Blockchain Adoption Toolkit

taliox

This toolkit, consisting of multiple questionnaires, helps you to figure out if blockchain is a reasonable solution for your problem and also gives hints about what kind of blockchain fits your needs best.

1. The **Suitability Check** provides a fast and initial test for checking whether Blockchain generally is a viable solution for your problem.

2. To further evaluate a potential blockchain solution you can check what **Consensus Method** might be feasible and if an additional **Off-Chain Storage** is needed.

3. If you're not sure whether you need a public, private, permission-less or permissioned blockchain or even something else to meet your confidentiality needs, first check your **Confidentiality Level** and then search for a fitting **Confidentiality Solution**.

Suitability Check

Consensus Method

Off-Chain Storage

Confidentiality Level

Confidentiality Solution

- Data History
- Transaction History
- Proof of Origin

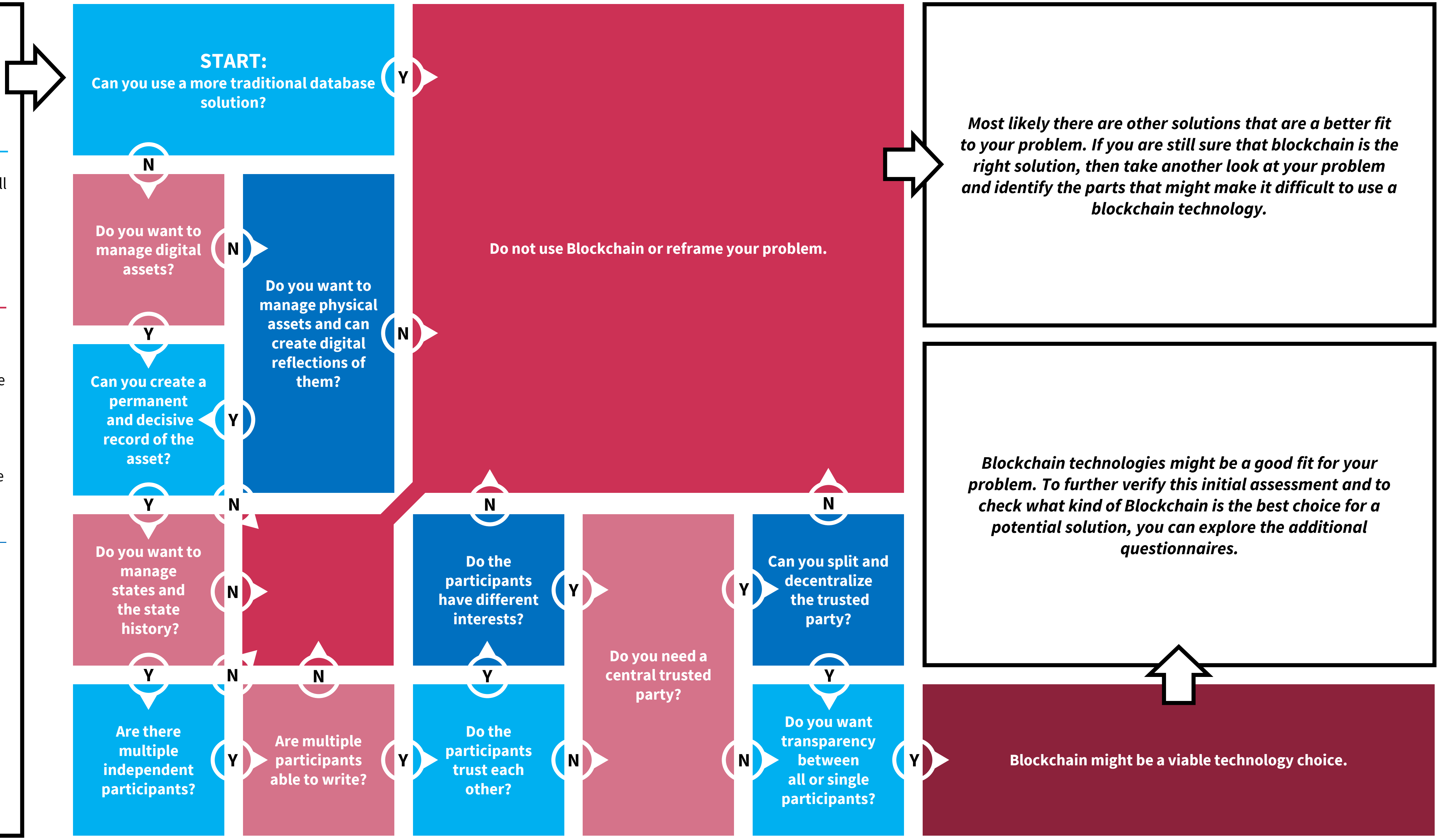
Blockchain Suitability Check

The following questions will help you make a quick initial assessment of whether blockchain is the right technology for the problem you are facing.

By referring to blockchain, all forms of the distributed ledger technology (DLT) are meant. DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator.

Y = YES

N = NO



START: Can you use a more traditional database solution?

Do you want to manage digital assets?

Do you want to manage physical assets and can create digital reflections of them?

Can you create a permanent and decisive record of the asset?

Do you want to manage states and the state history?

Are there multiple independent participants?

Are multiple participants able to write?

Do the participants trust each other?

Do the participants have different interests?

Do you need a central trusted party?

Can you split and decentralize the trusted party?

Do you want transparency between all or single participants?

Do not use Blockchain or reframe your problem.

Most likely there are other solutions that are a better fit to your problem. If you are still sure that blockchain is the right solution, then take another look at your problem and identify the parts that might make it difficult to use a blockchain technology.

Blockchain might be a viable technology choice.

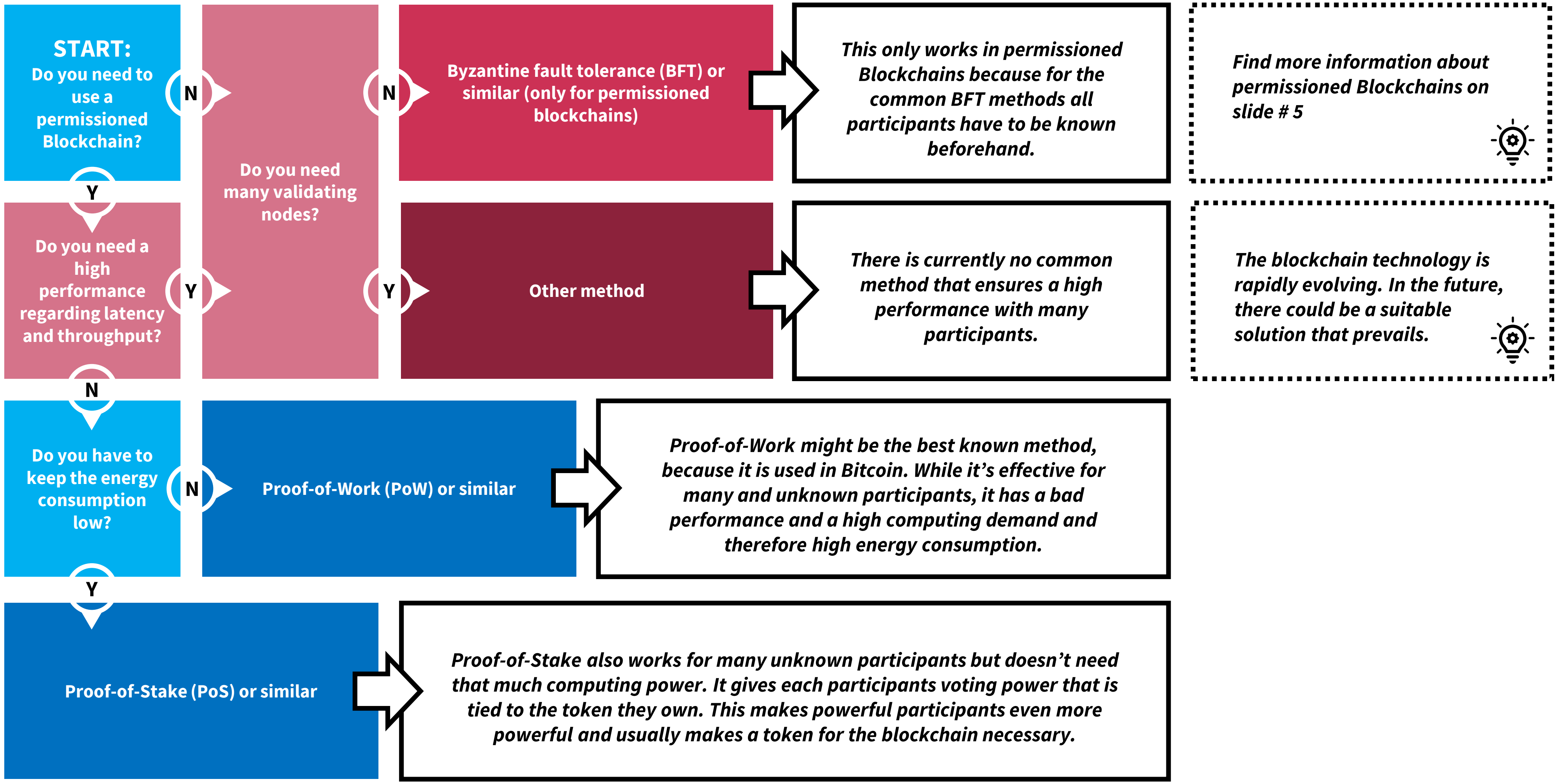
Blockchain technologies might be a good fit for your problem. To further verify this initial assessment and to check what kind of Blockchain is the best choice for a potential solution, you can explore the additional questionnaires.

Consensus Method

Each Blockchain should have at least two independent participants otherwise it would just be a normal (distributed) database.
To keep the system in sync it is necessary that all participants agree on the same data state. Since participants can't necessarily trust each other there can't just be a central entity that sets the state (even if it was determined democratically). This problem is known as the *byzantine fault.* To solve this problem an appropriate method must be used for consensus making.

Y = YES

N = NO



START: Do you need to use a permissioned Blockchain?

N → **Do you need many validating nodes?**

N → **Byzantine fault tolerance (BFT) or similar (only for permissioned blockchains)**

This only works in permissioned Blockchains because for the common BFT methods all participants have to be known beforehand.

Find more information about permissioned Blockchains on slide # 5

Y → **Other method**

There is currently no common method that ensures a high performance with many participants.

The blockchain technology is rapidly evolving. In the future, there could be a suitable solution that prevails.

Y → **Do you need a high performance regarding latency and throughput?**

Y → **Do you need many validating nodes?**

N → **Do you have to keep the energy consumption low?**

N → **Proof-of-Work (PoW) or similar**

Proof-of-Work might be the best known method, because it is used in Bitcoin. While it's effective for many and unknown participants, it has a bad performance and a high computing demand and therefore high energy consumption.

Y → **Proof-of-Stake (PoS) or similar**

Proof-of-Stake also works for many unknown participants but doesn't need that much computing power. It gives each participants voting power that is tied to the token they own. This makes powerful participants even more powerful and usually makes a token for the blockchain necessary.

Blockchain Off-Chain Storage

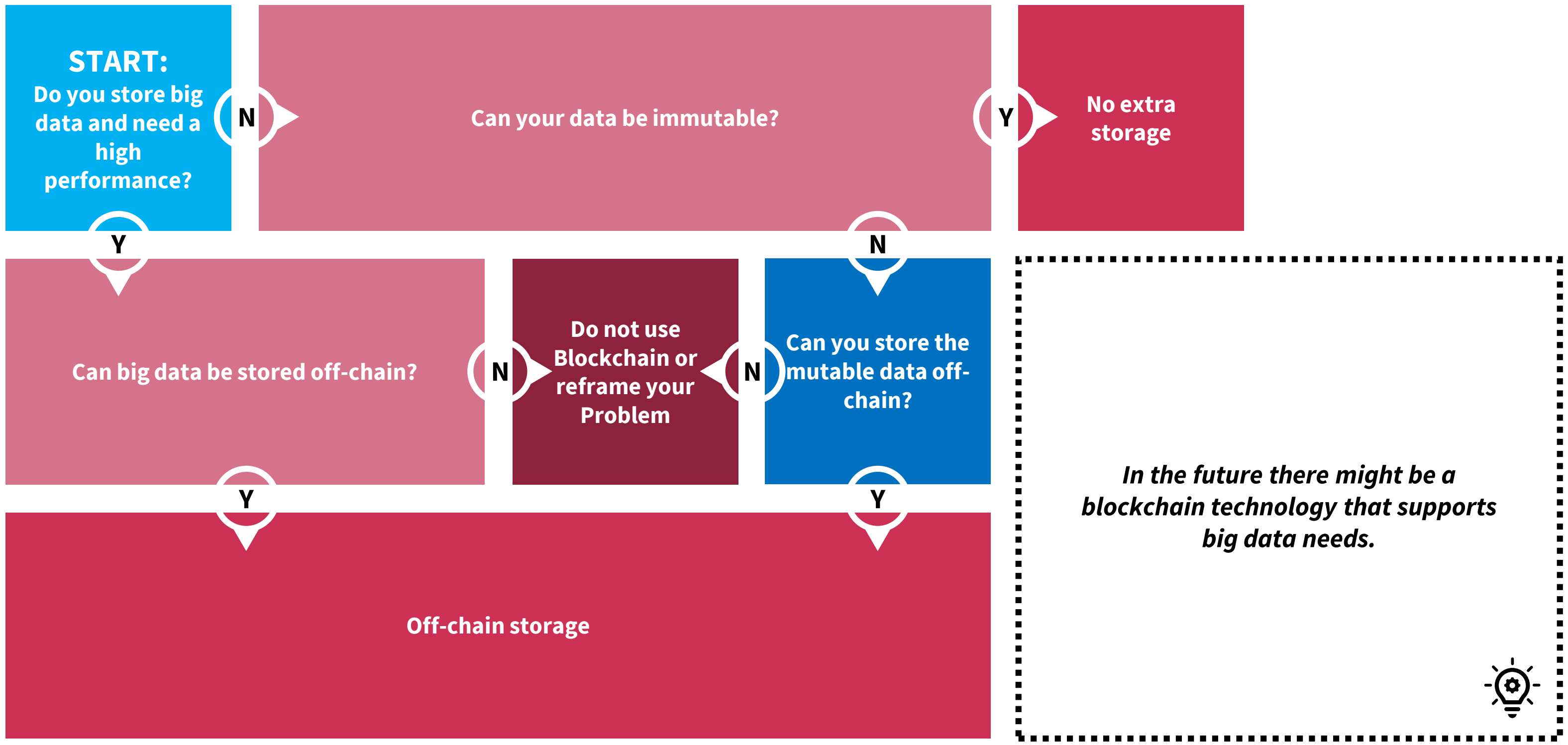
taliox

Blockchain Off-Chain Storage

Off-chain storage describes every storage that is part of the blockchain solution but stores the data not on the blockchain but in an other type of database. This is often necessary when it’s impractical or ineffective to store specific data directly on the blockchain. The data that is stored off-chain is typical connected to a transaction on the blockchain via an identifier.

Y = YES

N = NO



START: Do you store big data and need a high performance?

N

Can your data be immutable?

Y

No extra storage

Y

Can big data be stored off-chain?

N

Do not use Blockchain or reframe your Problem

N

Can you store the mutable data off-chain?

Y

Y

Off-chain storage

In the future there might be a blockchain technology that supports big data needs.

Blockchain Confidentiality Level

Blockchain Confidentiality Level

Most blockchain technologies can be classified via two dimensions:

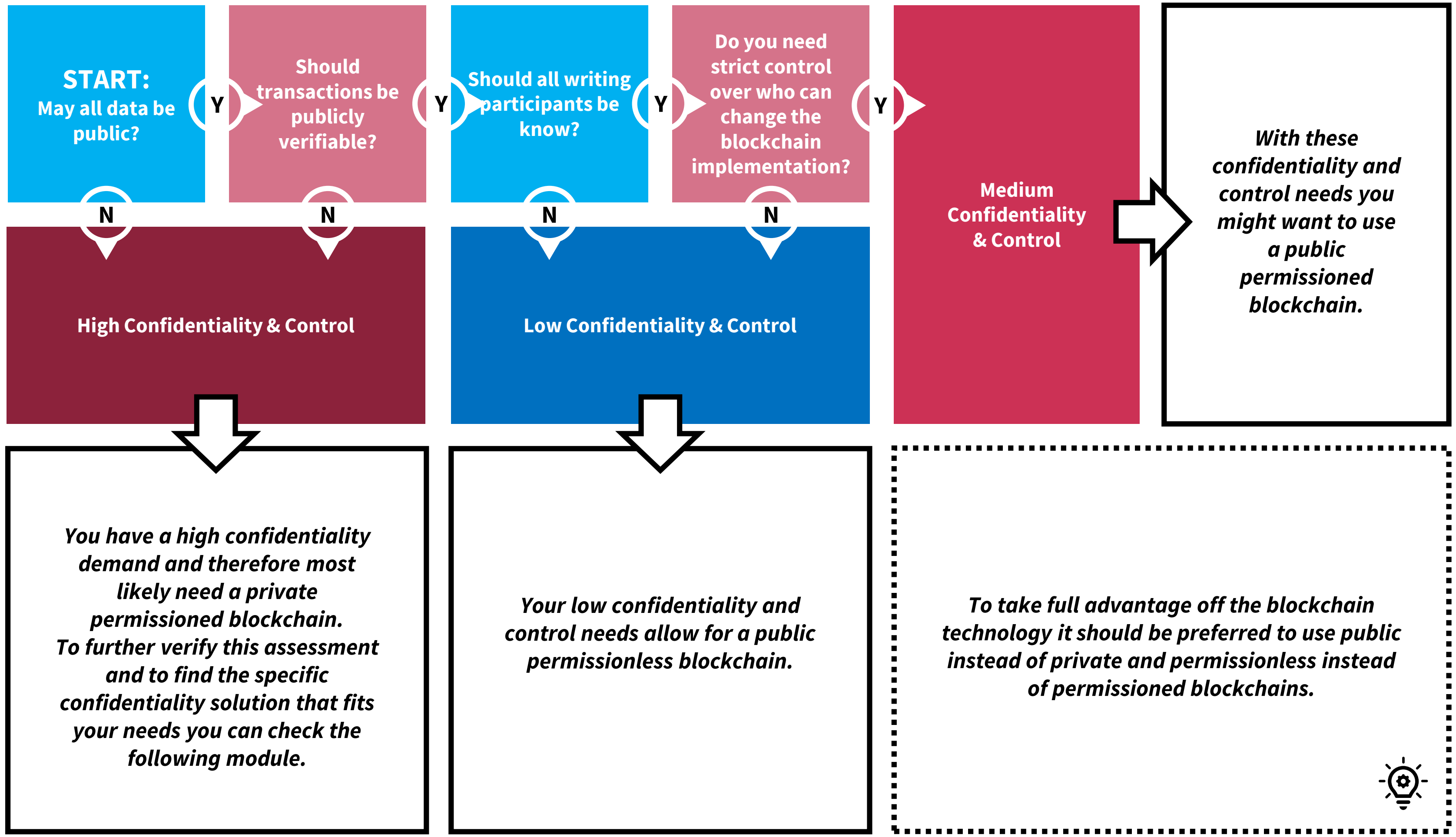
- Public and Private
- Permissionless and Permissioned

In a public blockchain all stored data can be accessed publicly. In contrast to this you need the corresponding access rights to access data in a private blockchain. Private blockchains are typically also permissioned and therefore restrict what each participant can do and require that each participant is registered before he can use the blockchain. Permissionless blockchains allow unknown (and not registered) participants to join the blockchain and take part in the consensus making.

Depending on your confidentiality and control needs different blockchain types are necessary.

Y = YES

N = NO



START:
May all data be public?

Should transactions be publicly verifiable?

Should all writing participants be know?

Do you need strict control over who can change the blockchain implementation?

Medium Confidentiality & Control

With these confidentiality and control needs you might want to use a public permissioned blockchain.

High Confidentiality & Control

You have a high confidentiality demand and therefore most likely need a private permissioned blockchain.
To further verify this assessment and to find the specific confidentiality solution that fits your needs you can check the following module.

Low Confidentiality & Control

Your low confidentiality and control needs allow for a public permissionless blockchain.

To take full advantage off the blockchain technology it should be preferred to use public instead of private and permissionless instead of permissioned blockchains.

Application Type

To get a better understanding on what confidentiality solutions might be applicable it can be useful to first get a better understanding on why you want to use a blockchain and what you want to achieve with the solution.

Potential Blockchain usages can be roughly divided into three types:

- Proof of Origin
- Data History
- Transaction History

The listed questions and examples can help you to identify which blockchain usages are applicable in your case.
If you can answer each question with "yes" it is likely that it is one of the usages, you want the blockchain for.

When you now what usage types are applicable for your case, you can do the corresponding questionnaires on the next slide to check which confidentiality solution is fitting.

Proof of Origin

Do you want to prove the origin or time of production for a good?

- *to prove that a document existed at a certain time (e.g. a contract)*
- *to prove who created something and when (e.g. music)*
- *to prove by whom the good was initially placed in the movement of goods (e.g. diamonds)*

Can you create a unique identifier for the good that does not allow conclusions about the nature of the good?

- *The hash value of a cryptographic hash function (for digital goods)*
- *A fixed identification number associated with the good that can not easily be changed (e.g. RFID transponders on goods or an engraving in diamonds)*

Is only the original origin relevant and not who the current owner is?

- *It is relevant who originally created a particular product, but not by whom and when it was traded (e.g. branded clothing)*

Data History

Do you want to create a history for specific data, creating a sequence of data points?

- *weather data*
- *latency information*
- *change history for documents*

Is it acceptable when the data is invalid at the time of saving, since only the sequence is needed?

- *E.g. sensor data. It is not possible to check whether the sensor supplies correct data, but still knowledge can be drawn from the analysis of the data history.*

Transaction History

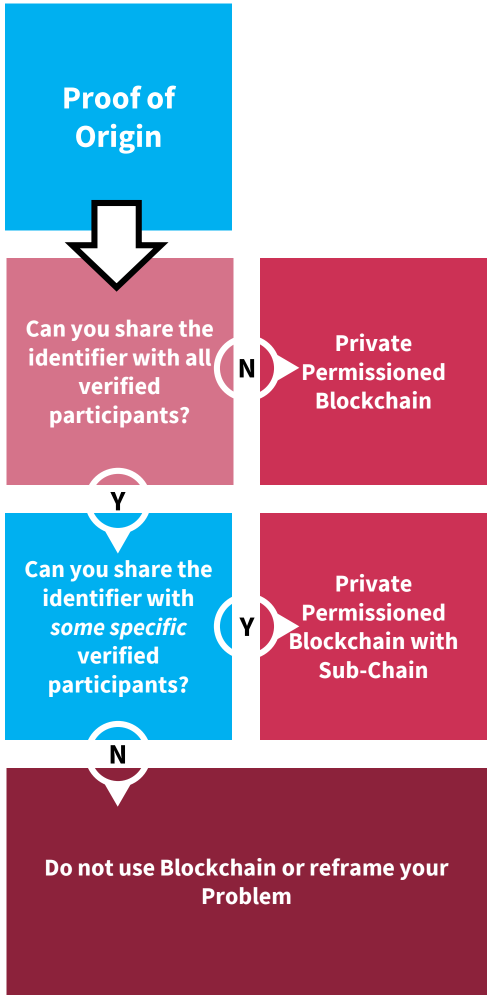
Do you want to create a transaction history that shows who owned which good and when he received it from whom?

- *currency*
- *goods tracking*

Do you need to verify the transaction to the extent that a simultaneous transfer of the same good to different participants is excluded?

- *e.g. participant A has 10 tokens and simultaneously tries to transfer 10 tokens to participant B and participant C*

Confidentiality Solution



Proof of Origin

Can you share the identifier with all verified participants?

N → Private Permissioned Blockchain

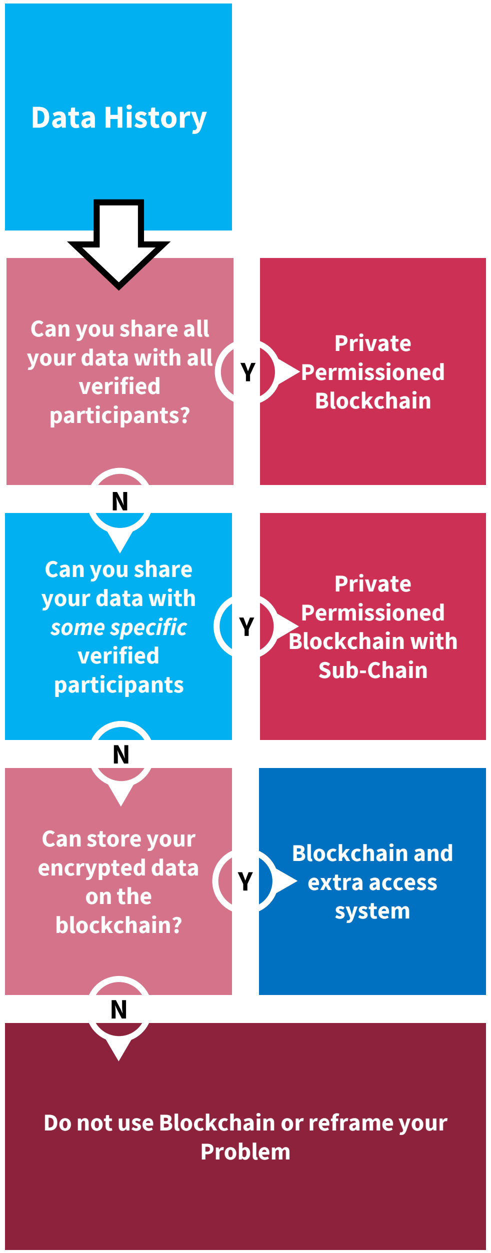
Y ↓ Can you share the identifier with *some specific* verified participants?

Y → Private Permissioned Blockchain with Sub-Chain

N ↓ Do not use Blockchain or reframe your Problem

Sub-chain

A sub-chain describes an extra blockchain connected to the main blockchain via identifiers or similar methods. A Sub-chain enables a subset of all participants to have private transactions with each other.



Data History

Can you share all your data with all verified participants?

Y → Private Permissioned Blockchain

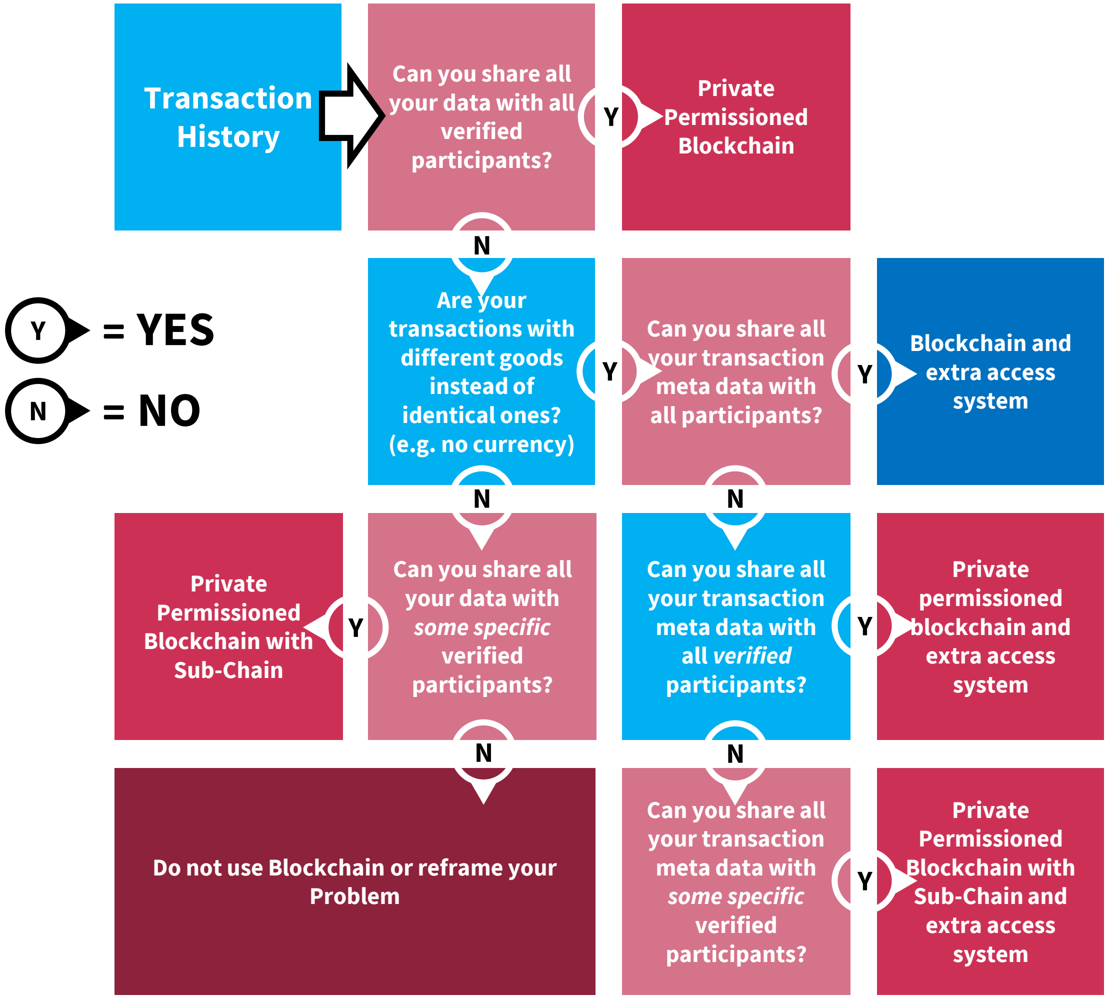
N ↓ Can you share your data with *some specific* verified participants

Y → Private Permissioned Blockchain with Sub-Chain

N ↓ Can store your encrypted data on the blockchain?

Y → Blockchain and extra access system

N ↓ Do not use Blockchain or reframe your Problem



Y = YES

N = NO

Transaction History

Can you share all your data with all verified participants?

Y → Private Permissioned Blockchain

N ↓ Are your transactions with different goods instead of identical ones? (e.g. no currency)

Y → Can you share all your transaction meta data with all participants?

Y → Blockchain and extra access system

N ↓ Can you share all your transaction meta data with all *verified* participants?

Y → Private permissioned blockchain and extra access system

N ↓ Can you share all your transaction meta data with *some specific* verified participants?

Y → Private Permissioned Blockchain with Sub-Chain and extra access system

N ↓ Can you share all your data with *some specific* verified participants?

Y → Private Permissioned Blockchain with Sub-Chain

N ↓ Do not use Blockchain or reframe your Problem

Extra access system

It might be necessary to store encrypted data on the blockchain. To control who has the decryption key for this data a system that manages these accesses must be put in place.