Learning Review

Blockchain Open Loop Cash Transfer Pilot Project

September 2018

www.ifrc.org
Saving lives, changing minds.

International Federation
of Red Cross and Red Crescent Societies

Introduction

In recent years, humanitarian work has become more complex with the growth of protracted crises, the impact of famine, climate change, urbanisation and the effect of mass population movements across all regions. There is increasing competition for limited resources from a growing number of actors and an ongoing struggle for humanitarian space. As needs outstrip resources, the sector needs to look at improving efficiencies whilst strengthening the quality and impact of its work.

Over the past decade, the use of cash transfer programming (CTP)[1] has increased. CTP is a disrupter: it is challenging the traditional humanitarian approach through the introduction of new actors, encouraging innovation and creating opportunities for financial inclusion. It is defining a new role for traditional actors and increasing the focus on accountability to affected communities. Well-designed, appropriate cash programmes bring greater choice and dignity to beneficiaries, while allowing humanitarian agencies to more efficiently and effectively meet the needs of affected populations. Just like any other method of aid delivery and programme implementation, CTP is constantly changing as the dynamics of disasters, donors, and the world changes.

Cash Transfer Programming must be relentlessly upgraded with new innovations and approaches to ensure vulnerable communities receive the best possible support.

Blockchain is one of the technological innovations being explored to make cash transfer systems more effective. Blockchain is a system of record that uses cryptography to secure data. The US Department of Commerce defines blockchain as "An immutable digital ledger system implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority." [2]

This definition highlights two key aspects of blockchain: firstly, information entered on a blockchain is immutable and cannot be altered, (i.e. additional information can be added, but existing information cannot be deleted), and, secondly, blockchain is a distributed system that does not have a single point of failure. Copies of a blockchain are stored on all computers on the network, making the system extremely difficult to hack or destroy.

Many blockchain use-cases are being explored in the humanitarian and development sectors. These include supply chain management, healthcare record systems, secure voting systems, peer-to-peer aid tracking and delivery platforms, secure land registries, and digital identification management[3].

The International Federation of the Red Cross and Red Crescent Societies (IFRC) has been actively exploring these trends. In early 2018, the IFRC applied and won a global fintech and Islamic Finance competition, which was organised by the Islamic Development Bank and IE Business School. The award will support the piloting of blockchain technology to increase the transparency and traceability of Islamic social financing. In December 2017, the IFRC was awarded a grant by the Norwegian Red Cross and Innovation Norway to conduct the Blockchain Open Loop Cash Transfer Pilot Project to explore how blockchain could add transparency and accountability to open-loop[4] CTP, and to investigate how the technology could provide people with digital identification.

Research suggests the potential for blockchain technology to undergird durable digital identification systems. This could provide an alternative identification to beneficiaries without a National ID and allow them to avail aid, particularly cash-based assistance. The pilot project investigated how digital IDs could be generated, maintained, and used in transaction tracking.

The objective of this report is to document the learnings from this Pilot and inform a way-forward for the IFRC to continue exploring the risks and benefits of blockchain technology, as well as to share the findings with other organisations that are considering the technology for similar purposes.

[1] *CTP refers to all programs where cash (or vouchers for goods or services) are directly provided to beneficiaries. In the context of humanitarian assistance, the term is used to refer to the provision of cash or vouchers given to individuals, household or community recipients; not to governments or other state actors. CaLP*
[2] *https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf*
[3] *Blockchain and Economic Development: Hype vs. Reality*

Figure 1: High-level process of Kenya Red Cross' cash transfer programming

Project Overview

In May 2018, the IFRC in collaboration with the Kenya Red Cross Society (KRCS) implemented the pilot project in Isiolo County, Kenya assisting over two-thousand households affected by drought. Isiolo County forms one of Kenya's twenty-three arid and semi-arid lands where drought conditions are prevalent, producing high livestock mortality and, in turn, food and livelihood insecurity.

KRCS has deep experience in CTP, having delivered cash-based assistance since 2011. KRCS has been one of the leading humanitarian actors in Kenya responding to the drought emergency that started in 2016. KRCS is also highly innovative, using a breadth of technologies to meet the needs of their programmes, from e-vouchers solutions to direct mobile money transfers.

The figure above shows the steps taken by KRCS in their cash transfer programming.

For the pilot project, the beneficiaries had already been registered from a previous cash distribution in Isiolo County. A subset of 2,000 households was drawn from the original group according to pre-established criteria. Relevant personal information—beneficiary name, phone number and national ID number—was uploaded to the data management system. To enable logging of transactions on the blockchain a set of public and private keys were generated for each beneficiary.

After finalizing the beneficiary list, a network of KRCS volunteers visited the communities to explain the Pilot Project objectives, process of receiving assistance, and how to contact KRCS if there were questions or complaints. The volunteers also delivered an informed consent statement in the local language and asked beneficiaries for permission to use their personal information to satisfy financial regulations to disburse cash. Consent was captured using mobile phones and recorded on the data management system.

A distribution plan was created that grouped beneficiaries by geographical area and included the amount they would receive[5]. The workflow to approve payments to beneficiaries involved a mechanism to ensure segregation of duties between the fund requester and the finance manager approving the disbursement. With the finance manager's final approval, cash was disbursed to beneficiaries through Safaricom M-Pesa, a mobile money transfer service with an extensive network in Kenya. Beneficiaries were familiar with the system and had received cash assistance before using their M-Pesa accounts.

Once Safaricom received the payment request and executed cash disbursement to the mobile wallets of beneficiaries, a record of the transaction was recorded on the data management platform and the blockchain. Given the blockchain's immutable nature, this

[4] *World Economic Forum defines open-loop payment system as "A payments network that enables otherwise closed-loop payment systems to share endpoints. For example, a card-based payment system that allows the ATM cards from one bank to be used at another bank's proprietary ATMs, or a remittance/money transfer system that enables funds deposited with one participating entity to be collected at another entity."* http://www.cashlearning.org/downloads/wefiprincipleshumanitarianpayments.pdf

[5] *Pilot provided cash assistance of 3,000 KSH + 49 KSH for transaction fee per household*

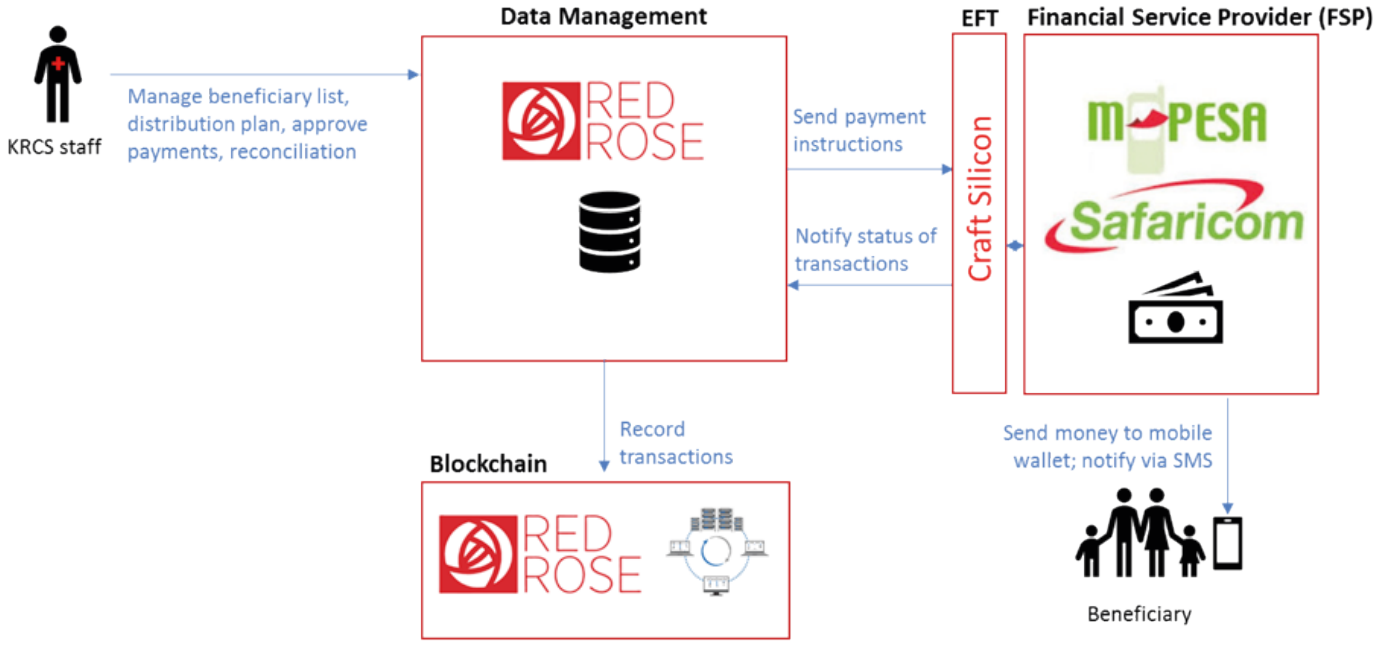

Figure 2 shows the basic system architecture and the interaction among the integrated systems used in the Pilot

technology provided an additional record and level of assurance that data in the data management and M-Pesa databases had not been tampered with.

Following the disbursement, nearly all beneficiaries immediately redeemed and spent their cash assistance. Within days of disbursement most had bought foodstuffs and medicine, repaid debts, and paid forward education fees addressing their specific basic needs, according to a survey done after the cash distribution.

The Solution

For the pilot project, KRCS pioneered a contextualized solution designed to promote timely delivery of aid while strengthening accountability to beneficiaries and donors. Several partners came together to combine different capacities into an end-to-end system: Red Rose implemented a data management system, which was integrated via an electronic funds transfer mechanism to Safaricom's M-Pesa mobile money network. In tandem, the data management system was also linked to a private blockchain built on open source technology to record transactions in an immutable manner.

Safaricom M-Pesa
A key factor underlying the pilot project's success was the widespread availability of mobile money networks in Kenya. Formed in 1997 as a subsidiary of Telkom Kenya, Safaricom Public Limited Company is the leading provider of mobile telephony in-country offering the M-Pesa mobile money service.[6]

KRCS has been using M-Pesa as its default delivery mechanism to deliver cash transfers to beneficiaries and to disburse staff per diems and volunteer allowances. However, the process for disbursement was cumbersome with manual initiation and reconciliation done via the exchange of spreadsheets. For the pilot project the system was fully automated using an Application Programming Interface (API) provided by M-Pesa that allows companies to connect through 3rd party applications to initiate cash transfers.

Craft Silicon
Craft Silicon is a financial solutions software company based in Kenya. The company developed an Electronic Funds Transfer (EFT) system for KRCS that directly integrates with M-Pesa and the KRCS internal financial system. The pilot project used the EFT to automate the disbursement by M-Pesa through the Red Rose data management platform, making the one-click approval of distribution possible. Instead of having a list of beneficiaries sent manually to M-Pesa, the EFT is used to request for immediate disbursement to individual beneficiaries for each call via the API provided.

Red Rose
Red Rose offers data management and delivery solutions for cash and in-kind assistance provided by humanitarian organizations. For the pilot project, Red Rose implemented an integration between their data management platform and the mobile money provider M-Pesa through the EFT. This allowed data to be managed from a centralized online portal, which facilitated beneficiary management, recording of consent, distribution planning, approval process for cash disbursement, tracking of assistance and reconciliation, data visualization and post-distribution monitoring.

[6] *M-PESA has two competitors, Airtel and Telkom. Since April 2018, Airtel and Safaricom subscribers have been able to transfer and receive money between networks at no extra charge, making most mobile money systems in Kenya interoperable (Safaricom and Airtel represent a combined 86.5% market share).*

Three features of the Red Rose data management solution were essential to the Pilot's success:

• First, the data collection tool works offline. Electric power in Isiolo County was limited, with frequent outages. Internet connection was only available through Safaricom hotspots, which were cumbersome and slow. Being able to collect data offline and upload it later when connectivity was available was a critical feature.

• Second, the data solution integrates with financial service providers and other third parties through an application programming interface (API) allowing communications between different platforms. This feature allowed KRCS to automate the distribution and reconciliation with M-Pesa.

• Third, the platform provided audit logs to document decisions and approvals, segregated duties between the requester and the approver of funds and provided an easy way to see who received what, allowing the tracking of funds down to beneficiary level.

Having a robust data management solution allowed KRCS to respond to beneficiaries on the ground more quickly. The status of payments could be provided, missing or erroneous information corrected, consent statements recorded, etc. Queries that had previously required days to respond to were answered in minutes due to the availability of data and easy access to it.

Multichain Blockchain

Launched in 2014 by Coin Sciences, Multichain Private Blockchain enables organizations to build their own chains using an off-the-shelf platform. Multichain allows organizations to build public and private chains, determine the target time for blocks, permission users, control block size, monitor metadata, and write chaincode.

With the support of Red Rose, a blockchain was implemented using Multichain's off-the-shelf solution, making use of its native algorithm to secure transaction data with cryptography and produce an immutable digital ledger. Four nodes were connected to this blockchain allowing IFRC, KRCS, and Red Rose to view transactions.

The blockchain recorded cash disbursements from the data management system, providing an additional layer of assurance that transactions were accounted for. Records were viewed via a custom-built interface, which could then be compared to the built-in audit logs available from the data management platform.

Figure 3 below shows an example of the cash disbursement transactions recorded in the blockchain and Figure 4 provides a view of a transaction. Very limited information and no personal information[7] was recorded on the blockchain during the Pilot to ensure that data was protected while the risks and benefits of the technology were being explored.

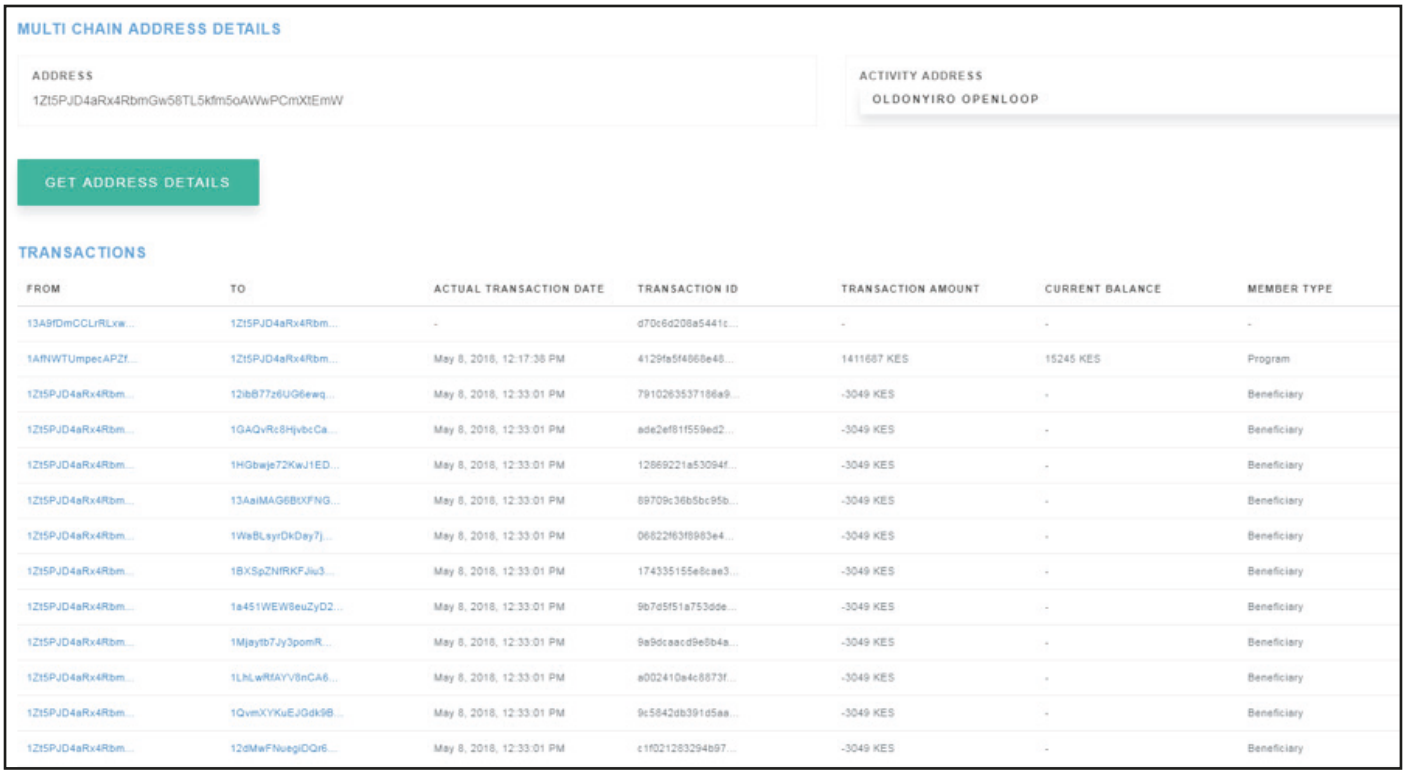

Figure 3: Snapshot of transactions recorded in the blockchain

[7] *See section on Challenges related to Data Privacy*

Figure 4: Snapshot of a cash disbursement transactions to a beneficiary recorded in the blockchain

Learning and outstanding questions

The project generated a significant amount of learning, leading to priorities for research moving forward:

Technological synergies: For a federated organization like the IFRC whose members utilise a variety of platforms for data collection and management, the modular approach used to develop the solution architecture provides flexibility to consider different applications to fulfil the required capabilities. The solution architecture also allowed to demonstrate that blockchain solutions can be implemented in lighter and less complicated manner, depending on the use-case and required capabilities.

Question: How could the architecture could be expanded to allow third parties (e.g. financial service providers) to record transactions directly on the blockchain?

Question: How could a public blockchain be incorporated and add value to the system?

Auditability: Blockchain technology provided an additional layer of security and integrity to data from CTP. Data is recorded, timestamped, and available for analysis and audit. Its immutable property helps triangulate discrepancies that may occur within an ecosystem of applications and therefore strengthen confidence in the programme. It offers auditors an independent way of verifying a compiled list of transactions against the records produced by the individual systems such as Red Rose or M-Pesa, keeping each of the systems honest and increasing confidence in the programme. Any discrepancies with the data could help flag an investigation early on. However, the ability to query data in the current solution was limited to a simple UI and command line interfaces.

In fact, the side effect of having a blockchain makes it harder to simply request the service provider to change the data. For example, when a disbursement is requested by mistake, it's easy to call M-Pesa to revert the transaction. But because of the integration with the data management platform and blockchain, the process for this change needs to be orchestrated so a record to update the data is reflected on the blockchain in addition to all the interacting systems. This ensures the auditor has a full view of the transactions, including the original disbursement request and a separate record to correct that request.

Question: What are the processes, tools, and skillsets needed to audit data on a blockchain?

Digital Identity: Due to time-constraints, only basic elements of digital identity were tested: each beneficiary profile established in the Red Rose data management platform was assigned a unique Red Rose beneficiary ID; on the blockchain, private and public keys were generated based on the Red Rose beneficiary ID; transactions were written on the blockchain using the public key corresponding to each beneficiary.

For the Pilot the same vendor Red Rose was managing the beneficiaries' personally identifiable information (PII), the blockchain infrastructure, and generation of digital IDs. The generation and management of the digital IDs would be better served if decoupled and managed as a separate capability that could be controlled by another system that would allow for cross-platform use.

There's a need to explore with third parties (such

as Safaricom) the use of digital IDs generated by humanitarian organisations as an alternative to government IDs. Currently, national laws in Kenya require Safaricom to collect government issued ID to provide a mobile phone number and to register for M-Pesa accounts.

Furthermore, there is also a need to allow beneficiaries to manage and maintain their own personal information. The concept of "self-sovereign" digital identities is being explored by technologists to enable ownership of personal information by beneficiaries instead of by humanitarian organizations and third-party providers. Rather than having humanitarian organizations and third-party providers repeatedly collect beneficiary personal information, a self-sovereign approach would empower beneficiaries to decide which relevant information to share with each service provider.

Question: Could a digital identity based on a self-sovereign approach provide greater data security, while allowing beneficiaries to control and manage their own personal information?

Question: To what extent would third parties (such as Safaricom) be willing to use digital ID's generated by humanitarian organizations such as Red Cross Red Crescent Movement as an alternative to government IDs?

Question: Would the use of digital ID's allow beneficiaries without official government ID's to establish a history of interactions with different organisations, thereby increasing their ability to access a wider set of social and financial services?

Beneficiary Consent: The pilot project raised important questions surrounding consent and data privacy. For beneficiaries, the consent process was uncontroversial. During a survey, four respondents expressed concern over the Pilot's use of their personal information, but they still opted to give their consent. In interviews beneficiaries explained that they trusted KRCS and that this trust extended to its partners. However, had beneficiaries not consented they would have not received assistance.

The Handbook on Data Protection in Humanitarian Action[8] published by the Brussels Privacy Hub and the ICRC in 2017 identifies several circumstances that can obviate the need to attain consent from beneficiaries. These include the physical endangerment and vulnerability of a data subject, the inability of a Humanitarian Organization to collect consent due to security in the areas of operation, the gross vulnerability of a data subject resulting in their inability to provide true consent, and the presence of technologies characterized by complex architecture and multiple parties to the point that the beneficiaries are not in the position to understand the benefits and risks of what they are consenting to.

In the case of the pilot project, Blockchain technology is a complex data structure involving multiple stakeholders. It is difficult to understand, even for information technology professionals. It remains unclear how informed consent can be obtained from beneficiaries for projects involving complex data structures like blockchain. Furthermore, as the ICRC notes, gross vulnerability can also diminish the need for a full consent process (ICRC 2017). Beneficiaries of the pilot project were under duress and vulnerable to insecurity due to drought conditions. If they did not give their consent, they would not have received assistance.

It must be noted that the process of obtaining consent for this Pilot was not only meant to record explicit beneficiary consent for personal data processing, but it was also used to ensure beneficiaries received communications on programme goals and objectives, how they would receive their cash assistance, and feedback and complaint mechanisms - this in and of itself has merit and is good programming.

In the future, however, IFRC will need to build a robust protocol on the legal bases—which includes informed consent—for obtaining and using beneficiary data involving complex data architectures and contexts.

[8] https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

Providing information on how personal data will be used is also a requirement regardless of which legal basis is used.

Data Privacy: The European Union General Data Protection Regulation (GDPR), which entered into effect on 25 May 2018, is reshaping international standards of data protection. Its release has prompted Humanitarian Organizations to reconsider and strengthen data protection practices. As an International Humanitarian Organization, the IFRC is not subject to GDPR requirements, however, it seeks to align its data protection practices with those of GDPR—which represent the gold standard—to demonstrate commitment in taking data protection seriously. Additionally, in working with National Societies such as KRCS, adherence to local laws related to data privacy is always observed.

Additionally, IFRC made extensive use of the Handbook on Data Protection in Humanitarian Action to guide data privacy protocols. An industry standard, the Handbook outlines data protection practices in the Humanitarian Sector and advances five principles of data protection:

1. Limitation and Further Processing: data recording should be clearly established at the outset of programs and confined to its purpose.

2. Legal bases for Personal Data Processing: analytics should only be performed on data if relevant to the program's purpose. If not, a new legal basis must be found.

3. Fair and lawful processing: data recording should be fair and non-discriminatory.

4. Data minimization: data recorded should be minimal.

5.Data security: data recorded should be secure, up to date, and accurate.

For the pilot, the beneficiary information collected included name, national ID number, and mobile phone number. This was collected in accordance with the Kenya minimal requirements for mobile money transfers and the principle of data minimization. No other data was collected, and Safaricom conducted data verification prior to processing mobile transfers to ensure accuracy and validity of accounts.

Since GDPR gives the right to data subject to be forgotten (i.e. they can request that their personal data be modified or deleted), it's unclear how this can be done with a technology that stores "unalterable" data. There are discussions on whether the pseudonymized IDs stored in the blockchain to refer to beneficiaries are considered personal information. The pilot project used a permission-based private blockchain to keep full control of the security of data.

Question: To what extent are GDPR and Blockchain technology compatible?

Intellectual Property: Collaboration with private sector partners was fundamentally important to the pilot project's success. Initially, the IFRC attempted to partner with a set of private sector companies with specific technology and know-how under a pro bono arrangement; however, negotiations around intellectual property (IP) were time consuming and it was not possible to reach agreement within the project's six-month timeframe. Ultimately, the IFRC opted to work with Red Rose, with which it had already secured a contractual agreement that included previously negotiated clauses on intellectual property.

Partnership discussions highlighted that the IFRC had limited experience negotiating intellectual property for technology-related partnerships. What constitutes intellectual property depends on the vantage point of each organisation and can range from a restrictive definition – e.g. patentable assets such as software code – to a much broader definition that encompasses organizational know-how, processes, and business models.
When IP is being developed that could have future

commercial value, agreeing on what IP is being contributed and created becomes increasingly important. While the private sector is focused on maximizing value for its shareholders, non-profit organizations are driven by humanitarian principles and seek partnerships that further their ability to address the needs of vulnerable people.

Question: To what extent are the public and private sector's approaches to intellectual property compatible given the two sectors differing motives for partnering?

Wrapping Up

As the Red Cross and Red Crescent Movement fulfils its Grand Bargain commitment to scale up cash transfer programming, better ways of implementing and supporting their cash programmes are necessary. Innovative technologies offer ways to address specific needs for CTP.

Blockchain technology offers a way to improve transparency and accountability through its unalterable distributed ledger. Coupled with data management and integration with open-loop payments such as mobile money, this solution enables more efficient, timely disbursement of cash at scale, while ensuring further controls and improved quality of service to beneficiaries.

This pilot project is the IFRC and KRCS' first step towards implementing such a solution. Due to the short timeline, the focus was primarily on understanding blockchain's potential for increasing transparency and accountability of CTP. There are more opportunities to explore blockchain technology for cash-assistance including the use of smart contracts to secure forecast-based financing arrangements, the deployment of durable, self-sovereign digital identifications, tracking of peer-to-peer donations and payments, and the use of cryptocurrencies.

Just as cash has been a positive disrupter for humanitarian assistance, blockchain also shows disruptive potential, provided its development is considered as part of a broader vision supporting CTP.