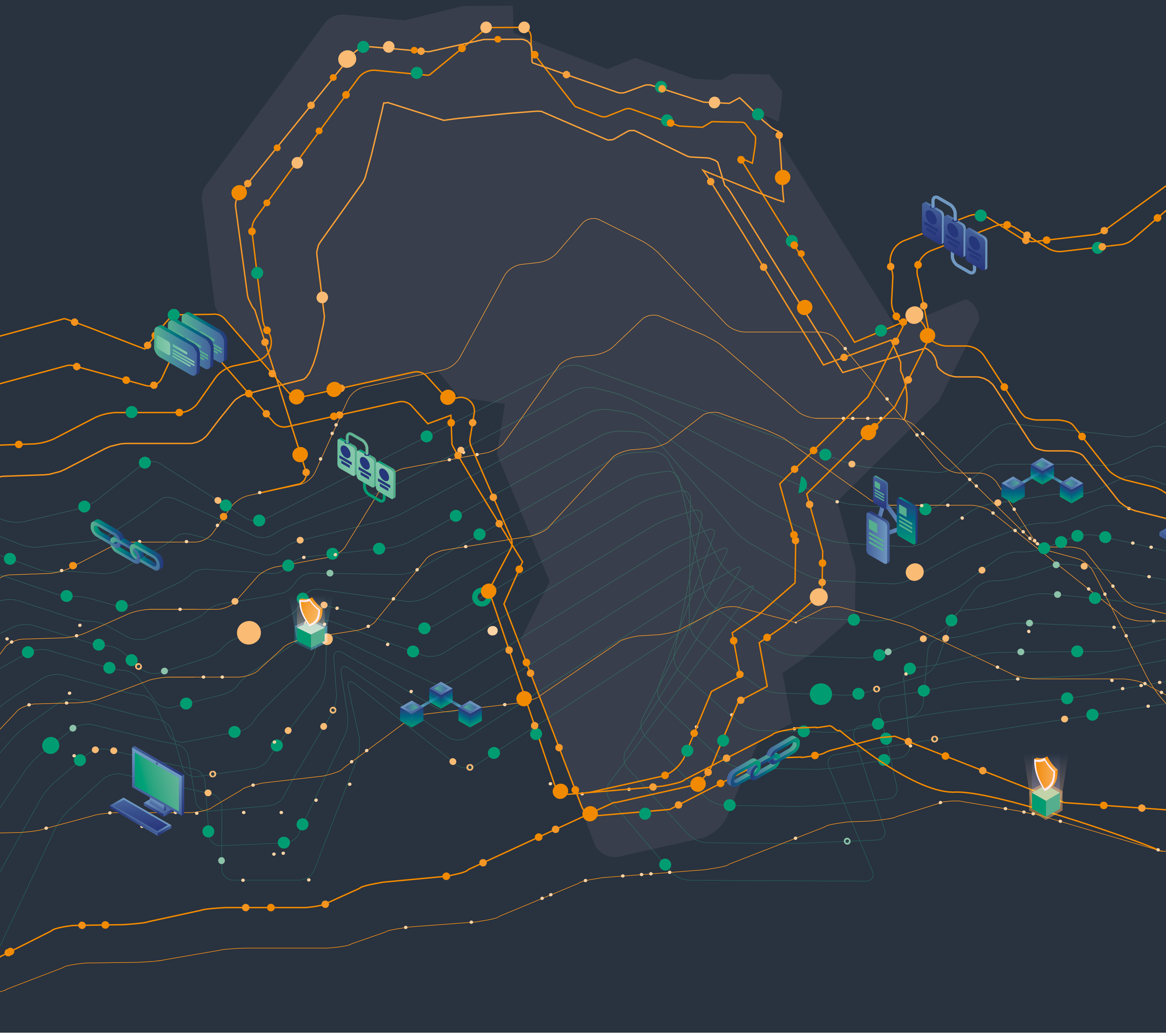
BLOCKCHAIN IN AFRICA:

OPPORTUNITIES AND CHALLENGES FOR THE NEXT DECADE

How African countries can take advantage of distributed ledger technologies as they are maturing



smart africa

CONNECT. INNOVATE. TRANSFORM

LIST OF ABBREVIATIONS

AML	Anti-money laundering
BIS	Bank for International Settlements
CBDC	Central bank digital currency
CDD	Customer due diligence
CFT	Counter terrorism financing
DLT	Distributed ledgertechnologies
FATF	Financial Action Task Force
INATBA	International Association of Trusted Blockchain Applications
KYC	Know your customer
RAPDP	African Data Protection Network *Réseau Africain sur la Protection des Données*
SME	Small and medium enterprises

german
cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

**Edited by Olivier Gakwaya, Dr Uta Meier-Hahn,
Dr Ralph Oyini Mbouna and Lars Wannemacher**

The Smart Africa Secretariat (SAS) and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) would like to thank the following authors who contributed to this white paper: Theodor Beutel, Olivier Gakwaya, Maike Gericke, Jonas Gross, Florian Henrich, Atilla Kaiser-Yuecel, Jan Krewer, Dr Uta Meier-Hahn, Benjamin Onuoha, Dr Ralph Oyini Mbouna, Dr Jörg Pohle, Dr Nina-Luisa Siedler, Lars Wannemacher, Sara Weiss, Franz von Weizsäcker

Kigali, Rwanda, 2020.

TABLE OF CONTENTS

PREAMBLE

Blockchain technologies have been finding real-world utility across Africa and the world at large over the last few years. The concept of blockchain is still getting traction daily and use-cases are still being understood as innovators and innovation ecosystems define new ways of bringing blockchain technologies into the real world. What we can be certain of is that these technologies have immense potential for addressing some challenges that Africa faces.

There are key principles that are inherent to blockchain, such as transparency, and decentralization which on the surface, can address many of Africa's challenges. From elections, to international remittance, as well as energy services and alternatives to banking; Africa has many developing systems that could benefit from this technology.

The purpose of this paper is to proffer a critical assessment of these technologies in order to understand them better. This in turn helps us to understand the potential use cases. We delve into essential use cases within this document related to key verticals that form the digital economy and Africa's immediate digital agenda. These include key aspects such as digital payments, governance, public spending and trade facilitation among others.

Its is important to offer a critical view of blockchain technologies and to be objective about what can work in Africa and what cannot work. We need to be certain that the use of blockchain does not amount to the surrendering of sovereignty and data protection rights. The technology we adopt must enhance Africa's progress towards a single digital economy.

At the end of it all, this paper gives a number of recommendations based on the understanding we have collectively developed.

We thank our partners from Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and a committed team from the Smart Africa Secretariat for the work they have put into this paper. It is through strategic partnerships such as these, that we will achieve great strides in our journey towards a single digital market.

Mr Lacina Koné
Director General of Smart Africa

EXECUTIVE SUMMARY

Few technologies have oscillated between public appreciation and depreciation, between hype and caution as much as as blockchain technology has since its inception roughly a decade ago. This paper offers a fresh view on blockchain technology as it is maturing. The purpose is to inform African decision and policy makers about viable use cases and about the policy choices that need to be made in order to take full societal advantage of distributed ledgers and related technologies.

As part of this paper, we look at blockchain with a focus on its key characteristics and remaining shortfalls that inform the following use cases. Besides drawing on the actual practicability of the specific use cases based on the technology as to date, we also considered the maturity of existing use cases in our selection. Now, we gathered those use cases that, at this point in time, appear most feasible, promising or as in the case of digital payments politically pressing for the African continent. The use cases are:

- Digital payment infrastructures, including central bank digital currencies,
- Public spending and governance,
- Peer-to-peer energy trading,
- Digital claims to land ownership,
- Digital claims to education credentials,
- Tracing agricultural goods along supply chains and
- Trade facilitation.

This list of use cases is far from being comprehensive. The innovation ecosystems constantly bring up novel applications of blockchain and combinations with various other technologies such as internet of things and artificial intelligence as well as common databases. The relevant topics of digital ID and, related, self-sovereign identity will be addressed in depth in a separate publication by the Smart Africa Secretariat.

> "Blockchain-based systems are neither generally compatible nor incompatible with regulatory dimensions of data protection, anti-money laundering and counter-terrorism-financing."

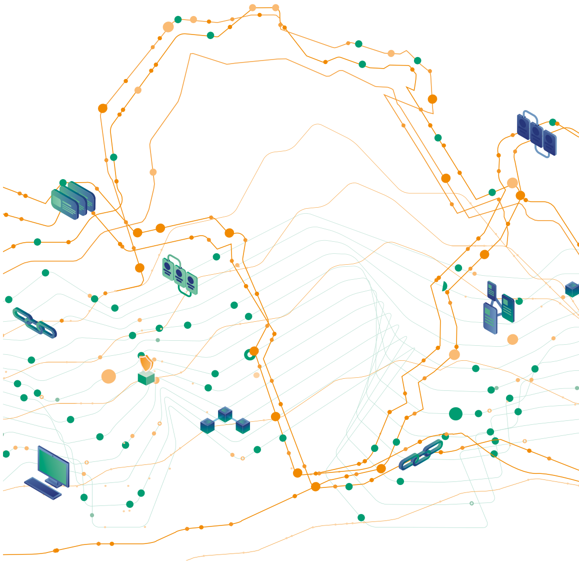
To inform African decision and policy makers, a bird's eye view on the interlinkage of blockchain technology into legislative and financial frameworks is required, to enable its continued and safeguarded use on the continent. A key component for such safeguarding are questions on the compatibility of blockchain technology and data protection on one hand and anti-money-laundering as well as counter-terrorism-financing on the other. We argue that blockchain-based systems are neither generally compatible nor generally incompatible with these regulatory dimensions. Still, the technology can be at tension with several themes that are central issues in data protection, including objectives chosen by the legislator, "secrecy" versus "transparency", "remembering" versus "forgetting" (or a "right to be forgotten"), updates and corrections, data subjects' rights, and regulatory oversight and enforcement - all of which are looked at within the scope of this paper.

In summary, any approach to regulate blockchain technology should commence with a clear consensus on regulatory objectives that are based on the particular positions of the governments involved. From there, regulatory means to realise these objectives can be drawn.

We conclude this report with the following recommendations to African decision and policy makers:

- **Strategy:** develop a pan-African blockchain strategy in accordance with the African Union's digital strategy.

- **Data protection harmonisation:** seek pan-African harmonisation of data protection by negotiating consensus on the regulatory goals. Leave regulatory means to individual countries while creating a



mechanism for mutual recognition of data protection laws. Mandate public authorities for monitoring and enforcing data protection laws, equip them with the necessary powers and resources.

- **Blockchain-specific considerations for data protection:** decide about policy options at the intersection of data protection and blockchain technology according to the values and policy goals of individual countries and the African community, not according to real or perceived technical constraints. Establish "data protection by design" provisions in data protection laws.

- **Financial regulation:** develop a pan-African concept for token classification, including security tokens, tokens representing financial instruments such as e-money and unregulated tokens. Create disclosure and registration regimes for security tokens. Introduce license regimes for service providers concerning security and other financial instruments tokens.

- **Capacity building:** support research and education about blockchain technology and blockchain governance. Foster skills, develop talent and stimulate innovation.

- **Push for interoperability and harmonised standards,** specifically to enable interconnectivity between different blockchains.

1. INTRODUCTION: BLOCKCHAIN TECHNOLOGY IN A NUTSHELL

Blockchain technology describes a new way of data handling. It refers to a specific form of distributed ledger architecture, which stores transactions in a list of blocks, which are linked cryptographically. Due to their similar use in the public discourse and despite the slight imprecision, the terms distributed ledger technology (DLT) and blockchain are being used interchangeably in this paper.

> "Digital ledgers, including blockchain, brought about a major change as lists of transactions are no longer stored in one central location."

Blockchain follows in a long tradition of physical and digital accounting technologies. Historically, traders used books of lists (i.e. ledgers) to track the goods they bought, sold and traded (i.e. transactions). In modern times, these ledgers became more diverse, as they included account balance sheets, cadastre systems or identity records. Until recently, however, they remained centralised, meaning that one entity was in control over the system - be it records on paper or in digital form. Digital ledgers, including blockchain, then brought about a major change as lists of transactions are no longer stored in one central location. Instead, multiple parties share control over simultaneously maintained copies of the same ledger.

An in-depth technical explanation of blockchain or DLT at large would go beyond the scope of this paper.[1] Additionally, for decision and policy makers the most important concepts to conceive are the characteristics of blockchain that make it appropriate for new private and public use cases. It also must be noted that no blockchain system exists in isolation. In order to provide many of the features noted below, any blockchain requires a trustworthy governance model.

In light of the purpose of this paper - which is to inform decision and policy makers about opportunities and preconditions for the implementation of blockchain technology - and acknowledging that there is not one genuine and universal definition of blockchain, we offer the following working definition of blockchain technology before looking at some specific properties, i.e. distribution, public and private blockchains, immutability, incentivisation and automation.

Working definition: A blockchain is an append-only list of transactions which are stored in blocks and secured through cryptography. A decentralised peer-to-peer (P2P) network of computers is processing, verifying and validating all entries.

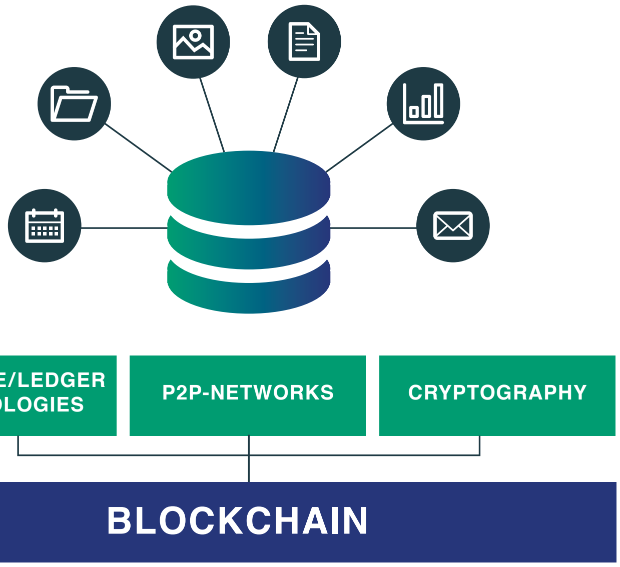


Figure 1: The technologies behind blockchain

[1] This chapter is particularly informed by Bogensperger, A., Zeiselmair, A. and Hinterstocker, M., 2018. *Die Blockchain-Technologie - Chance zur Transformation der Energieversorgung?*. Forschungsstelle für Energiewirtschaft e.V. (FfE). Available at: https://www.ffe.de/attachments/article/803/Blockchain_Teilbericht_Technologiebeschreibung.pdf [Accessed 8 May 2020].
For conceptual differentiation see e.g. Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., Vagneur, K. and Zhang, B., 2019. *Distributed Ledger Technology Systems: A Conceptual Framework*. Campridge Centre for Alternative Finance. Available at: http://dx.doi.org/10.2139/ssrn.3230013 [Accessed 8 May 2020].

1.1 Core features

Distribution: Blockchains are designed to be physically dispersed. The entries on a blockchain do not sit on a single server, e.g. of a bank or government agency, but are at the same time distributed across many computers that form a network. This means that original copies of the same data are stored in different locations. Even if part of the network goes down, the ledger remains accessible to all other participants in the network. In fact, unless all nodes in the network go down, the integrity, availability and operability of the ledger as a whole is maintained. This is a strong resilience property. Imagine proof of educational claims remaining easily available even if a university's server is destroyed in a natural disaster.

In order to ensure that these copies of the same data are fully identical and synced in real time, blockchain technology makes use of various consensus mechanisms. This enables participating parties of the network to computationally find consensus on what information is stored on the blockchain, and, thereby, put trust in the system and in one another without actually having to know the other participants in the network. Thanks to these consensus mechanisms[2] - and depending on their formulation - blockchains work without a centralised entity, e.g. an administrator managing the ledger.

Public vs. private, permissioned vs. permissionless blockchains: The attribute of distribution holds especially true for public permissionless blockchains.[3] By design, these blockchains operate on the open internet and allow for anyone to read, write and verify transactions by operating a node in the network. Public permissioned blockchains meanwhile are also accessible on the open internet, but they limit the ability to verify transactions to a selection of participants or by certain conditions. The openness of public blockchains potentially makes for a high degree of architectural and political decentralisation[4] and making them maximally resilient to malicious adaptation. In contrast, private, so-called federated/consortium/syndicate distributed ledger networks are managed by one or a number of entities that may limit read-and-write access of the blockchain and determine the ruleset for verification.[5]

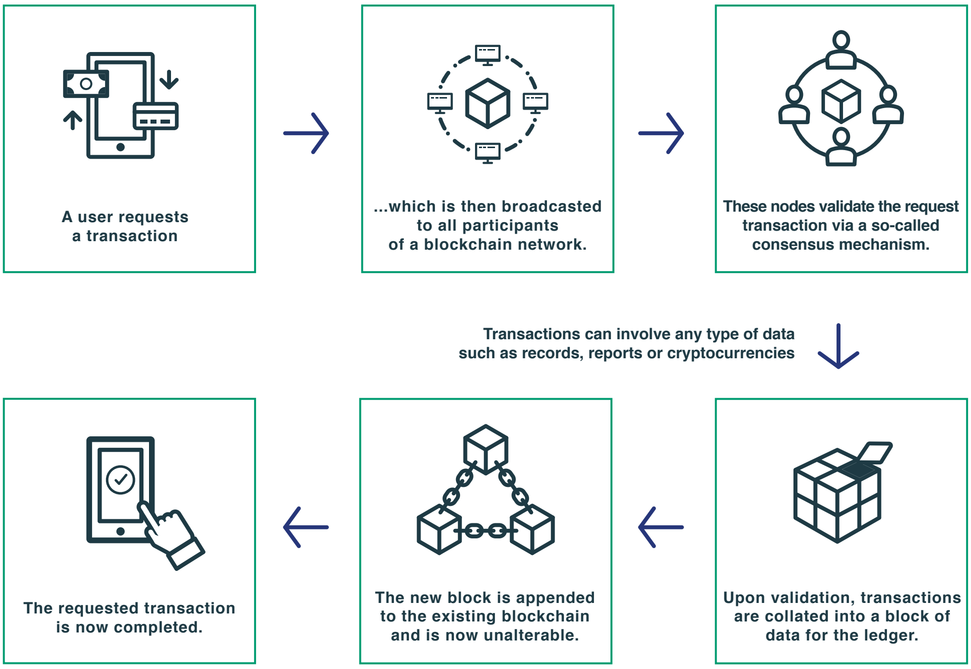

A user requests a transaction
...which is then broadcasted to all participants of a blockchain network.
These nodes validate the request transaction via a so-called consensus mechanism.
Transactions can involve any type of data such as records, reports or cryptocurrencies
Upon validation, transactions are collated into a block of data for the ledger.
The new block is appended to the existing blockchain and is now unalterable.
The requested transaction is now completed.

Figure 2: Transactions on a blockchain

[2] The most common consensus mechanisms currently include so-called Proof-of-Work, Proof-of-Stake and Practical Byzantine Fault Tolerance.

[3] Prominent examples of public blockchains are the Bitcoin blockchain - best known for the associated cryptocurrency -, and the Ethereum blockchain.

[4] Vitalik, B., 2017. *The Meaning Of Decentralization.* Available at: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [Accessed 8 May 2020].

[5] Prominent private blockchains are Hyperledger Fabric and Quorum; a large federated blockchain is the R3 Corda Network.

Immutability: Once a transaction is confirmed by the participating parties and written into the ledger, the protocol does not allow for any changes to be made after-the-fact. This is on the one hand due to the distributed logic and consensus mechanisms of the ledger, but also based on the particular structure of a blockchain. Here, new information is saved in self-referencing blocks that are added to an add-only chain [see Figure 2]. Previously stored information is not overwritten, and retrospective manipulation is nearly impossible in public and permissionless blockchains. The particular data structure of distributed ledgers and blockchains ensures the integrity of each individual ledger entry and the accuracy of the ledger as a whole. Any attempt to alter the data ex-post would be rejected by the consensus rule, and the attempt itself would become visible to all participating parties. This ensures an extremely high level of data integrity in public/permissionless blockchains. Immutability means that high data quality is particularly important in blockchain systems.

Incentivisation: In order to foster the trust in the status of the ledger that blockchain is widely praised for, the technology may rely on incentivisation mechanisms that encourage network participants to behave positively. As part of a blockchain's consensus mechanism, for example, participants may be rewarded (economically) when positively contributing to the system (i.e. by processing and validating transactions). An example for this reward system is the Bitcoin blockchain, where successful validation of new transactions is rewarded in the payout of bitcoins. In other scenarios, negative incentivisation is also possible, as participants are discouraged from malicious behaviour that would ultimately harm the system and themselves. Such incentivisation schemes, born from game theoretical principles, are a core characteristic of public/permissionless blockchain protocols. They can also be adapted for a variety of scenarios and use cases. By representing certain economic rewards or real-world goods in the form of digital tokens and by defining clear means to earn these tokens, participants of a blockchain can be encouraged to behave in desirable manners. An example of this are community coin systems that reward the purchasing of local goods instead of imported products.[6]

Automation: Unlike a centralised database held by a single entity, a blockchain continues to run even if individual participants or machines stop participating in the network. Just like the availability of stored data does no longer depend on a single machine within the network, the processing of code does also no longer run on a single computer or server. Instead, code can run directly on a blockchain, following the logical iterations that it was programmed to process: If transaction A has taken place, then transaction B will automatically be executed. This capacity is also known as smart contracts. Running such an if-then-statement independently from a centralised processing unit or server enables a new level of automation through blockchain technology.

1.2 Known limitations

A number of technical challenges remain as obstacles to a more widespread uptake of blockchain across sectors. Surely, this can be attributed also to the maturity of blockchain as a technology, which is continuously growing with further use cases across the globe.

Scalability: Currently, the number of transactions that can be executed per time unit on most blockchains is very limited. Due to the size limitations of individual new blocks on the chain and the redundancy of linked previous blocks, the speed of processing transactions is comparably low. Therefore, scaling blockchain-based projects to industry-scale is a key challenge that needs to be addressed or worked around.

Privacy: Most blockchains do not currently provide sufficient levels of privacy as required for government and enterprise applications. While the major public blockchains reveal data and metadata publicly and permanently, many private and permissioned blockchains allow some form of privacy. For instance, data may be public among the members of a particular blockchain consortium, but private to non-members. However, private and permissioned blockchains may not provide for the level of trust and immutability and heavily rely upon their off-chain governance structure to ensure reliability of their content.[7] Moving forward, both private and public blockchains are expected to enhance privacy based on so-called zero-knowledge proofs.

[6] See Gericke, M., 2019. *New Report Release: Community Currencies.* PositiveBlockchain.io. Available at: https://positiveblockchain.io/new-report-release-community-currencies/ [Accessed 8 May 2020].

[7] Off-chain governance refers to the rules that determine the operation of the blockchain system itself (governance of the infrastructure), whereas on-chain governance refers to rules such as incentivisation or smart contracts that are directly encoded into the blockchain (governance by the infrastructure).

Interoperability: To little surprise, the young technology has not seen sufficient streamlining through standards across sectors and industries. This leaves businesses with difficult decisions on the use of specific blockchains that are currently not interoperable. While projects are working towards an increase in interoperability, achieving this as an industry-wide standard will require additional time.

Infrastructure: Logically, any blockchain-based system will rely on the existence of functioning and reliable infrastructure, including internet connectivity. While the choice between a variety of blockchains (e.g. private vs. public) may to some degree alleviate this precondition, it remains a key factor of consideration for any implementation - especially in the African context.

> "The field of blockchain development remains in flux and is rapidly changing."

In addition to these technical challenges, blockchain technology also commonly faces a number of difficulties in its application due to its technical characteristics and their contextualisation in the real world. This specifically entails the following problems:

The digital representation of assets, also known as the **oracle problem:** Representing material and immaterial assets that are not yet in a digital form is an overarching difficulty across sectors. It needs context-specific solving before blockchain technology can be applied successfully. Examples include the traceability of assets in supply chains, e.g. for fashion, pharmaceutical drugs or agricultural goods.

Data quality: Strictly speaking, blockchain technology ensures data integrity and not data quality. The data stored on a blockchain is only as accurate as it was when entered. Especially as data cannot be retrospectively changed, high standards on data quality are required in the application of blockchain technology. In many scenarios, the entry of such high quality data onto the blockchain poses a particular challenge.

Smart contracts: The automation that blockchain offers by allowing lines of code to be directly programmed on-chain also comes with its own caveats. As the processed code can no longer be amended after it was stored on the blockchain, it needs to fulfil the highest quality standards - similar to data entered on-chain. However, experience of software development proves that programming bug-free code is virtually impossible. Considering this, the lacking ability to fix badly designed smart contracts or to update them when external factors make it poses a further complication for the use of smart contracts.

Integration: Blockchain systems can be difficult to integrate within existing system landscapes. It is thus necessary to include the integration with legacy systems into the technical design choices. Advances towards open, interoperable standards serve this goal.

As much as these limitations should be evaluated within the context of any blockchain-based project, one cannot overstate how the field of blockchain development remains in flux and is rapidly changing. Therefore, a look at the already feasible use cases and an outlook into the nearest future to ensure enabling environments for soon-to-be-realised approaches remains worthwhile.

2. THE EMERGING BLOCKCHAIN TECHNOLOGY ECOSYSTEM ON THE AFRICAN CONTINENT: USE CASES AND EXAMPLES

The main characteristics of blockchain technology - distribution, immutability and automation - can underpin both economic growth and social progress because they complement each other in a way that fosters trust in distributed ledger systems. There is no single point of failure or capture; records are tamper-proof; parties ideally have a shared interest in maintaining the system and automation prevents human error once information has entered the system. When put to operation with a solid off-chain governance model, this can lead to trust in transactions performed without the need of an intermediary.

> "The main characteristics of blockchain technology - distribution, immutability and automation - can underpin both economic growth and social progress."

For this report, the comprehensive PositiveBlockchain.io database conducted original research identifying a total of 69 active projects or completed pilots that apply blockchain technology for their focus on social good while servicing parts of the African continent. These statistics are relevant, because in the African project landscape, commercial benefits and social impact often go hand in hand[8]. Of these impact-focused projects, 57% have their headquarters on the continent, with the highest number of projects headquartered in Kenya, South Africa and Nigeria. Most projects with a core focus on social good are for-profit startup initiatives, followed by non-profit initiatives and public-private partnerships, the latter often including governmental initiatives and/or initiatives of key industry players. A blockchain ecosystem has started to emerge.

KEY PROJECT CATEGORIES

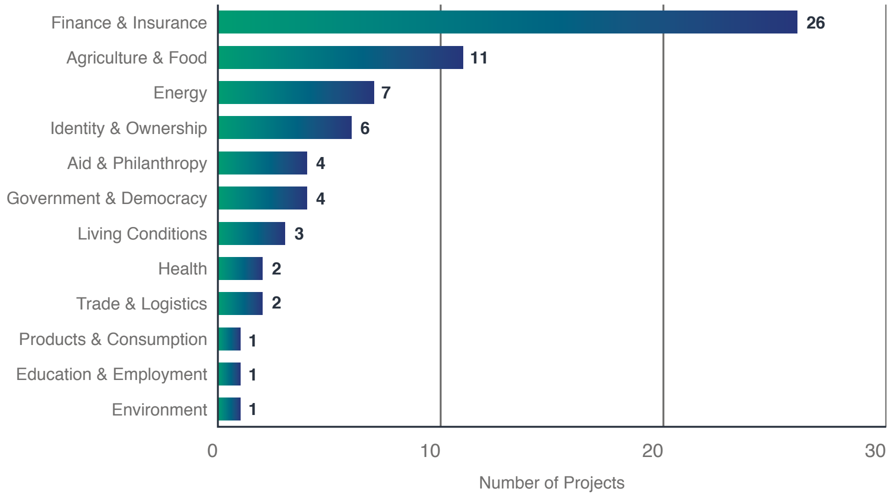


Figure 3: Blockchain projects in Africa by sector, according to PositiveBlockchain.io

[8] An example for economic and social impact are innovations in cross-border payments, which foster both the financial sector and benefit communities.

This section provides a snapshot of the blockchain ecosystem as it currently exists on the African continent. It is structured in a thematic order. Each theme is introduced in a way that highlights initiatives from the dynamic African project scape. It is then complemented with an explainer of the underlying use cases and links to additional resources in order to ease uptake and adaptation.

We will present the following use cases of blockchain pertinent to Africa. Most of which show how blockchain technology can ease cross-border transactions - and thereby complement existing efforts to that end on the African continent:

- Public spending and governance
- Peer-to-peer trading in off-grid scenarios
- Education credentials
- Land registration
- Tracing agricultural supply chains
- Trade facilitation

> "Blockchain technology can ease cross-border transactions."

2.1 Digital payment infrastructures: blockchain-based digital currencies from central banks vs. stablecoins

Financial solutions are the most common ones in the blockchain space. More than one third of the Africa-related projects that are recorded in the PositiveBlockchain.io database have their main focus in this area. This does not come as a surprise: Africans are early adopters of mobile money - more than half of global mobile-money service operators are located in Sub-Saharan Africa.[9] The continent has the highest unbanked population in the world, the fastest growing population, and the highest proportion of microbusinesses.[10] Some Africans already explore the possibilities of using blockchain-based financial services to reduce the cost of remittance payments, or speculate and invest using cryptocurrencies like Bitcoin. Others benefit from community-based lending solutions or community currencies. One of the biggest game changers, however, in the financial sector is the possible application of a digital payment infrastructure. It could be based on blockchain or another DLT; it could be operated by private actors, governments or in new forms of partnerships.

According to a survey of 63 central banks in 2018, whose catchment area covers 80% of the world's population, more than two-thirds of these central banks were working on the issue of central bank digital currencies (CBDC) at various stages. This includes both general-purpose, retail[11] CBDCs, which would provide a direct cash and electronic payment substitute, and wholesale CBDCs, which mainly involve interbank transfers and collateral.[12] Back then, no central bank indicated concrete implementation intentions yet. Since 2018, however, the playing field of digital currencies has changed. In particular, Facebook's announcement to create Libra[13] stimulated new discussions and rapid developments. This private sector driven initiative increased the pressure on existing - and in some cases slowly progressing - projects in the political arena. European, US and Chinese politicians subsequently com-

[9] Chironga, M., De Grandis, H. and Zouaoui, Y., 2020. *Mobile Financial Services In Africa: Winning The Battle For The Customer.* McKinsey. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/mobile-financial-services-in-africa-winning-the-battle-for-the-customer# [Accessed 8 May 2020].

[10] The World Bank, 2019. World Development Report. The World Bank. Available at: http://documents.worldbank.org/curated/en/816281518818814423/pdf/2019-WDR-Report.pdf [Accessed 8 May 2020].

[11] Applied to retail payments, DLTs can be used for money transfers denominated in fiat currencies. DLTs use so-called tokens to transfer values, e.g. information or monetary values, from party A to party B. Each of these digital DLT-based tokens must be fully backed by respective currency units deposited at a bank, an e-money provider, the central bank or another party. If the tokens are not fully backed by respective amounts of money, then it would not be possible for all clients to withdraw their funds, which would undermine trust in the project. Since the DLT itself cannot verify that backing, participants need to trust the e-money provider promising this fact. - That is the reason for license requirements for e-money providers.

[12] Bank for International Settlements, 2020. *Proceeding With Caution - A Survey On Central Bank Digital Currency.* BIS Papers No 101. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap101.pdf [Accessed 8 May 2020].

[13] In its original version (1.0) Libra has been described as a so-called stablecoin, linked to a basket of different financial assets, mainly currencies (US$, €, £, ¥) and government bonds. After facing a backlash from regulators in many countries, plans for a Libra version 2.0 were presented, which would omit operation in countries with weak currencies and would include modes of direct cooperation with regulators and central banks.

mented[14] on their plans to introduce digital currencies (and the threat they see in these private-sector-driven currencies).

The following section outlines different design options for digital payment infrastructures, discusses features and drawbacks and explains possible effects or lines of action for African countries.

2.1.1 Stablecoins

Stablecoins are crypto assets that are designed to minimise volatility by pegging their market value to an external currency. Currently, there exist various crypto asset projects like Tether, TrueUSD or Stasis, which issue tokens backed by fiat currencies (fiat-backed stablecoins). Holders of stablecoins must trust that all tokens are fully backed by assets - typically commodities, fiat currencies or cryptocurrencies. However, worldwide stablecoin issuers are currently not regulated (if they do not promise to return fiat) and therefore stablecoins are not covered by deposit insurance schemes. This imposes regulatory risk. Further, liquidity in stablecoins is limited. Hence, customers are exposed to a non-negligible risk that stablecoins could potentially default, besides apparent liquidity risk.

> "One of the biggest game changers in the financial sector is the possible application of a digital payment infrastructure."

So far, the following approaches to backing stablecoins have emerged: e-money and fiat-backed (either by commercial or central banks). The first refers to regulated stablecoins that are fully backed by fiat currencies as the issuing e-money institutions only issue DLT-backed tokens per unit of stored fiat. The latter describes digital versions of fiat currencies that merely differ in the security they offer, especially in times of a banking crisis.

2.1.2 Central bank digital currencies

Backing stablecoins by central bank money instead of commercial bank money decreases default risks for stablecoin holders, depending on the central bank's trustworthiness and track record. Driven by the developments around crypto assets and Facebook's continuous efforts to launch the Libra project, many central banks have recently announced that they will research the issuance of their own digital currencies, so-called central bank digital currencies (CBDCs) and thereby take a closer look at the application of DLT.[15] According to a recently published study by the Bank for International Settlements (BIS) this is the case for 70% of all global central banks.[16] Of the central banks participating in the study, 10% stated that they are likely to introduce such digital money in the short term (up to three years) and 20% in the medium term (up to six years).

Current retail CBDC projects

China is currently pioneering as they might already start their retail CBDC prototype for a digital yuan or a common digital currency of the BRICS states in 2020. There are also a number of initiatives by smaller countries: the Eastern Caribbean Central Bank is investigating the application of DLT for a digital Eastern Caribbean dollar. The Sand dollar of the Bahamas pursues a similar goal and is already available to Bahamian citizens in a pilot phase since December 2019. The so-called sovereign, a Marshall Islands crypto asset, shall also be issued in the upcoming months.

[14] See von Weizsäcker, F., Meier-Hahn, U. and Wannemacher, L., 2020. *Libra Vs. Governments: The Race Towards An Inclusive Global Payment Infrastructure.* Available at: https://medium.com/@GIZ_Lab/libra-vs-governments-the-race-towards-an-inclusive-global-payment-infrastructure-a1432124d8fc [Accessed 8 May 2020].

[15] Implementing a CBDC does not necessarily imply using DLT; it is one technology option next to regular databases. However, all the major CBDC prototypes (Sweden, China, Marshall Islands, Bahamas, Eastern Carribean Region) are based on DLT. Therefore, DLT seems to be highly relevant in the context of a CBDC.

[16] Boar, C., Holden, H. and Wadsworth, A., 2020. *Impending Arrival - A Sequel To The Survey On Central Bank Digital Currency.* BIS Papers No 107. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap107.pdf [Accessed 8 May 2020].

Within the European Union, the Swedish central bank (Riksbank) has been analysing the issuance of a digital version of the Swedish krona (e-krona) since 2017 and is already testing a DLT-based e-krona prototype. The German government's Blockchain Strategy is committed to the digital euro, and work is underway with the European Central Bank (ECB) and others to find appropriate solutions.[17] The current target is wholesale instead of retail, i.e. not the big disruption (a CBDC for private users), but "only" a payment infrastructure for the digital euro in interbank business, with some open questions about the operator model.

In international forums such as the G20, G7, and the World Economic Forum, CBDCs are prominently on the agenda. On the African continent, the Central Bank of Tunisia is currently examining the potential and options for action on CBDCs. It appears therefore only as a matter of time until first CBDCs will be introduced.

Motives for a CBDC introduction

Central banks' motives for introducing a retail CBDC are manifold. The survey of the BIS shows that they differ between advanced economies on the one hand and emerging market economies on the other hand: emerging economies mainly hope to increase financial stability by lowering the concentration of money in the banking sector, to increase the efficiency of payment transactions, i.e. transaction time and costs, and increase the security of digital transactions. Another hope by central bankers in emerging market economies is to increase financial inclusion by introducing a CBDC. A consumer-friendly CBDC with low entry barriers such as the opportunity to transact small units of CBDC without know-your-customer (KYC) requirements could ease the access to digital transaction services for citizens, who are currently excluded from the financial system (financially excluded). One can think of the example of M-Pesa in Kenya, where holders of mobile phones can transfer money from phone to phone. If a CBDC is implemented in a similar fashion and can be transferred peer-to-peer via phones more citizens would get access to the financial system. Nowadays, IDs and bank accounts are most often necessary to transfer money. However, many citizens in developing countries do not have an ID nor a bank account. On the precondition of eased KYC requirements such a CBDC could be a gamechanger and allow citizens even to some extent without ID and bank account to conduct payments.

> "A consumer-friendly CBDC with low entry barriers could ease the access to digital transaction services for citizens, who are currently excluded from the financial system."

Drawbacks of a CBDC introduction

Even though a CBDC introduction can have various benefits for the domestic payment system, there are drawbacks. These have to be addressed when considering the issuance of a CBDC. First, the introduction of a CBDC can lead to excessive disintermediation of the financial sector if citizens see CBDC as a close substitute for commercial bank money and transfer large amounts of their bank deposits to the central bank as soon as CBDCs are available. In this case, banks could lose sizable market shares. This could threaten the business of commercial banks, trigger liquidity shortages and in the worst case another banking crisis. Besides, monetary transmission mechanisms are poorly understood and need to be investigated further.

Secondly, data protection has to be ensured. Currently, wide-spread payment methods such as credit cards, mobile payments or cash payments have different degrees of data privacy. While in case of credit card payments, the credit card provider and potentially the partnering bank have insights into transaction data, cash is the only fully anonymous payment method. Issuing a CBDC without accounting for data privacy concerns would go against digital rights and not be desirable.

[17] The European approach to promoting the international significance of the euro digitally is moving, as was recently underlined by EU Council President Ursula von der Leyen. (The Economist. 2020. *America's Aggressive Use Of Sanctions Endangers The Dollar's Reign.* Available at: https://www.economist.com/briefing/2020/01/18/americas-aggressive-use-of-sanctions-endangers-the-dollars-reign [Accessed 8 May 2020].)

2.1.3 Fiscal and geopolitical dimensions

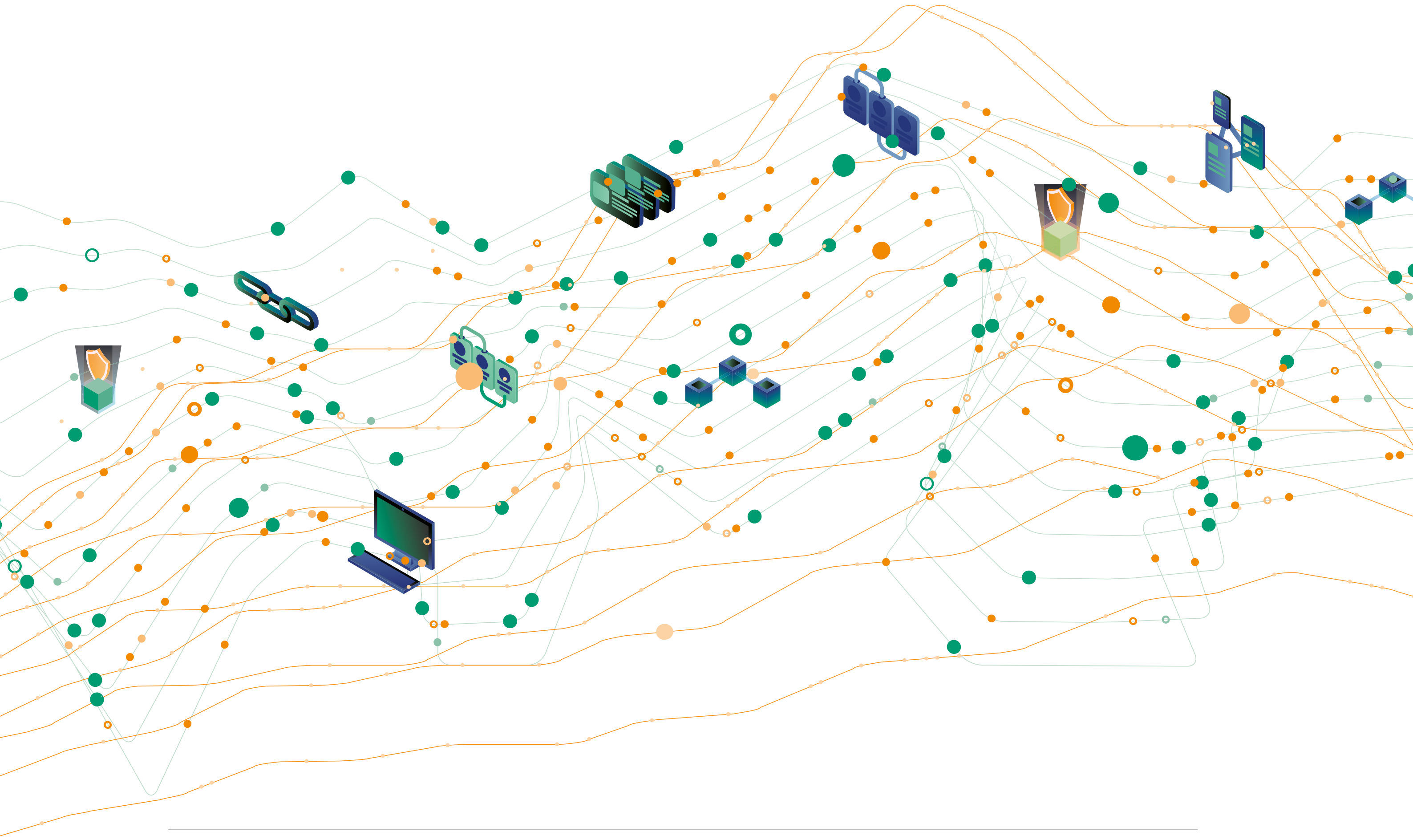
For developing countries, it is not only relevant to analyse the introduction of their own CBDCs, but also to assess implications from CBDCs implemented by other countries. If a neighbouring country, for example, would introduce an interest-bearing CBDC, this could lead to funds flowing into the neighbouring country, which would influence the respective exchange rates. This would have clear consequences for domestic economic activity and monetary policy. However, as no country has implemented a retail CBDC yet, the impact of the exchange rate remains speculative and should - like other unknowns outlined in this chapter - be an object of further research.

In the larger picture, the question which payment ecosystems will be of global importance in the future is not only important for banking, but also for geopolitical spheres of influence. Not only economic interests, sanction regimes, but also values can be anchored in the procedures of monetary and payment ecosystems. For example, how is personal data handled, how are mechanisms against money laundering and terrorist financing implemented, how high or low are the barriers to participation, how is technical and political interoperability anchored, how is the degree of centralisation or distribution of transaction processing (i.e. is it more likely to be a central database or more likely to be a syndicate blockchain between states with consensus protocols anchored in international law).

It appears likely that the need for international cooperation on CBDCs and the underlying payment infrastructures will continue to increase, and that foreign policy, security policy and economic policy objectives will be prominently reflected in this. Different stakeholders are likely to seek to enhance their geopolitical relevance in the longer term and take an active and also accelerated role in shaping the future of global monetary and payment ecosystems.

Further information on this use case:

- Report: Central Bank Digital Currency Policy-Maker Toolkit by the World Economic Forum[18]
- Research: Overview over current CBDC projects[19]



[18] World Economic Forum, 2020. *Central Bank Digital Currency Policy-Maker Toolkit.* World Economic Forum. Available at: http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf [Accessed 8 May 2020].

[19] Mehrländer, A., 2020. *Overview Over Current CBDC Projects.* Available at: https://doi.org/10.5281/zenodo.3817648 [Accessed 8 May 2020].

2.2 Public spending and governance

The global Aid Effectiveness Agenda promotes that partner country institutions should have a strong role in development cooperation. In reality, however, donors have developed their own customised procedures designed to minimise risks for the disbursement of development aid. Partner countries are left with the onerous task of collecting financial data and coordinating various donor requirements. As a consequence, the structural impact of development cooperation remains limited, as local systems struggle to adequately absorb funds.

Blockchain-based workflow tools can allow for efficient project implementation by offering functionalities to track expenditures in a collaborative and transparent way. They can help to coordinate the implementation of donor-funded investment projects by providing a shared and up-to date view on project-related expenditures and by allowing multiple parties to lock transactions in real time.

Example project TruBudget: Germany’s KfW Development Bank has developed the Trusted Budget Expenditure software (TruBudget, https://trubudget.net). It serves as a platform for all stakeholders involved in a development project or programme (e.g. ministries, agencies, donors, auditors). Each stakeholder receives specific rights based on their role in the project. The software mirrors specific workflow processes of project planning and implementation and allows for real-time information to be shared among the users. It would be designed in a way that it can interface (using APIs) with existing IT-systems of the involved country’s institutions. This means that crucial approval steps, such as a non-objection to a procurement process or a contract, or the release of payments, can be granted immediately without any delay. All activities are documented in the system and are traceable at all stages. The software is based on a private blockchain, which provides a tamper-proof database, thus adding the trust required by donors to integrate with country systems. TruBudget is a modular open-source software with APIs that is available to anyone free of charge.

Public spending applications of this kind can benefit partner countries and donors in several ways:

- The partner country is in full control of donor funded projects.
- Donors may channel funds through country institutions and trace project-related payments.
- The systems facilitate communication and data management.
- They promise to reduce transaction costs on both sides.

This, in turn, has the potential of increasing the structural impact of development cooperation by strengthening domestic governance structures and public financial management systems.

The operational model of this use case would see the software to be fully owned, utilised and adapted by the countries that receive funds. It can serve as a platform for donor-funded initiatives, which would assist donor harmonisation. Finally, countries would also be free to adapt and use the software for the implementation of domestic programmes and projects, again benefiting from the increased efficiency and transparency as the core feature of blockchain-based public expenditure tools.

"Blockchain-based workflow tools can allow for efficient project implementation by offering functionalities to track expenditures in a collaborative and transparent way."

2.3 Peer-to-peer trading of electricity

Africa’s growing population has key implications for energy demand. While population growth in urban areas increases demand for industrial production, cooling and mobility, it also implies an additional need for energy provision in rural areas. Despite progress in various countries, it is estimated that population growth might likely outpace such efforts. Although the global electrification rate reached 89% in 2017, uninterrupted access to electricity remains a global problem, especially in regions that are difficult to reach. Sub-Saharan Africa accounts for the biggest shortfall in electrification, where 573 million people are lacking access. Providing families in rural areas with access to affordable energy and replacing the use of expensive and environmentally harmful diesel and petrol generators is therefore another focus of emerging blockchain initiatives.

By 2023, the energy sector is foreseen to account for the second largest share of the forecasted global revenues of 23 billion US dollars for blockchain technology – just after the financial industry.[20] The ongoing trend of renewable energy goes hand in hand with an increase in decentralised energy generation and distribution. This specifically poses a major opportunity for the African continent, where the need for electrification may be covered in a decentralised manner – without the rigorous structures of centralised energy markets that exist in many developed countries.

To provide decentralised energy solutions, off-grid solutions for electrification such as microgrids have been identified as essential. Microgrids are small-scale electricity distribution systems which can be connected to the main electricity grid or operate independently in "island mode" (off-grid). They are often used for the distribution of electricity from renewable energy sources. In contrast to conventional energy trading, which is usually unidirectional, peer-to-peer energy trading within a microgrid environment allows for direct trading interaction between local energy prosumers and consumers.

In this context, blockchain technology holds the potential to facilitate trading interaction as it functions as a shared information and transaction platform for all market participants. Electricity generation and real-time demand are recorded on a blockchain by automatically documenting executed transactions between the participants using internet-enabled smart meters. The technology’s ability to make even small data transactions economically viable ultimately entails new degrees of participation and incentives.

> "Blockchain-based energy distribution poses a major opportunity for the African continent, where the need for electrification may be covered in a decentralised manner."

Electricity marketplaces are heavily dependent on data integrity. Therefore, one part of the solution needs to collect data streams from decentralised electricity feed-in. Validity of this data is best ensured by using tamper-proof cryptography-enabled hardware as well as an algorithm cross-checking various data sources against each other. Based on such validated data sources, a blockchain-based electricity marketplace cannot only unite the demand and supply side for energy purchases. It can also immediately settle transactions, by monitoring the delivery of electricity and processing corresponding payments. Smart contracts can ensure that electricity is requested, for example, when prices fall below a price threshold or when green electricity or local power is available.

Major challenges include hardware requirements and regulation. This specifically relates to the requirement of smart meter penetration. As in many countries, energy systems are often heavily regulated by the state or controlled by a state-owned-corporation, a matching legal framework is crucial for the implementation of energy trading in peer-to-peer microgrids. Even the upgrading of predominant hardware may require regulatory intervention.

[20] Peter, V., Paredes, J., Rosado Rivial, M., Soto Sepúlveda, E. and Hermosilla Astorga, D., 2019. *Blockchain Meets Energy - Digital Solutions For A Decentralized And Decarbonized Sector.* German-Mexican Energy Partnership (EP) and Florence School of Regulation (FSR). Available at: https://fsr.eui.eu/wp-content/uploads/Blockchain_meets_Energy_-_ENG.pdf [Accessed 8 May 2020].

Further information on this use case:

- Book Chapter: Microgrids: Applications, Solutions, Case Studies, and Demonstrations[21]
- Report: Energy progress report 2019 Sustainable Development Goal 7[22]
- Use case: Blockchain-enabled microgrid in Brooklyn[23]

2.4 Digital claims of identity and ownership

The topic of identity and ownership spans both legal personal identification as well as ownership of assets e.g. land or property, and personal attributes, e.g. a doctoral degree. Proving one's identity or ownership in the digital space as a way to access resources or exercise rights has become increasingly important. Blockchain technology may now deliver the needed infrastructure to provide digital proof of such claims. Therefore, applications of the technology for digital claims have sprung up across the globe with specific promises for the African continent. When it comes to identity management, projects like Gravity.Earth (https://www.gravity.earth/) provide trusted identities for the economically excluded, while initiatives like Lawyer's Hub (https://lawyershub.org/) in Kenya aim to tackle the issue of continued exclusion of minorities when moving from physical to digital identity systems. Another initiative in this area is the partnership of the Rwandan Government with WiseKey & Microsoft Azure for digital authentication, secure transactions, and legally binding signatures. [24]

2.4.1 Land registration

Land tenure is a legal or customary regime which determines who can use land, for how long, and under what conditions. Especially in developing countries, a large number of residential titleholders lack accurate documentation of property ownership due to flawed paperwork, forged signatures and defects in foreclosure and mortgage documents. In places where land tenure is more accurately documented, the registries most commonly rely on paper-based documentation. Such documentation is usually stored in a central location, making it vulnerable to loss, corruption or misuse. The loss or manipulation of land documents creates social conflict and negatively affects the trust in governmental services.

> "In the case of land registration, blockchain technology can increase the transparency of ownership changes reducing the possibility of manipulation of existing titles."

In the case of land registration, blockchain technology can increase the transparency of ownership changes reducing the possibility of manipulation of existing titles. Similar to the registration process with a traditional land registry, two citizens who have agreed on the sale of a land parcel go to the governmental administrator responsible for transactions of land. As they sign the sales contract, the administrator enters the details of the transaction into a blockchain-powered land registry database. Now, the public ledger will be provided with a privacy-shielded set of data. This would specifically entail a checksum computationally generated based on the details of the new land title, i.e. the fingerprint or hash of the full transaction. While the hash is captured and permanently stored on a blockchain, the full transaction details are being stored privately. Once the transaction is computationally approved by the network and added to the ledger, the transfer of ownership is immutably recorded and the blockchain becomes a single point of truth. This prevents document forgery and corrupt land transfers. If there

[21] Donahue, E., 2019. *Microgrids: Applications, Solutions, Case Studies, and Demonstrations. In: M. Ghofrani, ed., Micro-grids: Applications, Operation, Control and Protection.* University of Washington Bothell. Available at: https://doi.org/10.5772/intechopen.83560 [Accessed 8 May 2020].

[22] Tracking SDG 7 : The Energy Progress Report 2019, 2019. International Energy Agency; International Renewable Energy Agency; United Nations Statistics Division; World Bank; World Health Organization, Washington, DC.

[23] Brooklyn Microgrid, n.d. *Brooklyn Microgrid | Community Powered Energy*. Available at: https://www.brooklyn.energy/ [Accessed 8 May 2020].

[24] See Reuters, 2020. *Wisekey And Microsoft Collaborate To Support Rwandan Government Make Secure Transactions*. Reuters. Available at: https://www.reuters.com/article/brief-wisekey-and-microsoft-collaborate/brief-wisekey-and-microsoft-collaborate-to-support-rwandan-government-make-secure-transactions-idUSFWN1ML111 [Accessed 8 May 2020].

are doubts as to the validity of a land ownership claim, anybody can consult the public ledger for validation. A smartphone app or web platform could be used as a user interface to that end.

This decentralised land registry adds value through its immutability and resilience. The fraud and corruption scenarios that rely on the forging or "disappearing" of documents, or attempts to sell land more than once, are effectively discouraged by a timestamped hash on a public ledger. Once land titles are appropriately digitised and secured using blockchain, this would especially benefit marginalised groups in society, such as women or indigenous populations, who are often the victims of land fraud. For this, however, a quality assured and safeguarded approach throughout the implementation phase is required.

So far, Georgia has successfully implemented the use of blockchain technology for timestamping digital land titles. Their National Agency of Public Registry has further decided to extend their existing project, enabling mobile phone-based land transactions in the long run, which could speed up such processes to a matter of minutes. However, globally, there remains a long way to go as other implementations remain in the pipeline, for example, in Sweden and Ghana. Especially countries with competing systems or conflicted histories in the realm of land management, or countries without the needed high-quality datasets and preceding digitalisation efforts, may find it difficult to move onto implementation of a blockchain-based land registry.

Further information on this use case:

- Book Chapter: Blockchain and Land Administration[25]
- Preprint: Digital Transformation: Blockchain and Land Titles[26]
- Concept Note: Land registries on a distributed ledger[27]

2.4.2 Verifiable digital education credentials

Across the globe, the future of work shifts the focus from manual labour to knowledge work. Individuals now find themselves in a global labour market where it is key to differentiate oneself through a unique, up-to-date and continuously progressing skill set. When previously an individual may have undergone one-off training for a specific skill at a (physical) institution that has a reputation among a local community, the new reality of life-long learning, micro certificates and the unbundling of educational programmes from various institutions worldwide leads to new challenges. To provide employers or other administrations with an overview on a learner’s complex educational history, they would need reliable information about a learner’s educational path. The promise of blockchain-based education credentials is exactly that.

> "Learners, educational institutions and third parties will benefit equally from forgery-proof certificates and reduced costs from efficiency gains."

In order to increase trust in educational certificates, blockchain-based systems can be used for the verification of digital documents. This helps to re-establish trust among employers and the global labour pool by limiting the forgery of documents and increasing their recognition across national borders. The added value of verifying digital documents through a public blockchain is twofold. First, it lies in its reliability and robustness, resulting in an extremely high degree of availability and trustworthiness of the information provided by the blockchain-based verification process. Second, such a digital verification process with machine-readable certificates is quick, fair and globally accessible. In comparison, manual verification processes may involve time-consuming requests to issuing institutions and work flows prone to human error and

[25] Makala, B. and Anand, A., 2018. *Blockchain and Land Administration.* In: UNOPS, ed., The Legal Aspects of Blockchain. The World Bank. Available at: https://ideas.repec.org/b/wbk/wbpubs/31419.html [Accessed 8 May 2020].

[26] Eder, G., 2019. *Digital Transformation: Blockchain and Land Titles.* In: *OECD Global Anti-Corruption & Integrity Forum.* Available at: https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf [Accessed 8 May 2020].

[27] v. Weizsäcker, F., Eggler, S. and Atarim, E., 2019. *Land Registries On A Distributed Ledger.* GIZ Blockchain Lab. Available at: https://www.giz.de/en/downloads/giz2019-en-distributed-land-registry.pdf [Accessed 8 May 2020].

corruption. Ideally, learners, educational institutions and third parties will benefit equally from forgery-proof certificates and reduced costs from efficiency gains.

There are three user groups in the blockchain-based credentialing systems:

1. **Education providers** such as universities or schools issue certificates as digital originals and store so-called hashes of these files - which can also be called digital fingerprints - on a blockchain.

2. **Students** receive their certificates in digital form and can pass them on to third parties or upload them to professional online social networking platforms (such as LinkedIn) that are exploring automatic verification of digital certificates.

3. **Third parties such as employers or administrations** can then validate the submitted certificates electronically by comparing the document's fingerprints with those stored on the blockchain. They do not have to go through the cumbersome process of contacting the issuing institutions anymore.

Crucially, the technical infrastructure should be governed by a reputable consortium of institutions that is deemed trustworthy, similarly to how trust and power is (explicitly or implicitly) present in today's educational systems. A key role of this consortium would be to authorise schools and other educational institutions to issue digital certificates with their credentials.

A few educational institutions around the world have already implemented blockchain-based education credentials today. Standing out because of their open source approach are the software projects OpenCerts from Singapore, and recently AUTHER (http://auther.org), which is based on Blockcerts and widely-used standard OpenBadges. AUTHER has been developed by GIZ together with the Southeast Asia Ministers of Education Organization SEAMEO INNOTECH and the Technische Universität Berlin, piloting how such an open system can work in practice.

Further information on this use case:

- Concept Note: Blockchain-based education credentials[28]
- Whitepaper: Digitalisation of certificates with the support of blockchain technology[29]
- Whitepaper: Building the digital credential infrastructure for the future[30]
- Task Force: W3C Verifiable Credentials for Education[31]

[28] v. Weizsäcker, F., Meier-Hahn, U. and Wannemacher, L., 2020. *Blockchain-based education credentials*. GIZ Blockchain Lab.

[29] Netzwerk Digitale Nachweise, 2020. *Digitalisation of certificates with the support of blockchain technology*. Available at: http://netzwerkdigitalenachweise.de/static/doc//Whitepaper_digitales_Zeugnis_en.pdf [Accessed 8 May 2020].

[30] Digital Credentials Consortium, 2020. *Building the digital credential infrastructure for the future*. Digital Credentials Consortium. Available at: https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf [Accessed 8 May 2020].

[31] W3C, n.d. *Verifiable Credentials For Education Task Force.*Verifiable Credentials for Education Task Force. Available at: https://github.com/w3c-ccg/vc-ed [Accessed 8 May 2020].

2.5 Tracing agricultural supply chains

Almost half the African population relies on agriculture for employment and food, and the percentage can reach 70% in East Africa.[32] Yet, the sector and the farmers are not delivering their full potential as they are facing several issues such as the lack of access to financial resources and insurance, as well as the complexity and opacity of supply and value chains.

Supply chains are intrinsically complex flows of goods, money and services. Their traceability refers to the collection, documentation, and application of information related to all processes in the supply chain in a manner that provides guarantee to the end-customer and other stakeholders along the supply chain on the provenance, location and life history of a product. It represents the ability to conduct a full backward tracking to determine characteristics of the goods by means of records.

Often, the opaqueness of supply chains hinders customers from understanding the provenance of a product, as well as its social and environmental impact for smallholder farmers and other participants of the supply chain. While increasing numbers of customers seek out organically produced goods, industry fails to provide such goods at a satisfactory standard. Currently, the only way for customers to be promised higher standards is through certification schemes. These schemes tend to be too costly for single smallholder farmers and even corporates may shy away from the investment. Hence, farmers and workers may carry on receiving low prices for goods that could be distinguished as sustainably sourced.

> "The traceability of transactions enables higher transparency on how goods are being sourced, processed and transported."

In blockchain technology, a token is a digital asset that is stored on the chain and can be connected to a real-world value. Tokenisation in this context allows to uniquely associate information to goods and services of a certain time period. The advantage here is that every movement along the chain will be recorded. The traceability of transactions enables higher transparency on how goods are being sourced, processed and transported as each step along the chain of custody can be immutably recorded in real-time on a blockchain. This capacity to shed light on the origins of consumer goods is one of the more promising attributes of blockchain technology for local producers, logistical partners, and stakeholders along the supply chain. All logistical information would be secured on-chain and all parties would trust this single source of truth. Hypothetically, it could reward those using sustainable practices thanks to the increased price consumers may be willing to pay based on more trust that has been created using a distributed ledger.

However, there is no one-size-fits-all solution. Each supply chain has to be checked for its potential to leverage distributed ledger technology. The capacity to run blockchain-powered supply chains will largely rely on the willingness of all stakeholders involved and the ability to tokenise a traded good. The more unique and identifiable the good is, the more its digital twin will faithfully reflect its attributes. Unprocessed coconuts or pineapples for example are easier use cases for traceability as they can be easily marked and traced - off-chain and on a blockchain.

Furthermore, a data model that everyone can access is crucial in this context to fully leverage the value chain cooperation. When opting for a distributed model, the governance itself needs to be equally distributed and consensus on key aspects, including the technological setup and the data model applied, needs to be reached. Especially data quality and credibility have to be ensured. Individual data of single actors that is not crucial for other actors along the chain should not be accessible. A good balance between data transparency and privacy is required. Achieving good data quality is not part of the blockchain technology solution. There are different ways to achieve this goal, one is internet of things technology, where sensors monitor and record certain situations and environments. A second

[32] NEPAD, 2013. *Agriculture In Africa - Transformation And Outlook*. NEPAD. Available at: https://www.nepad.org/file-download/download/public/15582 [Accessed 8 May 2020].

approach is to diminish human error by educating and capacitating those handling the data, e.g. through training courses, guidelines, handbooks or auditing structures.

Further information on this use case:

- Report: Is there a role for blockchain in responsible supply chains?[33]
- Concept Note: Agricultural supply chain traceability[34]

2.6 Trade facilitation

Even today, 90% of international cargo is shipped by sea. Most commonly, for customs compliance, the shipping industry relies on paper documentation. Advance cargo information may, for example, only be transmitted 24 hours prior to a vessel arriving in the port, which leaves insufficient time for customs. The extended transit times that result for shippers are costly and time-consuming.

To reduce these costs and inefficiencies, the application of blockchain is envisioned as a promising use case. It would enable the exchange of information on international freight transports in real time. Customs authorities could process customs declarations more quickly thanks to the information being made available in advance. By using a blockchain-powered platform, all participants of the shipping process are brought together and can view or edit their relevant shipping files based on individual permissions. The added trust of using blockchain in this scenario, improves collaboration and automation. It also records all movements of the shipped goods simultaneously to the editions of documents and documentation. Goods shipments can be processed immediately pre-arrival or pre-departure and then released thanks to the availability of accurate and trusted documentation.

As an example: The German Alliance for Trade Facilitation is preparing a project together with Maersk and UNCTAD to prove the possible reduction in time and cost of international maritime trade. Together with customs authorities in the prospective pilot countries, Sri Lanka and Cambodia, the partners will work on the data integration solution, ASYHUB, for the smooth exchange of data between UNCTAD's automated system for customs data (ASYCUDA) and blockchain-based applications, such as the TradeLens data platform. Based on the experiences of the pilot countries, the approach is going to be scaled up in five more countries within the project and eventually all ASYCUDA using countries. This provides several opportunities for African countries with sea ports, for example, Togo, Côte d'Ivoire, and many others.

The global TradeLens platform already accounts for 20% of global freight ocean traffic, while ASYCUDA is used in over 60 countries. This evidences the potential for global scaling.

Further information on this use case:

- White paper: Overview of Blockchain for Trade[35]
- Working paper: Can Blockchain Technology Facilitate International Trade?[36]

[33] Tholen, D., de Vries, A., Daluz, A., Antonovici, C., van Brug, W., Abelson, R., Lovell, D., 2020. *Is There A Role For Blockchain In Responsible Supply Chains?*. OECD. Available at: http://mneguidelines.oecd.org/Is-there-a-role-for-blockchain-in-responsible-supply-chains.pdf [Accessed 8 May 2020].

[34] Wannemacher, L. and Mehrländer, A., 2020. *Agricultural supply chain traceability*. GIZ Blockchain Lab. Available at: https://www.giz.de/en/downloads/giz2020-en-agricultural-supply-chain-traceability.pdf [Accessed 8 May 2020].

[35] UNECE, 2019. *Blockchain For Trade Facilitation*. Available at: https://unctad.org/meetings/en/Presentation/cimem7p16_Lance%20Thompson_en.pdf [Accessed 8 May 2020].

[36] McDaniel, C. and C. Norberg, H., 2019. *Can Blockchain Technology Facilitate International Trade?*. Mercatus Research. Mercatus Center at George Mason University. Available at: https://www.mercatus.org/system/files/mcdaniel-blockchain-trade-mercatus-research-v2.pdf [Accessed 8 May 2020].

3. POLICY CONSIDERATIONS

The versatility of blockchain technology across the range of use cases outlined in the previous chapter comes with its own caveats. For each use case, it is not only a question of how to design a technological system, but also one of how to embed the technology in the legal and political environment.

> "It is not only a question of how to design a technological system, but also one of how to embed the technology in the legal and political environment."

Existing policies need to be established or updated in the context of blockchain technology and the necessary regulatory mechanisms need to be put in place. The role and uptake of African governments will be important, both from an adoption perspective, as well as with regard to the creation and enablement of the policy and regulatory environment.

This section presents policy choices to be considered by African decision and policy makers when designing the legal or political environment, including data privacy and financial regulations. It will look at the tensions between data protection and blockchain, at the technology's link to financial regulation and it will give examples of existing national strategies that regulate and - at times - promote blockchain technology.

3.1 Blockchain technology and data protection

The possible tension between blockchain technology and data protection regulation arises from the fact that both regulation, organisational implementation and technology determine social choices that in every-day life would be made rather context-driven. These determinations can be in conflict with each other. Blockchain technology can be at tension with several themes that are central issues in data protection, including

- objectives chosen by the legislator,
- "secrecy" versus "transparency",
- "remembering" versus "forgetting" (or a "right to be forgotten"),
- updates and corrections of data,
- data subjects' rights, and
- regulatory oversight and enforcement.

Blockchain-based systems are neither generally compatible nor generally incompatible with these dimensions of data protection. Therefore, this chapter foregrounds how different positions on each of these matters may inform both technology design and policy action.

Focus Box:
Status quo of pan-African data protection initiatives and harmonisation efforts

The current considerations of blockchain technology fit into overarching efforts to harmonise data protection across the African continent. Such a harmonisation of data protection regimes rather needs to be understood as a negotiated compromise instead of shared values. An example for this is the EU's General Data Protection Regulation. Despite it serving as a possible inspiration in terms of legal methodology, the Regulation does not suffice as a direct import to establish Africa's data protection framework for that would anticipate the yet to find African compromise.

Today, several initiatives for the harmonisation of data protection laws coexist. Over the last fifteen years, some regional frameworks have been developed, such as the 2008 East African Community Framework for Cyberlaws, the 2010 Supplementary Act on Personal Data Protection of the Economic Community of West African States, or the 2013 Southern African Development Community model law harmonising policies for the ICT Market in sub-Saharan Africa. In 2014, the first pan-African framework was adopted with the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The Malabo Convention's pace of ratification and adoption is still slow.

Almost 6 years after the Convention was signed, out of the 54 African countries, only 29 indeed do have data protection legislation (see figure on state of data protection regulation in Africa). While an increasing number of governments are planning to adopt such a framework, this situation creates uncertainty for many businesses that plan to develop digital products and services in Africa, in particular when these services require cross-border data transfers (see figure on the state of cross-border data flows regulation in Africa).

The harmonisation of the legal frameworks for the collection and processing of data in Africa still faces various obstacles:

- significant cultural and legal diversity across the continent, with different expectations regarding the good that shall be protected, such as privacy, fairness, dignity or fundamental rights and freedoms at large.
- variations in access to technology and online services among African states
- different levels of capability in the fields of technology and technology-related law and governance [37]

As part of the current efforts towards a harmonised framework, Smart Africa has launched a working group to support member states that want to develop data protection and policy strategies. The current situation poses an opportunity to form a digital single market in Africa. The working group will therefore also propose monitoring and support mechanisms for the harmonisation and adoption of data protection frameworks.

The international harmonisation of laws can, however, only be considered a first step. One of the major issues governments are facing today is the mismatch between existing regulatory frameworks and their enforcement. Enforcement depends on the existence of an independent administrative authority with a clear mandate and sufficient resources. In addition, enforcement and compliance depend on the level of awareness on privacy rules in both the public and private sectors and among citizens.

The enforcement of data protection frameworks will require important efforts on capacity building and educational programmes for data protection authorities. This applies in particular to the context of emerging technologies like blockchain which require a high level of expertise for regulators. A pan-African approach should be adopted here as well, in order to mutualise expertise and scarce resources, and to ensure harmonisation not only of national legal frameworks but of the specific implementation strategies countries adopt. The role of pan-African organisations, like the African Data Protection Network (***Réseau Africain sur la Protection des Données,*** RAPDP) will be crucial to this end.

[37] Internet Society and African Union, 2018. *Personal Data Protection Guidelines For Africa - A Joint Initiative Of The Internet Society And The Commission Of The African Union.* Internet Society and African Union. Available at: https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf [Accessed 8 May a].

State of data protection regulation in Africa

29 countries do have specific data protection laws	9 countries are currently drafting legislation
Algeria	Cameroon
Angola	Egypt
Benin	Eswatini
Botswana	Gambia
Burkina Faso	Malawi
Cabo Verde	Namibia
Chad	Rwanda
Côte d'Ivoire	Tanzania, United Republic
Equatorial Guinea	Zimbabwe
Gabon	
Ghana	
Guinea	
Kenya	
Lesotho	
Madagascar	
Mali	
Mauritania	
Mauritius	
Morocco	
Niger	
Nigeria	
São Tomé and Príncipe	
Senegal	
Seychelles	
South Africa	
Togo	
Tunisia	
Uganda	
Zambia	
The remaining countries do not have any specific data protection law.	

Figure 4: State of data protection regulation in Africa

State of cross-border data flows regulation in Africa

Cross-border data flows require contractual safeguards, prior authorization or adequacy decisions by authorities. (26 countries)	No prior restriction: ex-post accountability for data exporters (2 countries)	Absence of cross-border data flow restrictions (26 countries)
Algeria		
Angola		
Benin		
Botswana		
Burkina Faso		
		Burundi
Cabo Verde		
		Cameroon
		Central African Republic
Chad		
		Comoros
Côte d'Ivoire		
		Democratic Republic of the Congo
		Djibouti
		Egypt
Equatorial Guinea		
		Eritrea
		Eswatini
		Ethiopia
Gabon		
		Gambia
	Ghana	
Guinea		
		Guinea-Bissau
Kenya		
Lesotho		
		Liberia
		Libya
Madagascar		
		Malawi
Mali		
Mauritania		
Mauritius		
Morocco		
		Mozambique
		Namibia
Niger		
Nigeria		
		Republic of the Congo
		Rwanda
São Tomé and Príncipe		
Senegal		
	Seychelles	
		Sierra Leone
		Somalia
South Africa		
		South Sudan
		Sudan
		Tanzania, United Republic
Togo		
Tunisia		
Uganda		
		Zambia
		Zimbabwe

Figure 5: State of cross-border data flows regulation in Africa

3.1.1 From regulatory goals to legal techniques

Arguably, the particular regulatory approach is of less importance for ensuring harmonisation across Africa than finding a consensus on the regulatory goals. The specific provisions in the applicable data protection laws determine whether and how blockchain technology may be used in compliance with the law, and how laws must be designed to ensure that compliance is possible. However, African states should continue to develop and negotiate their positions on the different objectives first, and then debate which regulatory approach should be implemented to ensure that these goals are met.

Three basic approaches [see Figure 4] to regulating modern information processing can be distinguished that foster its positive and mitigate its negative implications:

- **The rights-based approach:** It is followed by many francophone countries and conveys rights to data subjects. These rights must then be safeguarded by data controllers and processors. Supervisory authorities come in to bear part of the burden of the individual.
- **The duty-based approach:** It is more common in anglophone countries and stipulates objective requirements and duties for data controllers and processors. The role of supervisory authorities in this approach is to complement the controllers' and processors' self-monitoring by external supervision.
- **Mixed approach:** Mutual reinforcement of individuals (who prompt enforcement of their rights) and processors who have to guarantee certain safeguards.

While these three approaches apply different means, they can all achieve the same regulatory outcome by setting similar standards to which information collection, processing and use has to adhere.

Rights-based and duty-based approach in practice

Imagine a scenario in which the operator of an e-commerce shop (the data controller) should provide information about the processing of personal data to the customer (the data subject): a rights-based approach would grant a right to request this information to the customer; a duty-based approach would require the shop operator to proactively inform its customers; and a mixed approach would include two separate provisions, one granting the right to request information to the customer and one imposing the duty to inform the customer onto the shop operator. Enforcement mechanisms to a) uphold the rights of the customer in the rights-based approach and/or to b) monitor the controller's compliance with his duties in the duty-based approach either follow existing legal procedures, such as sending a warning letter, filing a lawsuit or initiating supervisory procedures, or must be newly created.

> "The particular regulatory approach is of less importance for ensuring harmonisation across Africa than finding a consensus on the regulatory goals."

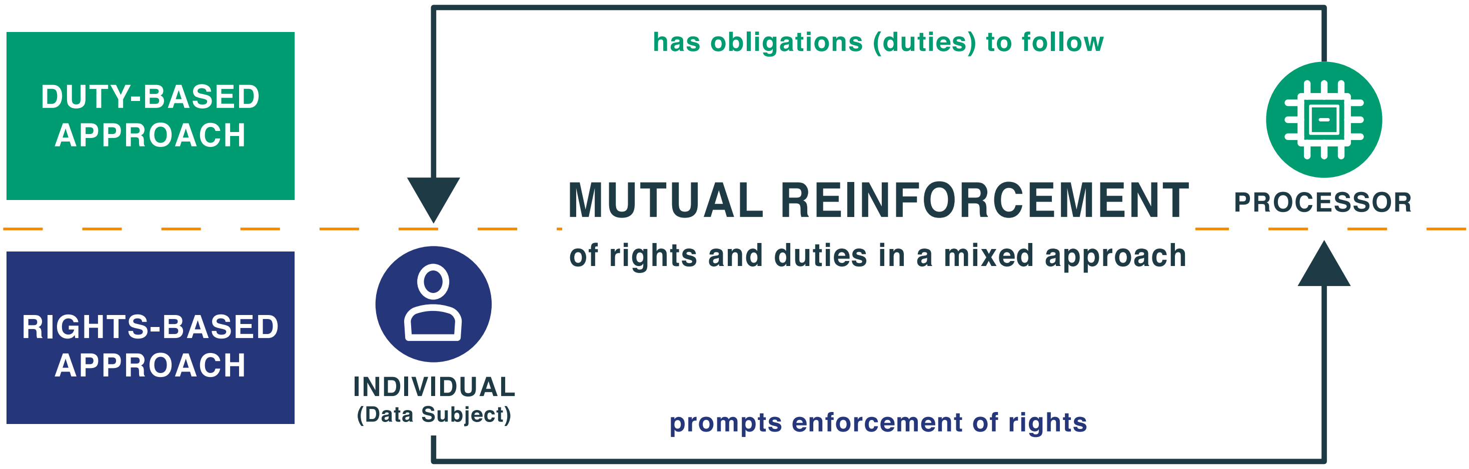

DUTY-BASED APPROACH
RIGHTS-BASED APPROACH
has obligations (duties) to follow
MUTUAL REINFORCEMENT
of rights and duties in a mixed approach
PROCESSOR
INDIVIDUAL
(Data Subject)
prompts enforcement of rights

Figure 6: Mutual reinforcement of rights and duties in a mixed approach

The pan-African harmonisation therefore essentially requires a negotiation of the desired regulatory outcomes. Such a directive - formally comparable to the EU's legal framework - would provide for a consented regulatory goal as well as general guidelines. It would further permit national characteristics in the directive's implementation in the Member States. In their own laws, Member States could include a provision that considers the laws of those other Member States equivalent who implement the same directive. This results in a mutual recognition of adequate levels of protection. The directive in combination with each member state's laws are thus a multilateral form of well-known bilateral arrangements of mutual recognition, such as the EU-U.S. Privacy Shield or double taxation agreements.

3.1.2 Legal design choices to operationalise data protection objectives for blockchain technology

> "Various regulatory means can serve to realise selected objectives; while means can have unintended effects beyond the intended outcomes."

A coherent process for designing data protection law with an eye for blockchain would start with finding consensus on the law's objective(s). This involves carefully selecting and defining the protected goods. These could e.g. be "privacy", "fairness", "personality rights", "dignity", "the individual", or "fundamental rights and freedoms".[38] It is important to note that these concepts are only similar at first sight. In fact, the very selection of the protected good has consequences for the next steps. These include framing risks, choosing legal means to safeguard against these risks and foreseeing the particular forms and implementations of blockchain technology that the law enables or impedes. Oftentimes, there are various regulatory means to realise selected objectives and means can have unintended effects beyond the intended outcomes.

With a view to blockchain technology, both regulatory means and objectives may create tension between the technology's design and data protection regulation, in areas such as:

- Secrecy versus transparency;
- Forgetting versus remembering;
- Updates and corrections of data
- The different roles of data subjects' rights.

In order to avoid possible tensions between blockchain technology and data protection regulation, several elements, described below, shall be included in design provisions for all data protection laws for blockchain technology to strive.

[38] There is no consensus either on the concept of "privacy", see Mulligan, D. K.; Koopman, C. & Doty, N. (2016), *Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy.* In: Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, p. 374.

Secrecy versus transparency

Every legal system has developed its own differentiated way of treating particular issues, events, practices and activities as secret, confidential, open or transparent. These differentiations reflect social and national history, past and present experiences as well as cultural and political values. In many cases, neither secrecy, confidentiality, openness nor transparency are meant to be an end in itself, but a means for achieving other ends.[39] The following design choices have to be made in blockchain systems.

- **General transparency rules out selective disclosure.** Only if particular information is generally kept confidential, it can be made available to particular persons, groups or organisations on a case-by-case basis, e.g. after examining their legitimate interest or for specific purposes only.[40] Confidentiality thus serves the end of making information selectively available. The use of a public blockchain would impede the regulator's ability to selectively disclose information, as it would be generally transparent.

- **Decentralisation can serve as a technical measure to safeguard transparency.** Some information might not only be made public as such, but in a sustainable way. For example, information made public in a very decentralised manner, impedes or defies attempts to monopolise the information or withdraw it from the public eye.

- **Blockchain systems present new ways to access information and require new digital literacy.** Distributed ledger technologies may create obstacles for those lacking particular technical means or skills, especially if applied to public information, this may widen the digital divide. Conversely, presenting information through the form of blockchain may also allow for completely new levels of access, e.g. through applying computational methods of analysis that were not possible on the datasets before.

As exemplified above, the application of DLT may challenge traditional structures and values regarding different forms of secrecy and transparency. It may, in fact, negate the very purposes they are intended to serve if introduced without considering the consequences. Putting information directly on a public blockchain, e.g. financial transactions as in the case of the Bitcoin blockchain, would make hitherto confidential data open to everyone. Putting previously public information on a private blockchain would make them inaccessible for the general public. The sudden transparency of formerly secret or confidential data may introduce unintended consequences, such as exposing individuals' financial, health, educational or application data to blackmailing, extortion or scams, or exposing journalists to parties whom they are investigating if their freedom of information requests are made public. In addition, it may undermine the purpose formerly served by secrecy or confidentiality.

Like every other form of digitalisation, the application of blockchains may create new kinds of metadata, with public blockchains also making these widely available. This could lead to unintentionally exposing individuals within organisations, who are merely tasked with appending information to the ledger. This new deluge of metadata will allow for new forms of data analysis and possibly surveillance.

To prevent unintended consequences, decisions on treating particular issues, events, practices, activities as secret, confidential, open or transparent should rest with the political decision-maker. Blockchain-based systems should then be designed, implemented and used according to these decisions, and not the other way around.

[39] For example, both the traditional openness of individual and corporate tax returns in Northern European countries and the equally traditional confidentiality of tax returns in Central European countries serve the same purpose: maximising the state's tax revenue. In the former case, the tax returns' openness allows for members of a community to monitor the tax honesty of their fellow community members, while in the latter case, the state promises to keep tax returns confidential if and only if they are submitted exhaustively and honestly covering all tax-related issues. Thus, tax return openness and confidentiality are means for the same purpose, with each state's choice of the former or the latter being historically contingent, originating from a particular value system at the time of its introduction, and forming and reinforcing the value systems of today.

[40] For example, in Germany residential registration data is generally confidential, but upon request, political parties are given access to this data to distribute election campaign information.

Forgetting versus remembering

Societies have developed different cultural, legal and institutional answers on how to cope with remembering and forgetting beyond the sphere of the individual and community memory. For example, forgetting is deeply enshrined in American culture as a society originating primarily from immigrants leaving their former home countries to start a new life in the New World, a culture that was reinforced over centuries with people moving westwards, leaving behind their old lives and starting anew somewhere in the West. While historically very different, Germany, for example, introduced a legislation to erase past criminal records with an eradication period of 5, 10, 15 or 20 years depending on the amount of the penalty as long as no new criminal offenses have been committed. This can be regarded as a form of "institutional forgetting". A similar approach has been taken by many truth commissions in the historical reappraisal of states' and collectives' dictatorships, crimes or civil wars. These societies' particular histories have strongly shaped their individual - and often highly political - approaches to remembering and forgetting, which have then been implemented in data protection laws, e.g. the "right to be forgotten" enshrined in Article 17 of the EU General Data Protection Regulation.

Distributed ledger technologies pose severe challenges to differentiated approaches to remembering and forgetting, e.g. regarding different parts of a record, changes over time, or the different treatment of different social actors. So, these - sometimes politically delicate - social agreements might be put under serious pressure. It is thus of vital importance to build a consensus in society regarding the treatment of collective and institutional memory and the consequences it entails, before rashly implementing DLT.

Updates and corrections of data

All data protection laws require data to be correct and kept up to date. This requirement poses severe challenges for the application of distributed ledger technologies, such as blockchains. With distributed ledgers, it is essentially impossible to correct false or update outdated information stored on the blockchain. Instead, blockchain technology only allows for adding new information to the (end of the) blockchain. Thus, every blockchain will show its entire history of entries, including those that were found incorrect, invalid, misleading or outdated. Anyone, including the data subjects, are only able to flag or revoke, but not to permanently remove such entries.

> "With distributed ledgers, it is essentially impossible to correct false or update outdated information stored on the blockchain."

While this issue of the non-modifiability is related to remembering and forgetting, it also raises its own distinct challenges. Not only does it expose every clerical error to the public, but it might pose severe challenges to every user of the blockchain. If a blockchain contains millions or billions of entries, users may be unable to ensure they have obtained the latest and correct information from the ledger. For example, the Bitcoin blockchain's total size has reached an astonishing 262 gigabytes in February 2020. Thus, the proliferation of distributed ledgers and their application in an ever increasing range of fields may lead to a situation where the ability of public administration, private businesses, civil society and individuals to make informed decisions based on valid, correct and up-to-date information may be severely hampered by the challenges of retrieving such data from distributed ledgers at reasonable transaction costs or at all. This may create negative consequences for those that depend on these actors' decisions, such as citizens, customers, patients or students. While this particular problem may be solved by centralising the blockchain, the very centralisation undermines many of the advantages of a decentralised or distributed system, such as its greater scalability, availability, resilience and fault tolerance.

The different roles of data subjects' rights

Data protection laws usually confer rights to the individual whose data is being processed, the data subject. These rights can be of different character: they may be ends in themselves, they may be means serving other ends, or both.

- **Data subjects' rights as ends in themselves - typical for rights-based regulatory regimes:** Data subject's rights are then concretisations of the more general rights that the law aims to protect, e.g. privacy or fundamental rights and freedoms. They are meant to guide the design, implementation and practices of information processing.
- **Data subject's rights as means to serve other ends - typical for duty-based regulatory regimes:** By conferring rights to individuals, these individuals are turned into stakeholders of their own that would help to enforce the provisions of the law out of their own, though conferred, interests.

> "It is thus highly recommended to establish 'data protection by design' provisions in all data protection laws."

The **EU General Data Protection Regulation** is an example of combining both. The rights conferred are ends in themselves, which directly bind controllers and processors. They aim to guide the implementation of appropriate technical and organisational measures in order to protect these rights ("data protection by design", Article 25). They are, however, also means to facilitate the detection of data protection breaches and the enforcement of the Regulation by distributing the power to question and control the controllers' data processing practices.

State of data subject rights in data regulations in Africa

	28 countries grant the right to **access** personal data 97% of countries with data protection laws	**27 countries** grant the right to **access and rectify** personal data 93% of countries with data protection laws	**20 countries** grant the right to **access, rectify and erase** personal data 69% of countries with data protections laws
Algeria	•	• •	
Angola	•	• •	• • •
Benin	•	• •	• • •
Botswana	•	• •	
Burkina Faso	•	• •	
Cabo Verde	•	• •	• • •
Chad	•	• •	• • •
Côte d'Ivoire	•	• •	• • •
Equatorial Guinea	•	• •	• • •
Gabon	•	• •	• • •
Ghana	•	• •	
Guinea	•	• •	• • •
Kenya	•	• •	• • •
Lesotho	•	• •	• • •
Madagascar	•	• •	
Mali	•	• •	• • •
Mauritania	•	• •	• • •
Mauritius	•	• •	
Morocco	•	• •	
Niger	•	• •	• • •
Nigeria	•	• •	• • •
São Tomé and Príncipe	•		
Senegal	•	• •	• • •
Seychelles	•	• •	• • •
South Africa	•	• •	• • •
Togo	•	• •	• • •
Tunisia	•	• •	• • •
Uganda	•	• •	• • •

Figure 7: State of data subject rights in data regulations in Africa

In the EU regulation, subjects' rights may include the right of information about the data that is held about them, the right to access these data, the right to rectification, the right to erasure - sometimes called the "right to be forgotten" -, the right to restriction of processing, the right to object, whether in general or to the sale of personal data, and the right to data portability.

These rights generally pose similar challenges regarding the use of blockchain technology to the respective duties: the right to rectification constitutes similar challenges to the duty to keep data correct and up-to-date, the right to erasure to the duty to delete personal data not necessary anymore for the purposes for which it was collected, etc.

Other data subjects' rights in the EU regulation, such as the right of information, the right to access, the right to restriction of processing or the right to data portability, pose no particular challenges to blockchain technology if it is designed, implemented and used in an appropriate manner to safeguard these rights.

It is thus highly recommended to establish "data protection by design" provisions in all data protection laws that require companies and other public and private organisations to implement technical and organisational measures at the earliest stages of the design of the processing operations, in such a way that safeguards data protection principles and data subjects' rights right from the start (see figure on state of data subject rights in data protection regulations in Africa).

3.1.3 Supervisory authorities and enforcement in the face of blockchain technology

Independent of a particular data protection law following a rights-based or a duty-based approach, supervisory authorities play a major role in all data protection regulations. Supervisory authorities complement data subjects in enforcing their rights in rights-based regimes, they add external monitoring to the controllers' self-monitoring in duty-based regimes, and they do both in mixed-data-protection regimes (see figure on state of data protection law enforcement in Africa).

Their tasks include, among others,

- to **monitor the application of the law,**
- to **advise** data subjects on their rights, data controllers on their duties as well as governments and legislators on legislative and administrative measures,
- to **create guidelines** and collect best practices and disseminate both to all stakeholders,
- to handle complaints lodged by data subjects and other stakeholders and investigate the subject matter of the complaint,
- to **conduct investigations** on the application of the law, including audits, issue warnings and reprimands, and impose administrative fines, and
- to **monitor relevant developments** regarding information processing technologies and practices that have an impact on data protection.

State of data protection law enforcement in Africa

	29 countries with **legal existence** of a data protection authority 100% of countries with data protection laws	**14 countries** with **established and active** data protection authority with a **clear mandate and resources** 58% of countries with data protection laws
Algeria	●	
Angola	●	
Benin	●	●
Botswana	●	●
Burkina Faso	●	
Cabo Verde	●	●
Chad	●	
Côte d'Ivoire	●	●
Equatorial Guinea	●	
Gabon	●	●
Ghana	●	●
Guinea	●	
Kenya	●	
Lesotho	●	
Madagascar	●	
Mali	●	●
Mauritania	●	
Mauritius	●	●
Morocco	●	●
Niger	●	●
Nigeria	●	●
São Tomé and Príncipe	●	●
Senegal	●	●
Seychelles	●	
South Africa	●	
Togo	●	
Tunisia	●	●
Uganda	●	
Zambia	●	

Figure 8: State of data protection law enforcement in Africa

> "Regulation must ensure that supervisory authorities' staff has adequate qualifications, experience, skills and resources."

In order to be able to fulfil their complex tasks regulation must ensure that supervisory authorities' staff has adequate qualifications, experience and skills and the authorities are provided with the necessary human, technical and financial resources, premises and infrastructure. To strengthen the pan-African harmonisation and enforcement of data protection and to allow the free flow of information, it is further recommended to establish provisions that enable and mandate supervisory authorities to cooperate with other supervisory authorities across Africa and beyond. These authorities need to be provided with the necessary resources to fulfil these tasks, which also includes the sharing of information and mutual assistance.

3.2 Financial regulation: considerations for distributed ledger technology applications in finance

Whenever blockchain (or DLT) systems are applied for the conduct of financial services, the service provider is subject to financial regulations of the jurisdiction it is operating in. Depending on the type of the service provided, or the activity carried out, disclosure, licensing or other requirements may apply. These might range from

- reliability checks for owners/shareholders as well as management of financial services,
- to solvency and liquidity rules and risk and compliance management requirements that traditionally apply for financial service providers,
- to consumer protection and security (market conduct) rules that also apply for non-bank financial service providers,
- to specific disclosure regimes, like prospectuses and/or filings.

The application of rules is context-specific and best identified in coordination with the financial regulatory authority of the concerned jurisdiction.

Traditional crypto-assets, i.e. the type of permissionless (public) tokens (e.g. Bitcoin), typically claim to not be governed by any particular party. Therefore, their issuance is difficult to regulate. During the hype of initial coin offerings, many tokens which fall under the securities regulations of various jurisdictions have been issued and publicly sold. All of those tokens have attracted the attention of financial policymakers and regulators internationally due to implications on the integrity and stability of the financial system.[41] Regulators are especially concerned about issues around consumer and investor protection (due to little or inadequate disclosure of risks involved in the acquisition of tokens) and the use of crypto-assets to cover up illicit activities, such as money laundering, terrorist financing, bribery, corruption or fraud. Such illicit financial flows are increasing, and DLT have become known as means of facilitating them. At the same time, the Financial Stability Board[42] emphasises that the technologies' underlying crypto-assets "have the potential to improve the efficiency and inclusiveness of both the financial system and the economy".

With the increasing use of crypto-assets globally, global standards and national regulations for financial integrity have become a key issue.[43] In October 2018 and June 2019 the Financial Action Task Force (FATF) moved on to update its standards (mainly the Recommendation 15) in order to clarify the application of anti-money laundering (AML) and counter terrorist financing (CFT) requirements on what it calls "virtual assets" and "virtual asset service providers," i.e. crypto-asset exchanges and wallet providers, in view of addressing the threat posed by illicit financial flows through crypto-assets

[41] See Financial Stability Board, 2018. *To G20 Finance Ministers And Central Bank Governors*. Financial Stability Board. Available at: https://www.fsb.org/wp-content/uploads/P180318.pdf [Accessed 8 May 2020] and Financial Stability Board, 2018. *Crypto-Assets: Report To The G20 On Work By The FSB And Standard-Setting Bodies*. Financial Stability Board. Available at: https://www.fsb.org/wp-content/uploads/P160718-1.pdf [Accessed 8 May 2020].

[42] The FSB is an international body that coordinates the work of national financial regulatory authorities.

[43] The FSB thus calls for further international coordination and more engagement by standard-setting bodies such as the (Committee on Payments and Market Infrastructures) CPMI, International Organization of Securities Commission (IOSCO) and the Basel Committee on Banking Supervision (BCBS).

to the integrity of financial systems. The updates include obligations for risk mitigation as well as for licensing and registration of such providers.[44, 45]

The FATF Recommendations are meaningful both to its member states and to non-members. Non-member states that do not follow the FATF standards have to expect sanctions, which make it more complicated to conduct international payments. Additionally, the existence of global standards for crypto-assets will increase the pressure on non-member states to position themselves vis-à-vis such new, interconnected global payment infrastructures. An effect of the FATF Recommendations is that they practically introduce a demarcation between two regimes: the compliant blockchain world and the non-compliant blockchain world. Outcomes of such an approach can be seen in Switzerland where compliant service providers are prohibited from doing business with non-compliant systems. A seamless transition is apparently not desired and is becoming increasingly difficult. This may be a relevant message for African countries that already struggle with cross-border financial transactions: virtual asset service providers are supposed to require a license or at least be registered publicly. Additionally, the so called travel rule is extended to the transfer of virtual assets, which means that virtual asset service providers need to obtain, hold and submit to the beneficiary virtual asset service provider information on the originating as well as beneficiary wallet account that are parties to a given transfer. Moreover, they must implement measures to monitor, freeze and prohibit transactions.

These requirements assume a central service provider and the industry initiated certain working groups to deliver technical solutions satisfying the FATF recommendations. However, it remains to be seen how FATF deals with truly decentralised tools. For the African continent, the so-called FATF regional communities help with implementation and channel feedback to the main organisation. The NGO Alliance for Financial Inclusion (https://www.afi-global.org/) additionally supports central banks and regulators in developing and emerging economies in their dialogue with FATF.

In addition to the public money laundering and terrorism financing monitoring needs, protecting investors by providing for a proper disclosure regime (especially prospectus requirements for public securities offerings) and protecting customers of finacial servicing offerings (like payment services, investment advice, custody of finanical assets) are core topics for financial regulatory regimes.

[44] FATF, 2019. *Public Statement On Virtual Assets And Related Providers.* FATF. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html [Accessed 8 May 2020].)

[45] For a legal interpretation see: DWF, 2019. *DWF Spotlight: FATF Recommends Regulating And Monitoring Virtual Asset Service Providers.* DWF. Available at: https://www.dwf.law/Legal-Insights/2019/August/Regulation-of-virtual-asset-service-providers [Accessed 8 May 2020].

Focus box: A blockchain-powered KYC layer for financial services and international trade

Much attention has been given to the ambivalent relationship between public blockchain architectures and the enforcement of KYC rules, which are critical means against AML and CFT. However, blockchain technology itself could also be used to address shortcomings of current KYC governance. Existing platforms for customer due diligence (CDD) in trade finance are known to not be very effective. Among the reasons are that existing KYC repositories lack focus on developing markets or that they focus on commercial banks only, but not on corporates and small and medium enterprises (SME). Beyond that, high subscription cost discourages financial institutions and entities from connecting with these platforms. As a result, KYC concerns still rank highest among the reasons for rejected transactions in trade finance.

Easing KYC has been identified as a lever to increase financial inclusion, foster innovation and drive competition in financial services long before blockchain. Now, the idea is gaining track to use blockchain technology in favour of KYC. Blockchain technology could offer the infrastructure to power a trustworthy KYC layer for financial services (sometimes referred to as collaborative CDD). As a distributed, digital repository, this KYC layer would facilitate the sharing of authoritative KYC information. It could provide a single source of primary data required to conduct CDD checks on counterparties.

Information would be independently verified prior to publishing on the repository. In addition to the host of such a blockchain-powered CDD platform, regulators could participate by verifying logged information. This way, information could be collated for KYC checks in line with globally recommended standards (such as FATF). Financial institutions, SME and corporate entities would upload their information on the repository using standardized KYC/AML templates.

Market participants would benefit from "one stop access" to KYC/CDD information. This would ease onboarding of customers, increase efficiencies and reduce regulatory risk. African economies could benefit from consistent CDD information for various entities on the continent.

3.3 Existing national blockchain strategies under review

Governments around the globe have devised blockchain strategies as instruments to deal with this new technology in terms of policy, oftentimes acknowledging the short half-life of any digital strategy. Cursory research identified more than a dozen explicit national blockchain strategies or strategy-resembling documents that have been published within the last three years.[46] Without claiming a systematic review - partially due to language barriers - this chapter presents common elements in these strategies and highlights different policy approaches towards a blockchain-enabled future, occasionally pointing out forks in the road that could lead to very different outcomes for the global blockchain ecosystem.

[46] See Appendix A.

3.3.1 Between promoting innovation and preventing crime

A recurring theme in all blockchain strategies under review is that they address the tension between promoting innovation and preventing crime. Governments want to be frontrunners in blockchain technology by enabling legislative frameworks for innovation and growth. They attempt to "lead by being proactive, open to business, attracting entrepreneurs and investors from all over the world" (Malta), provide "possibilities for field testing under real-world conditions" (Germany) or, be home to "international blockchain collaborations" (The Netherlands). At the same time, the strategies reflect that global concerns are rising with regard to money laundering, terrorism financing, bribery, corruption, fraud and other activities of financial crime. Blockchain technology has been associated ingloriously with such crimes, precisely due to the architectural properties that make blockchain an enabling technology for digital innovation, e.g. its distributed nature and cryptographic methods. This poses challenges to technology governance.

> "A recurring theme in all blockchain strategies under review is that they address the tension between promoting innovation and preventing crime."

In the financial sector, regulatory goals of promoting innovation on the one hand and preventing crime on the other appear most difficult to unite. This is because innovation in distributed ledger ecosystems requires openness, while preventing crime tends to relate to oversight mechanisms that are difficult to maintain in an extremely open environment. With this in mind, several governments plan to amend legislative frameworks relating to financial policy. Germany plans to allow digital securities. Australia wants to remove double taxation of Goods and Services Tax in the context of digital currency, effectively mandating taxation only when purchasing goods with digital currency, but abolishing taxation when acquiring digital currency. It further explores the possibility of using blockchain as a utility for sharing KYC information [see focus box A Blockchain-powered KYC-layer]. This could enhance competition in the financial sector, because it would alleviate an existing bottleneck-situation.[47] Hopes are high that using blockchain as a common KYC-layer could foster transferable KYC checks, thereby lowering switching rates, driving down fees in the banking sector and simplifying complex interest structures. As other strategies note, KYC-sharing could effectively complement national efforts to improve and foster ID services at large (Bangladesh).

At the same time, many governments see the need to close regulatory gaps (taxation, data protection) and create safeguards against the abuse of blockchain technology, e.g. to prevent corruption and crime and to protect consumers. One of the focus areas are initial coin offerings. Germany is considering to condition the publication of such crypto-tokens on the disclosure of baseline information that has been reviewed by the financial authority. Other governments focus on avoiding tax evasion through cryptocurrencies. The idea is to create taxation regimes for transactions that involve business activities in cryptocurrencies (Australia, Cyprus). This could imply treating token transactions the same as transactions with fiat currency per the Income Tax Law and consider block rewards to blockchain miners as ordinary income (Cyprus). Another set of measures concerns AML law. The FATF, which is a de facto standardisation body in this field, has adopted an interpretive note to its recommendations on distributed ledger services in June 2019. Some of the more recent blockchain strategies pledge to comply with the FATF and focus on regulating so-called virtual asset service providers, who act as intermediaries in blockchain ecosystems [see chapter Financial regulation].

[47] Currently, every provider of financial services is tasked with securing identification of new customers independently.

3.3.2 Capacity building and research

While sharing a sense of excitement about the still nascent distributed ledger technologies, most strategies emphasise the necessity to allocate funding to research, capacity building and knowledge transfer (Kenya, India, Bangladesh, Australia, Germany, France, Netherlands). It appears noteworthy that several strategies (France, Australia, Netherlands) explicitly recommend research approaches that are both interdisciplinary and applied. Here, research should involve both social and computer sciences and it should include students, universities and companies - especially SMEs - alike. This shows policy makers' matured view on blockchain as a contextualised technology with on-chain and off-chain governance aspects in comparison to the previously isolated focus on technology development. Several strategies reflect that the feasibility of blockchain-based applications very much depends on institutional, regulatory and ecosystem context. Governments further see the need to quickly educate both professionals and students about blockchain technology in order to build a professional skill base, also in native languages. This shall serve to satisfy in-country demand for expertise, including within administrations, and allow governments to position their countries as blockchain hubs.

> "Governments establish blockchain working groups, centers of excellence, innovation hubs and authorities."

Across blockchain strategies, a trend towards government-driven institutionalisation of blockchain policy and expertise appears prevalent. Governments establish blockchain working groups, centers of excellence, innovation hubs and authorities. These institutions are mandated with inward- and outward-oriented tasks. Inward-oriented tasks include offering expertise and guidance to legislators and regulators. Outward-oriented tasks include auditing and certifying technology arrangements, but also helping entrepreneurs navigate the regulatory system. Striving for international institutionalisation still appears to be less common and more restricted to particular aspects of blockchain policy. E.g., Germany explores the feasibility of creating an international dispute resolution authority that could address jurisdictional conflicts in blockchain-powered digital services.

3.3.3 Policy approaches

Governments take different policy and regulatory approaches when dealing with blockchain technology. These approaches are not always made explicit in the strategy documents, but a rough categorisation is possible. It might help decision and policy makers reflect about their engagement. Government involvement in blockchain development can be viewed along three dimensions:

1. timing of involvement,
2. degree of involvement,
3. role in development of (technical) standards.

Timing of involvement: ex-post and ex-ante approaches

Ex-post and ex-ante approaches to blockchain governance present different mindsets in the field of technology governance. They either make openness the starting point of digital policy or they start with caution and control. In many strategies, we can observe elements of both.

The **ex-post approach** stands for openness. It allows for permissionless innovation, meaning that all innovation with blockchain technology - both on the protocol and on the application layer - is possible unless declared otherwise. This fosters an innovation ecosystem that is open for unknowns. An expression of this is Uganda's Kampala Declaration, which pledges "non-regulation of the blockchain" until further research has been conducted.

In softer variations of this approach, governments create baseline protections and frameworks that guide innovation, e.g. by providing regulatory certainty. An example of a softened ex-post approach is the EU's or Australia's encouragement of innovation in the field of digital ID, as long as applications

> "'Regulatory sandboxing' is a fairly new supervisory concept allowing companies to pilot blockchain-based systems under priviledged regulatory conditions within limited time and scope."

link back to trusted digital identity frameworks that define requirements and different assurance levels (Australia, also EU eIDAS).

In contrast, the ***ex-ante approach*** focuses on pre-release certification of blockchain technology or platforms. Essentially, this approach makes blockchain-based innovation subject to permission. Governmental authorities take the role of auditors. In the field of financial regulation, the FATF recommendations about AML and CFT actually suggest such approaches. The Australian and the Maltese strategy, for example, state that digital currency exchange providers with in-country business operations will have to register with the regulator. While the advantages of the ex-ante approach lie in the minimisation of risks and a high degree of national control, it can also stifle innovation, especially from the startup and SME sectors where there is little capacity to engage in heavily administrative processes before understanding whether a product will be met with demand by the market.

An innovation-friendly **path in-between ex-post and ex-ante regulation** lies in so-called **regulatory sandboxing** (Kenya, Mauritius, Germany). "Regulatory sandboxing" is a fairly new supervisory concept allowing companies to pilot blockchain-based systems under priviledged regulatory conditions within limited time and scope. This way, the private sector can pilot systems, while governments with oversight can mitigate risks and learn along the way. Despite the popularity of the term however, there is little information yet on how sandboxing actually works with regard to blockchain.

Degree of involvement

Different degrees of governmental involvement with blockchain development can be identified in the strategies. They present different ways and intensities of interacting with and stimulating the ecosystem.

1. **Governments support private sector innovation** in industries and for use cases that are deemed to be of national relevance. This type of involvement resembles classical approaches of regional and sectoral economic support programmes.

2. **Governments act as first movers.** Here, governments drive the adoption of blockchain technology by implementing it in public administration for the purpose of good governance. The aim is to directly improve public service delivery, e.g. by making document processing more efficient or increase transparency and accountability through secure, tamper-proof and transparent handling of data. Application areas include managing licenses, permits and registries as well as import and export documents or pension data. By being first movers, governments act not only as regulators, but also as customers and/or users of blockchain technology. They gather hands-on experience and - by investing in software infrastructures - possibly create spillover effects on the private sector to promote innovation and economic growth.

3. **Governments operate and provide blockchain-infrastructure services.** In an attempt to increase sometimes national sovereignty and gain independence from existing blockchains that do not grant states a meaningful role in their governance setups, several governments reclaim their role as trust-providers and integrate blockchain governance into their political system. They enter the field of blockchain-as-a-service provision with national blockchain platforms. The European Blockchain Services Infrastructure may serve as an example of multiple governments sharing a single infrastructure, a model that may also be appropriate for African states. It shall initially enable public services, but shall soon open up to private sector use(r)s as well. Similar plans exist in Kenya, Bangladesh or India.

Role in development of (technical) standards

As blockchain technology is maturing, most strategies articulate that it should be a common goal to strive for widely accepted, interoperable technical standards because such standards can unlock network effects that will help the blockchain ecosystem to flourish. Harmonised (technical) standards are, among other things, the basis for inclusiveness and connectivity between blockchains, which could in turn enable interconnected markets as well as interconnected public blockchain infrastructures.

Similar to the field of internet governance, governments have different visions as to which stakeholder groups should be involved or lead the process of defining such global standards. Positions range from

- leaving standard development in the hands of the private sector and technical communities while confining their focus on legislative outcomes and generally embracing a language of technological neutrality to,
- leading standard development by working with international organisations such as the International Organization for Standardization,[48] emphasising public competencies and authority, to
- fostering multi-stakeholder approaches that facilitate collaboration across-industries, between public and private sectors as well as with civil society.

> "It should be a common goal to strive for widely accepted, interoperable technical standards because such standards can unlock network effects that will help the blockchain ecosystem to flourish."

While every government will have its own reasoning with regard to standard development, it seems worth mentioning that in emergent and connected, but for the most part unregulated industries, technical standards need the buy in of as many stakeholder groups as possible to become de facto norms.

[48] Australia is highlighting its leading role in promoting blockchain standardisation through the ISO where a new ISO technical committee (# 307) has been established for blockchain standards topics, including interoperability, terminology, privacy, security and auditing. Result of the group's work can be found in the catalogue (ISO, 2020. *Standards By ISO/TC 307 - Blockchain And Distributed Ledger Technologies*. ISO. Available at: https://www.iso.org/committee/6266604/x/catalogue/ [Accessed 8 May 2020]).

Focus box: Regulatory pioneers and blockchain usage by governments in Africa

Ethiopia

The Ethiopian Government partnered[49] with blockchain research and development company IOHK to develop blockchain applications for coffee shipments and other areas of agriculture. IOHK further announced[50] the use of Atala, an enterprise blockchain framework focused on governments in need of a municipal currency or a supply chain management system, in collaboration with the government of Ethiopia.

Ghana

In partnership with a blockchain technology platform, the Land Commission and the World Bank launched a pilot[51] project to register lands on a blockchain. The pilot project focused on 20 communities in Kumasi Ghana.

Mauritius

The Government of Mauritius[52] created a regulatory sandbox license allowing development of blockchain based solutions under the supervision of the financial services regulator. The Economic Development Board of Mauritius issued regulatory sandbox licences[53] to various FinTech companies.

Kenya

The Capital Markets Authority of Kenya was also among the first regulators in Africa to implement a sandbox environment for startups and blockchain/fintech companies to test blockchain applications, however excluding cryptocurrency projects[54] out of these incubation efforts in 2019.

Noteworthy are also the efforts of the government of Kenya, specifically its creation of a Blockchain and AI task force in 2018 and its publication of a comprehensive strategy[55] paper outlining regulatory approaches in 2019. After the country's fast adoption of mobile payment systems, the task force released a report identifying use cases and recommending the creation of financial and regulatory sandboxes for emerging technology applications.

The Government of Kenya also explored the use of blockchain in issuing a retail savings bond called M-Akiba.[56] Utilizing a blockchain platform for this service would enable the government to seamlessly manage a large number of small transactions and accounts.

Nigeria

Nigeria's National Union of Road Transport Workers launched[57] a blockchain- based passenger manifest system to ensure drivers and passenger information are securely captured in a digital, secure, transparent and fully auditable manner. The blockchain platform was deployed to monitor, track and analyze all the operations of the scheme in real time.

[49] Sundararajan, S., 2018. *Ethiopia Is Exploring The Use Of Blockchain Technology To Track The Supply Chain For Its Largest Export, Coffee.* Available at: https://www.coindesk.com/ethiopia-explores-blockchain-role-in-tracking-coffee-exports [Accessed 8 May 2020].

[50] Wolfson, R., 2019. *Cardano Founder Launches Enterprise Blockchain Framework In Collaboration With Ethiopian Government.* Forbes. Available at: https://www.forbes.com/sites/rachelwolfson/2019/04/30/cardano-founder-launches-enterprise-blockchain-framework-in-collaboration-with-ethiopian-government/#5eca31164e10 [Accessed 8 May 2020].

[51] The World Bank, 2013. *Project Performance Assessment Report: Ghana Land Administration Project.* The World Bank. Available at: https://ieg.worldbankgroup.org/sites/default/files/Data/reports/PPAR-75084-P132252-Ghana_Land_Administration.pdf [Accessed 8 May 2020].

[52] ConsenSys, 2019. *Which Governments Are Using Blockchain Right Now?*. Available at: https://consensys.net/blog/enterprise-blockchain/which-governments-are-using-blockchain-right-now/ [Accessed 8 May 2020].

[53] Economic Development Board, 2019. *EDB Issues Regulatory Sandbox Licences To Fintech Companies For Their Innovative Projects.* Economic Development Board. Available at: https://www.edbmauritius.org/newsroom/posts/2019/january/edb-issues-regulatory-sandbox-licences-to-fintech-companies-for-their-innovative-projects/ [Accessed 8 May 2020].

[54] Mwaniki, C., 2019. *CMA Locks Cryptocurrencies Out Of Innovation Hub.* Business Daily Africa. Available at: https://www.businessdailyafrica.com/markets/marketnews/CMA-locks-cryptocurrencies-out-of-innovation-hub/3815534-4993324-mh01pkz/index.html [Accessed 8 May 2020].

[55] Ministry of Information, Communications and Technology, 2019. *Emerging Digital Technologies For Kenya. Exploration And Analysis.* Ministry of Information, Communications and Technology. Available at: https://www.ict.go.ke/blockchain.pdf [Accessed 8 May 2020].

[56] M-Akiba, n.d. *M-Akiba.* Available at: https://www.m-akiba.go.ke/ [Accessed 8 May 2020].

[57] Avan-Nomayo, O., 2019. *Africa Using Blockchain To Drive Change, Part One: Nigeria And Kenya.* Cointelegraph. Available at: https://cointelegraph.com/news/africa-using-blockchain-to-drive-change-nigeria-and-kenya-part-one [Accessed 8 May 2020].

As earlier stated, House Africa, an indigenous Nigerian company has partnered with[58] the Nigerian Mortgage Refinancing Company to service land verification for all Nigerian commercial and mortgage banks.

Rwanda

The National Bank of Rwanda and Rwanda Utility and Regulatory Authority has established[59] a sandbox facility to test blockchain technology.

In 2018, the country announced[60] the world's first blockchain project to track tantalum from the pit to refineries in an effort to boost investor confidence of conflict-free sources of minerals.

Sierra Leone

The Government of Sierra Leone announced[61] it was developing a blockchain-based digital identification system. The project is said to be already in the first phase where all identity records are being digitised. In the subsequent phase, every person shall be issued a unique, non-duplicated and non-reusable national identity number. The system is planned to be up and running by 2020. The project is in partnership with the United Nations. It is also planned that credit history will be recorded on the digital ID, allowing people to access credit instantly.

South Africa

Next to the previously mentioned Next Einstein Forum, regulatory pioneers for blockchain include the South African Reserve Bank. For their blockchain pilot based on the Ethereum blockchain, the South African Reserve Bank was recognised with the inaugural "Best Distributed Ledger Initiative" award from Central Banking Publications.[62] The Reserve Bank in April 2019 further issued a tender notice[63] requesting for expressions of interest from prospective solution providers in order to explore piloting a CBDC. The Center for Affordable Housing Finance in Africa also piloted a blockchain-based property registry.

Tanzania

The government of Tanzania utilised blockchain technology to audit the public sector payroll thereby eliminating about 10,000 ghost workers[64] from the public sector.

Uganda

The Government of Uganda announced[65] that it was going to pilot a proof of concept land titles registry.

[58] Nigeria Mortgage Refinance Company, 2020. *NMRC Hosts Stakeholder Workshop On Building Credible Data To Drive Delivery Of Affordable Housing In Nigeria.* Nigeria Mortgage Refinance Company. Available at: https://nmrc.com.ng/nmrc-hosts-stakeholder-workshop-on-building-credible-data-to-drive-delivery-of-affordable-housing-in-nigeria/ [Accessed 8 May 2020].

[59] UNCDF, 2019. *The Fintech Landscape In Rwanda*. UNCDF. Available at: https://www.uncdf.org/article/5216 [Accessed 8 May 2020].

[60] Uwiringiyimana, C., 2018. *Rwanda Hosts First Tantalum-Tracking Blockchain.* Reuters. Available at: https://www.reuters.com/article/rwanda-blockchain/rwanda-hosts-first-tantalum-tracking-blockchain-idUSL8N1VM3W9 [Accessed 8 May 2020].

[61] The Republic of Sierra Leone State House, 2019. *Sierra Leone Gets Africa's First Blockchain National Digital Identity System.* The Republic of Sierra Leone State House. Available at: https://statehouse.gov.sl/sierra-leone-gets-africas-first-blockchain-national-digital-identity-system/ [Accessed 8 May 2020].

[62] South African Reserve Bank, 2018. *Press Statement*. South African Reserve Bank. Available at: https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8753/Project%20Khokha%20press%20statement%2006%20September%202018.pdf [Accessed 8 May 2020].

[63] South African Reserve Bank, 2019. *Request For Expression Of Interest From Prospective Solution Providers In Anticipation Of A Feasibility Project For The Issuance Of Electronic Legal Tender*. South African Reserve Bank. Available at: https://www.resbank.co.za/AboutUs/Departments/FinancialServices/ProcNew/Pages/Publications.aspx?sarbweb=9f333ff2-bf64-4708-a361-076bd6802ff4&sarblist=fdf9dae8-3990-44d4-b89a-c87649f22461&sarbitem=40 [Accessed 8 May 2020].

[64] Ng'wanakilala, F., 2016. *Tanzania Says Over 10,000 'Ghost Workers*' *Purged From Government Payroll*. Reuters. Available at: https://www.reuters.com/article/us-tanzania-corruption/tanzania-says-over-10000-ghost-workers-purged-from-government-payroll-idUSKCN0Y70RW [Accessed 8 May 2020].

[65] Economic Development Board, 2019. *EDB Issues Regulatory Sandbox Licences To Fintech Companies For Their Innovative Projects.* Economic Development Board. Available at: https://www.edbmauritius.org/newsroom/posts/2019/january/edb-issues-regulatory-sandbox-licences-to-fintech-companies-for-their-innovative-projects/ [Accessed 8 May 2020].

4. RECOMMENDATIONS FOR THE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY IN AFRICA

This report has presented specific opportunities and challenges that blockchain technology poses when applied in an African context to further capitalise on its potential. As the technology's concepts may mirror a sense of community present across the continent, it may also assist in further cultivating the overarching cross-continental harmonisation. As such, it offers ICT decision and policy makers the opportunity to support not only economic and social development in Africa, but also the continent's vision of "an integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in the global arena"[66].

However, the regulatory frameworks for blockchain are still very uncertain, thereby limiting institutional, government and widespread adoption. ICT decision and policy makers therefore need to work with stakeholders to understand the technology in detail in order to regulate it in a way to drive innovation and not stifle it. Previously mentioned regulatory pioneers are providing helpful examples in how collaboration on early innovations can take place. Additionally, it must be kept in mind that blockchain development also depends on internet development. Many blockchain applications and all blockchain protocols need network infrastructure to run on, i.e. typically internet connectivity. That is why fostering internet connectivity and internet access across Africa is a foundational recommendation. With regard to blockchain technology in particular, the following cross-cutting issues need addressing by ICT decision and policy makers.

[66] African Union. 2020. Vision Of The African Union. Available at: https://au.int/en/about/vision [Accessed 8 May 2020].

4.1 Strategy: entering a blockchain-enabled future with a plan

SUGGESTION:

Develop a pan-African blockchain strategy in accordance with the African Union's digital strategy.

RATIONALE:

Blockchain technology offers vast design options and can be implemented for a plethora of use cases. Any blockchain application requires thoughtfully arranging on-chain and off-chain governance. In this complex scenario, a blockchain strategy helps by developing a common objective and vision. On the national level, a blockchain strategy identifies country-specific opportunities, provides guidance on how to unleash these potentials and marks desirable as well as necessary growth areas. At the pan-African level, the opportunity is even greater: a pan-African blockchain strategy could be a tool to start bridging different jurisdictions and avoid high legal costs for blockchain systems to be compliant across the continent. If designed in an inclusive manner, the process of strategy development itself presents an opportunity to grow both the national and the African blockchain ecosystems. By harnessing contributions in a multi-stakeholder dialogue, the screening of opportunities and obstacles becomes more complete and potential lines of conflict can be reconciled early on. Such a dialogue or alternatively, a review mechanism, should include the private sector, the technical community, research and civil society. In the international context, a blockchain strategy presents a valuable document to communicate policy positions, signal aspirations and make states approachable for collaboration and investments.

HOW TO PUT THE SUGGESTION INTO PRACTICE:

Bring all parties from the existing ecosystem to the table on equal footing, including ICT and financial regulators, blockchain associations, businesses, innovation hubs, researchers and representatives from the digital civil society. Develop a common vision and plan for a promising and suitable blockchain journey. Many blockchain strategies plan for similar stages:

- Explore the technology: gather and analyse the plethora of possible use cases.
- Gather hands-on experience: conduct action research by initiating pilot projects to verify opportunities, identify hurdles and discard unfeasible applications.
- Broaden the knowledge base: encourage interdisciplinary research and foster in-country capacity building.
- Create innovation-friendly regulatory regimes and reduce regulatory uncertainties: address policy challenges that arise from the interplay of architectural properties and the in-country institutional landscape, e.g. in the areas of data protection, financial regulation, standardisation and interoperability. Consider engaging with existing and emerging bodies for standardisation and their resources, e.g. FATF for financial regulation, the International Organization for Standardization for market relevant standards, the Coalition for Automated Legal Applications for the coordination of legal questions and associations aiming at fostering the discussion between governmental bodies, research, science and private industry like the International Association of Trusted Blockchain Applications (INATBA).
- Focus and assign resources: identify application areas that are both viable and strategically valuable and devote resources to these areas.

4.2 Data protection harmonisation: creating equivalent levels of data protection across the African continent

SUGGESTIONS:

- Seek pan-African harmonisation of data protection by negotiating consensus on the regulatory goals.
- Leave regulatory means to individual countries while creating a mechanism for mutual recognition of data protection laws.
- Mandate public authorities for monitoring and enforcing data protection laws, equip them with the necessary powers and resources.

RATIONALE:

Harmonisation of data protection on the African continent would create legal certainty as African societies transform into the digital age. It is a precondition for a digital single market and a cornerstone for any cross-border blockchain-based service. A consensus on regulatory goals can be combined with general guidelines regarding the implementation. On this basis, harmonisation can be achieved by developing a framework and mechanisms for mutual recognition of existing data protection regulations. This would provide for an adequate level of protection across the African continent, while allowing for national characteristics in the implementation of data protection regulations in the laws of the individual African countries. Supervisory authorities play a major role in achieving data protection in practice. In order to fulfil their tasks of monitoring and enforcing data protection laws, they need to be equipped with proper mandates, powers and resources. Consistent application of data protection nationally and across Africa can be achieved by fostering their cooperation, information sharing and rendering mutual assistance. The role of pan-African organisations, like RAPDP will be crucial to this end.

HOW TO PUT THE SUGGESTIONS INTO PRACTICE:

- Set up a process to negotiate regulatory objectives and to find consensus between countries. Keep in mind that views on the parameters in question can strongly depend on the socio-historical, political and cultural context. That is why the EU General Data Protection Regulation can serve as inspiration, but not a copy & paste catalogue.
- Leave regulatory means to individual countries.
- When operationalising data protection goals, be aware of the use and possible interplay of different legal techniques (rights-based vs. duty-based approach).
- Countries should mandate other countries' laws on the directive to be equivalent and applicable.
- Build capacity of data protection officials responsible for harmonisation.
- Establish data protection authorities with clear mandate and adequate resources.

4.3 Data protection and blockchain: clarifying the viability of distributed ledger system designs

SUGGESTION:

Decide about policy options at the intersection of data protection and blockchain technology according to the values and policy goals of individual countries and the African community, not according to real or perceived technical constraints. Establish "data protection by design" provisions in data protection laws.

RATIONALE:

Blockchain technology can be very flexibly designed, thus, it can be political decisions that guide the design, implementation and use of such systems, and not the other way around. With the primacy of political decisions on what is to be protected and how, "data protection by design" provisions can guide the design, implementation and use of blockchain technology by applying appropriate technical and organisational measures to ensure the protection of the protected goods and to meet the requirements of the applicable laws, whether these requirements are formulated as objective duties, subjective rights, or both.

HOW TO PUT THE SUGGESTION INTO PRACTICE:

- When determining desired data protection outcomes with regard to blockchain technology, consider key parameters or tension points, including:
    - secrecy vs. transparency,
    - remembering vs. forgetting,
    - data subjects, enforcement and oversight.
- Let the design of blockchain-based systems follow data protection objectives and not vice versa.

4.4 Financial regulation: creating legal certainty without stifling innovation

SUGGESTIONS:

In order to reach the goals of innovation, business development and socio-political progress with the help of blockchain technology, legal certainty in financial markets regulation is one of the major preconditions. Therefore, ICT policy and decision makers, in close collaboration with financial regulators, may consider the option of developing a pan-African concept for token classification. This could include security tokens, tokens representing other financial instruments such as e-money or payment and unregulated tokens, e.g. voucher and club tokens. Disclosure and registration regimes for security tokens could be an instrument to achieve stakeholder protection. Policy and decision makers may also consider introducing license regimes for service providers concerning security and other financial instruments tokens, specifically taking into account compliance with the relevant FATF recommendations.

RATIONALE:

Financial regulatory regimes typically serve the protection of financial stability and investors as well as other financial services' customer protection. Some tokens might trigger concerns in this regard while others rather compare to instruments not typically caught by financial regulation (e.g. a voucher for a mere software license). In order not to stifle innovation beyond what is required by these goals, developers benefit from legal certainty about token classifications. As a consequence certain software might only be deployed if the applicable disclosure regime is obeyed or if entities hold applicable licenses. Developers might only offer such software as a service but not deploy their software themselves. In contrast, software issuing or servicing unregulated tokens can be freely deployed by anyone.

Anything that is marketed as an investment opportunity to the public could then trigger certain minimum disclosure rules (typically a prospectus) to ensure that the public has sufficient information at hand to come to an educated investment decision. It appears advisable to create legal certainty about such disclosure rules, which might ideally be harmonised across the continent to limit the legal costs of a compliant security token issuance.

Any service provider offering to deal with customers' financial instruments or assets could be regulated to prevent fraud and to ensure high quality best practices in order to protect the financial instruments belonging to third parties. In addition, monitoring financial transactions to prevent money laundering as well as terrorism financing is a common public interest which is typically outsourced by governments to the regulated finanical service industry. Hence, FATF recommendations require that virtual asset service providers are licensed or at least registered.

HOW TO PUT THE SUGGESTIONS INTO PRACTICE:

- Collaboratively, ICT and financial policy makers could (re)visit concepts from regions with already highly sophisticated financial regulation (EU, US and Asia) to carefully assess, evaluate and compare these in the blockchain context.
- When thinking about setting Africa-specific standards, policy and decision makers should consider that if the goals of the regulatory regime of another important economic area coincide with their own policy goals, (partly) mirroring regulation can lower the legal costs for projects to include Africa in their service offerings.[67]
- One option to enter into a discussion of regulatory concepts would be to join the Governmental Advisory Body of INATBA (initiated by the European Commission in 2019). The European Commission had been highly interested to interact with Africa in this regard and INATBA shall be much obliged to include African governmental representatives in their Advisory Bodies.

[67] Consider the general caveats that apply to importing regulatory measures from other legislative systems and jurisdictions, as explained in the chapter on data protection.

4.5 Capacity building: increasing readiness for uptake of blockchain technology in Africa

SUGGESTIONS:

Support research and education about blockchain technology and blockchain governance. Foster skills, develop talent and stimulate innovation.

RATIONALE:

The education levels on blockchain and other advanced technologies in Africa are low. On the one hand, this poses a problem for projects and initiatives to find and attract adequate talent for solution development. On the other hand, low levels of technology awareness and education can also pose a problem in the rollout and adoption of consumer-focused applications, especially in rural areas and the so-called "last mile".

HOW TO PUT THE SUGGESTION INTO PRACTICE:

- Build a network. The Smart Africa Secretariat could help in this task with its convening power.
- Map already existing initiatives and identify capacity development needs. Engage with research institutions[68] and blockchain associations[69] across the continent. Collaborate with blockchain innovation hubs.[70]
- Understand that especially for the African startup ecosystem, securing international collaborations and funding, as well as participation in international dialogue can be quite challenging. The participation in international industry events is often hindered by visa requirements and limited availability of travel funding, which makes startups often reliant on international mediators or team members to build connections. Previously mentioned groups, events and associations with a more international focus can play a key role in a better facilitation of those connections.
- Foster the meetup and event culture that is typical for blockchain. It serves to connect entrepreneurs to investors, policymakers, corporates and the larger ecosystem.[71]
- Create educational programmes for users, innovators and policy-makers alike. Leaders could go abroad for training, e. g. ministers of finance to understand blockchain and intensify collaboration between entrepreneurs and government.

[68] Within the scientific community, the Next Einstein Forum (NEF; https://nef.org/) plays an important role in connecting science, society and policy in Africa to the rest of the world. Its innovation index captures progress in STEM education, as well as output of innovation and investment.

[69] The following associations offer connections into the existing entrepreneurial ecosystem: Africa Blockchain Alliance, South African National Blockchain Alliance, Cryptography Development Initiative Nigeria, Blockchain Association of Kenya, Blockchain Association of Uganda, Cameroon Blockchain Business Council, Blockchain Tanzania Community, Blockchain Society Ghana.

[70] Hubs exist in Cape Town, Stellenbosch, Johannesburg, Lagos, Nairobi, Kampala, Yaonde, Addis Ababa and Gaborone.

[71] The largest Blockchain Conference on the African continent is held in Johannesburg, South Africa. Another relevant event is the Africa Tech Summit held annually in Kigali, Rwanda. Meetups already occur in hubs like Cape Town, Johannesburg, Nairobi and Lagos.

4.6 Public utility: a pan-African blockchain service infrastructure

SUGGESTION:

Explore the feasibility of creating and operating a pan-African blockchain service infrastructure that offers a testbed for researchers, enterprises and administrations to run blockchain-based applications.

RATIONALE:

For blockchain systems to sustainably deliver the benefits that DLT are praised for - i.e. immutability, automation and trust in transactions - they need to be operated in an assuring governance environment that provides certainty for blockchain-based service providers and users. As has been pointed out, this is not always the case with blockchains. Creating such off-chain governance arrangements can be as challenging as the technical design of blockchain applications itself. In addition, reconciling the openness of public, permissionless blockchains with governmental duties and jurisdictional realities can be singled out as the greatest challenge that inhibits the uptake of distributed ledger technologies at large.

A federated blockchain infrastructure to be maintained by a union of states could present a compromise. It could offer a common infrastructure that would allow administrations and enterprises to test and run blockchain-based services while catering for regulatory needs in the fields of data protection and finance. Such a collaboratively maintained blockchain service infrastructure could gain user trust, because the very fact that states with sometimes competing interests would maintain it together would indicate a healthy degree of scrutiny.[72] That is (one of) the distinct advantage(s) of a pan-African initiative over a national initiative.

In terms of industry policy, operating such an infrastructure would be an example of mission-driven economic policy where governments act as first movers. This may create spill-over effects. It can spur confidence in the overall still uncertain blockchain innovation environment. The availability of such an infrastructure would also lower the threshold for innovators to test the viability of their blockchain-based applications and business ideas. As a caveat, advances in harmonisation of data protection may be a precondition for the viability of such a project.

HOW TO PUT THE SUGGESTION INTO PRACTICE:

The biggest challenge in creating a common blockchain infrastructure among parties who cannot be assumed to share interests beyond receiving the benefits of a resilient, trustworthy and performant distributed ledger network service would be to bring them to the same table and get them to agree on the off-chain governance model. The Smart Africa Secretariat could serve as a neutral convener to help African states explore the idea to collaboratively maintain such an infrastructure. Technical inspiration can be taken from various national blockchain service infrastructures; governance inspiration can be taken from the European Blockchain Service Infrastructure.

[72] On the trust-generating role of distrust in governance see Sztompka, P., 1997. Trust, Distrust And The Paradox Of Democracy. WZB Discussion Paper, No. P 97-003. WZB Berlin Social Science Center. Available at: http://hdl.handle.net/10419/50255 [Accessed 8 May 2020].

4.7 Interoperability and standards: aligning with global standards and best practices

SUGGESTION:

Push for interoperability and harmonised standards, specifically to enable interconnectivity between different blockchains.

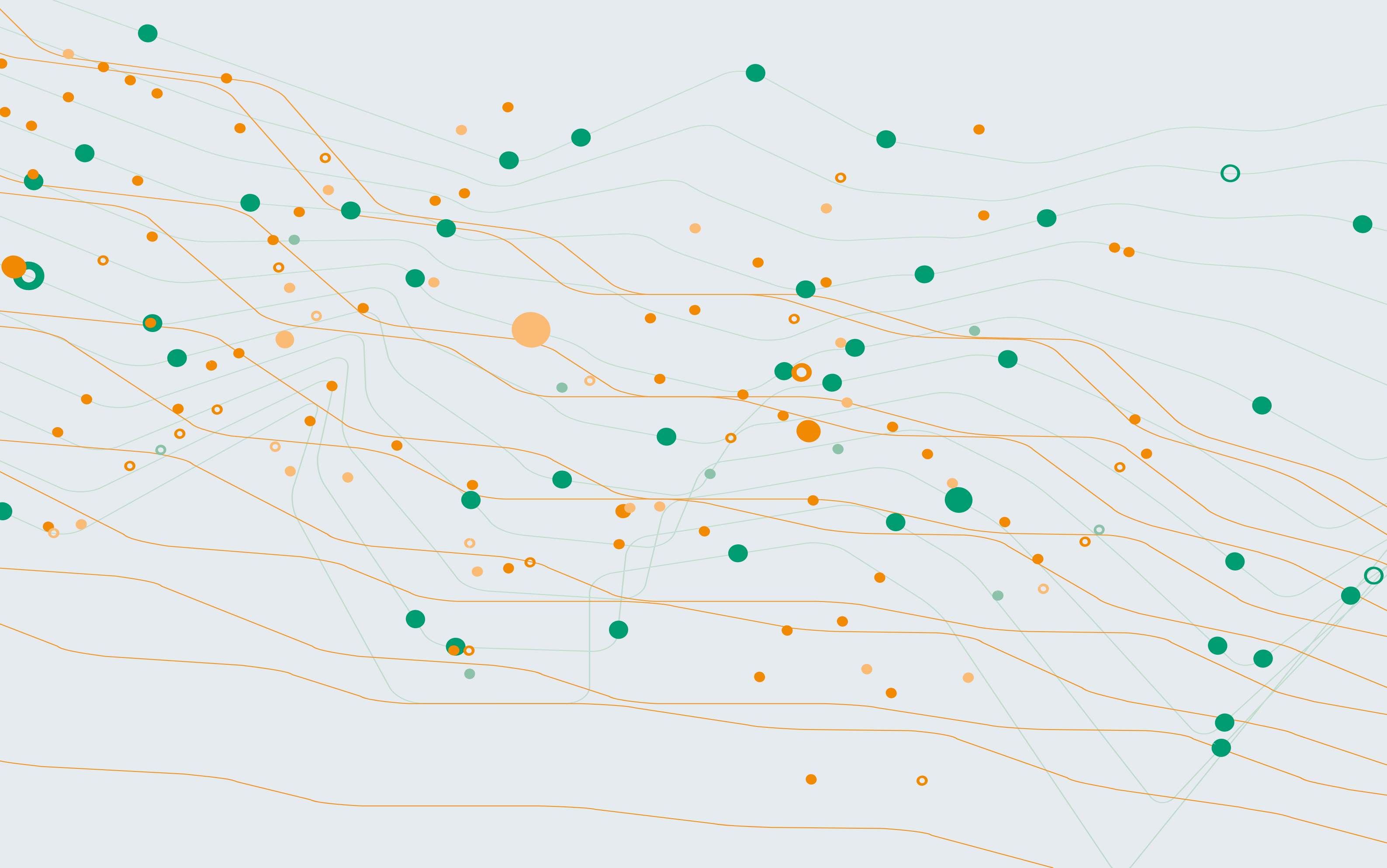
RATIONALE:

Integration points across various blockchain protocols and into legacy systems are often limited. Users of different blockchain networks cannot interact and transact with each other frictionlessly and without extra cost. Custom solutions need to be built to make blockchain systems interoperable with each other and with legacy systems, if possible at all. The introduction of adequate standards thus plays a key role in building scalable and interoperable systems across company, institutional and governmental levels. Common standards are also regarded as a cornerstone to achieve global interconnection of regional digital markets, e.g. markets for emission trading.

HOW TO PUT SUGGESTION INTO PRACTICE:

Interoperability of blockchain networks, protocols and applications remains an issue at the stage of research and development because it involves business model, platform and infrastructure aspects. The World Economic Forum lists[73] a number of organisations that currently work on the topic and could be approached for further information and collaboration.

[73] World Economic Forum and Deloitte, 2020. Inclusive Deployment Of Blockchain For Supply Chains: Part 6 - A Framework For Blockchain Interoperability. World Economic Forum and Deloitte, p.11. Available at: http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf [Accessed 8 May 2020].



5. APPENDIX: NATIONAL BLOCKCHAIN STRATEGY DOCUMENTS

State or Region	Title	Publication Date	Institutions involved	Reference
Australia	The National Blockchain Roadmap	**February 2020**	Department of Industry, Science, Energy and Resources	https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf
Bangladesh	National Blockchain Strategy	**January 2020**		https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/National%20Blockchain%20Strategy%20-%20Bangladesh.pdf
Catalonia	Blockchain Strategy of Catalonia	**June 2019**	Government of Catalonia	http://politiquesdigitals.gencat.cat/web/.content/Telecomunicacions/Blockchain/destacats-informes-descarregues/Estrategia-Blockchain-a-Catalunya-VF_1_EN.pdf
Cyprus	National Strategy	**2019**	Government and House of Representatives	http://www.parliament.cy/images/media/assetfile/Blockchain%20Strategy%20English_FINAL.pdf
Dubai	Dubai Blockchain Policy	**November 2019**	Dubai Future Council for Blockchain, part of the Dubai Future Councils	https://www.smartdubai.ae/docs/default-source/publications/reference-document--dubai-blockchain-policy.pdf?sfvrsn=19522b4_4
European Union	Cooperation on a European Blockchain Partnership	**April 2018**	European Council, European Commission	https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
France	Les enjeux des blockchains	**June 2018**	France Stratégie, an autonomous institution reporting to the Prime Minister	https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf
France	Solutions for a responsible use of the blockchain in the context of personal data	**September 2018**	Commission Nationale Informatique & Libertés (CNIL)	https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf
Germany	Blockchain Strategy of the Federal Government	**September 2019**	Federal Ministry of Economics and Technology (BMWi), Federal Ministry of Finance (BMF)	https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=8
India	Blockchain: the India Strategy Part I	**January 2020**	NITI Aayog, a Policy Think Tank advising the Indian government	https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf
Kenya	Emerging Digital Technologies for Kenya. Exploration and Analysis	**July 2019**	Ministry of Information, Communications and Technology, The Distributed Ledgers Technology and Artificial Intelligence Taskforce	https://www.ict.go.ke/blockchain.pdf
Malta	Establishment of the Malta Digital Innovation Authority, proposed Governance arrangements	**March 2018**	Parliamentary Secretariat for Financial Services, Digital Economy and Innovation, Office of the Prime Minister	https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF
Netherlands	Dutch Digitalisation Strategy 2.0	**June 2019**	Ministry of Economic Affairs and Climate policy	https://www.nederlanddigitaal.nl/documenten/publicaties/2019/11/13/english-version-of-the-dutch-digitalisation-strategy-2.0
South Korea	Blockchain Technology Development Strategy	**June 2018**	Ministry of Science and ICT	http://www.businesskorea.co.kr/news/articleView.html?idxno=23184
Uganda	Declaration on Fundamental Principles on the regulation of cryptocurrencies and the Blockchain	**July 2017**	University of Birmingham, United Nations African Institute for the Prevention of Crime and Treatment of Offenders (UNAFRI)	http://unafri.or.ug/wp-content/uploads/2018/04/Kampala-Declaration-on-Principles-on-regulation-of-cryptocurrencies-and-Blockchain-April-23.pdf
United Arab Emirates	Emirates Blockchain Strategy 2021	**April 2018**	Government of the United Arab Emirates	https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021