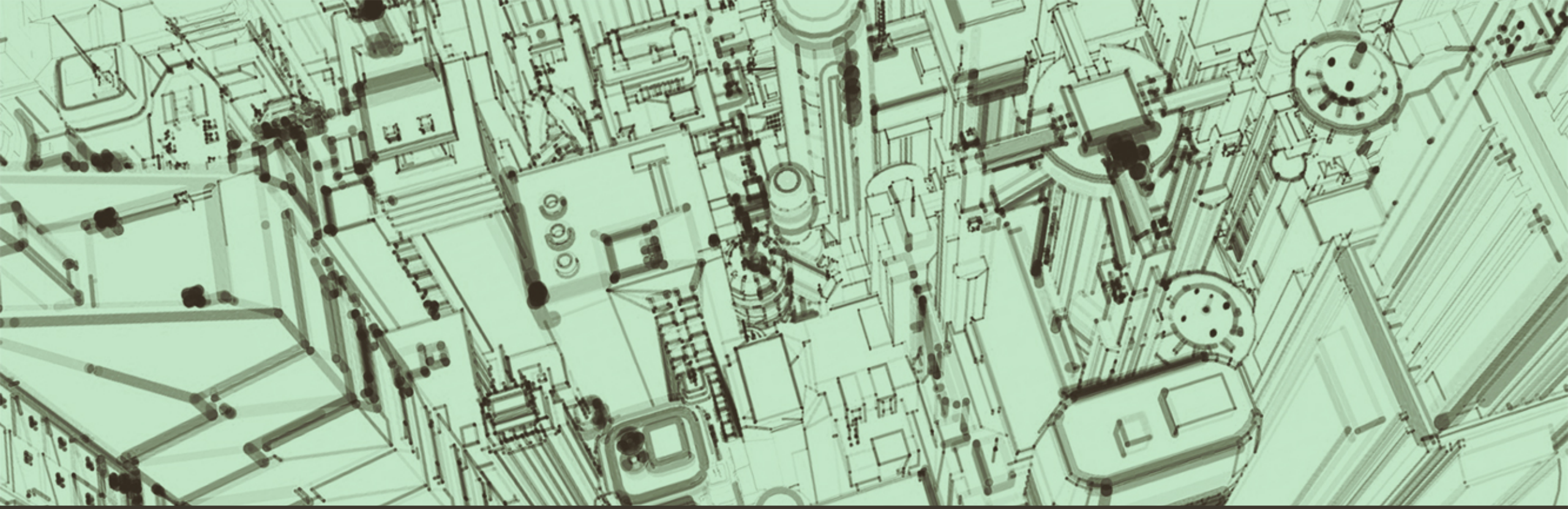


Private Law Society™ (PLS)

Enforcement of contracts through financial incentives

PLS Proposal

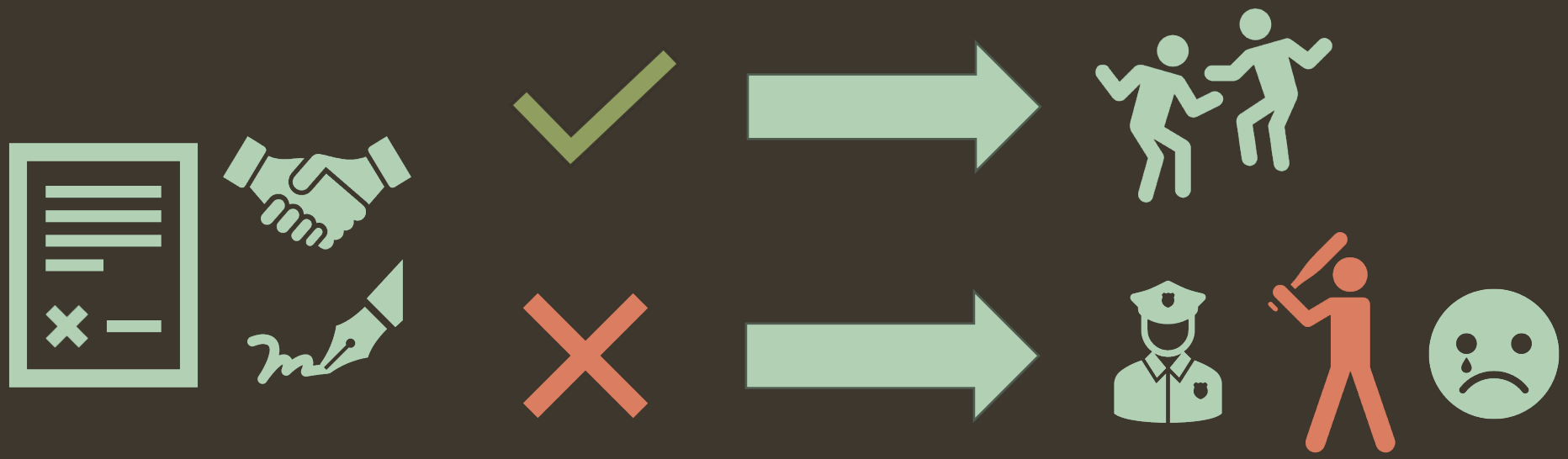
https://www.PrivateLawSociety.net

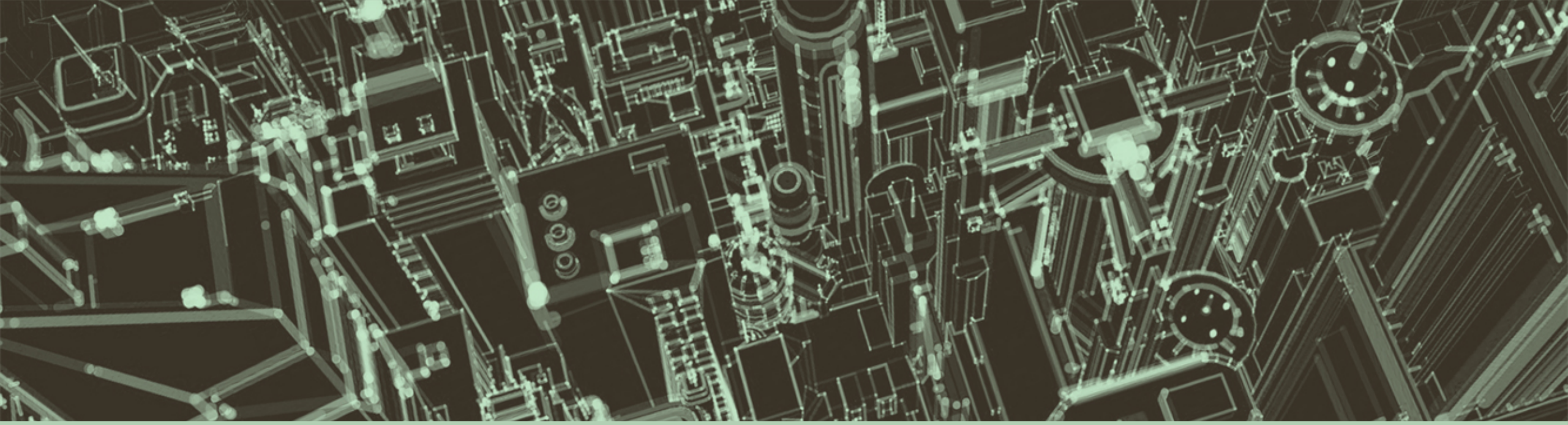
A Private Law Society (PLS) proposes a model for the *enforcement* of **contracts** through *financial incentives*, in a private, decentralized, and voluntary manner.

Solves the problem of *fear-based* incentive

The **PLS** opposes the outdated model of incentive through *fear* of suffering the consequences of the Law. Without the PLS, the use of **force** is necessary for conflict resolution.

Without PLS:



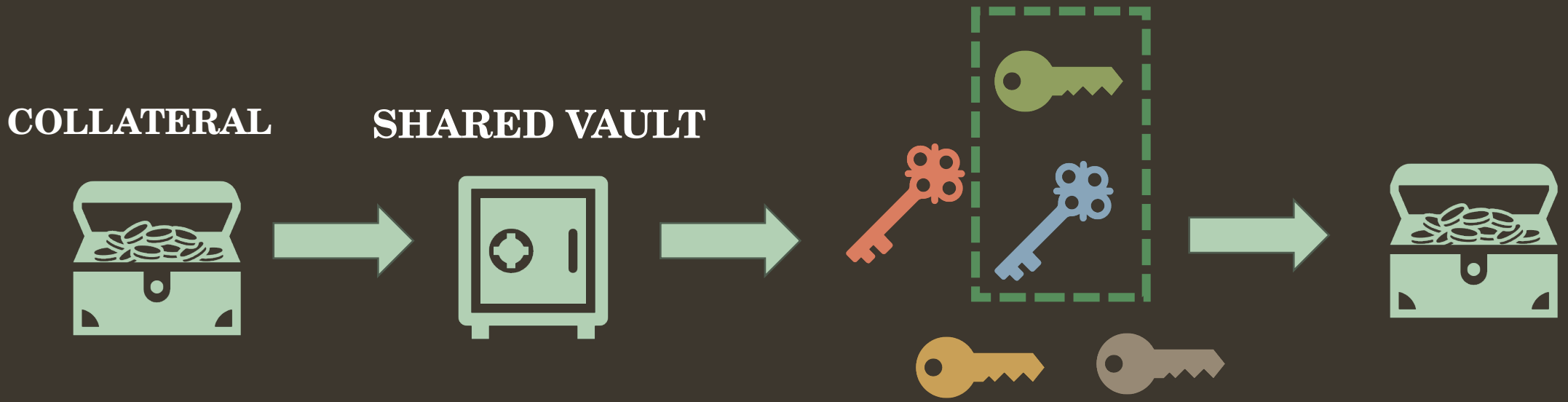


Mechanism Overview

Still without going into practical details

Financial incentive for contract enforcement

What differentiates the **PLS** from other arrangements is the **collateral** (prize) that will be used as a *guarantee* for contract enforcement. A monetary amount is deposited in a shared vault that only opens with the mutual collaboration of the parties involved. For example: **M** keys out of a total of **N**. Each key belongs to each of the involved parties (parties and arbitrators).

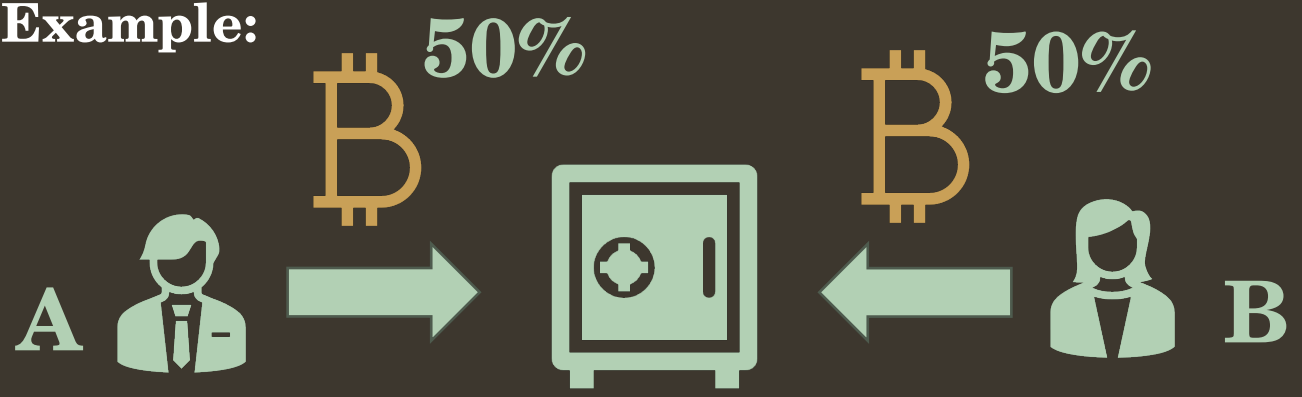


Control of the shared vault

One of the parties can deposit *all* the **collateral** or each party can deposit a *fraction* depending on what is specified in the contract.

A specific clause is recommended that indicates how the collateral will be distributed in case of compliance or breach of the contract.

Example:



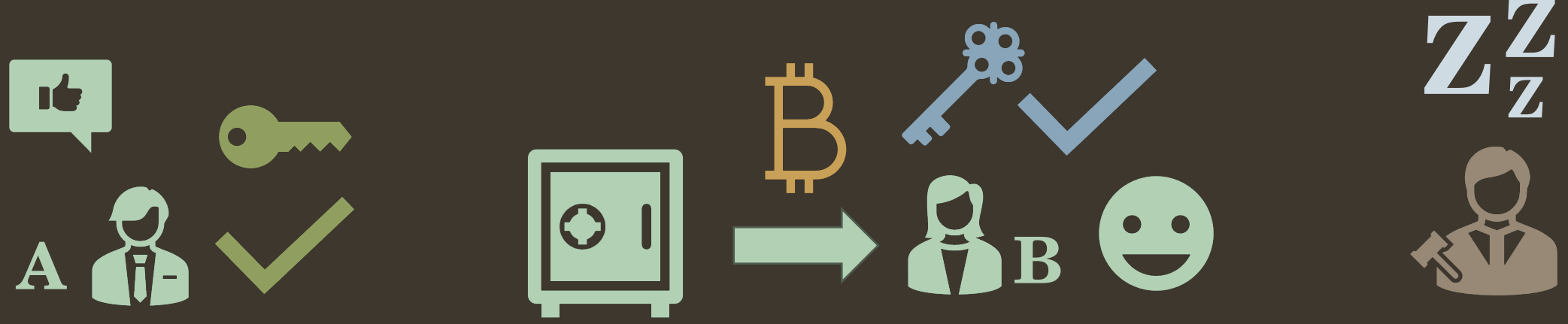
Example of a contract:

If the contract is fulfilled by B respecting the terms, all the collateral should be sent to B.

Case of success

When the interested parties are **satisfied** with the execution of the contract, they simply use their keys to open the vault and direct the **collateral** to the appropriate place. In this case, no arbitrator needs to interfere or participate in the transaction.

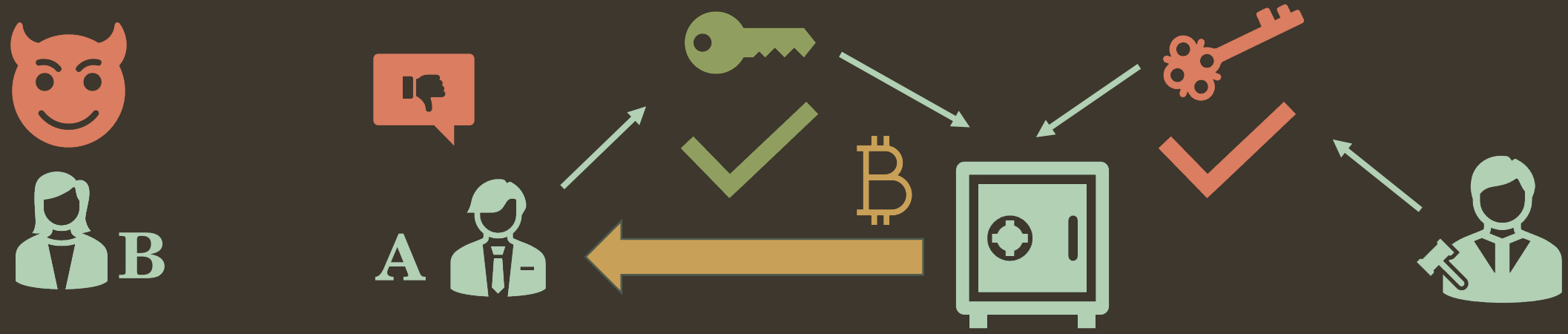
In the example below, the values are going to B, but it is possible for them to be sent even to a third party. Everything depends on how it is specified in the contract.

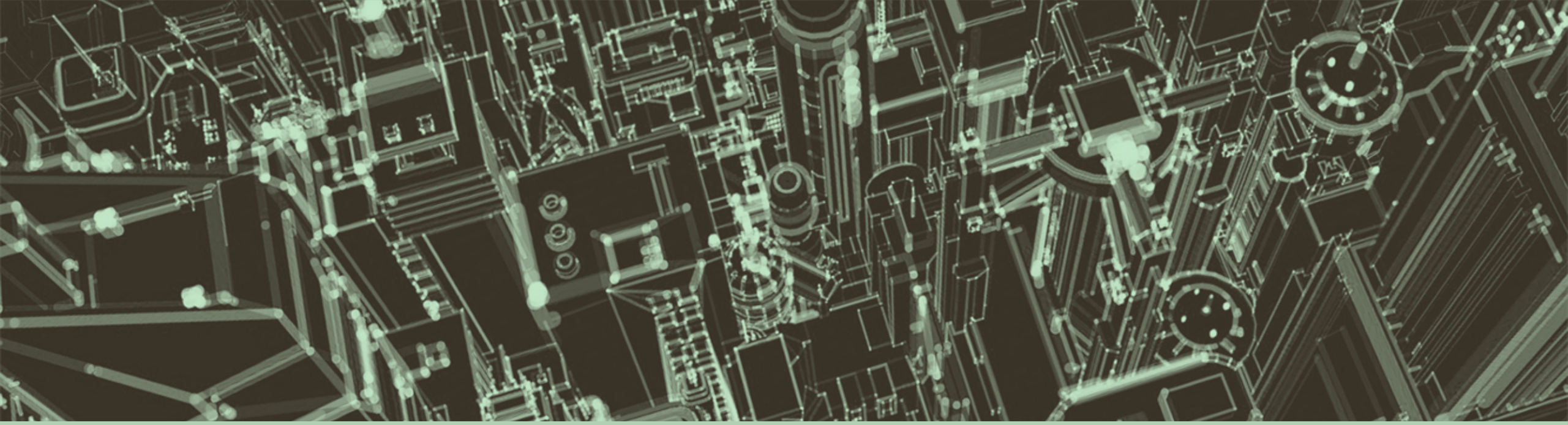


Case of dispute

When one or both interested parties enter into **conflict** due to disagreement on the execution of the contract, an arbitrator is called upon to analyze the situation, collect evidence from both parties, make a judgment, and render a **decision**.

The arbitrator may decide, for example, based on the clauses of the contract, that the entire value should return to A. In this case, A + the arbitrator need to sign to release the vault.





Step-by-step

How to use the PLS in practice

The PLS mechanism consists of:

1. Two interested **parties**.
2. A **collateral** that will be used as a *guarantee*.
3. A **file** that describes the *agreement*.
4. One or more **arbitrators** previously elected by the parties.

PARTIES

COLLATERAL

FILE (CONTRACT)

ARBITRATORS

Step 1: drafting the proposal

A contract proposal should be created in the form of a **file** in any format, such as a text file (.txt), MS Word (.docx), or PDF, e.g.

This file should contain the clauses and terms in a language understandable by all parties. It can be drafted by one of the parties and proposed to the other party(ies), drafted jointly, or with the help of a neutral third party.

Contract materialized in the form of a file

Step 2: upload & selection of the involved parties

Anyone involved – one of the parties or an arbitrator – in possession of the *final version* of the file representing the contract, can **upload** it to the PLS system.

This person then selects the parties through their **digital identities**. Currently, the PLS supports the **Nostr** protocol (a kind of semi-decentralized microblogging).

UPLOAD

PARTY 1

PARTY 2

ARB 1

Step 3: the involved parties sign

Each of the involved individuals, including **all parties** and **all arbitrators**, must log into the system and sign the file with their respective **digital identities**.

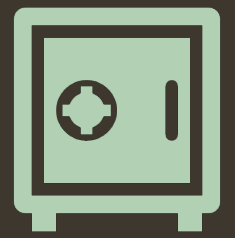
Step 4: the shared vault is created

With the signatures of all involved, a shared **vault** is created.

Immediately after everyone has signed, each involved party (including arbs) must *download* a JSON file with the metadata representing this vault.

VAULT (JSON)

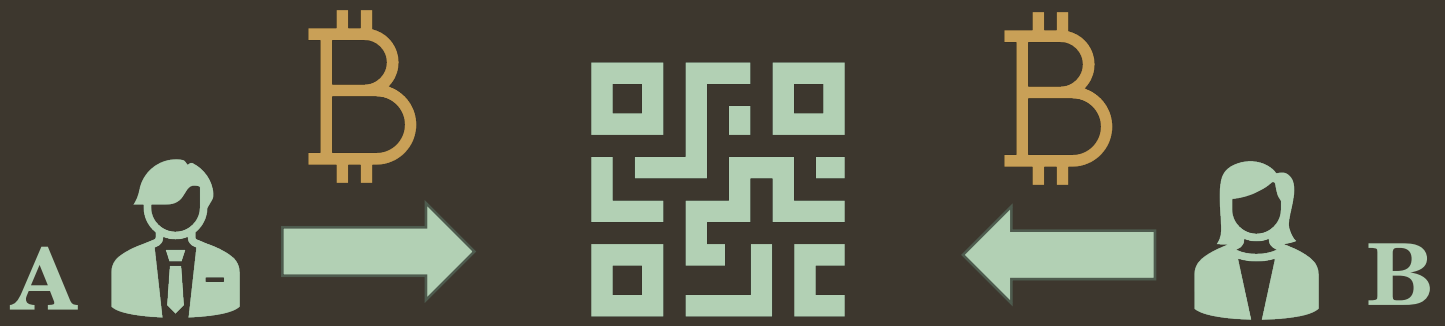
Each party must keep this file in a safe place as it will be used to access the **collateral** during the resolution of a contract.



Step 5: collateral deposit

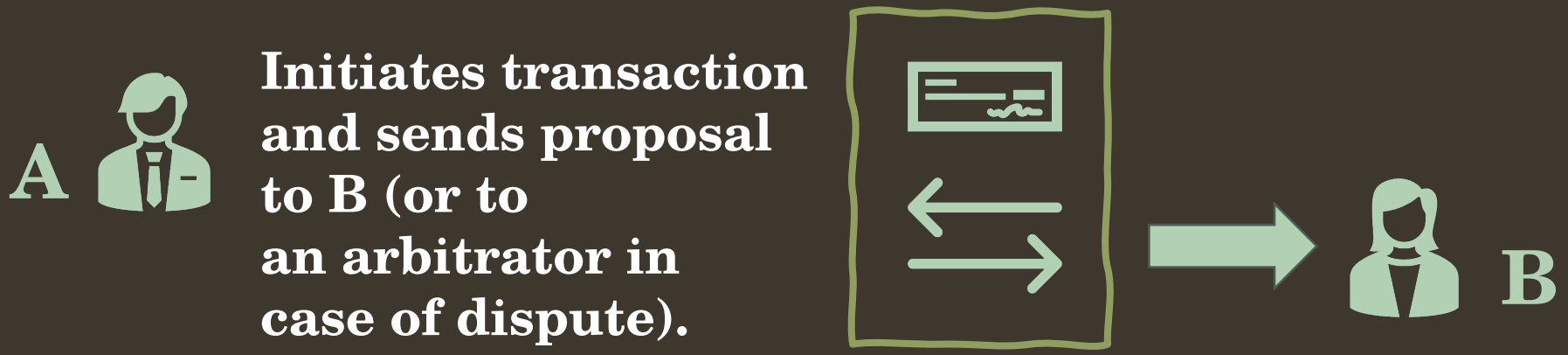
Now, each party has the opportunity to deposit an amount of **collateral** to serve as a *guarantee*. This amount will remain "frozen" in the vault until the **minimum quorum** can be reached to "thaw" it later. The amount and/or proportion of the value from each party depends on what is specified in the contract.

Currently, PLS supports deposits in Bitcoin (*onchain*) or L-BTC (Liquid).



Step 6: collateral redemption

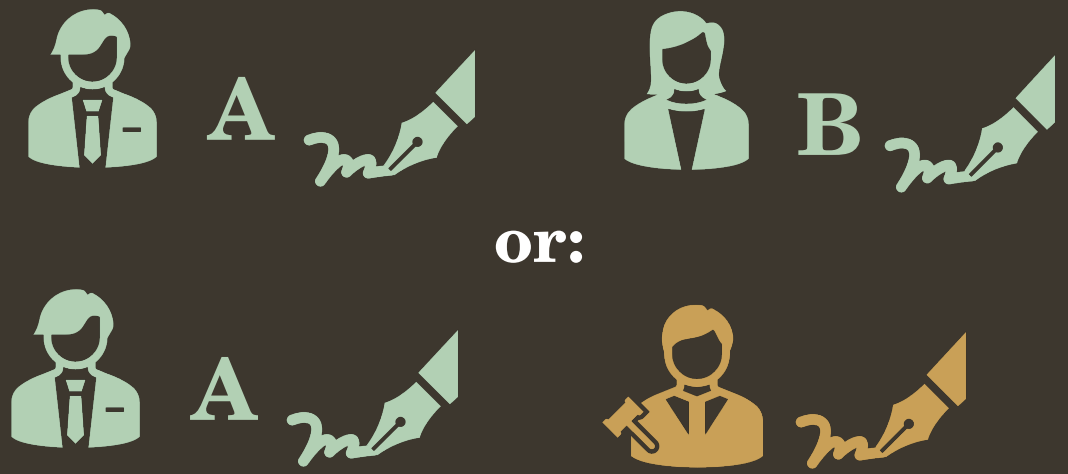
After the execution or breach of the contract, a **transaction** is initiated by any of the involved parties (any of the parties and/or arbitrator(s)) that specifies the destination of the **collateral**. This destination can be one or more arbitrary **wallets**. For the transaction to actually take place, another party and/or arbitrator(s) need to agree and sign as well. If no agreement is reached, the **collateral** remains "frozen".



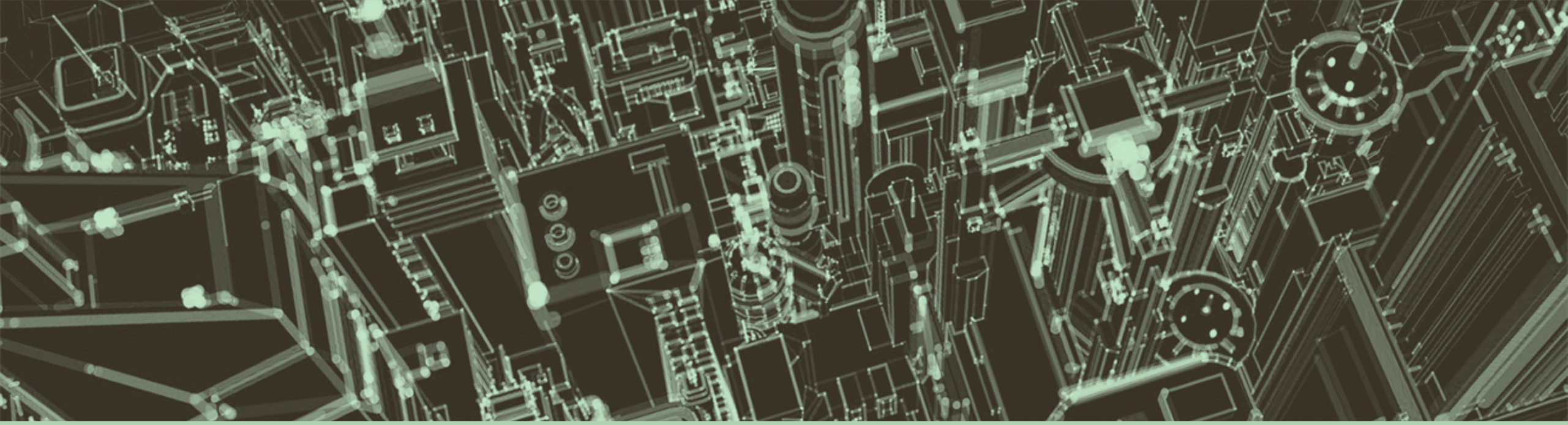
Example of transaction

A transaction can be, for example:

- Send 0.3 BTC to address XPTO.
- Send 0.1 BTC to address ABCD.
- Send 0.6 BTC to address DEFG.



Depending on the required number of signatures (**M** of **N**) the transaction is accepted and executed on the Bitcoin network or similar.



Advanced Topics

Challenges, advantages, and advanced issues

Unavailability of collateral

1) No one reaches an agreement, the collateral remains "frozen"

If none of the involved parties reach a **consensus** with the *minimum required quorum* of signatures by the vault, the collateral may remain "frozen". However, there is a strong incentive to achieve a *minimum quorum*: it is in no one's interest for the value to remain completely frozen.
For extreme cases, there is also a form of "time-based resolution" (see next slide).

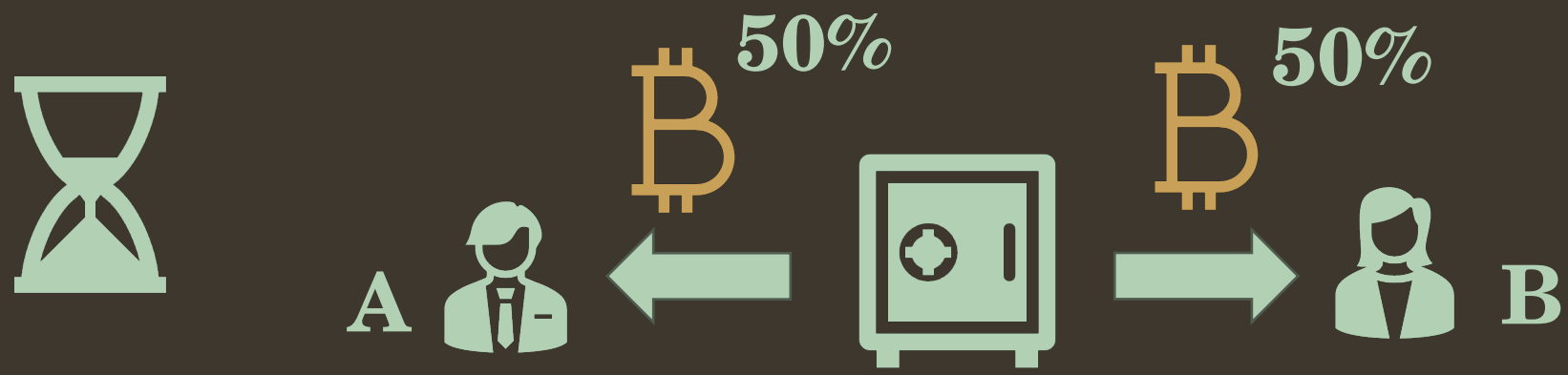
2) During the execution of the contract, the collateral becomes unavailable

The **collateral** (*guarantee*) becomes unavailable during the execution of the contract, which can be a problem especially if it is of great value or if the contract is long-term. However, historically Bitcoin has performed well against fiat currencies in the long term, thus there is an incentive to save Bitcoin.

Time-based resolution (*timelock*)

With the use of timelock technology, PLS allows for **time-based** conflict resolution.

If no action is taken after a specified period of time, the contract "expires" and then a specific solution (e.g., return of the collateral to all parties) is executed. This could be useful in cases of, for example, deaths or irreconcilable disagreement.



Advantages of PLS

1) Without the involvement of "violent authorities"

Note that in the PLS model, no "violent authority" (police) needed to be called upon to resolve a contract in case of a dispute. The financial incentive is often sufficient to encourage parties to collaborate towards a friendly resolution.

2) Uncensorable and private system

Also note that the **PLS** model is "uncensorable" by using decentralized network protocols like **Bitcoin** and **Nostr**, making it virtually impossible for external agents to interfere in private agreements.

Arbitration system and reputation

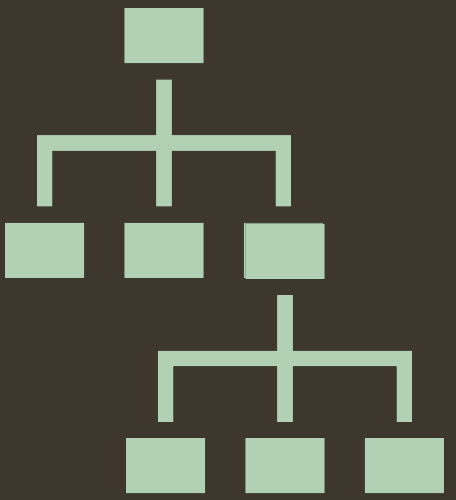
A *weak point* of this system might be the selection of arbitrators. A poorly chosen, biased, or unavailable arbitrator can ruin the resolution of a contract. Therefore, it is necessary that the **arbitration** ecosystem be improved over time.

A possible solution would be the use of reputation systems in the style of **WoT** (Web of Trust), or the hiring of professional firms dedicated to this with a strong reputation in the market.

Moreover, the financial incentive for the arbitrator(s) is also important: it is advisable to include a clause for a fee paid to the arbitration in case of a dispute, which will be taken from the **collateral**.

Custom signature scripts

The arrangement of signatures to open the shared vault is technically done with *Taproot scripts* (based on *Merkle trees*), enabling sophisticated setups and preventing collusion among arbitrators for undue access to the collateral.



For example:

Imagine a situation with 2 parties and 5 arbitrators.

- The vault *opens* if:
  - Both parties (even without arbitrators) sign.
  - One of the parties together with 3 out of the 5 arbitrators.
- The vault **does not** open even if all the arbitrators sign without one of the parties.

User experience and interface (UI/UX) improvements

Creating interfaces that are accessible to a lay audience is a significant challenge not only for PLS but for the entire Bitcoin ecosystem and decentralized systems in general.

With the tools currently available, a person with limited technical knowledge may find it somewhat difficult to use the system. Starting with, for example, creating an account on the **Nostr** network; and even managing **Bitcoin** collateral, which is still not an easy task for everyone.

The user interface/experience is constantly evolving, and volunteers are working to make it increasingly easier and more accessible.

How to use or collaborate?

To use the PLS system and/or collaborate with improvements to the *open source* project, please visit the official website:

`https://www.PrivateLawSociety.net`