Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA Digital Identity

The GSMA Digital Identity Programme is uniquely positioned to play a key role in advocating and raising awareness of the opportunity of mobile-enabled digital identity and life-enhancing services. Our programme works with mobile operators, governments and the development community to demonstrate the opportunities, address the barriers and highlight the value of mobile as an enabler of digital identification.

For more information, please visit the GSMA Digital Identity website at www.gsma.com/mobilefordevelopment/programmes/digital-identity

Follow GSMA Mobile for Development on Twitter: @GSMAm4d

This document is an output of a project funded by UK aid from the Department for International Development (DFID), for the benefit of developing countries. The views expressed are not necessarily those of DFID.

Acknowledgements

The GSMA Digital Identity programme thanks Margie Cheesman of the Oxford Internet Institute, University of Oxford, for her contributions to this research.

Contents

I.

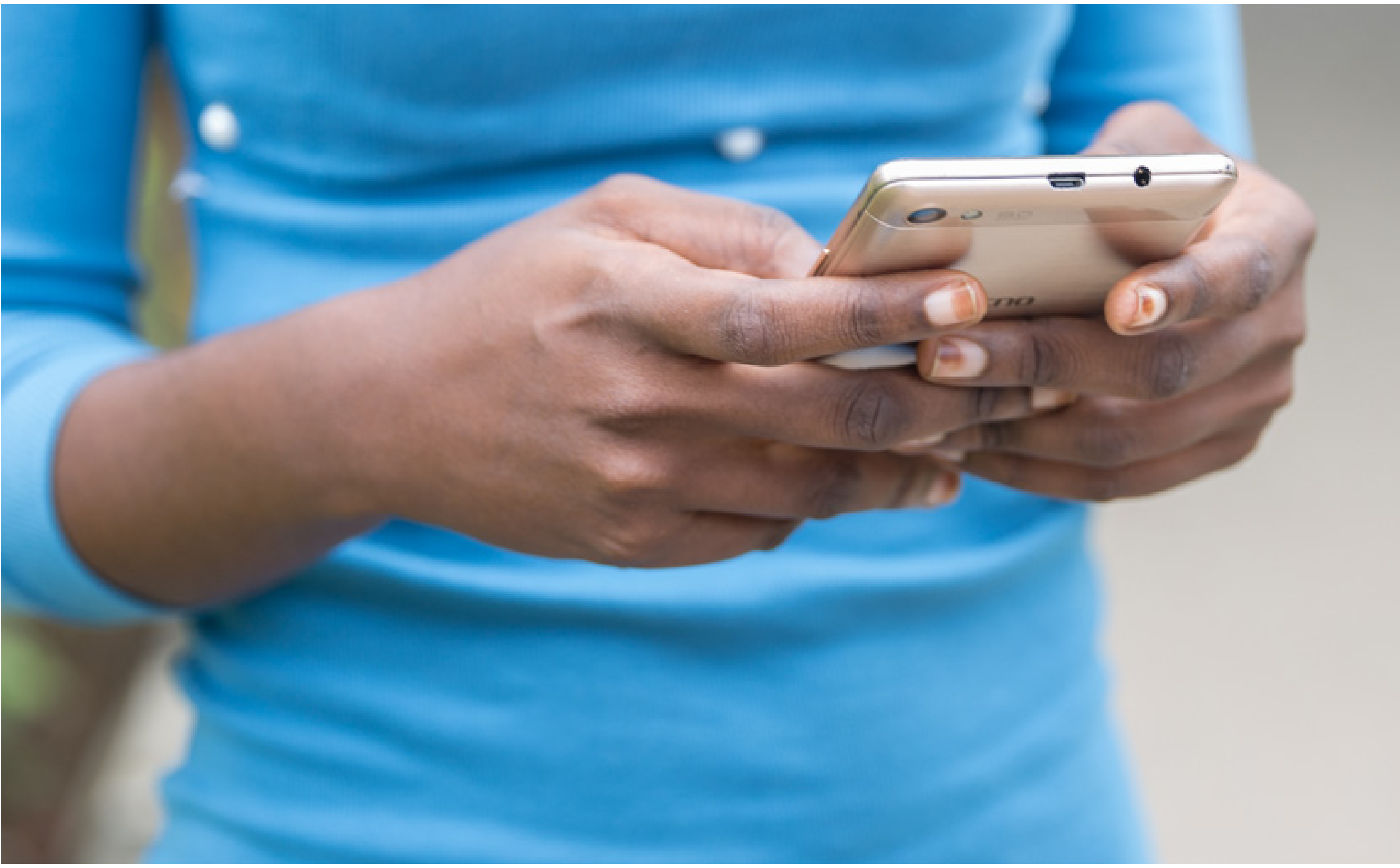
Introduction

A 2017 report from Accenture has found that the velocity and intensity of change in the development sector has reached an unprecedented level, with new players, businesses and funding models, societal expectations, demographic shifts, globalisation and digital technologies rapidly changing the face of the sector[1]. This research suggests that by investing in new digital technologies such as blockchain, Internet of Things (IoT) and Artificial Intelligence (AI), development organisations will be able to strengthen the efficiency of their programmes, reach a wider audience with fewer resources, and create new digital channels that optimise and personalise the experiences of their donors.

Of all the emerging technologies that are likely to shape the future of international development, perhaps none is getting more attention today than blockchain. But for many mobile network operators (MNOs) and their partners within the development sector, it has been difficult to judge whether the significant hype around this technology is justified. 'While excitement is understandable,' writes the Center for Global Development, 'it also creates a risk that organisations embrace and begin to rely on the technology before they fully understand it[2].' Certainly, some use cases are beginning to emerge that blockchain technologies are uniquely qualified to address, but like any other enabling technology we should not expect it to become a silver bullet for every development challenge.

To put it simply, blockchain is a secure platform that lets people and organisations share information with each other with an unprecedented degree of trust and transparency. This might sound mundane, but early blockchain projects are starting to transform the way people and institutions are able to collaborate, exchange value, share information, track assets and deliver vital services. The most interesting 'blockchain for development' use-cases are almost certainly still to be discovered, but many sectors (governmental, corporate, activist) and domains (benefits payments, medical records, performance rights, food chains and more) have started to explore the benefits of blockchain-enabled security, veracity and efficiency in distributed record-making.

A good starting point for evaluating how blockchain technology could continue to impact the development sector is to understand what a 'blockchain for development' use-case looks like. In this report, we provide short case studies that highlight how four blockchain platforms are currently being used to improve people's access to self-sovereign identities, bring new levels of transparency to the distribution of international aid, and improve the efficiency of humanitarian cash transfers. In these early days, it is still not entirely clear how MNOs will be able to support and derive value from future 'blockchain for development projects', or how their current role in the development space could soon be enhanced by blockchain technology. The case studies offer a starting point for addressing this knowledge gap, with early evidence showing that they could provide MNOs with new opportunities to support development partners, create new revenue streams, reduce their Know-Your-Customer (KYC) compliance costs and related barriers, and contribute to the UN's Sustainable Development Goals (SDGs).



[1] Ford, F. and Lobo, I. (2017). Digital disruption: Development unleashed Multiply innovation, collaboration and impact through digital in international development. Available at: https://www.accenture.com/t20170601T083538Z__w__/us-en/_acnmedia/PDF-40/Accenture-Digital-Disruption-Development-Unleashed.pdf#zoom=50

[2] Pisa, M. and Juden, M. (2017). 'Blockchain and Economic Development: Hype vs. Reality'. CGD Policy Paper. Washington, DC: Center for Global Development. Available at: https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality.

II. What is 'Blockchain'?

In 2009, an author (or authors) using the pseudonym Satoshi Nakamoto published a paper titled, *'Bitcoin: A Peer-to-Peer Electronic Cash System'*[3], which outlined a vision for a new kind of digital currency. According to Nakamoto, commerce between two willing parties on the Internet had come to rely almost exclusively on financial intermediaries – such as banks, credit card companies or third-party payments portals like PayPal – to authenticate and process payments. These intermediaries are necessary because all economic exchanges require trust; at the most basic level, we must have a reasonable expectation that the individuals or institutions with whom we transact will not take advantage of us, regardless of our ability to monitor their actions[4]. Financial intermediaries have built complex systems, processes and databases to help reduce our uncertainty when we buy or sell online, but these add time, cost and inconvenience to our digital transactions without fully eliminating the risk of fraud.

To enable this digital currency, Nakamoto argued that a new system was needed where trust was built on the basis that every transaction had to follow a set of rules, or 'protocols', that were governed by cryptographic proofs. Furthermore, rather than relying on a trusted financial intermediary, the transactions made on this system would be validated by a network of connected users who could reach a unanimous agreement, or consensus, about who owned or transferred value at any point in time. To achieve this, Nakamoto combined pre-existing computer networking and cryptography technologies in ingenious ways to create a platform that could act as a public ledger, or database, that anyone can access but no single person can control. By providing a decentralised, trustworthy, and immutable record of transactions, the platform allows individuals and institutions to collaborate, transact and share information with previously unheard-of levels of trust and transparency[5].

[3] Nakamoto, S. (2009). 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Available at: https://bitcoin.org/bitcoin.pdf

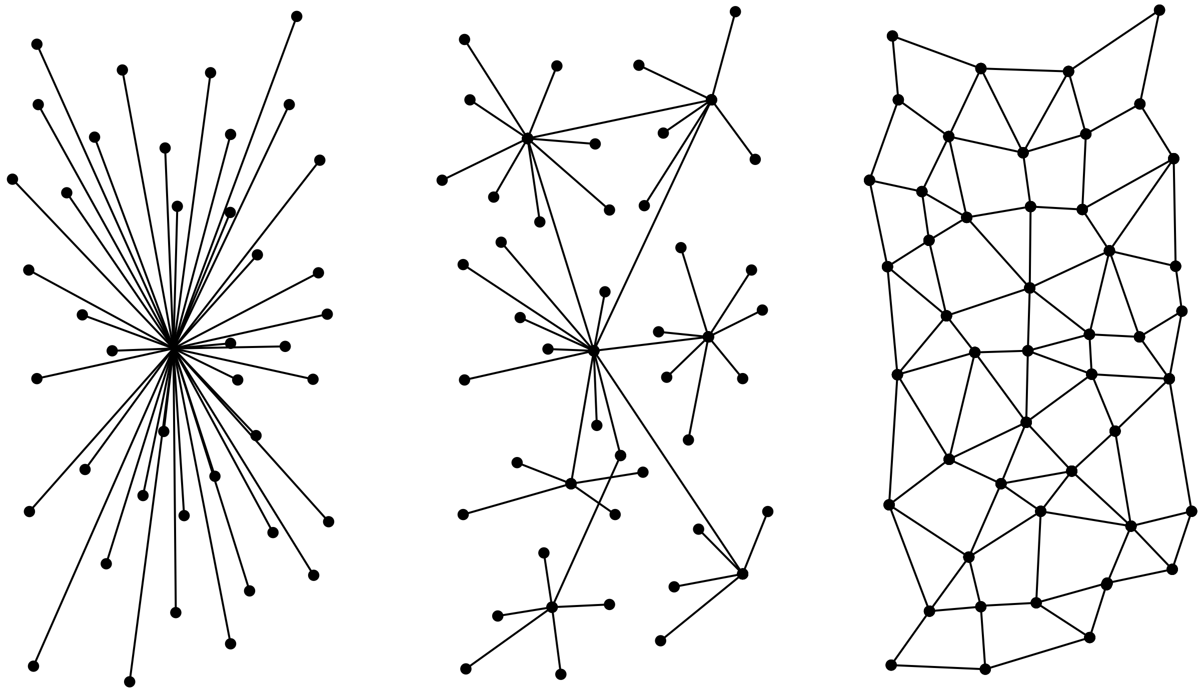
[4] Pisa, M. and Juden, M. (2017).

[5] Tapscott, D and Tapschott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World.* Penguin Publishing Group.

Today this kind of platform is known as a blockchain, and put simply, 'it is a machine for creating trust'[6]. 'The technology and cryptography that sits behind blockchain is complicated,' writes Don and Alex Tapscott in *Blockchain Revolution*[7], 'but the main idea is simple. It's a platform for everyone to know what is true[8], at least with regard to structured recorded information. As such, it holds the potential for unleashing countless new applications...that have the potential to transform many things'. Here is how it works.

Blockchains are ***distributed ledgers***, or shared databases. Similar to online document sharing platforms, all participants on a blockchain's network are given equal status and can submit, review and verify the records, or 'blocks' of information, in real time. When a block of information is recorded onto the blockchain by any user – whether this is a financial transaction between two people, a record of land ownership, or a refugee's personal details – the data is instantly and automatically duplicated onto all of the other connected computers (or 'nodes') on the blockchain, rather than the record staying with a single, centralised authority. By automatically distributing the blocks of information across the whole network, the blockchain ensures that every user sees the most up-to-date information, the database has no single point of failure, and no single institution can control how the information is recorded, audited or managed.

Types of Networks



Centralised
[A]

Decentralised
[B]

Distributed
[C]

Source: Baran, 1964

[6] The Economist, *'The Trust Machine'* (2015)

[7] Tapscott, D and Tapschott, A. (2016).

[8] As explained further in this section, the record is known as 'true' in the sense that it is peer-vetted, immutable and auditable; the information may well not be correct, as is the problem with any other database system

Distributing information in this way makes blockchain a powerful and efficient tool for sharing information across multiple organisations in real-time. In refugee contexts, a consortium of humanitarian organisations might use a blockchain to maintain an up-to-date record of the services they are providing to a refugee population, helping to ensure that they aren't duplicating records, wasting valuable resources or excluding individuals from receiving assistance. A blockchain could also be used to help individuals record and protect vital personal information that they don't want a single authority to control and manage, such as their right to land, their educational achievements, or their proof of citizenship. It could be extremely valuable, for instance, for a refugee or displaced person to have their citizenship status and other personal credentials permanently verified and recorded on a blockchain, enabling them to retain control over their vital information in instances of state-based oppression or persecution.

Unlike online file-sharing platforms, however, blockchains are ***immutable***. Once an entry has been made, the record is time-stamped and given a 'hash' – a unique, mathematically-generated identifier that automatically ties each new record to the entry that came before it. This means that it is impossible for any user to amend, delete or duplicate a single entry in the blockchain without noticeably affecting all of the entries that are part of the chain, making fraudulent activity immediately visible to the other users on the ledger. This ingeniously simple innovation helps guarantee the integrity of the data stored on the blockchain, and allows users to reach a unanimous consensus that every record is authentic and unchanged.

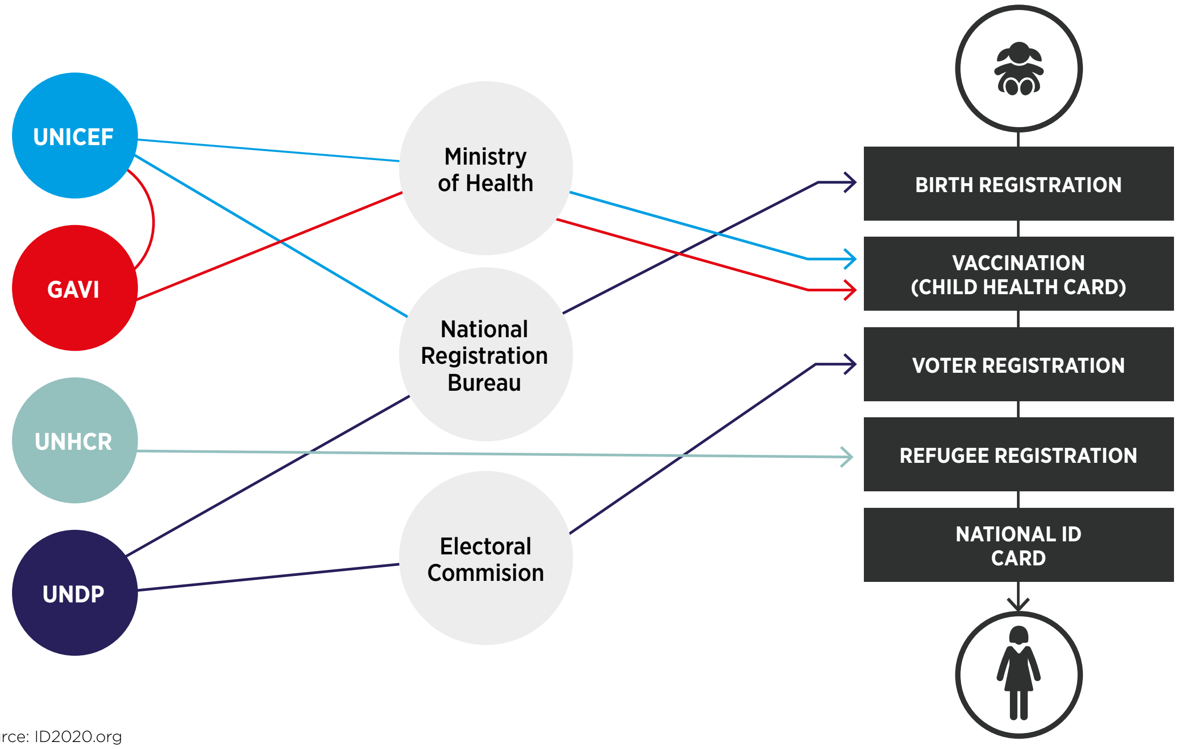
Blockchains can be designed to be either ***public*** or ***private***. Cryptocurrencies like Bitcoin run on totally decentralised, public blockchains; on these, anyone in the world can gain access the blockchain, view the flow of transactions, submit their own records, and participate in the consensus process[9]. The obvious advantage of a public blockchain is that no one individual or group of individuals is able to control the information which is contained on the blockchain, maintaining the technology's original virtues of neutrality and openness. Public blockchains can be a valuable tool for tracking the movement and provenance of assets, a feature that could help facilitate supply chain management by improving transparency and preventing fraud[10]. South African diamond specialist De Beers is investigating how to use blockchain to help differentiate legitimately sourced diamonds from those that have been sourced in conflict zones[11]. Starbucks has also begun to explore how the technology could be used to record each transaction that takes place in their coffee value chains, capturing highly-detailed information on the farmers that grow their beans and the weight, grade, and other specifications that are analysed by coffee buyers[12]. By connecting all of the 'nodes' in coffee value chains, one day blockchain might allow customers in a café to scan a QR code on their coffee cup, pull up information about their coffee's origin, and give the farmer who grew the beans a tip.

Contrary to public blockchains, a private, or 'permissioned' blockchain is operated by one organisation or group of organisations, and is only accessible to other individuals or organisations that have been granted permission to use it[13]. Increasingly, permissioned (rather than public) blockchains are beginning to proliferate as centralised organisations such as banks and humanitarian agencies investigate how to use the technology to collaborate with partners or improve their own internal processes. These can be characterised as 'incorporative' blockchain projects. The extent to which incorporative blockchain projects are still 'peer-to-peer' is debatable considering centralised intermediaries remain in place, but they also tend to be an easier starting point for organisations that wish to engage with blockchain.

[9] Buterin, V. (2015). On Public and Private Blockchains. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [Accessed 15 Nov. 2017].
[10] Pisa, M. and Juden, M. (2017).
[11] IT-Online. (2017). 'Blockchain's African Potential Goes Beyond Finance'. Available at: https://it-online.co.za/2017/08/18/blockchains-african-potential-goes-beyond-finance/ [Accessed 15 Nov. 2017].
[12] Hackett, R (2017). *'This Blockchain Startup Ties Coffee to Crypto'.* Fortune. Available at: http://fortune.com/2017/09/29/national-coffee-day-starbucks-blockchain/ [Accessed 15 Nov. 2017].

Permissioned blockchains are particularly advantageous when organisations want to maintain the confidentiality of the information that they store on the blockchain. For instance, in support of the ID2020 initiative[14], Accenture, Microsoft and Avanade have built a sophisticated, permissioned blockchain which connects existing record-keeping systems from private and public institutions into one database. The result is a rich set of portable, personal credentials that have been validated by multiple trusted parties, such as birth registration data from UNICEF; national ID numbers or voter documents issued by national registration authorities or electoral commissions; vaccination records from GAVI (a global vaccine alliance) and other non-government organisations (NGOs); and refugee registration data from UNHCR. In practice, this means someone arriving at a border crossing could use the information stored on the blockchain to prove he or she originated from an area where they faced violence or persecution, or that they qualified for emergency assistance or aid. In their host country, the same person could call up their school records to help them find employment, or to find information on their medical history in the event of a health emergency[15].

Accenture's blockchain prototype in support of ID2020



Source: ID2020.org

Lastly, blockchains are ***secure***. The information stored on the ledger is protected by a form of cryptography that provides each user with two types of 'keys' – one key is kept private, and the others are made public – which work together like the two-key system used to access a safety deposit box. The private key, similar to a password or PIN, gives a user the ability to 'lock' or 'unlock' their information and control when, and by whom, it is accessed. Other trusted 'nodes' on the network can then be given a public key so that they can read the unlocked information and double-check that it actually comes from the user. For example, when a blockchain is used to store a person's identity information – i.e. their name, age, address, citizenship status or credit history – the private key could give the user complete control over who is able to access their data, as well as which specific pieces of data they are able to see. An MNO or bank could then be given a public key, which allows them to view the unlocked KYC-related information and verify that they belong to the user.

[13] Lexology.com, (2016). *'Blockchain - Public or Private'.* Available at: https://www.lexology.com/library/detail.aspx?g=a381bb8a-3494-4f8d-9655-7f469cfddb23 [Accessed 15 Nov. 2017].
[14] For more information, see http://id2020.org
[15] Roberts, F. (2017). *'Microsoft and Accenture Unveil Global ID System for Refugees',* Fortune. Available at: http://fortune.com/2017/06/19/id2020-blockchain-microsoft/ [Accessed 15 Nov. 2017].

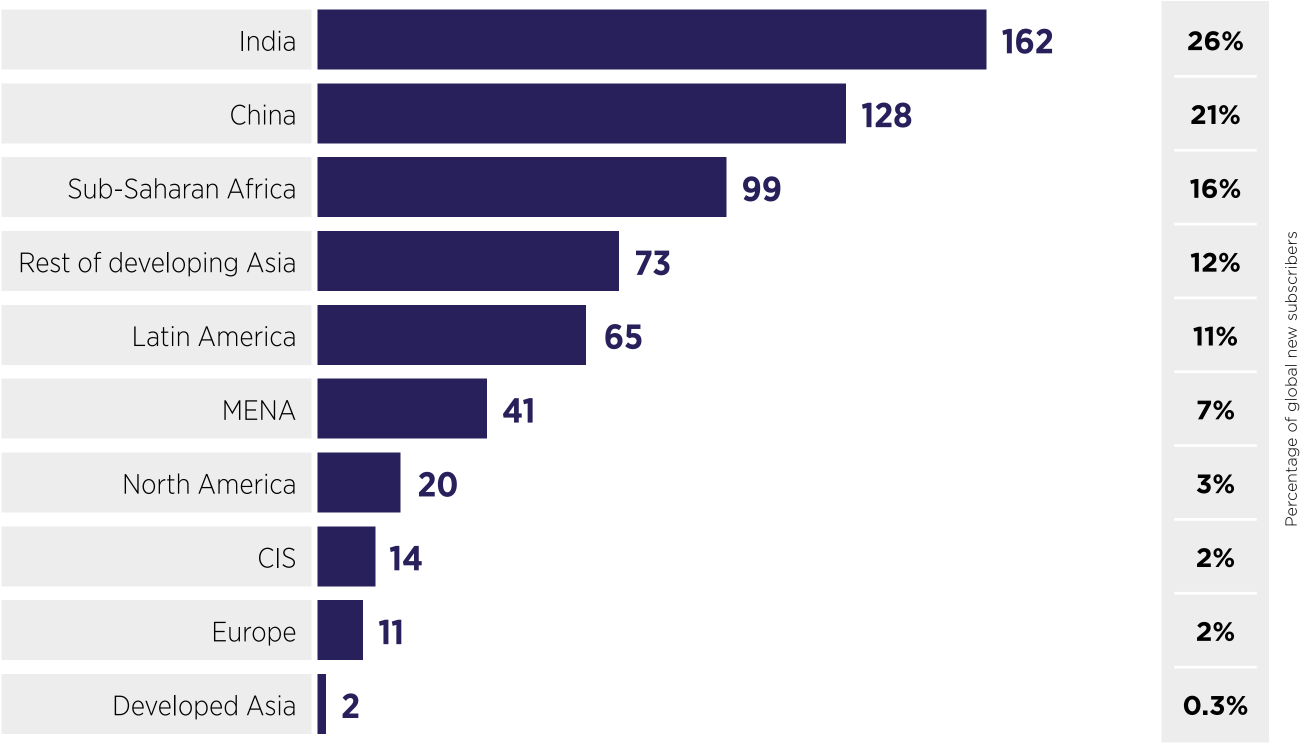
III. The Mobile Industry and Blockchain

Today's mobile ecosystem is increasingly connecting everyone and everything. By the middle of 2017, two thirds of the world's population had a mobile subscription – a total of five billion unique subscribers. By 2020, a further 620 million new mobile subscribers will be added, taking the global penetration rate to 75%[16].

Reaching the next billion subscribers will be the industry's toughest challenge yet. With developed markets approaching saturation, developing countries will account for nine out of ten new subscribers between now and 2020. Asia Pacific will represent two-thirds of new subscriber growth over that period, and annual growth in Sub-Saharan Africa – the world's most under-penetrated region – will also be significant.

Rising demand for data and more sustainable pricing will act as positive levers in ensuring mobile revenues continue to grow over the next four years, but the future outlook remains mixed. In Asia Pacific and Sub-Saharan Africa in particular, revenue growth has slowed sharply in recent years due to regulatory pressures, increasing competition, and a challenging macroeconomic environment. Across all regions, mobile operators will be looking for opportunities to implement new strategies that can drive overall growth and ensure the long-term sustainability of their operations. Investments in new technologies and deeper collaboration with start-ups will be essential to operators' own development, allowing them to create new avenues for revenue growth, generate cost efficiencies, and drive user acquisition and retention by enhancing or expanding their product offerings[17].

Net growth in mobile subscribers, Q2 2017 - 2020



Source: GSMA Intelligence

Note: Developed = 'High' and 'Upper middle' income countries (GNI per capita above $3,956). Developing = 'Lower middle' and 'Low' income countries (GNI per capita $3,955) as classified by the World Bank.

[16] GSMA (2017). *The Mobile Economy 2017.* Available at: https://www.gsmaintelligence.com/research/?file=9e927fd6896724e7b26f33f61db5b9d5&download

[17] GSMA (2017). *The Mobile Economy Asia Pacific 2017.* Available at: https://www.gsmaintelligence.com/research/?file=336a9db2ab3ed95bc70e62bf7e867855&download

It is within this context that many operators have started to explore opportunities to invest in the development and implementation of blockchain projects, forging partnerships with technology companies and dedicating new funds to blockchain research (see examples below). It is likely that much of this activity is happening below the radar, as the potential use cases for mobile operators receiving the most attention to date fit our definition of 'incorporative blockchain projects' – meaning they focus on lowering the cost of operators' own internal processes or expanding access to digital value-added services. Although blockchain projects such as this are outside the scope of this paper, a few well-publicised initiatives are worth highlighting here:

EXAMPLES OF OPERATORS WHO ARE INVESTING IN BLOCKCHAIN

In June 2015, **Orange Silicon Valley** launched ChainForce, an initiative that brings together innovative blockchain start-ups and forward-thinking corporations for short-term, collaborative pilot projects. Over eight to twelve weeks, corporations and start-ups work together to develop a Minimum Viable Blockchain App (MVBA), which ChainForce supports by providing limited development resources, mentorship, and business cases from their corporate partners to help orient the project. Today, ChainForce is exploring novel uses of blockchain related to digital identity, Internet of Things (IoT), provenance, insurance, supply chain and utility/energy Management[18].

Also in 2015, **Verizon Ventures** invested in a blockchain start-up, Filament, that developed a blockchain-based IoT solution which allows industrial assets to securely communicate with one another wirelessly, independent of cloud connectivity or any other third-party data platform. Verizon provided a new round of funding to Filament in 2017, with the intention to scale the offerings from paid pilots to large production-grade installations, and to build out a wider ecosystem of delivery partners, including large technology integrators, value-added resellers, and global industrial conglomerates[19].

At the beginning of this year, **Du** announced a pilot programme which uses blockchain technology to facilitate the secure transmission of electronic health records in the United Arab Emirates. The aim is to bring data integrity, security and trust to the relationship between health providers and patients. It intends to do this through a blockchain-based solution in partnership with the Global Blockchain Council, which is itself a partnership between industry and government[20].

GSMA's Mobile Connect is investigating how to use blockchain to make their existing, federated identity solution more convenient for users. For instance, they are exploring the possibility of introducing the concept of an 'identity wallet', through which a user could self-assert their attributes on the blockchain, which can then be validated by other entities such as banks or governments. By allowing Mobile Connect to manage the user's digital keys on a blockchain, users could interact with the platform using more 'humanised' identifiers, such as their mobile phone number. Mobile Connect is viewed as the ideal framework for supporting such wallets, and providing users with a simple means of authenticating their identities in a way which is both convenient and secure[21].

18. For more information, see: http://www.chainforce.org/#chainforce
19. Business Wire (2017). '*Filament Receives $15M in New Funding for Industrial IoT'.* Available at: http://www.businesswire.com/news/home/20170330005189/en/Filament-Receives-15M-New-Funding-Industrial-IoT [Accessed 15 Nov. 2017].
20. Rizzo, P. (2017). *'Mobile Telco Du Reveals New Blockchain Healthcare Partnership',* Coin Desk. Available at: https://www.coindesk.com/mobile-telco-du-reveals-new-blockchain-healthcare-partnership/ [Accessed 15 Nov. 2017].
21. Hazari, G. (2017). *'The Relationship Between Blockchain and Digital Identity'*, GSMA. Available at: https://www.gsma.com/identity/the-relationship-between-blockchain-and-digital-identity [Accessed 15 Nov. 2017].

IV.

Blockchain for Development

In recent years, the mobile industry has actively embraced and supported the introduction of the UN's Sustainable Development Goals (SDGs), with operators across the world identifying new ways of working in partnership with governments, the development sector and other key stakeholders to deliver impact in digital identity, financial services, health, agriculture, utilities, disaster resilience and gender equality. A 2015 review from the UK's Department for International Development (DFID) highlighted that the rapid expansion of mobile phones and internet access in poor countries offered unique opportunities to stimulate growth, enhance people's experience of services and as citizens, involve them in development work, cut fraud, help hold governments and other institutions to account, and support organisations responding to humanitarian emergencies[22].

Mobile devices and mobile connectivity will surely play an important role in future 'blockchain for development' projects, if only because these peer-to-peer networks largely depend on smartphones and other connected mobile devices to be the main interface between users and blockchain applications. However, it is less clear at this point what other opportunities these projects will present to mobile operators. To address this knowledge gap, in the following section we explore three emerging use cases for blockchain in the context of development, looking at how MNOs will be able to support, and derive value from, these projects.

The case studies are presented with one significant caveat: all four highlight platforms that are in the early stages of development. There is still much work to be done to prove that blockchain platforms such as these are cost-effective, secure, sustainable, and more appropriate than other enabling technologies. For that reason, the last section of the report unpicks the use-cases to help us consider whether they are technically feasible, what the social-contextual and stakeholder challenges might be, and how mobile operators could fit in.

22. Ranger, P., Chandler, J. and Arscott, B. (2015). *'DFID Review of Digital in Development Programmes'.* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/417521/Review-Digital-Programmes-Feb2015.pdf
23. World Bank (2017). *'Principles on Identification for Sustainable Development: Toward the Digital Age'.* Available at: http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

USE CASE 1

Blockchain and Self-Sovereign Digital Identity

When a person wishes to register to access services such as government subsidies, a mobile SIM card or a bank account, they are often required to prove their identity using government-issued, physical documents such as a national identity card, passport, or voter ID. However, at least 1.1 billion people lack any form of officially-recognised identity, and this problem disproportionately impacts rural residents, the poor, women, children, and other vulnerable groups, particularly in Africa and Asia. Furthermore, in many places identity systems remain fragmented and require individuals to hold several functional forms of identity, each of which might serve a different purpose, follow a different application process, and reach different segments of society.

In 2017 the World Bank, in partnership with the GSMA and a number of other public and private sector stakeholders, agreed to a set of common principles that are considered fundamental to maximising the benefits of identification systems for sustainable development[23]. Among these was the principle of *universality*, which advocates that countries should fulfil their obligations to provide legal identification to all residents—not just citizens—from birth to death. While government agencies have a vital role in providing legal identification, centralised identity systems inherently carry some risk, as they 'lock' individuals into a single authority with the power to deny their identity, hold documents for ransom, or even confirm a false identity[24]. Since the start of the civil war in Syria, it has become nearly impossible for Syrian citizens to replace or apply for new identity documents - those who fear political persecution are unable to approach government authorities, and many citizens applying from abroad have had their applications denied. It is estimated that up to 70% of Syrian refugees currently lack access to state-issued identity documents, which threatens their ability to access humanitarian assistance, move freely within their country of exile, seek employment, register the birth of their children, or move closer to voluntary repatriation or resettlement[25]. In other cases, individuals originating from poor, vulnerable, or disconnected segments of society will never have access to State-issued identity documents because the application process is too costly or inconvenient, or because their government lacks the capacity to issue identity documents to its citizens.

The belief that people should have greater control over their own personal identity and the value derived from it has led some ID experts to shift their focus to the development of "user-centric" or "self-sovereign" ID systems. In contrast to systems where institutions provide ID credentials, self-sovereign IDs are built to empower individuals to control the formalisation of their identity, manage their digital personas, and actively monetise their personal data[26]. As with any ID system, to be useful a self-sovereign ID must be convenient and trusted, as well as personal, persistent, portable, and private; that is, they should be unique to only one person, live with a person from life to death, be accessible from anywhere, and only given out with permission[27]. Until recently such a solution seemed technically infeasible, but blockchain technology appears to be making this possible[28].

[24] Allen, C. (2016). *'The Path to Self-Sovereign Identity'.* Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html [Accessed 15 Nov. 2017].
[25] Norwegian Refugee Council (2017). *'Syrian Refugees' Right to Legal Identity: Implications for Return'.* Available at: https://www.nrc.no/globalassets/pdf/briefing-notes/icla/final-syrian-refugees-civil-documentation-briefing-note-21-12-2016.pdf
[26] USAID (2017). *'Identity in A Digital Age: Infrastructure for Inclusive Development'.* [unpublished]
[27] Simonsen, S. (2017). '*5 Reasons the UN Is Jumping on the Blockchain Bandwagon',* Singularity Hub. Available at: https://singularityhub.com/2017/09/03/the-united-nations-and-the-ethereum-blockchain/ [Accessed 15 Nov. 2017].
[28] Pisa, M. and Juden, M. (2017).

Gravity: Improving access to mobile through KYC-compliant identities

In more than 140 countries, MNOs are now subject to mandatory SIM registration obligations which require customers to present Government-recognised identity credentials before a SIM card can be activated. Similar (or identical) Know-Your-Customer (KYC) requirements need to be met when customers open mobile money accounts. In most cases, these KYC regulations only allow customers to present identity documents that have been issued by government authorities, such as national identity cards, passports, or drivers' licenses. KYC processes can be expensive, time-consuming and potentially troublesome for service providers, particularly when MNOs are obligated to validate customers' ID credentials against a government database and are charged a fee for each validation query they make. In addition to the operating costs associated with customer enrolment, data protection and document management, cases of identity fraud can lead to heavy fines and damage a company's brand reputation. For many of the world's most marginalised people – such as rural residents, poor people, women and refugees – the lack of officially-recognised identity poses a major barrier to accessing mobile services.

This has led the Financial Action Task Force (FATF) to recommend that governments and regulators consider adopting proportionate, risk-based approaches to KYC, where those with less-official forms of identification are able to open accounts that have restrictions on the type and/or value of transactions that are permitted (e.g. a cap on the amount that a customer can send or receive using mobile money services per month). Here, there may be an opportunity for mobile operators, policymakers and other partners to develop acceptable substitute processes with lower levels of assurance, and to assist users in establishing their own trusted, self-sovereign identities.

The Blockchain Solution

Gravity describes itself as a 'next-generation identity solution' with an ambition to give everyone access to a mobile phone by creating a digital identity infrastructure that is fundamentally inclusive. To do this, they help individuals establish a trusted identity – or 'Proof of Existence' – that is independent from public infrastructures and non-dependent on official identity documents, postal addresses or banking systems. The platform has not been fully deployed to date, but Gravity has recently run a first pilot in Kenya registering 1,000 users over three days, and is currently working on a second pilot with an aim to register 10,000 people on their platform. While Gravity's end-to-end solution uses back-end blockchain technology to certify a customer's KYC-related information, the customer's experience and interaction with the app remains streamlined and easy: users do not need to know what blockchain is in order to use the platform, and the service works on any mobile device through a USSD menu or smartphone application.

Customers are guided through the enrolment process with help from a Gravity agent who visits them at their home or in their community. To begin, the customer uses a USSD menu in their own mobile device to self-declare their KYC-relevant information, including:

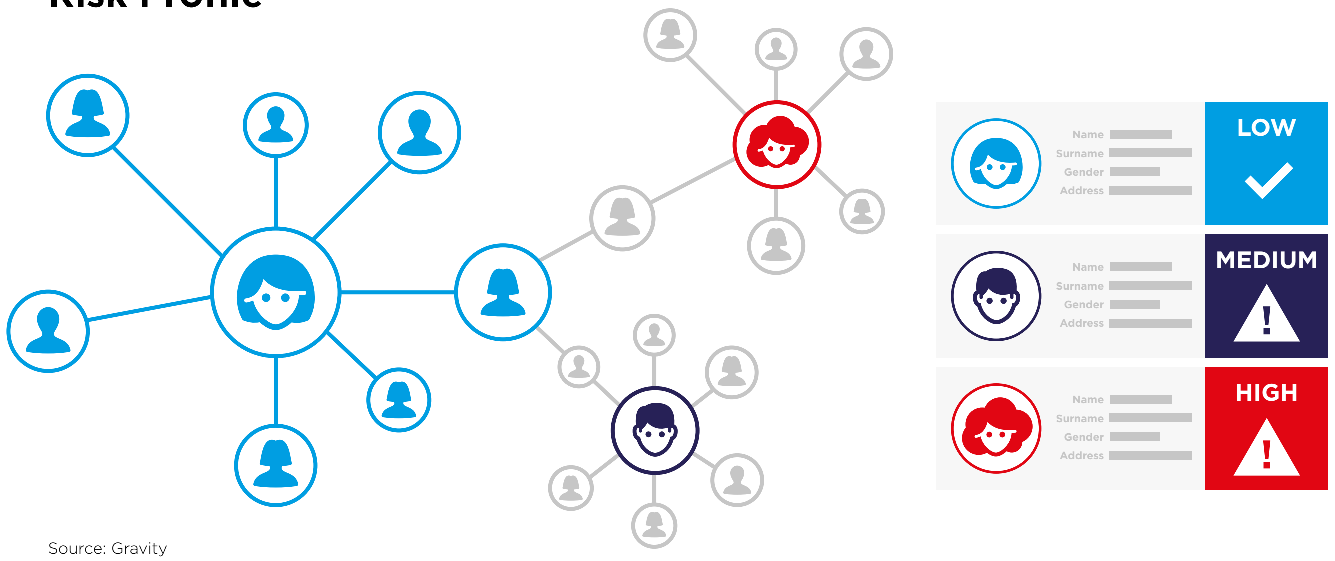
- First name
- Last name
- Phone number
- Date of birth
- Gender
- Nationality

All of these identity claims are then anonymously sealed on a public blockchain and stored on a second permissioned and cryptographically secured distributed ledger. At this point, confidence in the customer's identity is at a base level.

Next, the blockchain enables the customer's self-declared information to go through a process of 'distributed vetting'. As a last step in the enrolment process, the user provides contact details for five or more of their peers (typically family members or friends), who are subsequently sent an SMS message asking them to verify each of the identity claims. In this way, an entire virtual community becomes involved in validating the integrity of the user's identity. A machine learning scoring module ensures that inaccurate or malevolent information is rejected, and as a further incentive to Gravity's users to report information that is accurate, if the majority of their peers respond by confirming that the information is true, Gravity rewards the original user by providing them with free mobile airtime credit.

As more and more relationships are established and information is validated on the blockchain, confidence in the accuracy of the user's attributes – and hence the identity itself – grows organically, allowing Gravity to build a real-time risk assessment of each customer's profile. Additional critical fields of the KYC profile can be added subsequently, such as the user's National ID, birth certificate, professional licence for merchants, or any other information required by regulators. In these cases, the user will take a picture of the ID document through the app, and present the hard copy to a Gravity or MNO agent, typically a small shop owner. Upon verification, their identity score increases. Addresses also tend to be a key KYC requirement, and these can be self-declared on the application and reviewed by GPS location. Gravity is therefore not a substitute to official government-issued IDs, but complementary, bringing more flexibility and interoperability.

Risk Profile



Source: Gravity

Once a user's KYC-relevant information has been authenticated, mobile operators can be given permission to link into Gravity's blockchain to check a customer's KYC-related information and see the most current picture of their risk profile. Importantly, the encrypted, PIN-protected application gives each user the ability to remain anonymous and in full control of their personal details until they decide to share specific information, with a specific service provider, for a specific purpose. The solution complies *by design* to the EU General Data Protection Regulation (GDPR) requirements on personal data protection which is considered to be the most stringent anywhere. To help make the platform sustainable, Gravity plans to charge operators or any other data consumer a small fee to access the user's validated KYC information, a significant portion of which will go back to the users to reward them for using the service. As such, Gravity brings monetary value to the user's ID.

None of the platform's users – the customers, their peers, service providers, or even Gravity - are able to change or manipulate the information stored on the blockchain without detection, increasing MNOs' confidence that the information provided is true. Regulators also benefit from independent audit trails on KYC data. Gravity believes that blockchain-enabled, peer-to-peer authentication of identity-related data is more robust and less prone to fraud than many of the documents regulators currently accept as proof of identity.

Source: Gravity

For mobile operators, linking into Gravity's platform could significantly lower the cost of on-boarding new customers by reducing or eliminating the costs associated with traditional KYC/SIM registration processes, such as agent commissioning, back office procedures, and data systems. At the same time, the platform could help operators enhance their KYC and Anti-Money Laundering (AML) security by replicating the currently required information (name, date of birth, address) and adding additional levels of attributes, such as the user's income, occupation or next of kin. This could give MNOs access to the data they need to increase a customer's mobile money wallet limit, or to provide them with access to more sophisticated, targeted services (to the extent that any KYC compliance requirements have been met). The platform is also designed to improve the customer's experience with their operator by making it easier to navigate the SIM registration process and by providing mobile airtime rewards.

As a recognition of the platform's potential, in November 2017 Gravity won the Digital Africa Challenge on Citizenship and e-Government, beating a field of 770 start-up competitors. The awards ceremony took place at the Fifth Africa–EU Summit, which focused on youth and the demographic trends in Africa that are creating major challenges for young people in terms of migration, security and employment.

To support their initiative going forward, Gravity is hoping to work with MNOs who are willing to provide access to internal facilities, such as databases and procedures, to test the interoperability of the solution with its systems and to measure the impact on KYC/SIM registration-related costs.

For more information, see: www.gravity.earth

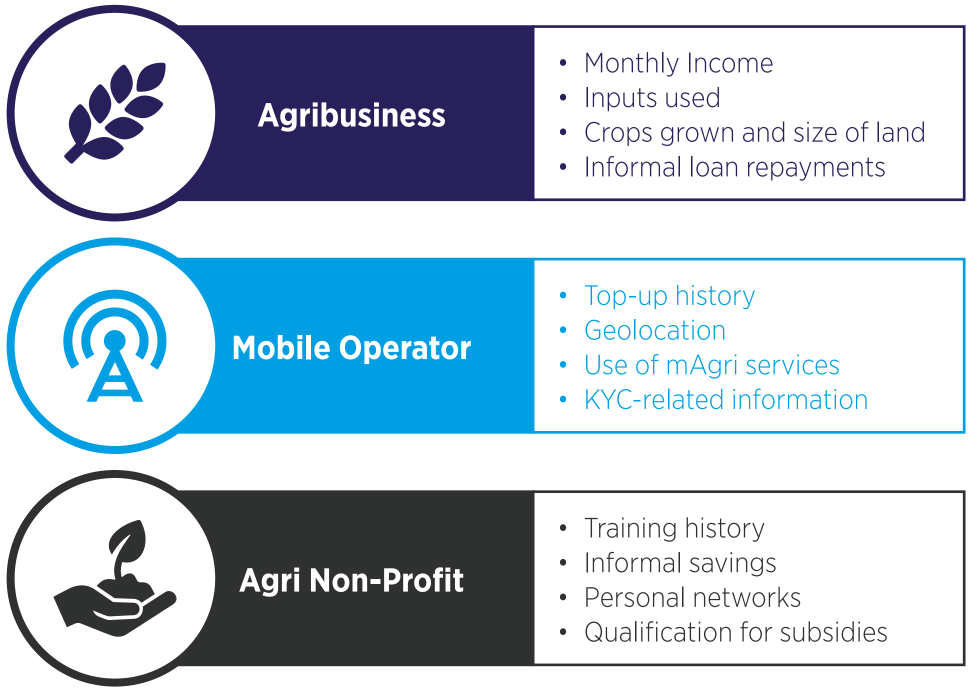
BanQu: Creating economic identities for smallholder farmers

An estimated 2.3 billion people depend on agriculture for their livelihoods, and according to the United Nations Food and Agriculture Organization, four-fifths of the developing world's food is a product of small-sized farms. Small, family-run farms are also home to the majority of people living in absolute poverty, and half of the world's undernourished people[29]. Supporting smallholder farmers, therefore, is critical to reducing poverty, hunger and malnutrition.

The rural poor are one of the least likely demographics to have access to an official proof of identity, which is increasingly essential to securing access to mobile connectivity, financial services and social protections. There is also a tension between fixed identities (i.e. the demographic and biometric details found on a person's legal identity), and the need for a more fluid 'economic identity' that accounts for one's shifting, dynamic life and economic profile.

Today, many smallholder farmers have limited access to the formal economy or formal financial products such as savings, credit or insurance, relying instead on multiple levels of financial intermediaries, or 'middlemen' who pass on costs to the farmer in the form of high interest or other fees. This is often because vital information about a farmer is collected, stored and used in silos by agribusinesses, mobile operators, non-profits and other service providers, providing each entity with an incomplete picture of the farmer's life and their unique economic situation:

[29] Fan, S., Brzeska, J., Keyzer, M. and Ha, A. (2013). *'From Subsistence to Profit: Transforming Smallholder Farms'*. International Food Policy Research Institute. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/transforming%20smallholder%20farms.pdf



Agribusiness

- Monthly Income
- Inputs used
- Crops grown and size of land
- Informal loan repayments

Mobile Operator

- Top-up history
- Geolocation
- Use of mAgri services
- KYC-related information

Agri Non-Profit

- Training history
- Informal savings
- Personal networks
- Qualification for subsidies

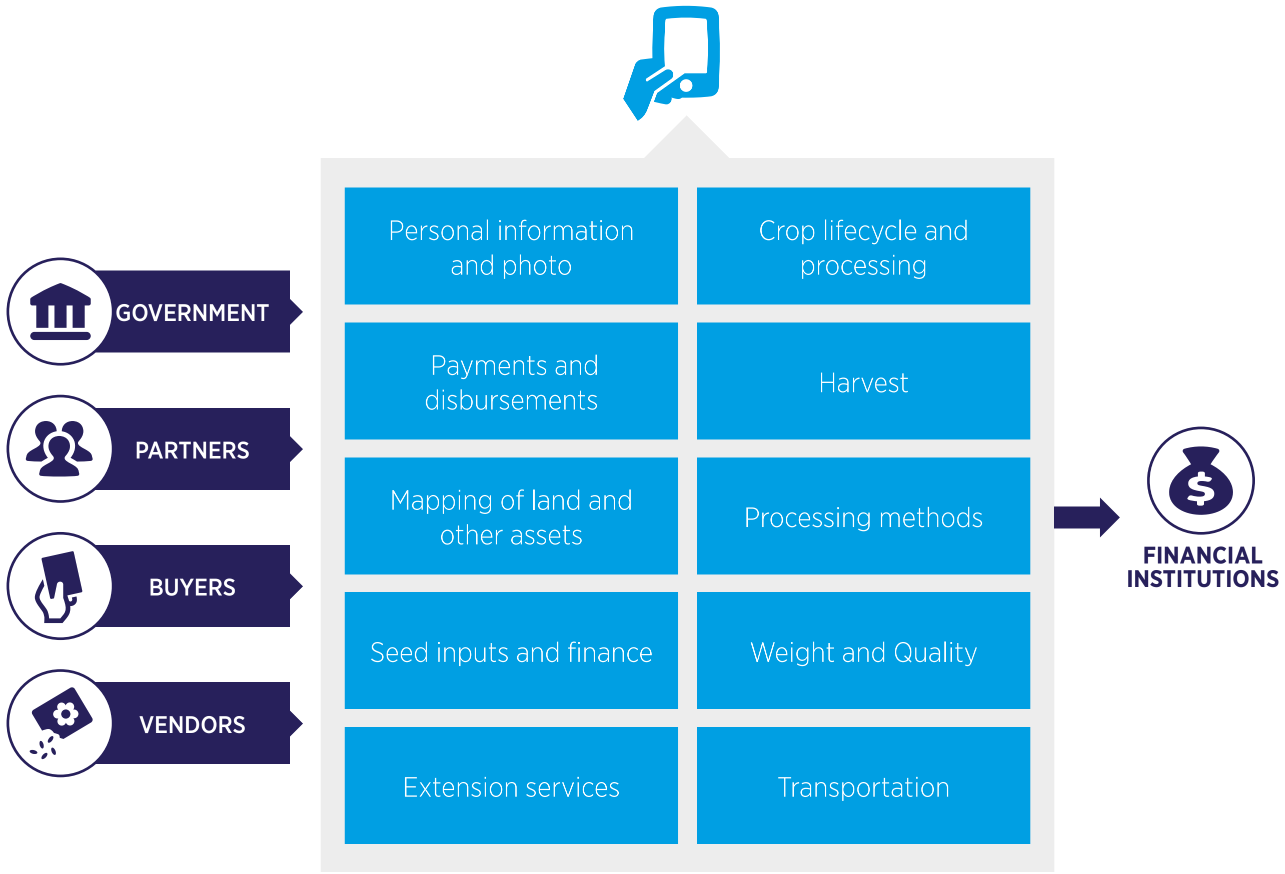
There is a need for new, digital approaches to identity that help farmers authenticate and take ownership of a wide range of personal data, such as their income, transactional histories, credit worthiness, rights to/ownership of land, geolocation, farm size, and other vital credentials.

The Blockchain Solution

BanQu's mission is to connect the world's poorest people to the global economy by providing them with a secure, portable digital identity. Their proprietary blockchain-based platform allows farmers to set up a unique digital profile and then connect with their peers, aid organisations, governments, banks, and payment companies to accumulate data on variety of personal and financial transactions. In a live production environment, BanQu has seen early evidence of success in Asia, where they are working with a global consumer product company to create economic identities as part of wider efforts to create a supply chain transparency tool. The application is designed to work on any mobile device, and is free to sign-up and use.

Through BanQu, anyone with a mobile phone is able to connect to the BanQu network and set up their economic identity. Knowing that farmers are unlikely to have access to physical documentation that verifies their economic credentials, the BanQu platform begins to create a unique, digital profile by capturing the user's selfie and a 'mashup' of other immutable (i.e. unchanging) characteristics. From there, the ethereum-based[30], permissioned ledger allows the user to connect to and interact with their 'banked network' - including family, friends, agribusinesses, service providers, and associated NGOs – who can use their own phones or BanQu's website to record and authenticate any of the farmer's personal and financial transactions. This might include property records, cash disbursements, the purchase of inputs, the quality of their harvests, health records, training records, or credit histories. As the BanQu user starts accumulating a transaction history and a registry of their assets on the BanQu blockchain, this information is used to build a traceable, vetted and farmer-owned 'economic identity' that can provide new or more targeted access to a wide range of formal services.

[30] Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralised applications.



GOVERNMENT

PARTNERS

BUYERS

VENDORS

Personal information and photo	Crop lifecycle and processing
Payments and disbursements	Harvest
Mapping of land and other assets	Processing methods
Seed inputs and finance	Weight and Quality
Extension services	Transportation

FINANCIAL INSTITUTIONS

Through the BanQu platform, the end user sees every transaction that is stored on the blockchain and maintains ownership of their personal information - as with the Gravity platform, the BanQu user decides what information is shared and with whom. When a farmer wishes to access new financial services, BanQu's platform gives banks or other FSPs the ability to check the identity components as captured in the blockchain, ensuring they are able to fulfil any identity-related regulatory and compliance requirements.

While the concept behind an economic identity seems simple, the technologies available before blockchain were not strong enough to make it a reality; according to BanQu, a centralised approach to managing user identities would be too cumbersome, too insecure, and too 'heavy'. A permissioned, distributed ledger on the other hand is powerful, light and easy to configure. Furthermore, the fact that the platform is distributed and consensus-driven means that an endless number of trusted partners can contribute to the blockchain, and with each new addition the strength of the farmer's economic identity is improved.

BanQu believes there are opportunities for mobile money providers to utilise the data collected through the BanQu platform to form a more complete picture of their customers. GSMA has seen success stories of innovative partnerships between mobile money providers, financial institutions, banks, fintech and technology companies that use customer data in innovative ways; the most notable being m-Shwari in Kenya, which uses algorithms to analyse a customer's use of M-Pesa and assess their credit-worthiness, assign individual credit limits, and lend to new applicants[31]. If allowed by regulators, MNOs could also use the platform to help lower the cost of on-boarding new mobile money customers, accessing all of the identity information needed to comply with KYC, AML, Counter-Financing of Terrorism (CFT) and Suspicious Activity Reporting (SAR) regulations.

For more information, see: www.banquapp.com

[31] For more information, see: http://cbagroup.com/m-shwari/

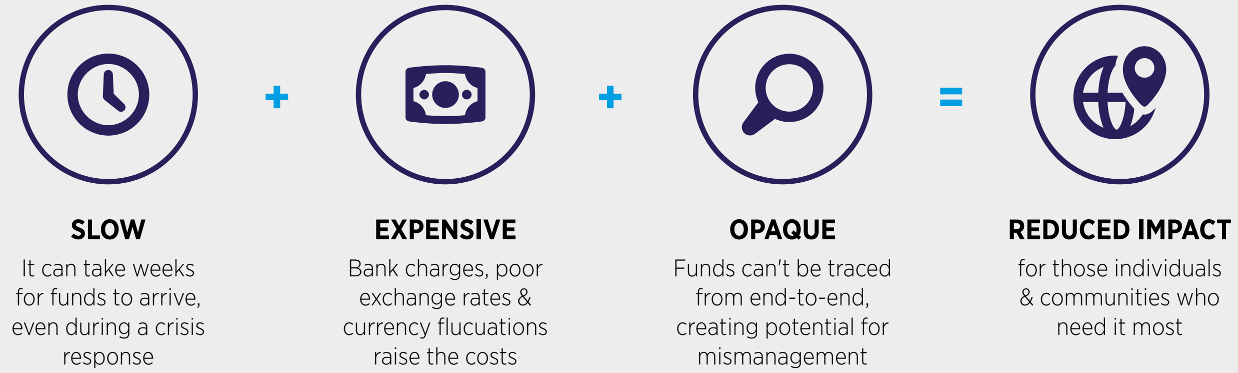
USE CASE 2

Blockchain and International Aid Delivery

In 2012, Ban Ki-moon, Secretary-General of the United Nations, closed the High-Level Panel on Accountability, Transparency and Sustainable Development by highlighting the severe impact of fraud on international aid, describing its impact as both direct and devastating. 'Last year,' he stated, 'corruption prevented 30% of all development assistance from reaching its final destination. This translates into bridges, hospitals and schools that were never built, and people living without the benefit of these services. This is a failure of accountability and transparency. We cannot let it persist.'[32]

Distributing and tracking funds to ensure they have maximum impact remains a challenge for the international development sector. Official development aid (ODA) is largely disbursed through legacy banking systems that are opaque, slow and expensive, with banking fees, exchange rates, and currency fluctuations chipping away at vital funds. Furthermore, once donor funds arrive in a country they are usually dispersed to a number of NGOs and other local implementing partners, creating an easy environment for donations to become lost or misappropriated.

More fundamentally, one reason for the lack of accountability in aid distribution is because development organisations have no way of tracing funds as they move between the donor and end beneficiary, making it impossible to fully measure the efficiency and effectiveness of aid. Donor funds might be routed through multilateral organisations, or pooled with other funds contributed by other countries or organisations, limiting the direct control they have over their expenditure.



SLOW + **EXPENSIVE** + **OPAQUE** = **REDUCED IMPACT**

SLOW
It can take weeks for funds to arrive, even during a crisis response

EXPENSIVE
Bank charges, poor exchange rates & currency flucuations raise the costs

OPAQUE
Funds can't be traced from end-to-end, creating potential for mismanagement

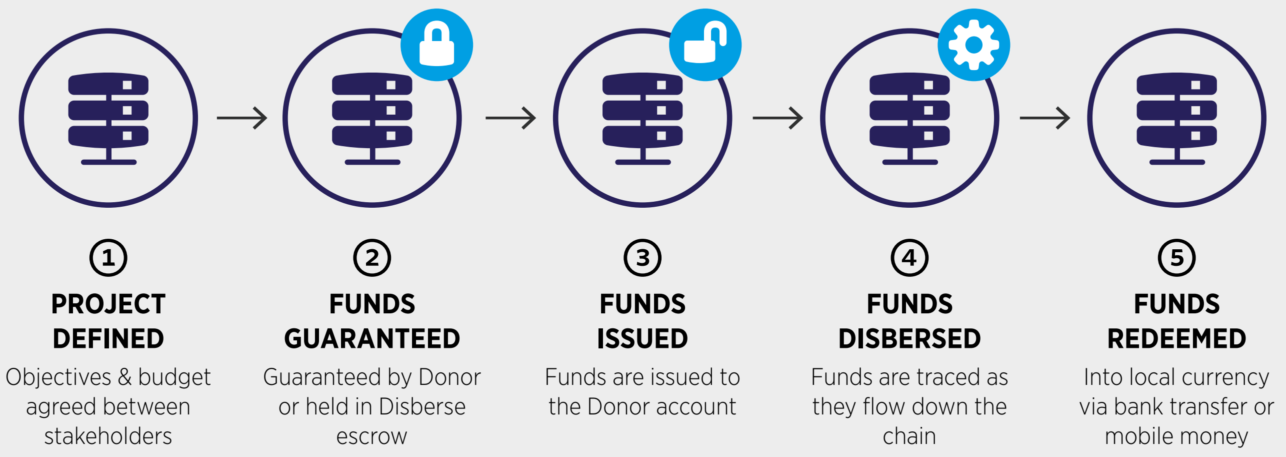
REDUCED IMPACT
for those individuals & communities who need it most

Source: Disberse

[32] United Nations (2012). *'Secretary-General's closing remarks at High-Level Panel on Accountability, Transparency and Sustainable Development'.* Available at: https://www.un.org/sg/en/content/sg/statement/2012-07-09/secretary-generals-closing-remarks-high-level-panel-accountability [Accessed 15 Nov. 2017].

The Blockchain Solution

Disberse is a fund management platform that aims to make the delivery of development and humanitarian aid more transparent, efficient and effective. Using a permissioned blockchain, they help donors, governments and NGOs transfer and trace their funds through the whole value chain, ensuring that vital resources actually reach the people they are intended to serve and are achieving the greatest possible impact.



1 PROJECT DEFINED
Objectives & budget agreed between stakeholders

2 FUNDS GUARANTEED
Guaranteed by Donor or held in Disberse escrow

3 FUNDS ISSUED
Funds are issued to the Donor account

4 FUNDS DISBERSED
Funds are traced as they flow down the chain

5 FUNDS REDEEMED
Into local currency via bank transfer or mobile money

Source: Disberse

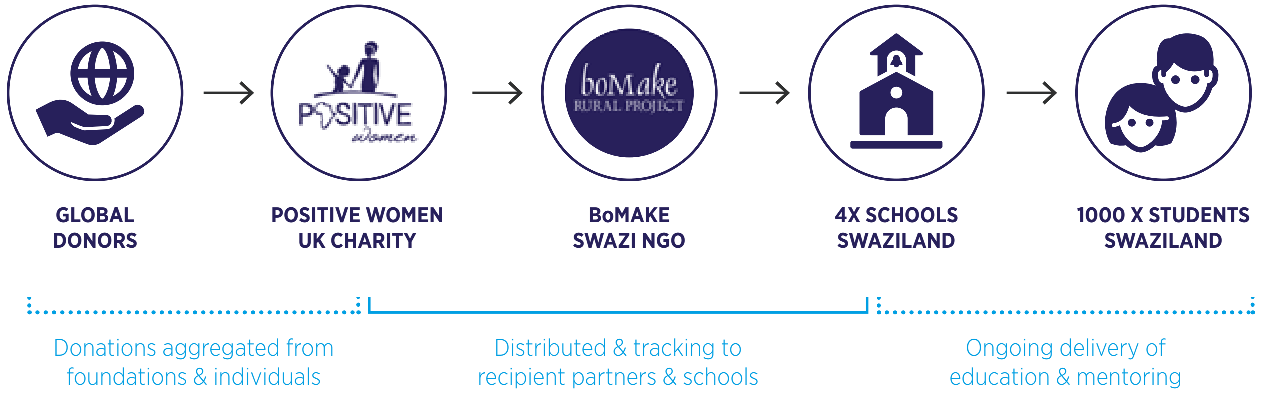
As a first step, Disberse works with the project stakeholders to outline the objectives and budget of a project, clearly defining the amount of money the donor is contributing and its intended purpose. This ‘supply chain’ of connected stakeholders might include a government department, NGO offices in both the donor and project country, local delivery partners, and the individuals or group receiving the benefit at point of delivery. Additional partners can be added to this chain at any time, as needed.

Each of the stakeholders in the chain must then open an account, or ‘wallet’ on Disberse’s platform, through which project funds will be traced. Next, the Donor guarantees the project funds by depositing them in Disberse’s escrow account in the form of fiat currency, such as USD or GBP. The funds are then ‘tokenised’, which means that the fiat currency is converted into digital value on a 1:1 basis; for every USD $1 or GBP £1 deposited, Disberse issues a digital token representing exactly that value to the Donor (just like e-money). These tokens can then be distributed to anyone, anywhere in the world through the blockchain’s wallet, and traced in real-time as ownership of the tokens is moved through the chain.

Importantly, the blockchain does not shift the project’s funds from one stakeholder’s bank account to another, as is done in the traditional aid disbursement process. Instead, the blockchain uses the digital tokens as a *representation* of value, and creates a permanent record on the ledger every time a stakeholder transfers their ownership of this value to the next organisation in line. Digital currencies like Bitcoin work in the same way, albeit on a public blockchain. The transfer of digital tokens can be validated and processed quickly, and will continue all the way down the chain until the tokens reach the final beneficiary; once this happens, the digital tokens can be exchanged for cash at one of Disberse’s local financial or corporate partners. In the end, the project funds only exchange hands twice: once when the Donor deposits the funds into Disberse’s account, and again when Disberse settles with their corporate partner in the project country. In this way, the platform removes several financial intermediaries, and their respective fees, from the international transfer process.

By the time the Disberse settles with their financial partner, the blockchain will have created an immutable record of every transaction that took place from donor to beneficiary, making it easy for organisations to track the flow of funds, to see exactly how every dollar of their donations was spent, and spot inefficiencies or weaknesses in the supply chain. Disberse also provides the organisation with this data for reporting, auditing, and compliance, giving previously unheard-of levels of transparency to the organisation, beneficiaries and donors.

In early 2017, Disberse implemented their first pilot by distributing and tracking funds from the UK to Swaziland in support of a girls’ education project. The funds were distributed from a UK NGO to a Swazi NGO, and then on to four local schools, supporting vulnerable girls left as orphans by the HIV/AIDS epidemic.



GLOBAL DONORS → POSITIVE WOMEN UK CHARITY → BoMAKE SWAZI NGO → 4X SCHOOLS SWAZILAND → 1000 X STUDENTS SWAZILAND

Donations aggregated from foundations & individuals

Distributed & tracking to recipient partners & schools

Ongoing delivery of education & mentoring

Source: Disberse

The pilot proved that Disberse’s permissioned blockchain provides the ideal platform for delivering aid. It enabled cheaper and faster transfers, both locally and internationally, as well as access to better exchange rates at the local level. Disberse saved the donor 2.5% on their transfer fees, which meant the NGO could fund an additional three girls to go to school for a year. The NGO was also able to see in real time how the funds were being distributed down the chain, and where funds were at any given time. As a result, the NGO didn’t have to chase local partners for receipts or proof of transactions, and it is hoped that the additional transparency will result in increased donations in the future.

Disberse has encountered some challenges that have to be addressed by any organisation working with blockchain, the biggest being the need to educate organisations on what blockchain is, how it works, and how it changes business processes - in this case, fund distribution. This can take time, but Disberse insists that once partners see the value and benefits the technology can provide, the platform sells itself[33]. Evens so, in the short term Disberse believes that the platform is likely to get more interest from smaller NGOs, rather than bigger and more bureaucratic organisations. Regulations around international money transfers have also been a significant overhanging challenge. Here, Disberse have benefitted from participating in the FCA ‘regulatory sandbox’, which allowed them to explore their relationship with existing regulatory infrastructures in a secure environment. They will continue to refine their business model, but believe that the combined transparency improvements and cost savings will enable them to create a viable business based on transaction fees that can compete with legacy financial institutions.

Disberse is interested in exploring opportunities to link their platform to mobile money services, potentially by allowing beneficiaries to exchange Disberse tokens for mobile money credit rather than cash. In the short term, linking to Disberse’s platform could allow MNOs to generate new sources of revenue by facilitating the disbursement of international aid, but in the future, these use cases could also expand to include the delivery of emergency funds in humanitarian crises, social cash transfers, and results-based financing.

For more information, see: www.disberse.com

[33] Fearn, N. (2017). *‘Interview: Ben Joakim, CEO of Disberse’.* TechDragons. Available at: http://techdragons.wales/interview-ben-joakim-ceo-of-disberse/ [Accessed 15 Nov. 2017].

USE CASE 3

Blockchain and Humanitarian Cash Payments

An unprecedented and ever-increasing number of people were forced to leave or flee their homes due to conflict and persecution in 2016, with the global displaced population reaching nearly 64 million by mid-year. Over 21 million of the displaced are refugees, who have traversed international borders to escape considerable physical, economic and social hardships such as new and unresolved conflict, human rights violations or persecution. Having left behind their home, livelihoods, possessions and social networks, refugees must rely on their host government, the United Nations High Commissioner for Refugees (UNHCR) and the international community to ensure that they are able to live in safety and have access to vital support and assistance[34].

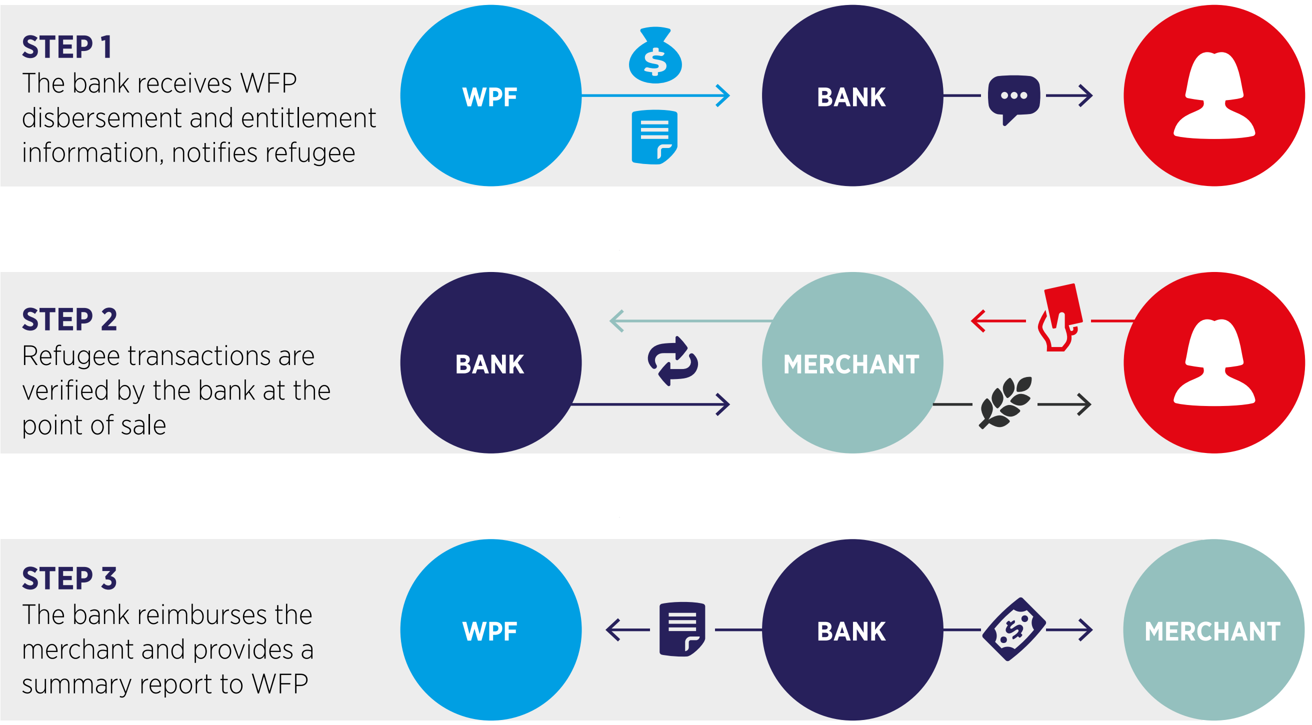
Over the past decade, the World Food Programme (WFP) has significantly increased their use of cash transfers to provide assistance to refugees and other people in need. In 2016, a total of 14.3 million people in 60 countries received cash assistance from WFP, up from 9.6 million in 2015 and only 3 million in 2010[35]. When deployed in the right context, cash transfers have been found to empower people to make their own choices about what they eat, and also reduce the need to resort to negative coping strategies, such as selling valuable assets, to buy food. WFP advocates that cash transfers also reduce the cost of providing food assistance, thus maximising the number of people that can be reached.

Traditionally, in order to transfer cash to beneficiaries WFP has had to work closely with a financial service provider, such as a local or national bank. At the beginning of each month, the bank is given an entire month's worth of cash for distribution, alongside of a list of beneficiaries and the amount of cash to which each is entitled. WFP estimates that in Jordan alone, monthly transfers to banks can total over USD $10 million. Once a beneficiary is notified by the bank that they have been granted a cash entitlement, they are able to go to a designated merchant and make a purchase, typically by using a physical card as a proof of ID. At the point of sale, the transaction is authorised by the bank, who verifies that the refugee's remaining entitlements are able to cover the cost of their purchase, and in time the merchant is reimbursed by the bank using the funds deposited in WFP's account. At the end of the month, the bank sends WFP a summary of their transactions and reports any issues with distributions.

[34] GSMA (2017). *'Refugees and Identity: Considerations for Mobile-Enabled Registration and Aid Delivery'*. GSMA. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Refugees-and-Identity.pdf

[35] For more information, see: http://www1.wfp.org/cash-transfers

WFP's Traditional Humanitarian Cash Transfer Process



STEP 1
The bank receives WFP disbersement and entitlement information, notifies refugee

STEP 2
Refugee transactions are verified by the bank at the point of sale

STEP 3
The bank reimburses the merchant and provides a summary report to WFP

There are four key challenges with this process. First, advancing large sums of money to a financial service provider creates a financial risk for WFP, especially when this is done in fragile markets where financial institutions are more likely to fail or commit fraud. The process is also expensive, costing WFP and other large humanitarian agencies millions of dollars every year – not only in banking fees, but also to cover the cost of tracking and reviewing thousands of banking transactions. For beneficiaries, there are also risks associated with privacy – sharing, misplacing or misusing sensitive personal information is especially dangerous for refugees, particularly those who are seeking protection from oppressive regimes. Finally, there is an issue of accountability – humanitarian organisations do not have their own 'record of reality', relying instead on the information provided to them at the end of each month by the bank.

WFP's Blockchain Solution

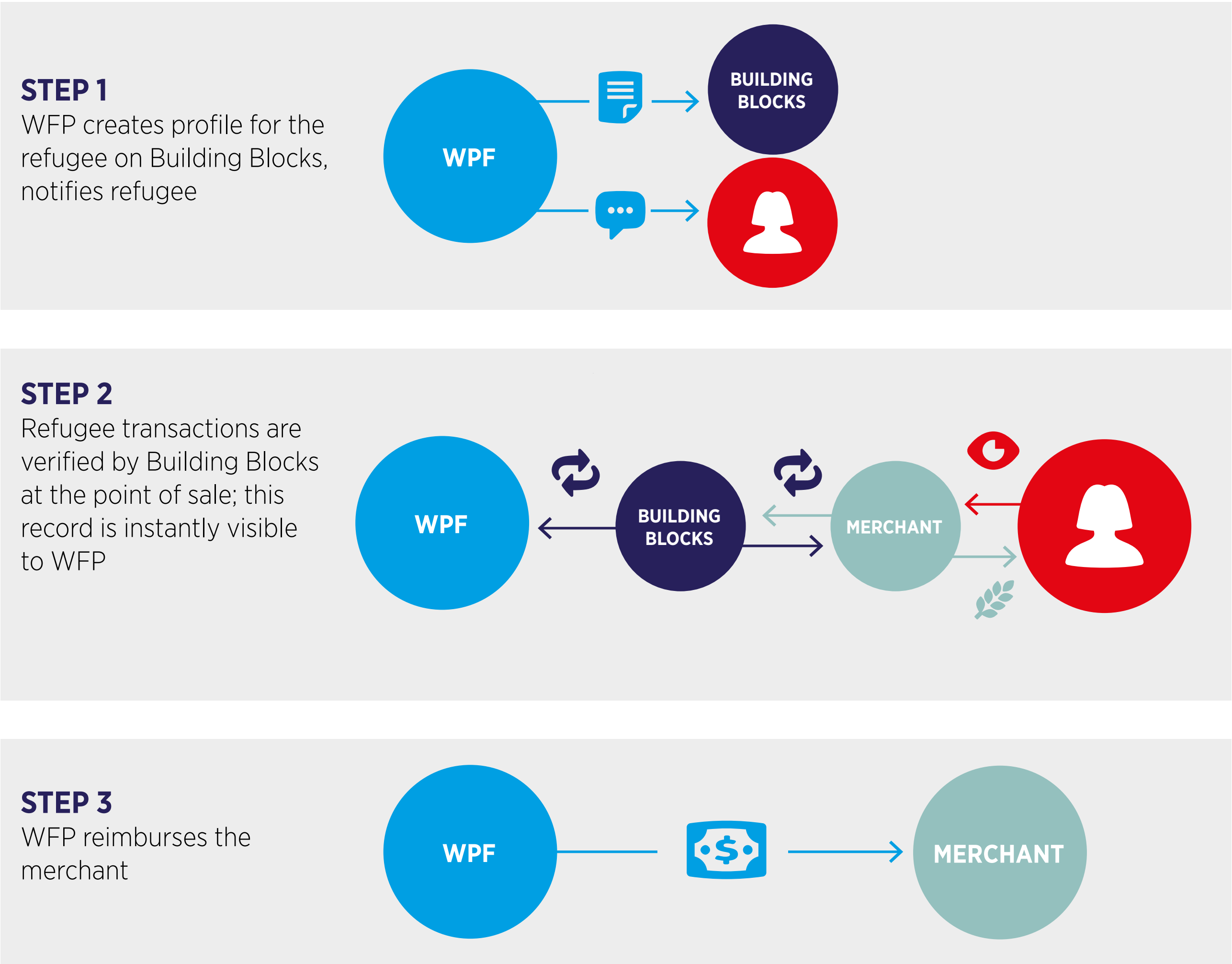
WFP's journey with blockchain began by investigating how the risks and inefficiencies in the cash transfer process could be improved. In January 2017, they launched a small pilot in Sindh province, Pakistan, to test core assumptions around the ability of blockchain technology to authenticate, record, and reconcile cash and food assistance transactions. After seeing positive results, the project moved into full-development and the 'Building Blocks' platform, which utilises a private blockchain, was rolled out in Jordan. Between May and November 2017, Building Block has been used to transfer USD $1 million in food vouchers to 10,500 Syrian refugees in Jordan, using the system to facilitate more than 220,000 individual transactions[36].

Crucially, the platform removes WFP's reliance on an intermediary bank to verify transactions and distribute funds. Rather than sending the bank sensitive information on each beneficiary, WFP can create secure profiles for each refugee on Building Blocks, where they only need to record two pieces of information: the refugee's entitlement, and a unique ID number given to each person or family. This ID number is linked to the biometric data stored in UNHCR's refugee database, which means that beneficiaries are able to authenticate themselves at merchants by simply scanning their irises, rather than having to reveal personal details such as their name or age.

When designing their new blockchain solution, WFP recognised the importance of not changing the beneficiaries' experience with disbursements – both in terms of the technology used (electing to use the iris verification system that already existed in Jordan) and the social value beneficiaries gained from the shopping experience (meaning refugees could visit merchants as frequently as they wanted). Once a beneficiary receives a message from WFP saying that they have an entitlement, they can go to an approved merchant and make a purchase, in the same exact way they did in the traditional process. At the point of sale, the merchant uses a connected device to authenticate the refugee's transaction against the entitlement information stored on Building Blocks, automatically confirms that the beneficiary has the 'credit' available to make their purchase. Every transaction is recorded on the refugee's profile, and WFP uses this information to pay the supermarket directly, using their corporate bank.

[36] For more information, see: http://innovation.wfp.org/project/building-blocks

WFP's Blockchain-Enabled Humanitarian Cash Transfer Process


STEP 1
WFP creates profile for the refugee on Building Blocks, notifies refugee

STEP 2
Refugee transactions are verified by Building Blocks at the point of sale; this record is instantly visible to WFP

STEP 3
WFP reimburses the merchant

With the new blockchain-enabled system, WFP has eliminated a significant portion of the fees previously paid to the bank and simplified its reconciliation and payment process. The blockchain provides WFP with a permanent, real-time record of every transaction, compiling information on when each transaction happened, which beneficiary conducted the transaction, where the transaction took place (at which supermarket), and the transaction amount. Every single transaction is verified instantly on the blockchain, allowing WFP to make payment to merchants as frequently as desired. Building Blocks has also eliminated the need to advance funds to a bank, reducing finical risk. With an estimated initial development cost of less than USD $100,000 (and minimal ongoing maintenance costs), the return on investment has been significant. WFP has set an ambitious goal to use Building Blocks to deliver cash transfers to 100,000 individuals by early 2018. By the second quarter of next year, the system could cover the entire Syrian refugee population of Jordan, or 500,000 people[37].

[37] Wong, J. (2017). *'The UN is using ethereum's technology to fund food for thousands of refugees'*, Quartz. Available at: https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan/ [Accessed 15 Nov. 2017].

WFP has pointed out that everything they have done through their platform so far could be done on a traditional IT system, without blockchain. However, they advocate that the real value of the technology will become evident once they begin to cross organisational boundaries and allow other humanitarian organisations to link to the database. In fact, while WFP currently operates Building Blocks on its own, the platform has been designed to allow multiple parties to contribute and share information. Currently, refugees in Jordan are likely to be registered multiple times, as different beneficiaries, by multiple NGOs, and refugees have to wait longer than necessary to obtain assistance because it is often unclear what support they have already received. Soon, WFP hopes to use the new blockchain system to empower beneficiaries with more control over, and access to, their information. This will become possible as more agencies join the blockchain, connectivity in camps improves, and smartphone devices become more ubiquitous.

Despite the platform's success, some challenges remain. Because blockchain is still a largely unproven, nascent technology, it is tough to argue that there are no bugs or issues with Building Blocks, especially when it is common to hear concerns about Bitcoin-related security breaches even though Building Blocks does not currently use any cryptocurrencies. Furthermore, WFP recognises that standards related to storing and managing refugee ID's is not fully developed yet, and there is still some uncertainty around how blockchain-enabled identity platforms fit into existing regulations.

In the near-term, WFP is hoping to start leveraging mobile money as a convenient and safe means of cash disbursement. In this scenario, WFP would open their own mobile wallet with an operator. When a beneficiary wants to 'cash out' their entitlement by transferring it to their personal wallet, or if a merchant would like to be reimbursed for a refugee's purchase via mobile money, the blockchain can be used to approve the transaction and initiate the transfer of credit. In time, delivering vouchers or entitlements through mobile money channels could allow beneficiaries to save unused funds, or even transfer entitlements to their family and friends. The blockchain backbone will allow beneficiaries to seamlessly redeem their entitlements through mobile money, ATMs, or supermarkets.

For more information, see:
http://innovation.wfp.org/project/building-blocks

V. Evaluating Blockchain for Development Projects

The applications developed by Gravity, BanQu and Accenture (for ID2020) suggest that permissioned blockchains provide the ideal platform for supporting self-sovereign identity services. The technology enables any individual with a mobile phone to anonymously record and manage their sensitive personal data, while giving the user complete control over how and with whom their information is shared. This ensures the identity systems remain *portable* and *private*. The fact that the information recorded to the blockchain is immutable and vetted by the customer's peers (or banked network) means that the ID is also *persistent* and *trusted*. And finally, by allowing service providers to securely tap into the platform, the ID system becomes highly *convenient*. By definition, this meets the standard requirements for sustainable, inclusive identity systems.

The case studies also indicate that self-sovereign identity systems could offer MNOs new opportunities to significantly lower the cost of on-boarding new customers and fulfilling SIM registration and KYC requirements. GSMA Intelligence has also found that mobile operators are well placed to verify a user's attributes on self-sovereign identity solutions due to their unique range of credentials[38], including their network credentials (customer's SIM and mobile number), customer account credentials (customer account data, point of presence locational data and billing), and personal credentials (individual biometrics and PIN codes). By leveraging these assets and helping to validate their customers' identity claims, MNOs have the opportunity to provide customers with access to more sophisticated identity-linked services, and potentially create new sources of revenue by providing identity-as-a-service.

It is likely that operators in emerging markets will be the first to capitalise on these opportunities, as social reputation-based identity systems have the most immediate need in places where access to legal proof of identity is limited. However, partnerships and business models that can adapt to decentralised approaches to identity must be in place for these kinds of blockchain projects to be successful, and this is a difficult task.

[38] GSMA, The Mobile Economy 2017. Page 29.

Self-sovereign identity systems will require a willingness from global institutions, governments and other service providers to collaborate and share sensitive information outside of their internal, trusted silos. Despite the widely accepted belief that blockchain technologies replace the need for human trust, it is crucial to point out that with permissioned ledgers the user must still trust the people who designed the application, the platform owners and the verifiers of data that is recorded on the chain.

Fundamentally, these systems will need government backing, and in many emerging markets, legal and regulatory frameworks around identity are often unclear and fragmented, and there are no standards for how to use unproven technology such as blockchain to store, manage and share citizen data. Regulators will need to determine who is legally responsible for the data in 'self-sovereign' ID systems – the user, or the platform provider? They will also need to grapple with questions such as: how will users and regulators know that the platforms and personal data are sustainably secure? And how does the use of blockchain for producing, using and sharing data fit within existing legal and regulatory practices?

Until questions like these are addressed, MNOs and other formal service providers will likely be reluctant to start tapping into these blockchain applications to validate or access data, and potentially risk their reputation with government and regulators by using technology that has not been properly vetted. However, Disberse has shown that small-scale pilots run in cooperation with regulators, government and service providers could create a regulatory 'safe sandbox space' where stakeholders can become more comfortable with the technology and define how blockchain can be used for KYC and identity purposes, leading to greater social and economic impact.

While the self-sovereign identity platforms appear libertarian and paradigm-shifting, the 'incorporative' platforms developed by Disperse and WFP – which focus on improving the efficiency of administrative systems and internal processes – might offer a more imminent opportunity for the mobile industry and development community to start working with blockchain technologies. The platforms fit more neatly within existing institutional frameworks and processes, appear to be sustainable and scalable, and are less likely to feel 'radical' for the end beneficiary. With Building Blocks, for instance, refugees do not know that blockchain is being employed, and the way they manage their cash transfers remains completely unchanged.

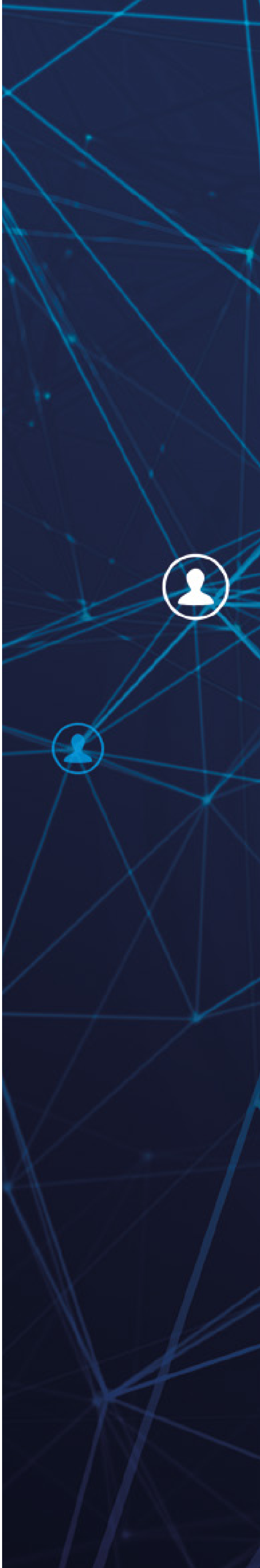
In general, it will likely be easier to introduce blockchain technologies that are designed to be private and permissioned as there is less risk and fewer unknowns, as all participants on the network are known to each other. However, there is some risk that permissioned blockchains will perpetuate the fragmentation of identity management and service delivery by keeping knowledge and data trapped in organisational silos. There is hope that the trust, transparency and security offered by blockchain will remove any remaining excuses organisations might have for avoiding collaboration and data-sharing, helping the sector move from an 'organizational focus' to an 'issues focus'. Here, MNOs and the development sector could learn from the financial service industry. Since 2014, a consortium of over 100 global financial institutions and regulators have been collaborating on blockchain-related initiatives through a software firm called R3. With support from over 2,000 technology, financial, and legal experts, these organisations have created a distributed ledger platform, called Corda, which is designed to automate legal agreements between partners and support interbank trading and settlements. R3 was born out of a common frustration amongst banks and other financial institutions with multiple generations of disparate legacy financial technology platforms that struggle to interoperate, causing inefficiencies, risk and spiralling costs[39].

Lastly, the success of the Disberse and WFP platforms indicate that the role operators play in the humanitarian and aid delivery spaces could soon be enhanced. Blockchain-enabled platforms that leverage mobile money services could provide a more convenient, cost-effective and transparent way for humanitarian organisations to transfer entitlements to refugees, and for donors to transfer project funds across international borders. The high uptake of mobile money services in developing markets – particularly among the segments of society which are targeted by development aid – suggests that operators should explore opportunities to link into and support these platforms. In doing so, they are likely to find new, exciting ways to support the delivery of aid, expand their customer base and generate new sources of revenue.

[39] For more information, see: https://www.r3.com/about/

gsma.com

To download the full report please visit
the GSMA website at www.gsma.com



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601