process is a one-way process: a hash generator can generate a hash from a document but it is impossible to generate a document from a hash. This is the way that a blockchain ensures that none of the transactions are modified or tampered with since each new block includes a hash of the information block as well as of the previous blocks.

Identification via public / private keys

Each participant in a blockchain is identified with a public / private key pair. The public key is a string that constitutes a publicly available ID number and identifies a person. A private key is a password that is mathematically linked to the public key. When a user authenticates on a blockchain using their public key, they also enter their private key into the blockchain software to verify that both are truly mathematically linked. The user can then write a new transaction, i.e. initiate a transfer of asset that is linked to his/her public key by also entering the private key that is linked to that public key.

The function of issuing tat pair cannot run in reverse. It is practically impossible to generate the private key knowing the information about the public key.

Public and private, open and permissioned

Blockchains are also characterized by a set of rules and governance principles that are encoded in their software. These define the types of assets that will be traded, under which conditions the trades happen, and who is allowed to participate in these trades.

From a technical perspective, each device that is part of the blockchain network (and is running the software) is a node that is connected to the other nodes running the software. If anyone can set up a node and participate in the network, it is generally called a public blockchain. In that sense, all cryptocurrency blockchains are public blockchains.

Furthermore, when anyone is able to add data to the blockchain, it is considered being open. If permissions are required to add data to the blockchain, then it is permissioned.

In some case, there are restrictions as to who can set up a node and transact with the other participating nodes and only specific devices can participate to trades that only occur within a closed user group. This is called a private blockchain. Implementations that are usually limited to an enterprise or an enterprise and its limited group of business partners / suppliers are usually ran on private blockchains. The same distinction applies when referring to open and permissioned blockchains[25].

Software integrity

The architecture of the blockchain ensures software integrity, which means that only identical copies of the blockchain software can interact with each other. When a copy is changed, it creates a totally different chain that has forked from the original one, which is why it is known as a 'fork'. There have been multiple forks since the introduction of the Bitcoin protocol, giving birth to Bitcoin Cash and Bitcoin Gold for instance.

Software integrity ensures that all devices on the network can trade with each other without the need of any third-party.

Blockchains do not 'talk to each other'

Blockchain technology is still in its relative infancy. The optimism related to its potential for accreditation of education, formal and informal learning needs to be tampered with the realities of early-stage technology. We may compare the technology to the early days of the internet where there were several separate technical approaches to constructing computer networks (see Hardjono, 2018). Like then, he says, they key to moving things forward lies in figuring out how to make these individual systems work together.

In the 1970s and 1980s, a combination of academic and US military research led to the construction of a common infrastructure that allowed individual networks to share resources, especially in the event that one of the networks was attacked. We know it as the internet protocol suite, which includes the transmission control protocol (TCP) and the internet protocol (IP)—the bedrock of today's internet.

Hardjono (2018) argues that today's blockchain developers should borrow a concept from the internet protocol suite called the datagram, which is a common unit of information that can move across different networks. A startup called Aion is working on answering that question. The company is developing what it calls "token bridge" that will let holders of Ethereum-based tokens back up their assets on another blockchain—initially, one built and run by Aion—without duplicating the actual monetary supply. The process relies on a group of computers, also called nodes, that have the ability to recognize valid transactions and write new ones to each chain. The nodes that form the bridge will also have a process for reaching agreement amongst themselves and deciding whether to respond to a certain transaction on one of the chains by executing a corresponding one on the other.

A significant difference between the pre-internet days and the blockchain world is the money: today's competing protocols are often backed by billions of dollars of investment. That will probably ensure that many will succeed, meaning the future may be ruled by numerous blockchains – in which case interoperability will be key to mainstream adoption. Whatever we end up with, it probably won't look like the internet—but it could be just as transformative.

(25) The most popular examples of permissionless blockchains are Bitcoin and Ethereum. Public permissioned blockchain include Sovrin. For examples of private permissioned blockchain see Ethereum Enterprise, Hyperledger, Bigchain DBconsortiums and Blockchain HELIX)

GDPR and blockchain

The General Data Protection Regulation passed by the European Union in 2016 has now come into full force and will affect any company holding data relating to private EU citizen independent of the base of that company. While this regulation is currently limited to the EU and may have no relevance to the Africa context, it is likely that other jurisdictions will follow suit and get inspiration from it, if not simply copy it, posing challenges in the context of blockchain implementations (Toth, 2018; Blockchain Bundesverband (2018).

The most challenging issue raised by GDPR with regards to blockchain implementations is the 'right to be forgotten': EU residents must be able to request that their data be transferred to another data storage provider or simply be deleted. This is obviously something that cannot be achieved on a public blockchain:

1. Data stored on blockchains is immutable and tamper-proof, which will make deletion a challenge;
2. Blockchains are distributed, which limits control on the data that is stored on them;
3. Smart contracts are by definition automated decisions and may be contested.

There are a few options that could be investigated to ensure compliance with GDPR requirements. Levering on Blockchain Bundesverband, 2018; and Chainfrog, 2017:

1. Blockchains can be built that require permission to read the information on the blockchain, limiting the parties who can transact on the blockchain and establish can serve the network by writing new blocks into the chain. Ripple, for instance, runs a permissioned blockchain. The startup determines who may act as transaction validator on their network, and it has included CGI, MIT and Microsoft as transaction validators, while also building its own nodes in different locations around the world.
2. A blockchain developer may choose to make the system of record available for everyone to read, but not allow anyone to be a node, serving the network's security, transaction verification or mining. This could become a mix-and-match situation.
3. With permissioned blockchains, this may or may not involve 'proof of work' or some other system requirement from the nodes. There is some politics around this, as there are those who consider private blockchains that do not use any proof of work (that is, blockchains with no mining) not to be blockchains at all, but simply shared ledgers.
4. Record personal data only pseudo-anonymously: blockchains (such as Bitcoin for instance) allow individual data to be recorded pseudo-anonymously. In that scenario any of the data stored must not enable anyone to identify the person behind the data (phone numbers, IP addresses etc).
5. Encrypt the data: if the data stored on the blockchain is encrypted, the destruction of the decryption key would be equivalent to the deletion of the data since the data would not be accessible anymore. This approach carries some risks but could be explored.
6. Store the data in a referenced encrypted database: store the data on a private encrypted database instead of on the blockchain itself. A hash of the data can be included on the blockchain to ensure that the data in the database has not been tampered with. Copies of the decryption keys for the data could also be encrypted and stored on the blockchain and deleting data would then equate to deleting the relevant entries in the database.
7. Ensure that all smart contracts have a roll back option or secure explicit consent when a user wants to activate a smart contract.

There are just initial thoughts about the implications of GDPR and how they could be addressed. Should the Foundation decide to proceed with a pilot, these considerations may well need further investigation and discussion with policy-makers.

Annex 5: Technical Characteristics of Credentials

Advantages and Challenges of Different Credentials Architecture

The following table is replicated from Borhene and Keevy (2018). It explains how decisions on the technology of the credentials architecture have an impact on scope, functionality, mobility, security, trust, privacy and participation.

ARCHITECTURE	***SCOPE & FUNCTIONALITY***	***MOBILITY***	***SECURITY, TRUST & PRIVACY***	***PARTICIPATION***
CENTRAL REPOSITORY	**A central** database containing credential data is populated by education providers. Employers and other third parties check data using an **online web lookup**.	Student is **not** part of the digital process, so does not have a digital artefact per se, and cannot control access to their online record.	For **privacy**, student consent is either **implied** (as the record is provided by the education provider) or **paper-based** (where the third party needs to prove that they have student consent to verify by uploading a signed consent form). A central datastore increase risk of attack / **security** breach. To establish **trust** in the service, communications by education providers with third parties are key to adoption.	The simplified workflow makes the systems easier to build and therefore participate in. However, participants ultimately **need to populate data into repository**. Technical complexity of participation usually depends on the complexity of the data needed by the repository.
EXCHANGE NETWORK	**A secure B2B network** between education providers	Sometimes providers send records directly to	**Being a closed network** by definition, participants are known	Because implementation involves technical data standards and exchange

	enabling them to **send and receive** records.	other providers **without** student involvement. Consent is either implied, or students can initiate the 'push' of records themselves **via systems connected to the network.**	and vetted, enabling **trust**. **Underlying secure communication protocols** for exchange means that participants can be sure that what they receive is authentic.	protocols, **the technical bar to participation is relatively high** for education providers to send via the network. It is usually easier to receive via vendors.
HUB & SPOKE	**Hybrid of (1) distributed repositories (one per school)**, connected via (2) an **exchange network, with (3) student and third party** portals and (4) an external **integration** hub.	**Students have 24 x 7 access** to, and control over, access to their records. **Zero intervention required** by education providers in order for students to share records with a third party.	**Education providers** each maintain their own repositories. **Cryptographic signing plus access control** ensure record security, authenticity and integrity. **Student** controls who can access their record and for how long. **Various methods of verification** via the network or via a trusted web portal.	Participants ultimately **need to populate data into their repository**. Complexity is dictated by the data to be exported. Simpler alternatives available (PDF) where data is difficult to export.
BADGE FRAMEWORK	**Badges** are images (PNG files) with embedded data according to an open standard. **Supporting workflow** elements defined for issuing, receiving and verifying badges.	Students **store** and **control** the sharing of their badges. Badges are **fine-grained**, shareable and stackable credentials.	Badges are trusted usually based on **where they are hosted** or **cryptographic signing** by the issuer. **Endorsement**/Web 2.0 model. **Anybody can issue a badge for anything**.	It is easy to **issue** badges so participation is straightforward.

			This has created a negative perception of badge trustworthiness in a formal context.	
PUBLIC BLOCKCHAIN	**Hashes of records** are written to a public blockchain by education providers. The **records** themselves are given to the student. **Third parties verify** the records received from students against the public blockchain.	Student **possess the record** themselves and therefore control sharing of it. Verification requires that students must **never** use (a) their blockchain wallet keys and (b) their **records**. **A cost of decentralisation** is that education providers lose their digital connection with alumni and cannot easily collect mobility statistics as credentials are use.	Blockhain confirms that the owner of cryptographic Key A issued a particular record to the owner of Key B at Time T. It does **not** confirm that an education provider is who they claim to be. **Comprehensive verification** requires additional layers sometimes involving verification **via the issuer's website which contradicts the blockchain paradigm**. Blockchain depends 100% on **cryptography** and therefore the security off issuers' private keys are vital. Quantum computing may pose a threat to current blockchain algorithms ECDSA by 2027. Quantum Resistant Ledger Technology is a work in progress.	It is easy to **issue** records onto a blockchain so participation is simple for education providers. **Blockchain only handles verification** of records – the exchange and archival of credentials require complementary solutions to be built. The **participation burden shifts to the student** as they now have the responsibility of maintaining their records and keys in the long term.

Technical Characteristics of a Credential

Technical characteristics are those which arise from the standard and technological medium of the credential. Several characteristics are actually a combination of the standard and technology. The table below explains these characteristics:

Characteristic	***Definition*** **(The credential should…)**	***Standardisation aspect*** **(The standard for issuing the credential should…)**	***Technology aspect*** **(The technology for issuing the credential should…)**
Measurability	represent an identifiable and measurable experience, skill or fact	define the measurement and description system used by the credential	N/A
Uniqueness	represent a distinct experience, skill or fact, attributable to the holder	define a way to uniquely identify the specific credential	not allow for the holder to make new original copies
Personal	be attributable to a single, identifiable person	define the method of ensuring who the credential is intended for	include a mechanism to only allow use by its intended holder
Security	not be falsifiable	N/A	not permit the holder to issue or modify a credential
Verifiability	allow for its authenticity to be verified	include a way to keep evidence of the issue of the credential	N/A
Self-Provability	be proof of its statement, in and of itself.	N/A	allow for the authenticity of the credential to be verified without resort to third parties
Immutability	not be changeable	ensure that the statement remains true for the period of validity of the credential	ensure that the credential cannot be edited.
Revocability	be withdrawable	specify under which conditions a credential may be withdrawn	allow a credential to be revoked by the issuer

Stackability	allow for credentials of the same type to be added together to form a greater whole	describe standardised unit to be used by the credential	allow for credentials to be issued in a standardised format
Transferability	allow for conversion into different credentials	describe how credentials may be transformed into other credentials	allow for a credential to created out of a set of other credentials
Collectability	allow for the holder to control and physically possess it	N/A	permit the user to store the credential themselves in a place of their choosing
Standardisation	always be issued with the same characteristics under the same conditions	define a reproducible procedure for the issue of credentials	N/A
Transparency	be backed up by published standards and evidenced	be published	allow for the credential and its standards to be linked
Recognisability	be available in a language and format that allows for wide use and acceptance;	be issued in a widely-spoken language	be issued in a widely-used and/or open format
Traceability	allow for the conditions which led to the issue of the credential to be audited	include clear processes for taking and keeping records	allow for credentials to be linked with the evidence of their issue
Shareability	be easily shareable	N/A	allow for the credential to be easily shared with a third party, and returned or reclaimed by the holder
Affordability	have low issue and verification costs	N/A	be low-cost
Robustness	be supported by reliable technology		the technology used to issue, display and share the credential should be always available

Comparison of Technologies for Credentialing

CHARACTERISTIC	DEFINITION *(THE CREDENTIAL SHOULD…)*	TECHNOLOGY ASPECT *(THE TECHNOLOGY FOR ISSUING THE CREDENTIAL SHOULD…)*	PAPER	DIGITAL UNSECURED	DIGITAL PKI	NOTARIZED BLOCKCHAIN	ISSUED ON BLOCKCHAIN
UNIQUENESS	represent a distinct experience, skill or fact, attributable to the holder	not allow for the holder to make new original copies	Original copies easy to make	Original copies easy to make	Nearly impossible to make original copies	Nearly impossible to make original copies	Nearly impossible to make original copies
PERSONAL	be attributable to a single, identifiable person	include a mechanism to only allow use by its intended holder	Not possible	Not possible	Possible	default	default
SECURITY	not be falsifiable	not permit the holder to issue or modify a credential	easy to falsify	easy to falsify	Nearly impossible to falsify	Nearly impossible to falsify	Nearly impossible to falsify
SELF-PROVABILITY	be proof of its statement, in and of itself.	allow for the authenticity of the credential to be verified without resort to third parties	Not possible	Not possible	Possible	Possible	Possible

IMMUTABILITY	not be changeable	ensure that the credential cannot be edited.	Cannot be edited but can be destroyed	Can be edited and destroyed	Cannot be edited but can be destroyed	Cannot be edited or destroyed	Cannot be edited or destroyed
REVOCABILITY	be withdrawable	allow a credential to be revoked by the issuer	Cannot be revoked	Cannot be revoked	Can be revoked	Can be revoked	Can be revoked
STACKABILITY	allow for credentials of the same type to be added together to form a greater whole	allow for credentials to be issued in a standardised format	Cannot be stacked	Can be stacked	Can be stacked	Cannot be stacked	Can be stacked
TRANSFERABILITY	allow for conversion into different credentials	allow for a credential to created out of a set of other credentials	Cannot be converted	Cannot be converted	Cannot be converted	Cannot be converted	Can be converted
COLLECTABILITY	allow for the holder to control and physically possess it	permit the user to store the credential themselves in a place of their choosing	Can be fully controlled and held by user	Can be fully controlled and held by user	Can be controlled and held by user but relies on external verifier	Can be fully controlled and held by user	Can be fully controlled and held by user
TRANSPARENCY	be backed up by published standards and evidenced	allow for the credential and its standards to be linked	Does not allow linking	Allows for linking	Allows for linking	Allows for linking	Standards inbuilt into chain

RECOGNISABILITY	be available in a language and format that allows for wide use and acceptance;	be issued in a widely-used and/or open format	possible	Possible	Possible	Possible	Possible
TRACEABILITY	allow for the conditions which led to the issue of the credential to be audited	allow for credentials to be linked with the evidence of their issue	Not possible	Possible	Possible	Possible	possible
SHAREABILITY	be easily shareable	allow for the credential to be easily shared with a third party, and returned or reclaimed by the holder	Sharing is possible physically or by making copies	Sharing is possible	Sharing is possible	User can detail conditions under which credential is shared	User can detail conditions under which credential is shared
AFFORDABILITY	have low issue and verification costs	be low-cost	High cost	Effectively free	Medium cost	Medium cost	Medium cost
ROBUSTNESS	be supported by reliable technology	the technology used to issue, display and share the credential should be always available	No real availability limitations	Very little availability limitations	Requires centralised certificate issuers to be running.	Only requires any node on the network to be running	Only requires any node on the network to be running