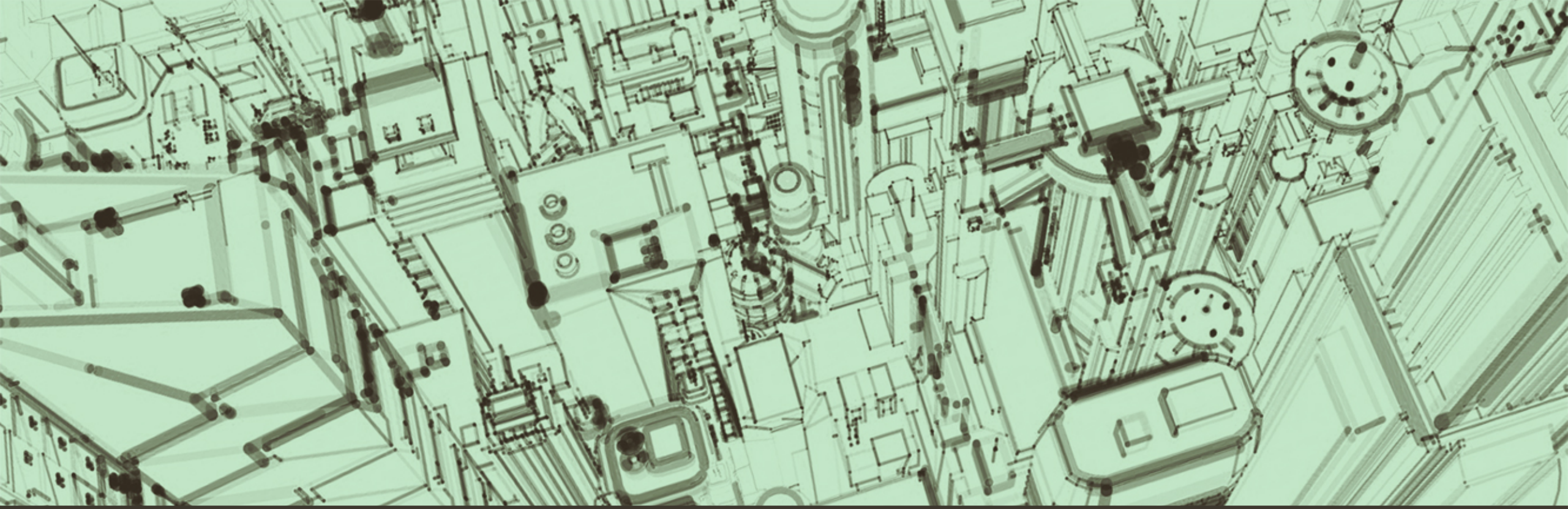


Private Law Society™ (PLS)

Enforcement de contratos através de incentivo financeiro

Proposta da PLS

https://www.PrivateLawSociety.net

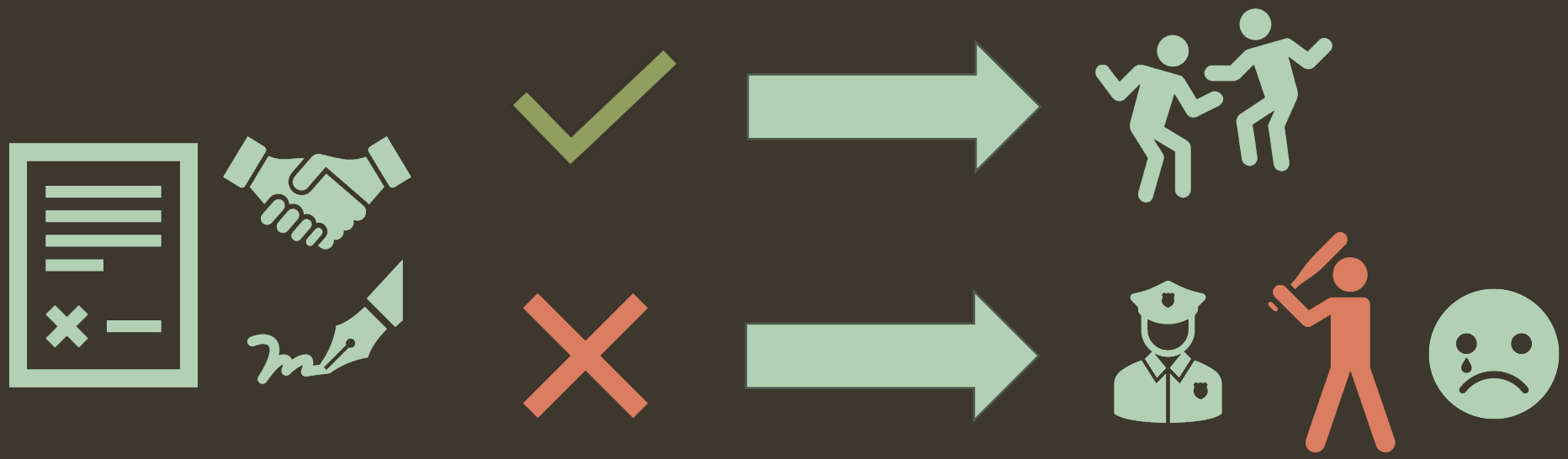
A Private Law Society (PLS) propõe um modelo para o *enforcement* (“fazer-valer” ou *execução*) de **contratos** através de *incentivo financeiro*, de forma privada, descentralizada e voluntária.

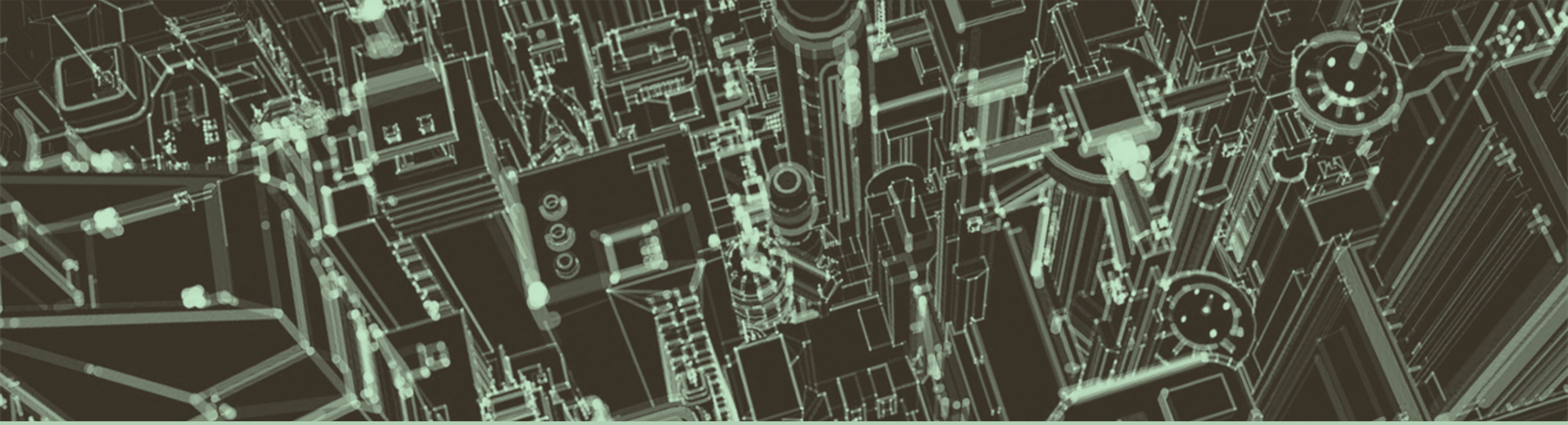
Resolve o problema do incentivo por *medo*

A **PLS** faz oposição ao modelo ultrapassado de incentivo por *medo* de sofrer as consequências da Lei.

Sem o PLS é necessário o uso da **força** para a resolução de conflitos.

Sem PLS:



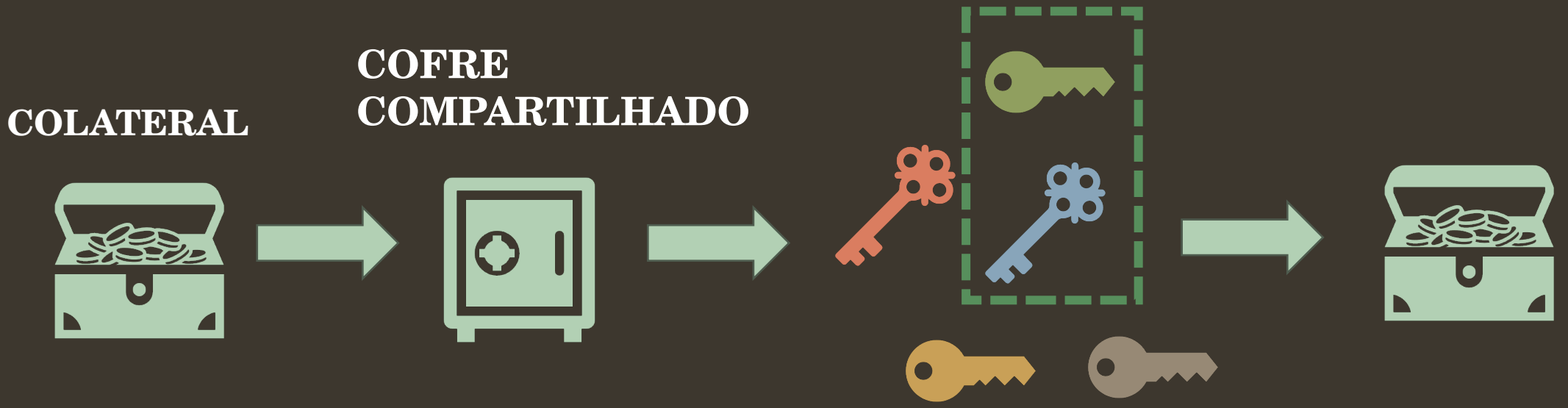


Visão geral do mecanismo

Ainda sem entrar em detalhes práticos

Incentivo financeiro para execução do contrato

O que diferencia o PLS de outros arranjos é o **colateral** (prêmio) que será usado como *garantia* de execução do contrato. Um valor monetário é depositado em um cofre compartilhado que só abre com a colaboração mútua dos envolvidos. Por exemplo: **M** chaves de um total de **N**. Cada chave pertence a cada um dos envolvidos (partes e árbitros).

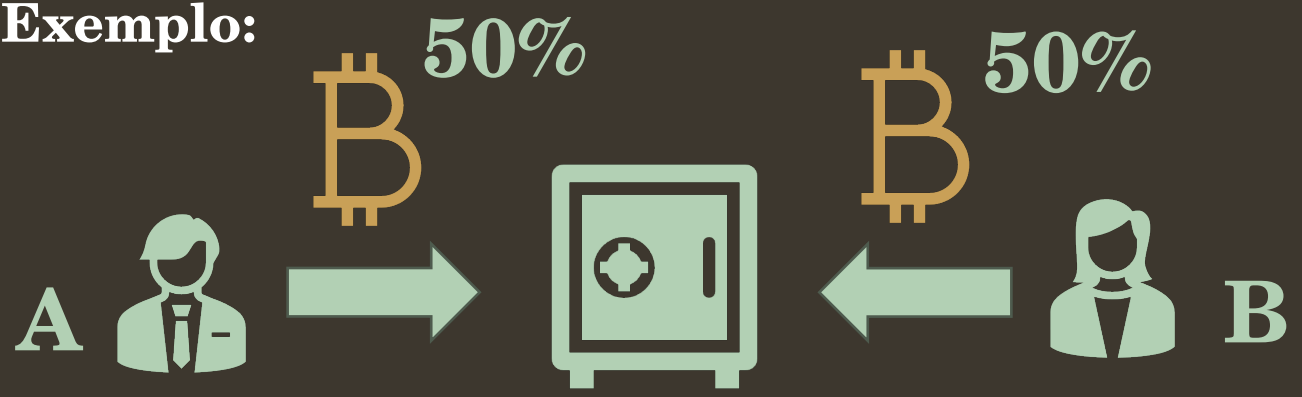


Controle do cofre compartilhado

Uma das partes pode depositar o **colateral** *todo* ou então cada parte deposita uma *fração*, dependendo do que estiver especificado no contrato.

Recomenda-se uma cláusula específica que indica como o colateral será distribuído em caso de cumprimento ou quebra do contrato.

Exemplo:



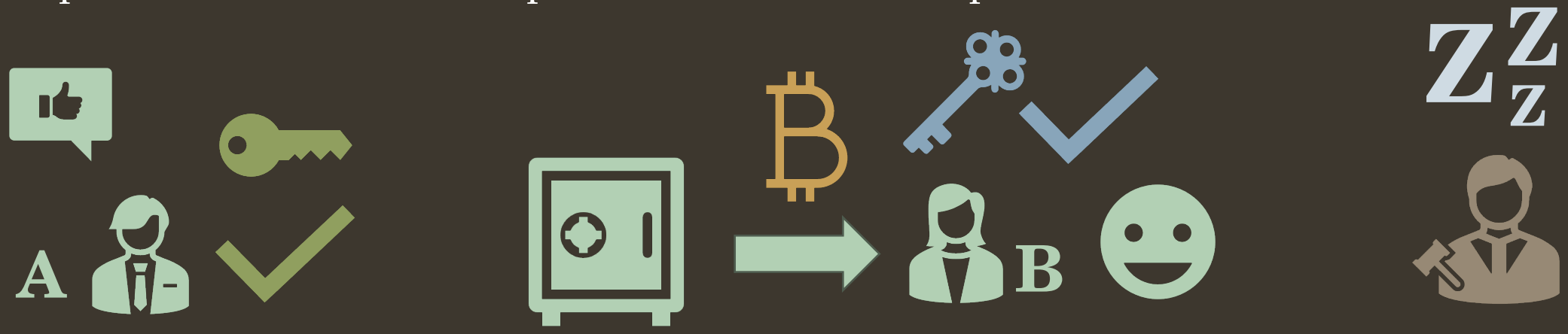
Exemplo de contrato:

Caso o contrato seja cumprido por B respeitando os termos, todo o colateral deve ser enviado para B.

Caso de sucesso

Quando as partes interessadas estão **satisfeitas** com a execução do contrato, basta que elas usem suas chaves para abrir o cofre e direcionar o **colateral** para o local devido. Nesse caso, nenhum árbitro precisa interferir ou participar da transação.

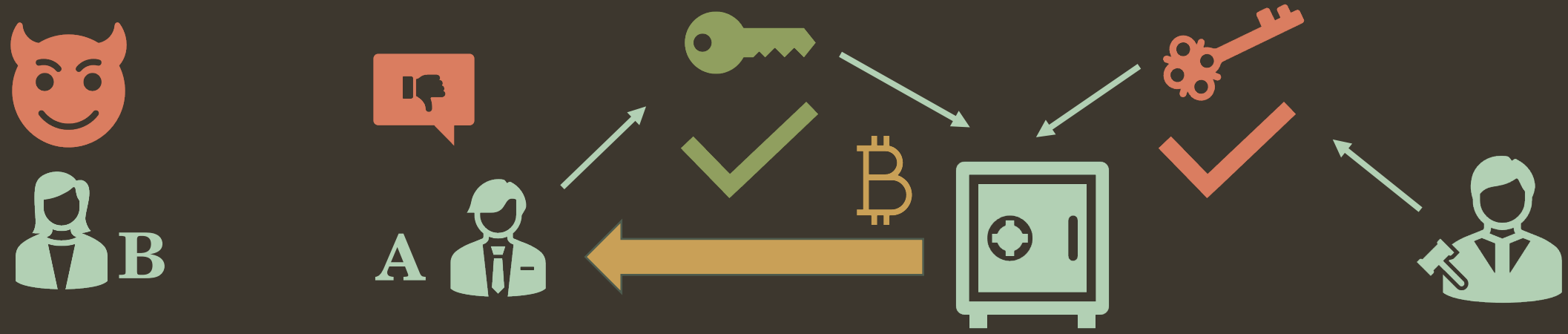
No exemplo abaixo os valores estão indo para B, mas é possível que eles sejam enviados até para um terceiro. Tudo depende de como estiver especificado no contrato.

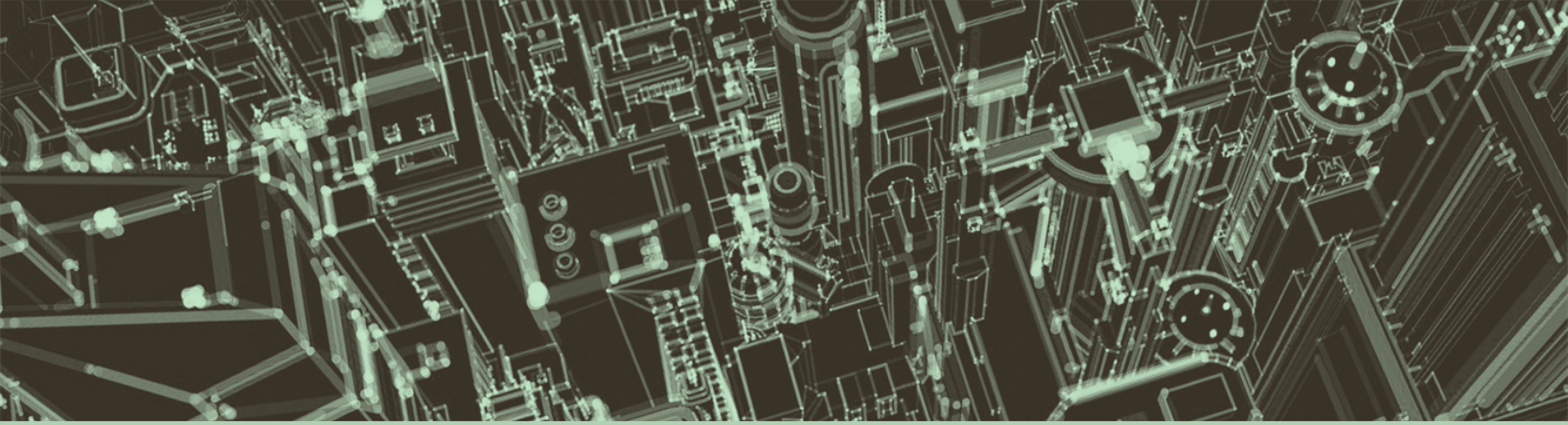


Caso de disputa

Quando uma ou ambas as partes interessadas entram em **conflito** pela discordância da execução do contrato, um árbitro é acionado para que analise a situação, recolha as provas de ambas as partes, faça um julgamento e tome uma **decisão**.

O juiz pode decidir, por exemplo, baseado nas cláusulas do contrato, que o valor todo retorne para A. Nesse caso, A + o árbitro precisam assinar para liberar o cofre.





Passo-a-passo

Como é usar o PLS na prática

O mecanismo é composto por:

1. Duas **partes** interessadas.
2. Um **colateral** que será usado como *garantia*.
3. Um **arquivo** que descreve o *acordo*.
4. Um ou mais **árbitros** previamente eleitos pelas partes.

PARTES

COLATERAL

ARQUIVO (CONTRATO)

ÁRBITROS (JUÍZES)

Passo 1: elaboração da proposta

Uma proposta de contrato deve ser criada em forma de um **arquivo** em qualquer formato como, por exemplo, um arquivo texto (.txt), MS Word (.docx) ou PDF.

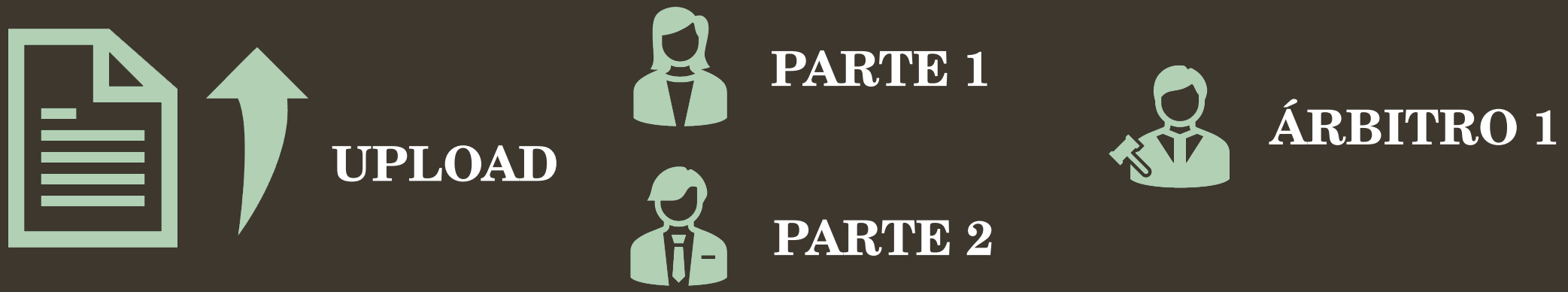
Esse arquivo deve conter as cláusulas e termos em uma linguagem inteligível por todas as partes. Ele pode ser elaborado por uma das partes e proposto à(s) outra(s) parte(s), elaborado em conjunto ou então com a ajuda de um terceiro neutro.

Contrato materializado em forma de arquivo

Passo 2: *upload* & escolha dos envolvidos

Qualquer um dos envolvidos – uma das partes ou algum árbitro – em posse da versão final do arquivo que representa o contrato, pode **submetê-lo** ao sistema PLS.

Essa pessoa escolhe então as partes através de suas **identidades digitais**. No momento, o PLS suporta o protocolo **Nostr** (uma espécie microblog semi-descentralizado).



Passo 3: os envolvidos assinam

Cada um dos envolvidos, incluindo **todas as partes** e **todos os árbitros**, devem entrar no sistema e assinar o documento com suas respectivas **identidades digitais**.

Passo 4: o cofre compartilhado é criado

Com a assinatura de todos os envolvidos, um **cofre** compartilhado é criado.

Logo após a assinatura de todos, cada parte envolvida deve fazer o *download* de um arquivo JSON com os metadados que representam esse cofre.

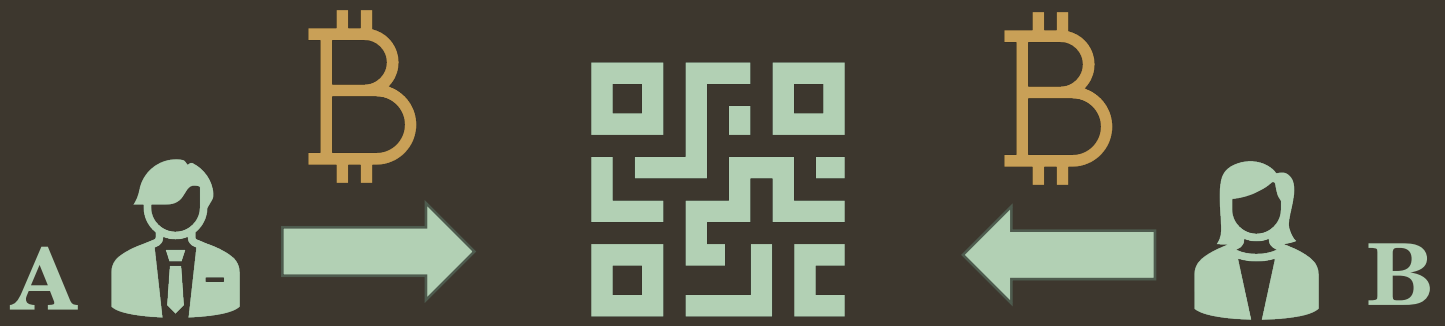
COFRE (JSON)

Cada parte deve guardar esse arquivo em local seguro pois ele será utilizado para acessar o **colateral** durante a resolução de um contrato.

Passo 5: depósito do colateral

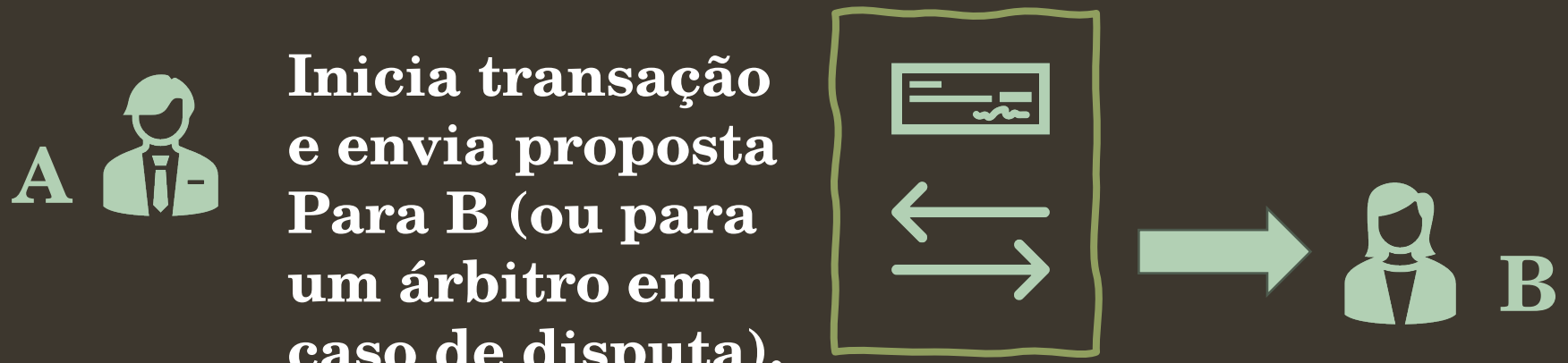
Agora, cada uma das partes tem a oportunidade de depositar uma quantia de **colateral** para servir de *garantia*. Esse valor ficará "congelado" no cofre até que **o quórum mínimo** possa ser atingido para "descongelá-lo" depois. A quantidade e/ou proporção do valor de cada parte depende do que estiver especificado no contrato.

Atualmente, a PLS suporta o depósito em Bitcoin (*onchain*) ou L-BTC (Liquid).

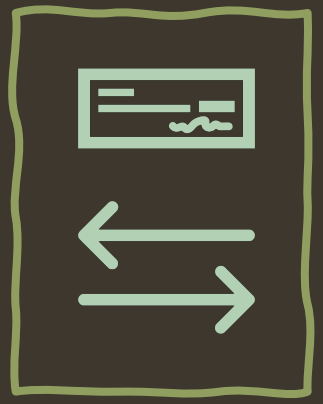


Passo 6: resgate do colateral

Após a execução ou quebra do contrato, uma **transação** é iniciada por qualquer um dos envolvidos (qualquer uma das partes e/ou árbitro(s)) que especifica o destino do colateral. Esse destino pode ser uma ou mais **carteiras** quaisquer. Para que a transação seja efetuada de fato, outra parte e/ou árbitro(s) precisam entrar em acordo e assinar também. Se ninguém entrar em acordo, o **colateral** permanece “congelado”.



Exemplo de transação

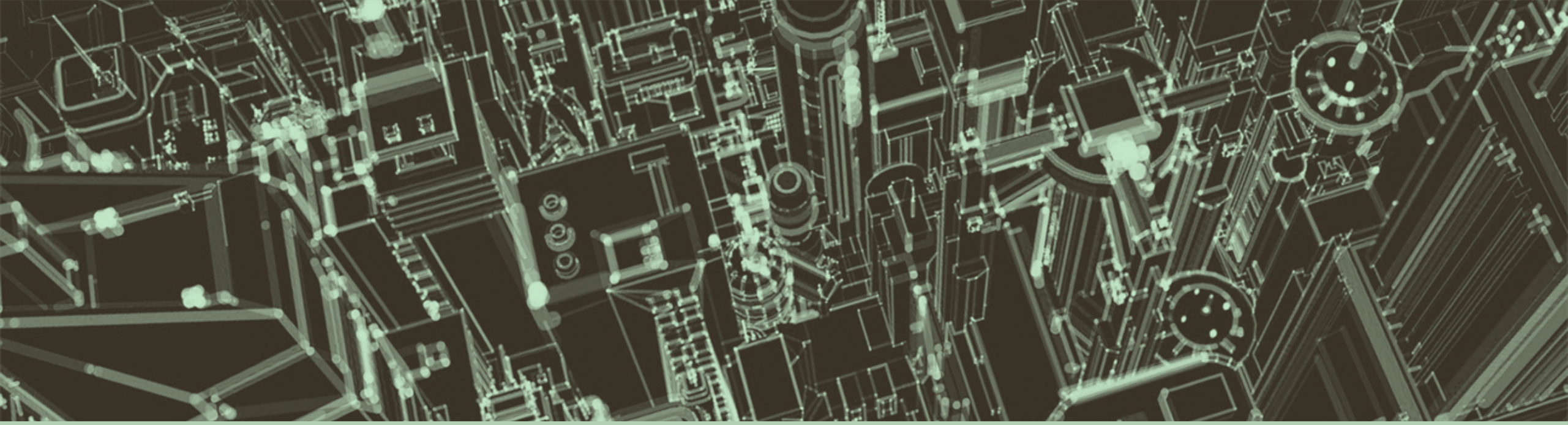


Uma transação pode ser, por exemplo:

- Envia 0,3 BTC para o endereço XPTO.
- Envia 0,1 BTC para o endereço ABCD.
- Envia 0,6 BTC para o endereço DEFG.

ou:

Dependendo da quantidade necessária de assinaturas (**M** de **N**) a transação é aceita e executada na rede Bitcoin ou similar.



Tópicos avançados

Desafios, vantagens e assuntos avançados

Indisponibilidade do colateral

1) Ninguém entra em acordo, o colateral fica “congelado”

Se nenhum dos envolvidos entrar em **consenso** com o *quórum mínimo* de assinaturas exigidas pelo cofre, o colateral pode ficar “congelado”. Porém, há um grande incentivo para que seja atingido um *quórum mínimo:* não é interesse de ninguém que o valor fique completamente congelado.

Para casos extremos, há também uma forma de “resolução por tempo” (ver próximo *slide*).

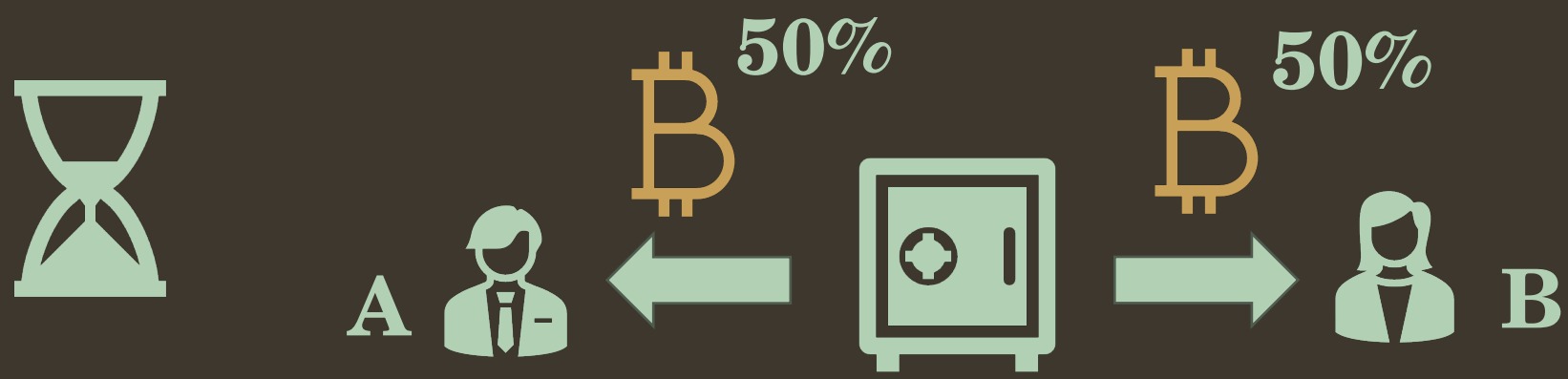
2) Durante a execução do contrato o colateral fica indisponível

O **colateral** (*garantia*) fica indisponível durante a execução do contrato, o que pode ser um problema especialmente se ele for de grande valor ou se o contrato for de longo prazo. Porém, historicamente o Bitcoin tem desempenhado bem frente a moedas fiduciárias em longo prazo, portanto há um incentivo para que se poupe Bitcoin.

Resolução por tempo (*timelock*)

Com o uso da tecnologia *timelock*, o PLS permite a *resolução de um conflito* por **tempo**.

Se ninguém agir após um determinado intervalo de tempo, o contrato “expira” e então uma solução específica (e.g.: devolução do colateral para todas as partes) é executada. Isso poderia ser útil para os casos de, por exemplo: falecimentos ou discordância irredutível.



Vantagens

1) Sem a participação de “autoridades violentas”

Note que no modelo da PLS nenhuma “autoridade violenta” (polícia) precisou ser acionada para que um contrato fosse resolvido em caso de disputa. O incentivo financeiro muitas vezes é suficiente para que as partes colaborem para uma resolução amigável.

2) Sistema incensurável e privado

Note também que o modelo **PLS** é “incensurável” por utilizar protocolos de rede descentralizados como o **Bitcoin** e **Nostr**, sendo praticamente impossível agentes externos interferirem em acordos privados.

Sistema de árbitros e reputação

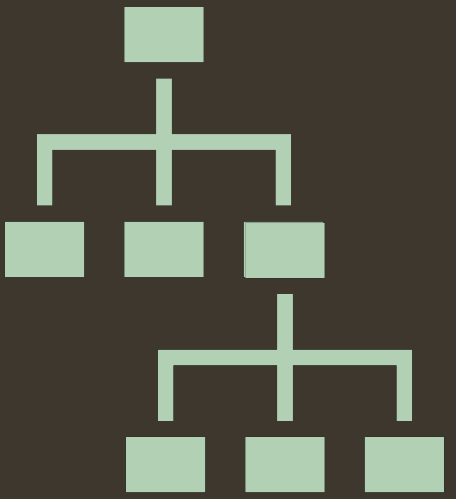
Um *ponto frágil* desse sistema pode ser a escolha dos árbitros. Um árbitro mal escolhido, tendencioso ou indisponível pode arruinar a resolução de um contrato. Dessa forma, é necessário que o ecossistema de **arbitragem** seja aperfeiçoado ao longo do tempo.

Uma possível solução seria a utilização de sistemas de reputação no estilo WoT (Web of Trust), ou então a contratação de empresas profissionais dedicadas a isso e com grande reputação no mercado.

Além disso, o incentivo financeiro do(s) árbitro(s) também é importante: é recomendável que se coloque uma cláusula para um valor pago à arbitragem em caso de disputa, que será retirado do **colateral**.

Scripts personalizados de assinaturas

O arranjo das assinaturas para abrir o cofre compartilhado é tecnicamente feito com *scripts Taproot* (baseado em *árvores de Merkle*), possibilitando arranjos sofisticados e evitando o conluio entre árbitros para acesso indevido ao colateral. **Por exemplo:**



Imagine uma situação com duas partes e 5 árbitros.

- O cofre se *abre* se:
  - As duas partes (mesmo sem árbitros) assinarem.
  - Uma das partes em conjunto com 3 dos 5 árbitros.
- O cofre ***não*** *se abre* mesmo se todos os árbitros assinarem sem uma das partes.

Melhorias de UX / UI

A criação de interfaces que sejam acessíveis a um público leigo é um grande desafio não só ao PLS mas a todo o ecossistema Bitcoin e de sistemas descentralizados em geral.

Com as ferramentas que temos atualmente uma pessoa com pouco conhecimento técnico pode ter certa dificuldade para utilizar o sistema. Começando por – por exemplo – criar uma conta na rede Nostr; e até mesmo manipular o colateral em Bitcoin, que ainda não é uma tarefa fácil para qualquer um.

A interface / experiência do usuário final está em constante evolução e voluntários trabalham para que isso tudo se torne cada vez mais fácil e acessível.

Como usar ou colaborar?

Para usar o sistema PLS e/ou colaborar com melhorias ao projeto *open source*, dirija-se ao site oficial:

`https://www.PrivateLawSociety.net`