EXPLORING THE ADVANTAGES OF BLOCKCHAIN TECHNOLOGY FOR SMALLHOLDER FARMING
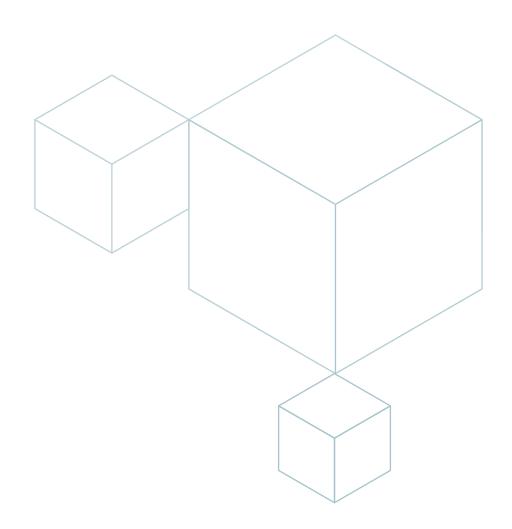
EXPLORING THE ADVANTAGES OF BLOCKCHAIN TECHNOLOGY FOR SMALLHOLDER FARMING

IFAD

Investing in rural people

TABLE OF CONTENTS

Acknowledgments

While this Brief was prepared for IFAD's staff and partners, the views expressed are not necessarily those of IFAD.

INTRODUCTION

Distributed ledger technology (DLT)/blockchain is an exciting new technology that may prove to be a radical innovation. Similar to the steam engine and the Internet, which triggered previous industrial revolutions, blockchain has the power to revolutionize existing economic and business models. It has the potential to deliver productivity gains to multiple industries, including the financial sector, energy markets, supply chains, intellectual property management, "virtual firms", the public sector and beyond. Its ability to provide disintermediation, improve transparency and increase auditability can significantly reduce transaction costs, introduce efficiency into existing value chains, challenge revenue models and open new markets. In short, a blockchain is a database which is shared across a network of computers. One can add to it but not change previous data within it. The network runs constant checks to ensure the authenticity of the database. While the most noted use of blockchain is in the cryptocurrency bitcoin, its application is now used for many other collaborations. It is a foundational technology of a platform that allows designing a secure way to record transactions and circulate it among signatories, or any kind of target group with an Internet connection. At its core, it is an extremely democratic ledger that cannot be arbitrarily manipulated and easily shareable.

For agriculture in poor countries, blockchain has the potential to improve financial management, provenance, traceability and transparency in food chains and to enable the creation of new markets and products.

This briefing note is intended as a primer on blockchain and a spur to begin considering how best to capitalize on blockchain technology to achieve IFAD's objectives. Several development agencies have already expressed their vision of blockchain and discussions continue among them on how best to tap into the opportunities of blockchain for agriculture.[1]
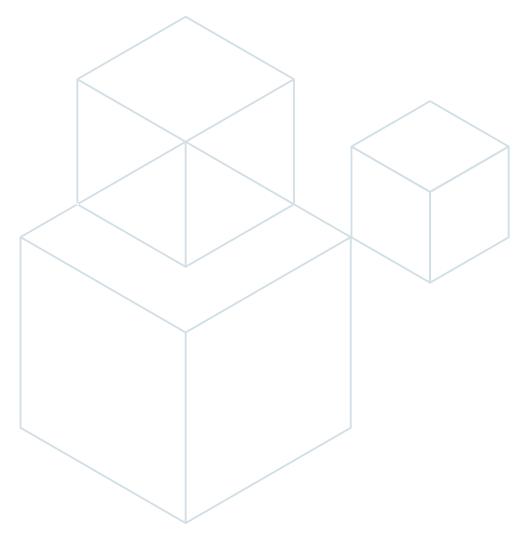
This note also explores potential applications for blockchain in IFAD's business. It offers a useful overview of potential directions for IFAD to consider as well as recommendations for initial steps the Fund can take.

Blockchain applications are in the early stages of development. Not only is the technology itself new, but its prerequisites (smartphone usage, connectivity, education and the skills to manage cryptographic keys) are often lacking. As of today, hardly any real-world problem has been solved by blockchain, but we can say it solves the problem of "trust".

---

1. Brussels Briefing n. 55 "Opportunities of blockchain for agriculture".
https://brusselsbriefings.net/2019/04/26/next-brussels-briefing-n-55-opportunities-of-blockchain-for-agriculture/

According to reports in a 2017 issue of Harvard Business Review, "Bank of America, JPMorgan, the New York Stock Exchange, Fidelity Investments, and Standard Chartered are testing blockchain technology as a replacement for paper-based and manual transaction processing in such areas as trade finance, foreign exchange, cross-border settlement and securities settlement."

Through its mandate, IFAD must aim to ensure that rural people are able to benefit from the opportunities brought about by blockchain technology. In determining IFAD's approach to blockchain, the most important criteria should be the technology's risks, competitiveness, longevity and fundraising capabilities, in addition to its coherence with IFAD's objectives. Applying these criteria, the most promising application areas of blockchain technology in smallholder agriculture are remittances, land titles and supply chains. Ultimately, only active proofs of concept will reveal the potential of blockchain, but IFAD could also engage in related activities, such as building knowledge and competencies and by expressing a well-thought-out vision on realistic and fair blockchain applications.

DISTRIBUTIVE LEDGER TECHNOLOGY/BLOCKCHAIN

A blockchain is a digital transaction ledger, maintained by a network of multiple computing machines that are not relying on a trusted third party. Individual transaction data files (blocks) are managed through specific software platforms that allow the data to be transmitted, processed, stored, and represented in human readable form. Every transaction is disseminated through the network of machines running the blockchain protocol and needs to be validated by all computer nodes. The key feature of a blockchain is its ability to keep a consistent view and agreement among the participants (i.e. consensus).[2]

Blockchain may prove particularly valuable in emerging market economies, although serious challenges and risks (both technical and regulatory) will need to be addressed before it achieves widespread adoption. Questions remain about blockchain's scalability, interoperability among different networks, security, transition costs, data privacy and governance. Business leaders and policymakers will need to think long and hard about when and under what conditions a blockchain initiative may be warranted.

In traditional systems, a central authority (such as a reserve bank or land registrar) maintains and controls a ledger of information. For example, banks maintain a financial ledger of who holds money, and governments maintain a ledger for information such as identity and titles. These entities also act as the trusted agent in any exchange: banks handle financial transactions, and governments maintain titles.

Distributed ledger technology (DLT) and blockchain enable transactions between members of complex networks without the need for central authorities or middlemen. Everyone maintains a copy of the shared ledger and independently confirms its validity through consensus. Everyone has access, but no one is in control. Only through consensus are new records and amendments allowed to the ledger, and no one can alter past entries. Eliminating centralized authority can increase speed, lower transaction costs and enhance security.

2. Francesc Xavier Prenafeta Boldú, IRTA Institute of Agrifood Research and Technology. The Rise of the Blockchain Technology in Agriculture and Food Supply Chain. September 2018.

Evolution of blockchain

Blockchains first got their start in the early 1990s, but they really took off with the introduction of bitcoin. Bitcoin is a peer-to-peer electronic cash system launched by Satoshi Nakamoto, a mysterious, pseudonymous person or cabal that laid out a white paper on how blockchain could be applied to bitcoin, in 2009. It is "based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without any need for a trusted third party" (Nakamoto).[3] Bitcoin was originally backed by techno-libertarians seeking to establish a currency outside of government control.

Bitcoin's commitment to the self-sovereignty of its users and pseudo-anonymity in transactions also opened the platform to illicit activities, which tarnished its reputation with governments and the public alike. Despite these problems, the development of bitcoin has continued. In January 2019, its market capitalization was approximately US$60 billion.[4]

Today, bitcoin is used as payment by millions of people, including a growing remittances market. Ethereum, a blockchain-based start-up, was launched in 2014 as an open-source, public, blockchain-based distribution system for any kind of decentralized application. Because of these extended abilities, it is often called Blockchain 2.0. Ethereum introduced the possibility of smart contracts, or deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents.

3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
   Retrieved from https://bitcoin.org/bitcoin.pdf
4. Bitcoin trading volume. https://data.bitcoinity.org

HOW IT WORKS

DLT and blockchain technology allow transactions between parties that are secure and transparent but that do not require the presence of a centralized regulating third party such as a financial institution or government.

Transaction information (such as from whom, to whom, and amount) is stored in sets of information called "blocks" which are encrypted, time-stamped and given a unique fingerprint ID (called a "hash").

These blocks are sent to participating members (or nodes) on the network who verify the transaction (i.e. by checking all the hashes in all the blocks). Once the information is verified, the block is linked to the previous block using the hash in a continuous chain back to the original transaction. Information within the block cannot be changed without changing the hash, and changing the hash would result in the block no longer being correctly linked in the chain.

Box 1: Irreversibility and immutability
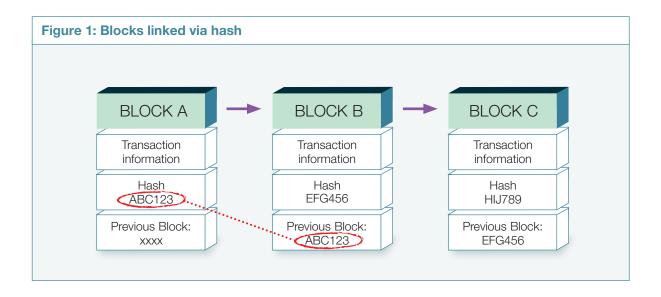
In simplistic terms, we can think of the immutability of a blockchain like that of sending an email to a distribution list. The data in that message becomes immutable. In order to change the data, all members of the distribution list would have to tamper with or delete the email (or persuade administrators of Gmail, Outlook, or any other email service to do so). From the point of view of the control, that email is immutable – it cannot be undone or modified without the consensus of the entire distribution list and the risk of getting caught.
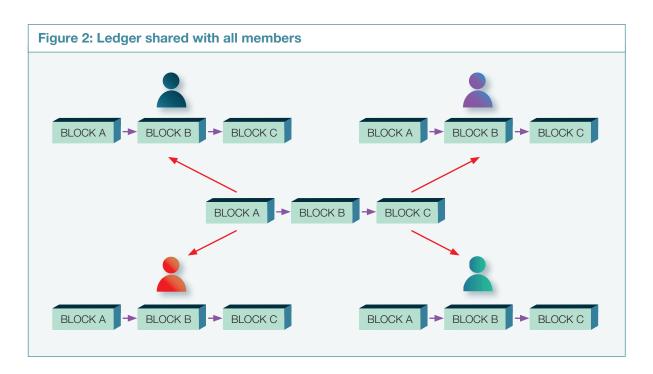
So the immutability is relative, and it is related to how difficult it is to change something.

The same thing happens in a blockchain. Once a piece of data has been recorded or a transaction has been made, it is impossible to delete or change it, or rather, it is extremely easy to realize that someone is trying to modify some information.[5]

It could only be cancelled if the rest of the participants agreed with the modification. That is why it is often said that this technology is irreversible and immutable, in other words, that there is no practical way to roll back and change or edit any data that has been recorded in the blockchain.

---

5. Ethereum. Blockchain - What exactly is the Blockchain and how does it work? What uses can be given to it? (2018) Available at: https://www.miethereum.com/en/blockchain-guide/

Figure 1: Blocks linked via hash

Figure 2: Ledger shared with all members

Thus, past information cannot be changed without invalidating it within the chain. Trust in transactions is not brokered by intermediaries – as has been the case until now, with banks and other institutions or providers – but is embodied algorithmically in the transaction itself.

Furthermore, the ledger is shared (or distributed) among all actors in the network so that all participants "agree" on the validity of a block.

The nodes[6] that verify each block are called "miners",[7] and they are incentivized to perform these complex computations in exchange for rewards (such as bitcoins). This consensus-based process (known as "proof of work" in bitcoin) to ensure encryption of the data requires intense computational power, which some believe is wasteful and restrains the scalability of blockchains. However, it is this feature that guarantees the chain's robust security, making it more resilient to attacks. Changing a past transaction (or block) means convincing a majority of ledger holders as part of a peer-to-peer network to agree on the changed information, which is difficult if not impossible to do, because of the massive amount of computational input it would require.

Taken together, blockchain offers:

- decentralization/disintermediation: no external authority or centralized governing body (e.g. government, bank) is required to regulate transactions
- security/immutability: encryption on each block makes it difficult to change information in the block; links between blocks are invalidated if information is changed
- transparency: all parties can see transactions and agree on their validity
- permanence: entries cannot be changed or deleted; new or "updated" data can only be entered consecutively (not overwritten).

Blockchain is often considered a general-purpose technology, like an electric motor, which can facilitate innovation in multiple industries. Beyond financial transactions, assets can be created directly on the network. Cryptocurrencies and rights to real-world assets can be given a digital representation on the network (referred to as "tokenized assets"). Because, in theory, any real-world concept can be given a digitized representation and cryptographically secured, almost any process can be facilitated using blockchain.

Public networks versus private networks

Blockchain networks can be public or private. Public networks are open and accessible to anyone wishing to join. They have no restrictions on membership, and data stored on these networks is visible to all participants in encrypted format. Bitcoin is an example of an open network. Public networks do not have a central authority; instead, they rely on network participants to verify transactions and record data based on an established protocol. On a public network, sensitive data is encrypted to ensure privacy.

---

6. Nodes form the infrastructure of a blockchain. They can be any kind of device (computers, laptops or even bigger servers). All nodes on a blockchain are connected to each other and use peer-to-peer protocol that allows all nodes to communicate with each other with the network as well as spread information on transactions. In the case of the bitcoin, we know about 10,000 nodes that use standard ports to maintain the global infrastructure. (https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f).

7. For a transaction to be verified and placed on the blockchain, complicated mathematical problems, requiring a lot of computing power and use algorithms, must first be solved. This is known as mining. People who use their computers to perform these calculations – the miners – receive rewards in the form of new currency (https://coinlu.com/what-is-blockchain-technology/).

By contrast, **private networks** do not allow access to data without prior permission. Permission levels may be tiered, such that different entities and individuals may have varying levels of authority to conduct transactions and view data. Private networks are closer to relational databases currently used by large corporations, where there are "trusted" nodes or system administrators who control access and rights. Although private networks lose the benefits of decentralized validation, they can still offer reduced transaction costs.

Established companies, particularly those in the financial industry, are gradually adopting private distributed ledgers for internal use, as well as for conducting transactions with trusted partners. Doing so allows them to experiment with this new technology while maintaining data confidentiality. It also allows them to comply with regulations, something that is not possible under the conditions of complete anonymity of public networks (Niforos).[8] That said, public networks are hardly ever completely anonymous. Most of them are pseudonymous[9] networks that fit in regulatory frameworks, and often the actors within the network comply with the rules such as Anti-Money Laundering (AML), Know Your Customer (KYC) and Combating Financing of Terrorism (CFT) regulations.

Private networks are practical and encourage other companies to adopt the technology, but they are paradoxically more vulnerable to external attacks because they are typically owned by a single individual or corporation, making them centralized and less secure than public blockchains.[10] Both public and private networks face challenges with interoperability to freely share information across all coexisting blockchain networks.[11]

There is heated debated about the relative merits of public and private networks, and each has its own philosophy and design principles. Public networks offer immutability and transparency of encrypted data. They offer freedom of use, inclusion, disintermediation, sovereignty and privacy. Private networks provide more control for implementers. It is likely that private networks will persist as commercial interests and status quo will be difficult to overcome.

However, there is room for "partially decentralized" blockchains. In these, the right to read the blockchain may be public, or restricted to the participants, or have hybrid routes that allow members of the public to make a limited number of queries. Additionally, data from a private blockchain can be periodically fingerprinted (hashed) and sent to a public one, which can provide additional audit ability (Niforos).[12]

---

8. Niforos, M. Blockchain in Financial Services In Emerging Markets: Part II. EMCompass Note 44, August 2017. Washington D.C.: International Finance Corporation (World Bank Group).

9. Pseudonymity is the near-anonymous state in which a user has a consistent identifier that is not their real name: a pseudonym. In pseudonymous systems, real identities are only available to site administrators. Pseudonymity allows users to communicate with one another in a generally anonymous way. Pseudonyms are typically user-chosen names. Pseudonymity helps maintain user privacy. (https://whatis.techtarget.com/definition/pseudonymity)

10. The Blockchain Council (https://www.blockchain-council.org/blockchain/are-private-blockchains-better-than-public-blockchains/).

11. The importance of blockchain interoperability. https://medium.com/wanchain-foundation/the-importance-of-blockchain-interoperability-b6a0bbd06d11

12. Niforos, M. Blockchain in Financial Services In Emerging Markets: Part II. EMCompass Note 44, August 2017. Washington D.C.: International Finance Corporation (World Bank Group).

HOW DLT/BLOCKCHAIN IS BEING USED

The blockchain ecosystem is currently in full experimentation mode, bringing new innovations and hybrid solutions. Consortia are emerging globally to discuss and provide solutions, address governance and industry standard issues, and provide regulatory insights. These include the Ethereum Enterprise Alliance (EEA) and China Ledger, which are attracting participation from dozens of major industry players, innovators, regulators and governments (Niforos).[13]

Currently, blockchain is primarily used in financial services to enable digital payment systems and remittances. Financial service providers (FSPs) are testing more complex financial instruments and transactions such as insurance, deposits, lending, capital-raising and investment management.

Beyond financial services, blockchain represents a paradigm shift in business and government. In principle, any type of asset can be tokenized, tracked and traded through a blockchain. Blockchain can serve as a registry, inventory system and transaction platform for recording, tracking, monitoring and transferring rights to different asset classes – including intellectual property, votes, digital identity, health data and real estate. Information about the origin of goods, identity credentials and digital rights can be securely stored and traced with a distributed ledger.

Potentially, DLT could replace (partially or entirely) the government's role as the direct authority in authenticating identity, issuing certificates and validating land titles. It could play a large role in storing health records, disseminating social security benefits and managing votes and civic participation.

Existing organizations, corporations and joint ventures currently work in federations with shared databases and an internal central body that settles transactions for participants

---

Box 2: Examples of current blockchain usage

- **Financial services:** Tempo is a French company offering a blockchain-based remittances service based on the Stellar network. It offers fast service at low rates.
- **Cooperatives:** Australian-based Agunity uses blockchain and smartphones to create a circle of trust for small farmer cooperatives.
- **Asset ownership:** The local government of Andhra Pradesh, India registers land titles with the aid of blockchain. Farmers can retrieve and transfer land titles using mobile apps. It is not an easy experiment. Read more here.

---

13. Niforos, M. Beyond Fintech: Leveraging Blockchain for More Sustainable and Inclusive Supply Chains. September 2017. EMCompass Note 45. Washington D.C.: International Finance Corporation (World Bank Group).

and keeps track of fair distribution of transactions and identity management (examples include SWIFT, eIDAS and many more). Blockchains could improve efficiency and security in these federative solutions. Similarly, wherever actors share databases, blockchain could add efficiency and an extra layer of security. For example, supply chains are an obvious candidate for blockchain improvements.

Future development

Blockchain technology will surely mature over time. However, as with the adoption of the Internet since the 1990s, it may take some time before blockchain becomes part of daily life. That said, adoption of open public blockchain-based financial services by "unbanked" people might happen faster than expected, as has been the case in Kenya with M-Pesa. M-Pesa is a mobile phone-based money transfer, financing and microfinancing service, launched in 2007 by Vodafone for Safaricom and Vodacom, the largest mobile network operators in Kenya and Tanzania. In just seven years, M-Pesa had more transfers than the total joint banking sector in Kenya (DFIN511).

Blockchain applications are in the early stages of development. Before they can really take off, not only the technology but also the preconditions to use the technology (access to a smartphone, wireless connectivity, education and skills to manage cryptographic keys) will need to be in place. Adoption also requires shifts in behaviour and mindset: blockchains disrupt the current way of doing business. The complex and encompassing technology requires new ways of thinking.

While no one can predict precisely what will happen next, the following are reasonable expectations for the future of blockchain:

- Blockchain and cryptocurrencies will have an accelerated disruptive and innovative effect on societies beyond national boundaries.
- More cryptocurrencies will be invented, and digital identities and money will flood the globe.
- Decentralization of financial services will continue, functions will be more and more open-sourced, and key management will increasingly become an individual task requiring competence that will necessitate training and development.
- Costs of financial services and the cost of storing value are likely to drop to near zero.
- Creating immutable digital proofs and signatures that are time-stamped on an open public blockchain will go hand in hand with creating a fairer world.
- Blockchain applications as a spin-off of open public cryptocurrencies will be integrated into everyday products and daily life.
- Blockchain technology will eventually demonstrate its ability to scale.
- Regulatory and law enforcement will lag behind, because the speed of innovation will outpace legislation.
- In principle, the technology will be equally available to a community of users, holders and/or developers, who can all join or leave at will. This equal access is expected to persist.
- Personal information security and privacy will be increasingly important to protecting property and possessions and enhancing inclusion.

IFAD'S ROLE

At first glance, it may be difficult to see how blockchain is relevant to IFAD's objectives. How do shared networks and cryptocurrencies help a struggling small farmer? But looking at the design principles of blockchain – immutability, transparency, free use, inclusion and privacy – reveals how closely aligned blockchain is with IFAD principles.

As was true at the advent of the Internet, most people do not yet see the advantages of using blockchain over existing "traditional" methods. But forward-thinking people developed the Internet into what it is today, and it is now difficult to imagine a world without it. IFAD can facilitate a similar transition with blockchains.

However, the use of DLT/Blockchain does have its challenges, which IFAD should keep in mind when deciding on a path:

- Blockchain technology is still in its infancy.
- Blockchain is a complex and still quite a niche area of expertise, consisting of mathematics, encryption and decentralized computer networks. It can be difficult to explain to decision-makers in our programme countries when it comes to investing resources in its adoption.
- Early adoption by only a few parties might cause resentment by others. The self-confidence of some forerunners of the technology could be perceived as challenging for those who feel left behind.
- For instance, it is fact that donor-advised funds have seen a significant increase in donations from holders of cryptocurrencies, who are looking for alternative ways to eliminate growing capital gains taxes and maximize the market value of their donations.[14]
- The legal framework has yet to catch up to blockchain use, particularly with respect to Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulation and enforcing compliance.
- The individual responsibility that blockchain disintermediation implies may be undesirable to some users.
- Blockchain technology requires infrastructure, such as smartphones, Internet coverage and electricity, which may be significantly lacking in poorer areas.

Despite these risks, and by anticipating the likely course of blockchain applications, IFAD has begun to intervene in both small and large ways to encourage usage and development, such as:

---

14. Fidelity Charitable 2018. 2018 Giving Report. https://www.fidelitycharitable.org/docs/giving-report-2018.pdf

- Promote internal awareness:
  - continue to follow blockchain developments and learn from past major innovation applications
  - focus on IFAD's mission, linking IFAD's values to the benefits of blockchain (such as privacy, disintermediation and efficiency)

- Promote external awareness and discussion:
  - advocate for pro-poor blockchain applications at high levels of government, business and civil society
  - encourage policy dialogue among appropriate stakeholders
  - assure governments of their institutional and regulatory capacity over blockchain applications

Each of the above steps involves minimal risk to IFAD. Of course, actual proofs of concept (PoCs) will benefit IFAD most. The areas of remittances, title and value chains offer the most promising areas in which to develop PoCs.

Remittances

Through blockchain technologies, there are opportunities to reduce remittance costs and improve access to remittances and other financial services in rural areas. Blockchain systems like RippleNet and Stellar, for instance, aggregate FSPs across borders. These networks allow FSPs to process remittances in real time and expand to markets that are expensive to reach. Stellar services FSPs that target unbanked populations, aiming to increase interoperability by enabling better and faster communication between FSPs across the globe. The connection can be between a donor, mobile wallet and online banking apps and services with the wider world of financial infrastructure, helping people to move easily between currencies, cryptocurrencies, air time (mobile phone minutes) or other store of value.[15] IFAD could explore using such network systems that improve the effect of sending and receiving money by integrating remittances and financial services. There are two possibilities for achieving this goal.

The first is using **blockchain-enabled remittance network systems** as described above. These can bypass the correspondent banking model to arrange settlement payments between pay-in and pay-out remittance service providers (RSPs) and avoid the related fees charged by banks. If designed properly, blockchain-enabled remittance systems can avoid interfering with the banks' partnerships with RSPs or have the banks unexpectedly withdraw from existing agreements, as is increasingly observed globally.

Blockchain ledgers reduce KYC costs while ensuring the traceability of operations for entitled financial supervisory authorities. As such, compliance costs currently borne by RSPs are reduced and savings can be passed on to customers. Likewise, blockchain-enabled remittance systems can also rely on cryptocurrencies, removing or limiting foreign exchange fees. This represents a significant share of the price charged by the traditional RSPs. Service providers of open public remittance services are becoming

---

15. The Economist Intelligence Unit (2019). Venture into the future of giving: the potential of emerging technologies in the giving sector.

more and more replaceable. End users will simply skip costly or unfair services if IFAD empowers them to do so.

Another remittance-related opportunity is to promote **financial inclusion-ensuring identification**. Lack of ID is one of the main barriers to accessing financial services and ensuring KYC compliance. IFAD could support using niche FSPs that use blockchain to provide cross-border services between remitters and remittance-receiving families, or humanitarian organizations, with the objective of providing lower costs and increased transparency. Blockchain-enabled programmes permit to authenticate customers who lack official IDs or bank accounts. IFAD would need to be cautious to promote state-of-the-art biometric systems implemented by project-participating RSPs. It would require open-source functionality, proven data security and formal individual ownership of biometric data ("You own your biometric data; I own mine"). Centralized biometric systems reintroduce the same dependencies and vulnerabilities that currently exist.

These opportunities come with challenges:

- **Ensuring access for a broad range of FSPs across many networks:** Cryptocurrencies are open source. Independent parties will build adapters or Application Programming Interfaces (API). IFAD could support such development or, as part of IFAD-supported projects, codes can be used or existing codes can be copied and further developed.
- **Technological illiteracy:** Ensuring access for technologically illiterate users is one of the biggest challenges. Overcoming illiteracy could start by ensuring that children in smallholder families get involved and learn to use a mobile phone. Put sufficient maintenance services in place to ensure that the smartphone will be used rather than sold off.

Land title registry

Land title registries suffer from numerous problems including incomplete, erroneous or missing documentation; incorrect or conflicting entries; ownership provenance; corruption in oversight; and paper's vulnerability to damage or destruction. Additionally, changing ownership can be cumbersome due to legal inconsistencies, incomplete and insecure data, unnecessary third parties and fraud.

A blockchain-based land registry would address many of these issues. Documentation would be both immutable and transparent thanks to encrypted records. Corruption would become more difficult, as cryptographic keys would be necessary to change ownership of a land title. Vulnerability of smallholder landowners would be mitigated by the data safety property of blockchain. Third-party title middlemen would become unnecessary.

Blockchain can support the disintermediation and transparency of these ownership processes, as well as offering the option of Collective Fractional Ownership. IFAD should not only support the development and usage of blockchain in establishing titles, it should also encourage the legal sector to recognize and accept this technology.

Agricultural value chain

DLT offers several options for improving the efficiency of agricultural value chains.

Smart contracts allow users to digitally facilitate, verify or enforce the performance of a contract without third parties. They are appropriate in areas where problems arise from failure to meet the right and timely execution of contracts. Smart contracts are automatically triggered when the conditions for execution are met. For example, smallholder payment could be tied to product delivery, and the transparent information on contract fulfilment could serve as a virtual credit history for future financing. However, it should be noted that the current state of this technology is still rather experimental. As the technology is further developed, IFAD could support initiatives that ensure that smallholders are in a position to benefit from it.

Blockchain could be used for **collateralization** to track and secure products and to transfer ownership as products move through the value chain. Because commodities can be tokenized, they can be tracked, and their condition (owner, amount, quality, issues) can be recorded at each stage of the process. In this way, product delivery and product quality (organic, fair trade) can be certified, and weak points in the chain could be identified. Similarly, real-time monitoring could be used in IFAD-supported projects. The transparency of blockchain networks can be used to monitor and share information about project activity or actors, which can help ensure that project goals are being met.

Identity services using blockchain are probably the most extensive field to explore. Identity touches the core design principles of open public blockchains, such as freedom, self-sovereignty, privacy, inclusion, store of value and transfer of money, as well as basic principles of society, such as citizenship, human rights, safety, security, taxation and law. Identity services have implications for citizenship, complying with AML, KYC, CFT, anti-child trafficking and women's rights, among others. It is a wide field. For agriculture in particular, identity services could be used to establish credit, open accounts and transact payments while meeting AML/KYC requirements.

Unique **financial products and services** can be developed using blockchain: microfinance delivery, colored coins, cashless transfers and insurance risk-sharing. Owning blockchain-based digital money and making transactions with this money can enable smallholders to participate in more markets and receive money from overseas. Colored coins can be used to restrict the spending to certain products or services: if financial institutions can ensure that funds are used for appropriate agri-inputs (e.g. feed, fertilizer) and that loans are automatically repaid as part of product sale, they may be more willing to make financing available to smallholders.
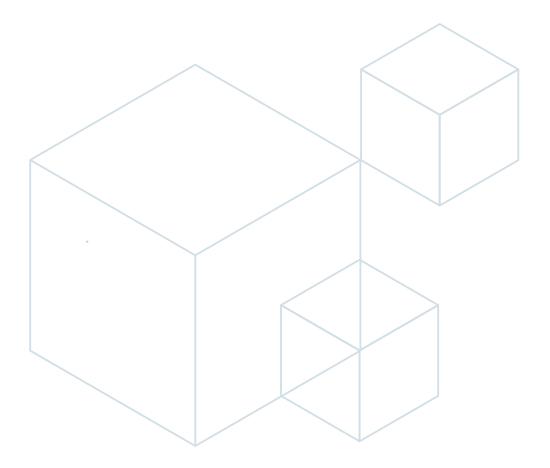
CONCLUSIONS

IFAD should continue to explore and support the opportunities offered by blockchain technologies that could benefit smallholder farmers. The study on blockchain commissioned by IFAD suggests that open public blockchain solutions represent the greatest potential for change and that they are the best path forward for IFAD. However, the study also acknowledged that private or hybrid blockchain solutions can also benefit the organization, and they may be preferred by potential partners. Each shows great potential for improved efficiency and data security. Among the findings of this study are the following:

- Blockchain technology can support the strategic objectives of IFAD. Because IFAD staff are already engaged in exploring realistic applications of DLT, IFAD has the potential to move relatively quickly to adopt blockchain into its work.

- In the field of open public blockchains, IFAD has the opportunity to make its mark, entering an arena that, so far, has not been utilized by other agencies.

- Risks and challenges in blockchain applications can be mediated through careful design and implementation.

- Blockchain implementation within established financial structures can be costly. However, the benefits could be greater when applied in areas with little or no financial infrastructure.

- IFAD does not need – and possibly does not have the capacity – to compete with other agencies by following their approaches to DLT implementation. Instead, IFAD can develop its own unique approach and, in doing so, enhance its standing in its field.

- Internally, IFAD can develop the institutional expertise to assess, apply and secure the privacy of blockchain innovations.

- The three main areas of blockchain application that seem most promising for IFAD's support for agricultural smallholders are remittances, land title registries and the agricultural supply chain. Each offers opportunities to enhance smallholders' independence, production and security – representing promising areas for PoCs.

- Risks for smallholders in implementing blockchain applications include: a lack of Internet connectivity, smartphone costs, theft or loss of keys used for encryption and access to wallets, and negative social pressures (e.g. women's status in some communities).

- Just as computer skills have become common without an understanding of the technology behind computing operations, use of many services that depend on the "behind the scenes" blockchain technology will become widely established.

- IFAD can build its blockchain knowledge and competency through a number of actions, including regular staff study groups and workshops, focused external training and empowerment of staff to identify opportunities for blockchain implementation.
- A comprehensive regulatory framework for blockchain application does not yet exist, but IFAD can begin engaging with blockchain innovation mindful of local and current rules.

RECOMMENDATIONS

Going forward, the study makes the following recommendations for IFAD:

- Ensure the blockchain applications it implements:
  - have practical applications
  - are low risk
  - are in line with IFAD objectives
  - provide a competitive edge
  - are future-proof
  - have fundraising capabilities by using cryptocurrency-based philanthropic projects
  - are invented by or supported by IFAD colleagues.

- Keep an open mind with regard to the design principles of blockchains, their applications and the issue of open public versus private blockchains so that the Fund can benefit from innovation and be able to satisfy the preconditions necessary for successful implementation.

- Consider how best to support practical infrastructure in rural areas of developing countries so that blockchain developments are given a head start (e.g. smartphone usage, charging and Internet connectivity).

- Proceed despite the lack of regulatory frameworks or perfect blockchain applications. By implementing these technologies now, IFAD will contribute to development in this field, increase its own knowledge and capacity, and enhance its reputation.

- Consider how it can contribute to the development of blockchain applications in third-party blockchain platforms.

- Avoid:
  - exiting the path of prudent investment management for risky returns of investment in cryptocurrencies without knowing the exact context or sufficient competence and knowledge within the organization
  - doing routine, day-to-day business with complex technology still in its infancy
  - committing to centralized parties or suppliers through contracts.

- Focus on three main areas in developing and implementing blockchain applications with agricultural smallholders:
  - remittances
  - land title and registry
  - supply chain and traceability.

- Invest in a programme of blockchain capacity-building among staff, setting up study groups, workshops and learning events. IFAD should also establish a core group of staff focused on supply chains and traceability, remittances and land title registry.
- Consider articulating an opinion on the IBM Food Trust platform for public-private partnership arrangement for the benefit of smallholder-inclusive value chain development in a few programme countries. There are over 40 clients in the system today, with Walmart and Carrefour as two of the trust anchors.
- Build blockchain competency through staff training and empower all staff to identify, select and make choices about blockchain implementation and technology.
- Coordinate efforts in both open public blockchains and private blockchains through two teams that will, together, contribute to the understanding of the design principles – creating an opportunity to become a well-respected knowledge leader and stimulate real innovation.

APPENDIX 1 - GLOSSARY

A **tokenized asset** is a representation of a digital asset. It typically does not have intrinsic value, but it is linked to an underlying asset that could be anything of value.

Distributed ledger technology refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared and synchronized across a distributed network of different network participants.

A **blockchain** is a particular type of data structure used in some distributed ledgers. Blockchain stores and transmits data in packages called "blocks" that are connected to each other in a digital "chain". Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.

Distributed ledgers (DLs) are a specific implementation of the broader category of **shared ledgers**, which are simply defined as a shared record of data across different parties.

DLs are categorized as **permissioned (private)** or **unpermissioned (public)**, depending on whether network participants (nodes) need permission from any entity to make changes to the ledger.

Distributed ledgers are categorized as **public** or **private** depending on whether the ledgers can be accessed by anyone or only by the participating nodes in the network.

A **shared ledger** can be a single ledger with layered permissions or a distributed ledger, which consists of multiple ledgers maintained by a distributed network of nodes, as defined above.

Digital currencies are digital representations of value that are denominated in their own unit of account, distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money.
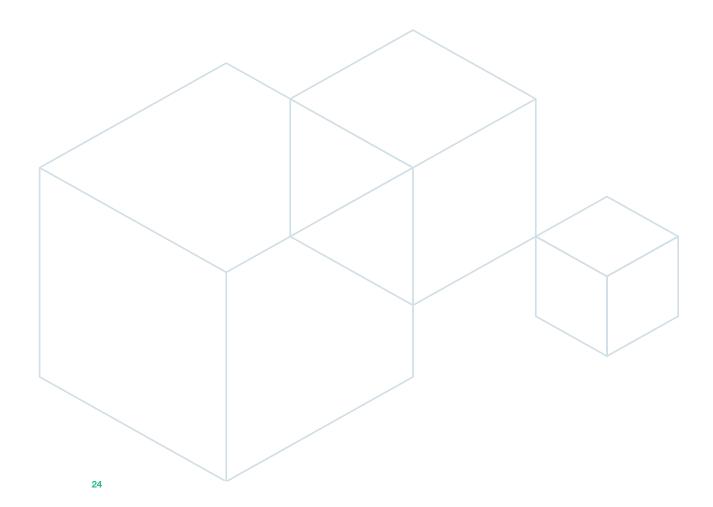
Cryptocurrencies are a subset of digital currencies that rely on cryptographic techniques to achieve consensus, for example bitcoin and ether. The bitcoin blockchain is an example of a public, "unpermissioned" ledger, in which anyone can view data on the ledger, write new transactions, and participate in building consensus around the validity of a given transaction.

Colored coin is a method used to represent and manage real-world assets with the bitcoin blockchain. Bitcoin's scripting language allows the encoding of some information into the blockchain along with performing transactions. Colored coins are bitcoins transferred within a transaction that has additional info. The information added to a colored coin may represent such assets as stocks, promises, transaction info, etc.

Those are real-world assets that are – once included in the blockchain – immutable, easy to transfer, transparent and secure. For example, a restaurant can issue a promise to offer a free dinner to token holders by making a bitcoin transaction that has additional information about the terms of such an offer. Companies may issue colored coins with blockchains of many platforms. Colored coins can also be used with smart contracts, making a coin available for use only if specified terms are fulfilled. https://cointelegraph.com/tags/colored-coins

Nodes are network participants in a distributed ledger network.

Public key cryptography is an asymmetric encryption scheme that uses two sets of keys: a public key that is widely disseminated and a private key that is only known to the owner. Public key cryptography can be used to create digital signatures and is used in a wide array of applications, such as HTTPS Internet protocol, for authentication in critical applications and also in chip-based payment cards.

Contacts:

Michael Hamp (PhD)
Lead Regional Technical Specialist
Rural Finance, Markets and Enterprises
Asia and the Pacific Region
Sustainable Production, Markets and Institutions Division
m.hamp@ifad.org

Maria-Elena Mangiafico
Knowledge Management Specialist
Environment, Climate, Gender and Social Inclusion Division
Strategy and Knowledge Department
m.mangiafico@ifad.org