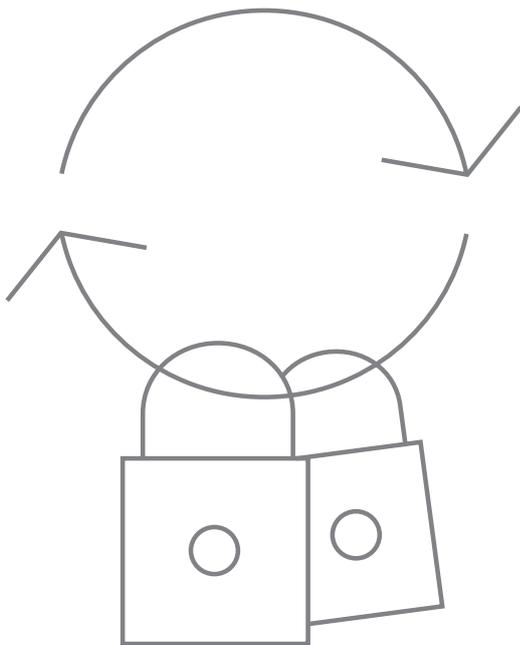


Blockchain for Humanitarian Aid Decision Tree

This decision tree acts as a guide to explore the potential and limitations of using blockchain for humanitarian aid.



Brought to you by



HumanityX



Feel free to contact us. Kate Dodgson, Innovation Fellow, HumanityX, k.dodgson@humanityx.nl

How to use it?

To start this decision tree, you should define a functionality of humanitarian aid which could be improved. For example, “Cash-based transfers from an NGO in Australia to beneficiaries in Vanuatu.”

The decision tree will then help you to explore whether and how blockchain could support your operations.

Which steps to take?

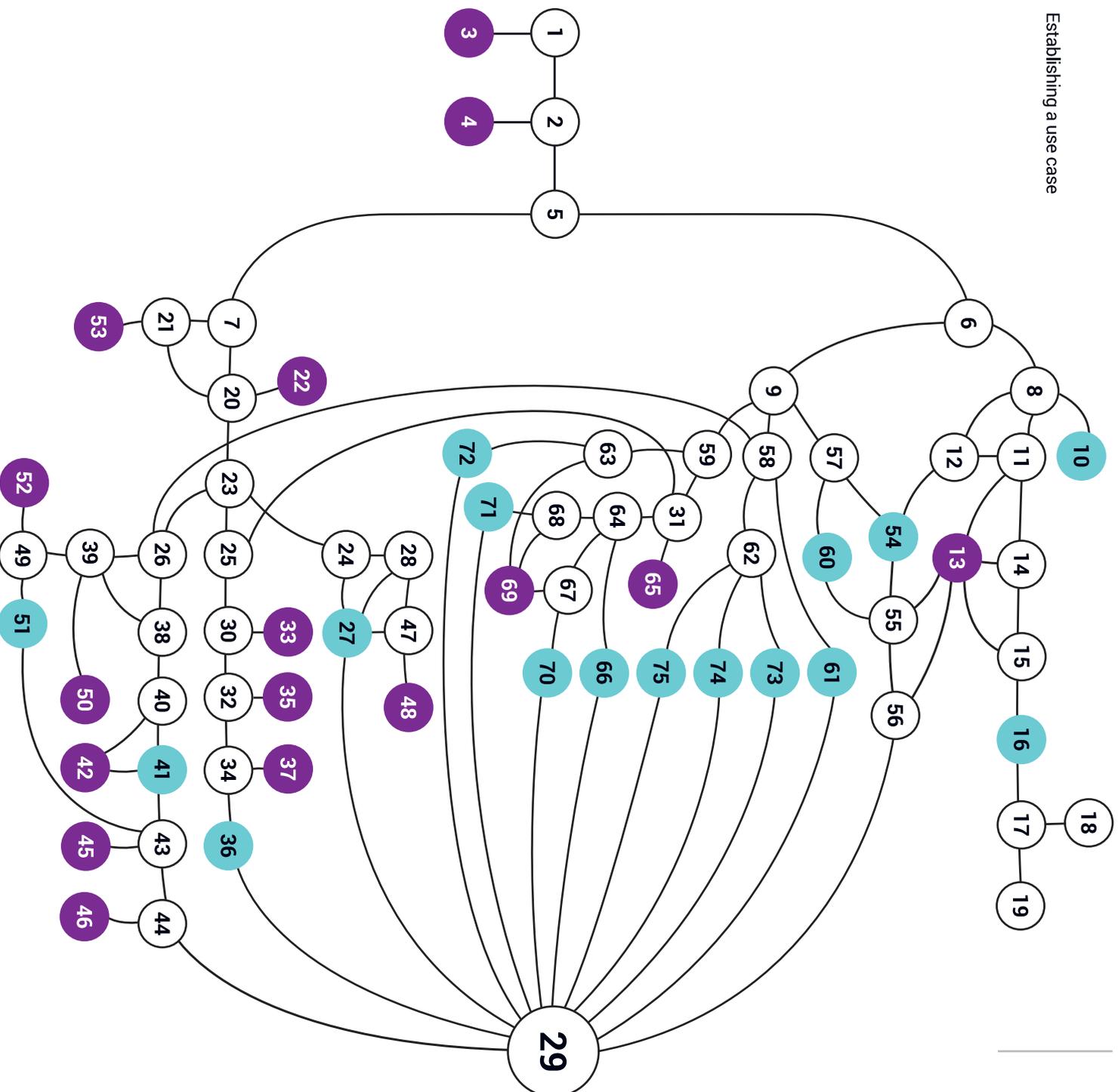
The decision tree will guide you along several paths to assess the relevance of blockchain on the basis of potential and existing use cases. Some paths along this decision tree will be very short and will take only a few minutes. Others will be longer and more complex and may take up to 20 minutes.

Let's explore!

We hope that this decision tree helps users understand the complexities of both blockchain and the humanitarian context it could potentially apply to. Feel free to retrace your steps and explore different paths.

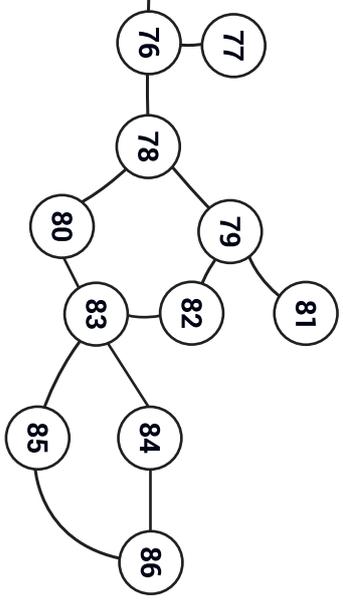
Happy navigating!

Establishing a use case



Blockchain Specifications

- No blockchain dead-ends
- Potential blockchain opportunities



1

Do you need a database?

Yes – 2 page 1

No – 3 page 1

2

Will this database be storing personal identifying information?

Personal identifying information (PII) is any information that can be used to identify, contact, or locate an individual, either stand-alone by itself or in combination with other easily accessible sources.

Yes – 4 page 1

No – 5 page 1

3

You do not need blockchain.

Blockchain is, fundamentally, a ledger. If you do not need a ledger (database) then you do not need a blockchain.

4

Do not use blockchain.

It is currently not recommended to store personal identifying information in a blockchain. Consider an encrypted database instead.

5

For what kind of records/data?

Financial – 6 page 2

Non-Financial – 7 page 2

6

For what kind of currency?

Cryptocurrency (Bitcoin and Alcoins) – 8 page 2

Cryptocurrency is a digital asset which acts as a means of value exchange. It is based on cryptography and is entirely represented online – i.e. it does not exist as a physical item. All value is transferred online through the blockchain and as such, cryptocurrency is described as ‘on-chain’.

Fiat (\$ £ €) – 9 page 3

Fiat currency (pound, euro, dollar etc) exists off-chain ie. physically in cash and digitally in bank accounts. Blockchain technology can be used to record where this money is, but it cannot actually move the money itself – this still needs to be done off-chain.

7

Is your data currently in digital form?

Yes – 20 page 6

No – 21 page 7

8

What is your main motivation for considering cryptocurrency?

(You can explore all options)

Alternative source of donations – 10 page 3

To bypass local depreciating/unreliable currencies and markets – 11 page 4

For example, World Vision International have considered using a cryptocurrency in South Sudan. By the time they have transferred and converted US dollars to the South Sudanese Pound (which is very volatile), they have lost a lot of value. A stable cryptocurrency could potentially overcome this.

More transparency for financial transactions – 12 page 4

No/poor/expensive traditional financial infrastructure where we are operating – 12 page 4

9

What is your main motivation for considering blockchain?

(You can explore all options)

Access – 57 page 17

Transparency – 58 page 17

Integrity of data/records – 59 page 17

10

EXAMPLE USE CASE

It is possible for charities/NGOs to accept donations in cryptocurrencies.

Despite strict regulations on charity financing and operations, a number of charities accept donations of some of the major cryptocurrencies. These charities tend to be newer charities, and often have a technology, medical or innovation focus. Some include the Electronic Frontier Foundation, Multidisciplinary Association for Psychedelic Studies, Wikileaks, Code to Inspire, Internet Archive and Watsi. The cryptocurrencies accepted include Bitcoin (BTC), Ethereum (ETH) and Litecoin (LTC).

While still a new method of fundraising and donations, accepting cryptocurrencies can be quite fruitful – particularly for small charities. “Pine” is a pseudo-anonymous crypto-philanthropist that sought to give away the vast majority of his Bitcoin wealth (\$86 million at time of pledge). Small charities such as Watsi were overwhelmed with the unprecedented and generous donation of \$1 million in BTC.

Larger charities will struggle to accept cryptocurrencies such as Bitcoin as they must first overcome large amounts of internal red tape and bureaucracy. UNICEF, for example, are interested in accepting cryptocurrency donations, however, are struggling to get it approved by their finance and legal teams.

There are also issues of Know Your Customer (KYC) and Anti-Money Laundering (AML) as it is very difficult to check the source of cryptocurrency and whether or not it has come from undesirable donors.

Check with your legal and finance teams to determine whether or not your organisation can satisfy KYC and AML, and if so, whether it wants to accept cryptocurrency donations. If so, it is very easy to set up a cryptocurrency wallet which is a place where you can store cryptocurrencies. It is likely that you will eventually want to exchange the cryptocurrency for fiat money, and when you do so you will need to use a cryptocurrency exchange.

End of decision tree

11

Will using crypto cause problems with the government of the country you are operating in?

Some governments have determined that cryptocurrencies are not legal in their jurisdiction. Even governments which have not made such a declaration may not appreciate their sovereignty being challenged through bypassing the local official currency. Upsetting the local government may result in you being barred from operating there and/or strain crucial relationships with the government.

Yes – 13 page 4

No – 14 page 4

12

Could this be done by tokenising fiat rather than using a crypto?

Tokenising fiat is the process of representing normal currency on the blockchain. Normal currency (pound, euro, dollar, etc) exists off-chain ie. physically in the real world and digitally in bank accounts. Blockchain technology can be used to record where this money is, but it cannot actually move the money itself – this still needs to be done off-chain. If wanting to transparently record the movements of money, fiat can be turned into a 'token' (representative) on the blockchain and its movements monitored through the blockchain.

Yes – 54 page 16

No – 11 page 4

13

Do not use blockchain.

14

Do the beneficiaries/end-users have access to phones/internet?

Beneficiaries and end-users of blockchain applications can vary greatly and it's important to consider who will actually be using the blockchain application. For example, in the World Food Program's Building Block's project, the beneficiaries are the refugees who use the cash-cards, however, the end-user of the blockchain application is the store who processes the payments. Therefore, in this scenario, it is the end-user (the stores) that require access to smart phones/internet and not the beneficiaries.

Blockchain runs online therefore it is crucial that there is stable internet access and sufficient bandwidth. While some transactions can occur offline (and processed later once an internet connection is established), it greatly reduces the speed and overall efficiency of using blockchain.

Yes – 15 page 5

No – 13 page 4

15

Will the beneficiary/end user be able to use the cryptocurrency either through trading or by exchanging into fiat?

In order for the cryptocurrency to have value, it must be usable. This can occur if the whole community accepts the cryptocurrency and can therefore use it to exchange goods and services amongst one another. If this is not the case, then there must be the ability to exchange the cryptocurrency into a local currency that can be used as a means of exchange.

Yes – 16 page 5

No – 13 page 4

16

POTENTIAL APPLICATION

Cryptocurrency can potentially be used for disbursing financial aid.

Continue – 17 page 5

17

Is stability of the currency a priority for you?

Yes – 18 page 5

No – 19 page 6

18

You can either use an already established fiat-pegged crypto, or you can create your own cryptocurrency.

A fiat-pegged cryptocurrency is a cryptocurrency which is attached (pegged) to a bank-issued currency such as USD. For example, Tether pegs its token (USDT) to USD. 1 USTD = 1 USD.

There are numerous problems facing fiat-pegged cryptocurrencies, for example, financial regulations and the lack of adoption. As such, it is currently not recommended for humanitarians to invest in or use a fiat-pegged currency.

The alternative option is to create your own cryptocurrency. Read here for a hypothetical example of what this could look like. Note that in the current state of the humanitarian sector and cryptocurrencies, it is highly unlikely to be successful. Blockchain technology needs to mature, cryptocurrencies need to become more mainstream, and the humanitarian sector needs a safer and easier introduction to blockchain technology.

End of decision tree

You can potentially use an already established cryptocurrency such as BTC, ETH or XLM.

Cryptocurrencies are currently unpredictable and unstable. Their value can rise and plummet within hours and it is impossible to predict their future value. As such, it is very unlikely that a humanitarian organisations would dare risk losing money by utilising an already established and un-pegged cryptocurrency (un-pegged means the cryptocurrency is not attached/pegged to a fiat currency). Nevertheless, smaller more experimental social impact organisations may embrace the opportunity to quickly and effortlessly increase their funds (for example when their chosen cryptocurrency increases in value).

In the future, cryptocurrencies may also stabilise making their use more realistic for humanitarian organisations.

In either of these circumstances, organisations can consider two different types of cryptocurrencies: large and widely used cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH) and Stellar Lumens (XLM), or smaller sector-specific cryptocurrencies such as GiftCoin.

Big cryptocurrencies such as Bitcoin have the advantage of being widely-used and more widely accepted. They are therefore easier to trade and exchange. Smaller cryptocurrencies such as GiftCoin have supposedly been tailored to suit charities and non-profit causes, however, minimal adoption of them means they have minimal function and use.

Humanitarians are advised to research cryptocurrencies by reading Cryptocurrency Whitepapers (i.e. documents explaining/pitching the cryptocurrency), assessing the ICO (i.e. Initial Coin Offering - this is the process of 'selling' the cryptocurrency in order to launch it) and undertaking general due diligence.

End of decision tree

Does this data include large amounts of non-transactional data?

In the current state of blockchain's maturity, it is not advisable to store large amounts of non-transactional data on-chain, particularly personal identifying data or sensitive data. Blockchain can be used to represent transactions of data, however, the underlying data itself may be best stored elsewhere ie. off-chain. For example, say a blockchain is being used to record land title registrations. A blockchain record may describe that Sally has sold X house to Bill on 8 April. Extra documentation that could be included in this transaction could be copies of the certificates, drawings of the house, legal documents etc. While it is possible to include this extra documentation, blockchain technology is not yet primed to store large amounts of this extra material and currently is advised to be stored off-chain. At this point in time, a blockchain application would function best if it only included transactional records.

Yes - 22 page 7

No - 23 page 8

Can it be digitised? Ask yourself these questions when trying to determine whether your physical item can be digitised:

If your data is simply in hard copy (paper receipts, physical logbooks), then it can easily be digitised by entering this information into digital form. Problems arise, however, when your data represents physical items which do not yet have a digital record. For example, if you want to record the movements of a tuna fish from ocean to fork, how can you attach a digital record to the fish?

Questions to consider when determining whether or not your physical item can be recorded in a digital manner:

- What size and shape is the physical material being tracked?
- What technologies are available to connect the physical material to its digital signature equivalent?
- What physical and chemical transformation is applied to the materials tracked?
- Is the technology connecting the physical material to the blockchain tamper proof? (source)

Current technologies used to digitally represent physical products include: Radio frequency identification (RFID), 2D barcode, near field communication (NFC), smart tags and QR codes.

Provenance, a blockchain software company based in London, uses blockchain to trace tuna from hook to fork. When tuna is caught, it is tagged with a QR code or RFID or other hardware technology. But soon enough, the tuna is turned into other products ie. when it gets broken up and put into cans. They plan to implement the concept of 'process as a contract' on the blockchain to handle this part.

"Tally-O [already established traceability software which Provenance interoperates with] uses mass balancing to account for the amounts of ingredients used in the transformation. For example, the calculation for a can of Fair Trade skipjack tuna might be 200 g of certified skipjack tuna and 10 ml of olive oil. The details of this calculation will be sent to the process contract once the transformation has taken place, and the identifier then encoded in a label that will be passed with the transformed product down the chain." (source)

It's important to note that if the state of your product changes, for example, wheat turning into bread, you will need to rely on every transformation being recorded accurately by each party into the blockchain record. Blockchain only represents the digital truth – that is, what the writing party tells the blockchain it is representing. It is therefore crucial that each party involved in product transformation and blockchain recording has incentive to record accurately and truthfully.

Yes – 20 page 6

No – 53 page 15

23

What is your main motivation for considering blockchain?

(You can explore all options)

Transparency – 24 page 8
for supply chain: provenance and asset tracking

Integrity of data/records – 25 page 8

Collaboration/sharing data – 26 page 9

24

Is there incentive for all actors along the supply chain to use a blockchain application?

To enable full traceability of products along the supply chain, all actors who move the product must be incentivised to record the product and its movements on a blockchain application.

Currently, different actors use different methods to record product movement - from paper records and receipts to siloed database management systems. A blockchain platform would aim to have all parties use the same system so that a product's entire journey can be tracked.

However, there needs to be incentives for the actors to move away from their current systems and onto a blockchain platform. For example, Walmart and IBM are working to track pork supply chain in China. In this pilot, Walmart has buying power and can presumably use that to require its suppliers to use blockchain.

Smaller companies/organisations without this kind of influence may struggle. IBM's blockchain team have suggested that in some supply chains, various actors may have to be subsidised in order to encourage the move to blockchain.

Yes – 27 page 9

No – 28 page 10

25

Why do you want to improve the integrity of your data/records?

For reconciliation and auditing – 30 page 10

For tamper-proof records – 31 page 10

26

Are the other parties trusted?

Trust in this sense means that you would be happy for these other parties to modify a database that you “own”.

Yes – 38 page 12

No – 39 page 12

27

POTENTIAL APPLICATION

Supply chain is one of the strongest use cases for blockchain technology.

Supply chain is often described as the strongest use case of blockchain beyond cryptocurrencies. This is because many of the benefits of blockchain – transparency and decentralisation in particular – help with endemic problems faced by current supply chains.

Due to the complexity of modern supply chains, tracking products end-to-end is near-impossible. This consequently means consumers do not know the provenance of their product, nor its authenticity.

IBM is currently leading the pack in developing blockchain applications for supply chain. They have already piloted several projects including with MAERSK and Walmart.

While blockchain is looking promising for commercial supply chains, humanitarian supply chains operate under very different circumstances and pressures. Characteristics of humanitarian supply chains include: unpredictable demand, difficulty obtaining data from operations, unpredictable working environment, short-lead time, variables such as geography, political situation, weather, and of course the non-profit nature of the operation.

Can blockchain overcome these hurdles? Better still, can it help remove them? Unfortunately very little work has been done to test this. As blockchain is still new and expensive, most progress will be in the private sector. The humanitarian sector may be years away from exploring it.

However, the UK Department for International Development are currently exploring this potential, and hopefully others will too.

In the meantime, humanitarians may be more interested in blockchain for commercial supply chain in which they may be involved in (procurement, ethical sourcing etc).

Go to Blockchain Specifications – 29 page 10

28

Could smart-devices automatically record product movements and transactions?

For example, if you were tracking water supply chain (ie. monitoring water distribution from a water aid truck operating in Ethiopia) could a smart meter record water levels which could be automatically uploaded and recorded on the blockchain? Using the Internet of Things in this manner could potentially by-pass the requirement to incentivise actors to input data as it would all be automated. This obviously requires advanced smart-devices and good internet connection.

Yes - 27 page 9

No - 47 page 14

29

Blockchain Specifications

Welcome to the second part of the Blockchain decision tree.

Continue - 76 page 22

30

Do you face any of these challenges with your current system?

Too costly; slow; risky/harmful to allow a third party (intermediary) to access data (such as sensitive data).

Yes - 32 page 11

No - 33 page 11

31

Do you want your records to be permanent?

Yes - 64 page 19

No - 65 page 19

32

Are you trying to remove an intermediary?

Yes – 34 page 11

No – 35 page 11

33

Re-think blockchain.

A centralised database and/or using an intermediary will likely be cheaper and more efficient.

34

Can these intermediaries legally be removed? For example, certain regulatory bodies cannot be replaced or removed.

Whether or not an intermediary can be removed/skipped is entirely dependent on the context and situation. It's best to consult your legal and finance teams to see whether the particular intermediary can be by-passed or whether they are required to be used by law/regulations.

Yes – 36 page 12

No – 37 page 12

35

You do not need blockchain.

If you are simply trying to find a cheaper, faster, alternative to your current system then blockchain is unlikely the solution for you (yet). Blockchain is still maturing and set-up and maintenance costs are expensive, so are only worthwhile pursuing if utilising several of blockchain's features (such as disintermediation + efficiency and speed).

36

POTENTIAL APPLICATION

Blockchain enables peer-to-peer transactions which can remove the need for intermediaries. This could be beneficial in circumstances where you are currently forced to share sensitive data with a third party in order to process a transaction.

Go to Blockchain Specifications – 29 page 10

37

Do not use blockchain.

38

Do all parties have unified interests?

Yes – 40 page 12

No – 39 page 12

39

Do any of these other parties need write permission (Do you want them to be able to add data?)

Yes – 49 page 15

No – 50 page 15

40

Do you nevertheless have valid concerns about external risks such as hacking, corruption, fraud, duplication?

Yes – 41 page 13

No – 42 page 13

41

POTENTIAL APPLICATION

The decentralised and distributed nature of blockchain gives it stronger security than a centralised database. For example, beneficiary registration

Blockchain-based databases offer better security than centralised databases. This is because centralised databases present one point of attack whereas blockchain ledgers are distributed and far more difficult to hack or manipulate. For organisations that wish to share information with one another, but in a more secure way than using a shared-access centralised database, blockchain may be an option.

Oxfam GB considered this in a workshop looking at blockchain for beneficiary registration. The conclusion was that while it is feasible and would reduce duplication of records, labour and expenses, work needs to be done to convince NGOs to share data. If only one NGO is unsure of the system – or is under legal or policy restrictions regarding sharing data – then the whole system’s effectiveness would be greatly reduced if not destroyed.

Therefore, if considering using blockchain as a shared database, organisations must be certain that there is incentive and cooperation amongst all participants.

Continue – 43 page 13

42

You do not need blockchain.

If you trust the other parties and do not fear security/fraud then you should consider a centralised database instead. It will be more efficient and cheaper to set up.

43

Do you have a data responsibility policy that will cover sharing data and/or issues like the right to be forgotten?

Yes – 44 page 13

No – 45 page 14

44

If you are collaborating with external parties, do all of them have data responsibility and sharing policies which are compatible with yours and each others?

Yes – 29 page 10

No – 46 page 14

45

Do not use blockchain until you have a suitable policy.

It is inadvisable to use blockchain unless and until you have a suitable data policy at your organisation. This policy will need guidelines regarding the storing, sharing and deletion of information. It will further need to consider regulations such as the General Data Protection Regulations and other possibly relevant provisions such as the 'right to be forgotten'. It may be that your organisation's most suitable policy is incompatible with sharing information with external organisations and/or needs the capacity to delete information. If this is the case, blockchain is not a suitable technology to pursue.

46

Do not use blockchain until all collaborating parties have suitable policies.

47

Could you separate parts of the supply chain which would be worthwhile tracking in isolation from the rest?

It may be that end-to-end tracking is not possible, but parts of the journey can be tracked. For example, could you track certain parts of the journey such as when a mineral leaves a mine (ie. Tungsten) until it reaches a smelting factory where it is turned into other products? Using blockchain for tracking supply chain end-to-end is an enormous undertaking and it may be that it happens slowly and incrementally.

Or could other parts of humanitarian logistics benefit from blockchain? Such as for procurement, inventory pre-positioning, transportation, distribution centres?

Yes – 27 page 9

No – 48 page 14

48

Blockchain will not benefit your supply chain management/logistics.

If you can't get supply chain actors on board, there is no point having a blockchain system. Blockchain technology is still in early trials in supply chains. It is likely that to get to scale, big companies need to use their influence to encourage parties along the chain to adopt blockchain. The less parties along the chain that adopt blockchain, the less useful the application and the less transparent the journey. It may even destroy the story of the journey and render the process ineffective.

49

Is there a legitimate reason one of the parties cannot be in charge/control of this database?

Yes – 51 page 15

No – 52 page 15

50

You do not need blockchain.

If you just want to give the other parties read-access then you can use a master/slave database.

51

POTENTIAL APPLICATION

Blockchain allows non-trusting parties to interact and transact with one another without any one person/organisation being in charge.

Continue – 43 page 13

52

Re-think blockchain.

A centralised database such as a managed database may be best suited for this scenario. For example, Helios – the software that Oxfam uses for their supply chain – has an information sharing function whereby participating organisations can see one another’s shipments and orders. However, the sharing can only occur with other users of Helios.

53

You cannot use blockchain.

Your data needs to be digitised in order to be represented on blockchain.

EXAMPLE USE CASE

Tokenising fiat enables you to transparently record transactions on the blockchain while avoiding the volatility and regulations of a cryptocurrency. See for example, Sikka.me

Sikka is a blockchain project funded by and built in-house at World Vision Nepal. Using the Ethereum blockchain, Sikka creates tokens on the blockchain which represent Nepalese Rupees. Sikka tokens are pegged (attached) to the Nepalese Rupee at a conversion of 1:1.

The purpose of Sikka is to provide a means of asset transfer (value exchange) for people who cannot access banks and/or other financial infrastructure. This could be following a disaster, or for those who lack official identity and a bank account.

Sikka tokens can be texted to such people who can then either exchange the tokens for Rupees at local shops, or use the Sikka tokens to trade in goods and services. Transactions only require an SMS (on a feature phone), and are tracked on the blockchain.

Sikka does not use cryptocurrency and therefore is not restrained by crypto regulations and laws. Tokens are all pegged to fiat currency. Read here for more information about Sikka: [Sikka Whitepaper](#).

Continue – 55 page 16

55

Do beneficiaries/end-users have the hardware and connectivity to operate this application?

You need to assess what kind of hardware and connectivity the beneficiaries have and whether or not it is sufficient enough to operate on (or connect to) a blockchain.

For example, in the case of Sikka, a feature phone with SMS capacity is all that is needed for beneficiaries to access Sikka tokens. Sikka's research found that only 30% of the population have access to a smartphone, however, nearly 100% have a mobile phone subscription (even taking into account those who have two subscriptions). Therefore it was assessed that the only feasible way for this project to work is if it could be used on a basic phone through SMS rather than a smartphone requiring Internet.

Yes – 56 page 17

No – 13 page 4

56

Do beneficiaries/end-users have the knowledge to operate wallets and public/private keys?

In order to store and trade tokens such as Sikka, a beneficiary would need access to a digital wallet (somewhere to store the tokens). Further, in order to access this wallet, the beneficiary needs a public and private key which act effectively as passwords/pins to access the wallet. While these concepts involve complex cryptography, the beneficiary need not understand the technology behind it. They just need to understand how to operate the wallet, and how to keep their keys (access pin) safe. Organisations must be satisfied that users understand that losing their private key (pin number) will likely result in them losing access to their funds.

Sikka have simplified this process by storing wallets on their servers and associating them with beneficiaries' SIM cards. This means that if a beneficiary's phone doesn't work or they lose their phone, there is still a record of how much money they have and can spend/redeem. Wallets can only be accessed at approved network vendors or financial cooperatives. Read more at Sikka.

Yes - 29 page 10

No - 13 page 4

57

What is your problem with access?

Remoteness – there is no/insufficient traditional financial infrastructure where we are operating - 54 page 16

Disintermediation – we want money to be able to go peer-to-peer - 60 page 18

58

Why do you want to add transparency?

To monitor impact/results of the NGO/charity - 61 page 18

To monitor money flow and transactions - 62 page 18

To enable/improve collaboration between multiple people/funds - 26 page 9

59

Why do you want to improve the integrity of your data/records?

For tamper-proof records - 31 page 10

For reconciliation/auditing/monitoring and evaluation purposes - 63 page 19

60

POTENTIAL APPLICATION

Blockchain enables peer-to-peer transactions. This provides a more direct way for donors and NGOs to access beneficiaries and end-users.

Note that in order to transfer donations peer-to-peer, you will need to have a system whereby legitimate beneficiaries are identified. The role of beneficiary identifier is likely to be an intermediary which could be a local NGO or perhaps even another branch of your organisation. While blockchain won't assist you to 'skip' this intermediary, you can avoid using them to transfer money. For example, if Charity UK wanted to transfer tokenised funds to victims of the Nepal earthquake, rather than transferring Charity Nepal the money and accruing international banking fees, they could use Charity Nepal to identify the beneficiaries and then use blockchain to transfer the beneficiaries tokenised money directly - bypassing Charity Nepal's bank accounts. Charity Nepal nevertheless may need funding from Charity UK to support this work, however, this can occur through a separate payment.

AidTech are currently working on a blockchain peer-to-peer donations platform.

Continue – 55 page 16

61

EXAMPLE USE CASE

Smart contracts can be used to release money upon charitable/impact milestones being reached. See Alice.si

Transparency in social impact funding can be improved by using blockchain technology. Alice.si, are the most advanced platform doing this. On Alice's platform, charities declare their projects and goals and set milestones for achieving them. Money donated to the project is only released incrementally, upon completion of each milestone. Once a milestone has been achieved, a smart contract (contractual requirements put into code which self-execute upon completion of requirements) will release the funds to the charity. All of this can be monitored on Alice's dashboard. If a milestone is not achieved, donated money automatically reverts back to the donor. See Alice.si for more information.

Go to Blockchain Specifications – 29 page 10

62

Why?

Delays – current transactions are too slow – 73 page 21

Missing money – Unidentifiable or unattributable fees – 74 page 22

Too many conversions and fees – 75 page 22

63

Do you face any of these challenges?

Costly, inefficient, risk/harmful by allowing a third party to access data.

Yes – 72 page 21

No – 69 page 20

64

Have your data been or are you at risk of being...

hacked – 66 page 19

fraudulently altered/manipulated – 67 page 19

corrupted/lost destroyed – 68 page 20

65

You should not use blockchain.

Blockchain records are permanent and cannot be deleted – only appended to (note that they are not completely infallible, but it is very difficult to alter them). If you need the ability to delete data, for example, under the GDPR's right to be forgotten, then you should not use blockchain.

66

EXAMPLE USE CASE

The Estonian E-government system now partially runs on blockchain technology. They moved to blockchain after they were hacked in 2007 and wanted a more robust and secure platform.

Go to Blockchain Specifications – 29 page 10

67

Could you use an existing technology that shows track changes and therefore identifies alterations?

Yes – 69 page 20

No – 70 page 20

68

Can you store this data in more than one place so that if one version is corrupted or destroyed, the others will be ok?

Yes - 69 page 20

No - 71 page 20

69

You do not need blockchain.

70

POTENTIAL APPLICATION

Blockchain technology is append-only meaning you can identify when a record has been changed.

Go to Blockchain Specifications - 29 page 10

71

POTENTIAL APPLICATION

The decentralised nature of blockchain means that if one ledger is corrupted, the non-corrupted versions will ignore and override it. This means the blockchain ledger always displays the digital truth.

Go to Blockchain Specifications - 29 page 10

EXAMPLE USE CASE

The World Food Program's Building Blocks saved 98 % in bank fees by using blockchain. By cutting out an intermediary bank, they no longer had to reconcile the bank's data with their own. The blockchain recorded all the transactions which enables immediate and complete auditing. Further, the WFP no longer has to provide a 3rd party (the bank) with sensitive information about refugees.

The most advanced blockchain pilot in the humanitarian sector is the World Food Program's Building Blocks. It operates in Jordan and currently supports around 100,000 Syrian refugees.

The WFP is moving away from in-kind donations towards cash-based transfers. It works as follows: the WFP finds a local bank and provides the bank with details of all the beneficiaries on the program. The bank then creates bank accounts for each of the beneficiaries and gives them a card loaded with the money. The WFP provides the bank with funds in advance. Then every month, the bank sends records of the transactions to the WFP who will reconcile and audit it. This process is costly, slow, and requires the WFP to provide beneficiaries' information to a third party (the bank).

Building Blocks replaces the bank with the blockchain. Now, when a refugee uses the bank card in a store, the transaction is recorded on the WFP's Ethereum permissioned blockchain. Once a week, the WFP will add all the transactions up and then transfer the shop the money they owe, directly from the WFP's bank account to the shop's bank account.

This process means the WFP can better control the list of beneficiaries and no longer have to share their details with a third party. There are also large savings - 98% of costs - from not having to do reconciliation with the bank's data.

Considered a success, Building Blocks is continuing to be piloted, and the WFP is looking at expansion and possibly even utilisation of a cryptocurrency.

This project was criticised by some as it effectively functions as a centralised database and doesn't utilise all of blockchain's potential. However, it's perfectly reasonable to start off with simple applications of blockchain with the view to testing, iterating and expanding. The WFP has chosen a safe and controlled implementation, and hopefully will continue to develop their plans.

Go to Blockchain Specifications – 29 page 10

POTENTIAL APPLICATION

Blockchain can process/execute transactions quickly as it bypasses the need for intermediaries. If transferring an off-chain asset such as fiat, then the blockchain will confirm the transfer quickly (from seconds to minutes), however, off-chain actions (such as actually swapping possession of the money) still need to occur.

Go to Blockchain Specifications – 29 page 10

74

EXAMPLE USE CASE

Charity Dorcas tested blockchain by transferring money from their Dutch to Albanian offices. They compared this process to the traditional banking system in which the same transfer had attracted an unidentifiable and unattributable fee. The blockchain process showed where the money was at all times meaning that such a fee would be identifiable and traceable.

Dorcas' blockchain pilot was under the lead of the START Network and used the Disberse platform. The amount of money moved was € 5 000 and accrued € 0 in bank fees. This is in comparison with a previous transfer using the traditional banking system which attracted a bank fee of € 57.29 – € 11.29 of which was charged by an unknown intermediary somewhere along the chain.

Go to Blockchain Specifications – 29 page 10

75

EXAMPLE USE CASE

Fund Management Platform – Disberse – used blockchain to transfer money from a UK charity to a Swaziland charity. By cutting out some of the intermediaries along the way (banks/exchanges) they saved 2.5 % in fees. This was enough money to support three girls' education for one year.

Go to Blockchain Specifications – 29 page 10

76

Do you want to process large quantities of transactions quickly?

Throughput (the amount of transactions confirmed/processed) is currently one of the biggest scalability issues facing blockchain technology. While Bitcoin can process around 3 – 7 transactions/second, Visa can do around 2 000. If your project requires super quick and frequent transactions, blockchain is not yet ready or capable to handle this.

Yes – 77 page 23

No – 78 page 23

Most blockchains cannot yet process large amounts of transactions in short periods of time.

The amount and speed of transactions per second depends on what blockchain you will be using. For example, at time of publication (June 2018) Bitcoin can process around 4 transactions/second. Bitcoin Cash (a forked [different] version of Bitcoin), however, can process around 61/second.

The speed of transactions mainly depends upon the underlying system and particularly the protocol design related to the consensus mechanism (how to confirm blocks) and blockchain size (how much data you can fit in a block).

If you want to know the speed or quantity of transactions that a blockchain can process, then simply search into Google: "Transaction rate of [name of blockchain]" and you will find results.

If designing your own blockchain, you will need to speak with the developer(s) to determine how important speed and throughput is. Unfortunately blockchain currently faces a trilemma: decentralization vs scalability vs security. If you want to improve the scalability (the amount and speed of transactions) then you're going to have to sacrifice on either the decentralization or security of your blockchain. The trilemma of blockchain is an issue that many blockchainers are currently working on.

End of decision tree

Who would you like to be able to read (view) the transactions recorded on this blockchain?

Blockchain can offer complete transparency in that it can be designed to allow the entire general public to view each and every transaction. This is how the Bitcoin blockchain is designed. If anyone wants to view any Bitcoin transaction that has ever happened, they can download the Bitcoin software, become a 'node' (a computer that runs the software) and view all the transactions.

However, not all projects desire such transparency and as such, there can be limits placed on who can view the transactions.

Humanitarian blockchain projects are likely to include sensitive information – whether about internal operations of the NGO, or about the beneficiaries (although note that it is currently highly discouraged to put personal identifying information about beneficiaries on the blockchain). Therefore, humanitarians might want to consider who can view all the transactions on their blockchain.

Anyone/everyone (public) – 79 page 24

Just people/organisations I have approved – 80 page 24

79

Who would you like to be able to write (add) transactions?

Something to consider: Do you have a data responsibility policy that will cover sharing data?

Anyone/everyone (public) – 81 page 25

Just people/organisations I have approved – 82 page 25

80

Permissioned, private blockchain

A permissioned, private blockchain limits who can read and write (add) to the blockchain. This can be operated/run by one single organisation or by a consortium.

This kind of blockchain would be suitable for occasions/situations when multiple NGOs/charities or multiple internal bodies want to share information in a database, but do not want it accessed by the general public at large. For example, in disaster response, a group of NGOs could use it for beneficiary registration and/or financial mapping of disbursements. It could also be used for humanitarian logistics whereby all the parties along the supply chain are satisfied that they can enter information without exposing themselves to commercial risk.

A criticism leveled at this kind of blockchain is that it is basically a glorified shared database. It doesn't utilise all of blockchain's innovations (decentralisation, security, transparency etc). The less parties involved, the less 'nodes' there are operating the blockchain software. This means the blockchain database is easier to hack. Bitcoin for example, is public and has so many nodes that it would be near impossible to hack/override.

Further, there is only transparency for the consortium, as the public cannot view the transactions.

When deciding whether or not to use a permissioned, private blockchain, you should compare it with current existing centralised database technologies. As blockchain is still in its infancy, it may be cheaper to use an 'older' more established database system.

Continue – 83 page 26

81

Permissionless, public blockchain

Permissionless, public blockchains are entirely open for anyone to join – to read and to write (add to). The most (in)famous blockchain of this type is Bitcoin.

The benefits of this kind of blockchain is that it is entirely transparent, no one owns it, and it has very high levels of security.

Every person who downloads and participates in this kind of blockchain (which you do by downloading the software) becomes a 'node' and can access an up to date copy of the ledger. The more nodes that exist, the harder it is for anyone to tamper with the ledger, as they will be forced to override a majority of all the nodes in existence. This is why the bigger, public blockchains such as Bitcoin have better security than smaller private blockchains with fewer nodes.

Nobody owns or operates this kind of blockchain, and the governance is left up to the participants who implicitly agree to the rules by downloading the software and participating as a node.

While this is a truly revolutionary use of technology, it doesn't present many opportunities for the humanitarian sector yet.

Humanitarian projects are likely to need some sort of control over the governance and infrastructure. They also likely need to control who can add to and/or read the ledger. As such, it is highly unlikely that any humanitarian project would seek this kind of blockchain. Nevertheless, some NGOs/charities may become involved in a public, permissionless blockchain either by utilising the Bitcoin network (ie. by accepting Bitcoin donations) and perhaps in the future, a humanitarian cryptocurrency may run on such a network.

Due to the unlikelihood of humanitarians using this kind of blockchain at this point in time, the decision tree journey ends here.

End of decision tree

82

Permissioned, public blockchain

Permissioned, public blockchains are often described as hybrid blockchains. The ledger is open for the public to view, however, only whitelisted participants can add to it (write permission).

This could be useful in instances where NGOs/charities want public scrutiny such as donations spending. NGOs and charities would be in charge of adding transactions such as donations and disbursements to the ledger, and the general public could monitor the transactions to ensure the right amount of money has gone to the right destination. Note that this kind of cooperation and transparency is already being attempted through IATI (International Aid Transparency Initiative), which acts as a centralised database where donors can voluntarily publish details of their donations and programs. As such, it is not yet clear whether blockchain would offer any further advantage to the current IATI system.

Continue – 83 page 26

Will this be a consortia project or will you be running/governing it yourself? (intra-organisation)

Big organisations may choose to run their own, internal blockchain. This is what the World Food Program have done as their blockchain is only accessible from within the WFP. This use of blockchain attracts criticism as it is hardly decentralised and has lower levels of security.

Alternatively, and more promisingly for the humanitarian sector, a blockchain project can be run as a consortium where numerous organisations work together to share information. A (private sector) example of this is the R3 consortia which is a collective of financial organisations which are working together to build a blockchain for the financial sector.

A consortium of humanitarian organisations could potentially design and implement a blockchain which streamlines humanitarian response. This is a very appealing prospect for disaster response and humanitarian organisations, and has the potential to reduce duplication and costs and improve speed and efficiency. Picture large INGOs, charities, grass roots NGOs and governments using a real-time shared system which only requires beneficiaries to be registered once and that maps who is operating where and with what supplies.

However, there are many factors to consider when deciding whether to form a consortium. Continue along the decision tree to see some of the most crucial issues.

Something to consider: Where would you like consensus to be decided?

Consortia (group) decision – 84 page 26

Within your organisation – 85 page 27

Do you want to design and build your own blockchain or use an already established platform (blockchain as a service?)

Your consortium can either hire a company with an already established blockchain (such as Disberse or IBM), or it can attempt to design and build its own blockchain. The second option is considerably more laborious and there are lots of technical, operational and managerial considerations. This decision tree presents some of the more major considerations, but by no means covers them all. Further investigation will be needed to make this decision.

I want to build my own blockchain – 86 page 28

You will need to hire a team to build the platform

I want to use already established blockchain ie. Disberse or IBM's hyperledger – 86 page 28

85

Do you want to design and build your own blockchain or use an already established platform (blockchain as a service?)

Your organisation can either hire a company/consultancy with an already established blockchain (such as Disberse or IBM), or it can attempt to design and build its own blockchain. The second option is considerably more laborious and there are lots of technical, operational and managerial considerations. This decision tree presents some of the more major considerations, but by no means covers them all. Further investigation will be needed to make this decision.

I want to build my own blockchain – 86 page 28

You will need to hire a team to build the platform

I want to use already established blockchain ie. Disberse or IBM's hyperledger – 86 page 28

Further considerations for designing your blockchain application

Risk aversion and innovation appetite of your organisation. Are senior figures interested?

Do you have funding to maintain this project beyond the start-up costs?

Do you have the human capacity to run this?

Hiring blockchain talent is a difficult task as the amount of blockchain professionals is not keeping pace with their demand. Further, talent is snapped up quickly by the banks and fintech sector. If your organisation decides to hire its own internal blockchain team it must be prepared for stiff competition from other sectors. Beyond the blockchain staff you will need to hire, it is likely that other staff members will need to be familiar with how the platform works as they will be the ones utilising it. Consider whether your staff have the capacity and desire to be trained on a new technology.

Process for joining or leaving consortia?

Joining and leaving a blockchain network is not simple. This is because in permissioned blockchains, participants hold stakes in the network and have various data ownership rights and obligations. Deciding the process for joining and leaving a consortium blockchain network is something that should happen in the beginning when governance and operating modalities are being hashed out.

Who will be the designated entity to oversee the solution from a technology and management perspective?

One organisation or one group (such as a working group or committee) will need to take a managerial role in order to make decisions on behalf of the entire consortium (or if this is an organisation's internal blockchain, one particular group). Their role includes decisions regarding updating the platform, dealing with software exploits, handling members and their roles etc.

Can it be added-on/be compatible with legacy systems?

"A blockchain solution is rarely just that – greatest value is achieved when it is part of a greater network alongside legacy components (e.g., relational databases and web applications)."
Deloitte, Taking Blockchain Live.

When working in a consortium, there will be numerous legacy systems which the potential blockchain application should fit and interface with. You will need to assess this in order to determine whether blockchain is worthwhile.

Consortia members – who should be included?

Size of your organisation – bigger organisations are often harder to satisfy/convince as they are largely departmentalised and subject to red-tape.

End of decision tree