Introduction to TumbleBit

BC2 Bootcamp

Nicolas DORIER, CTO, Code Monkey

February 2017

One-Way Payment Hubs in a Nutshell

手短に：片道のペイメントハブ

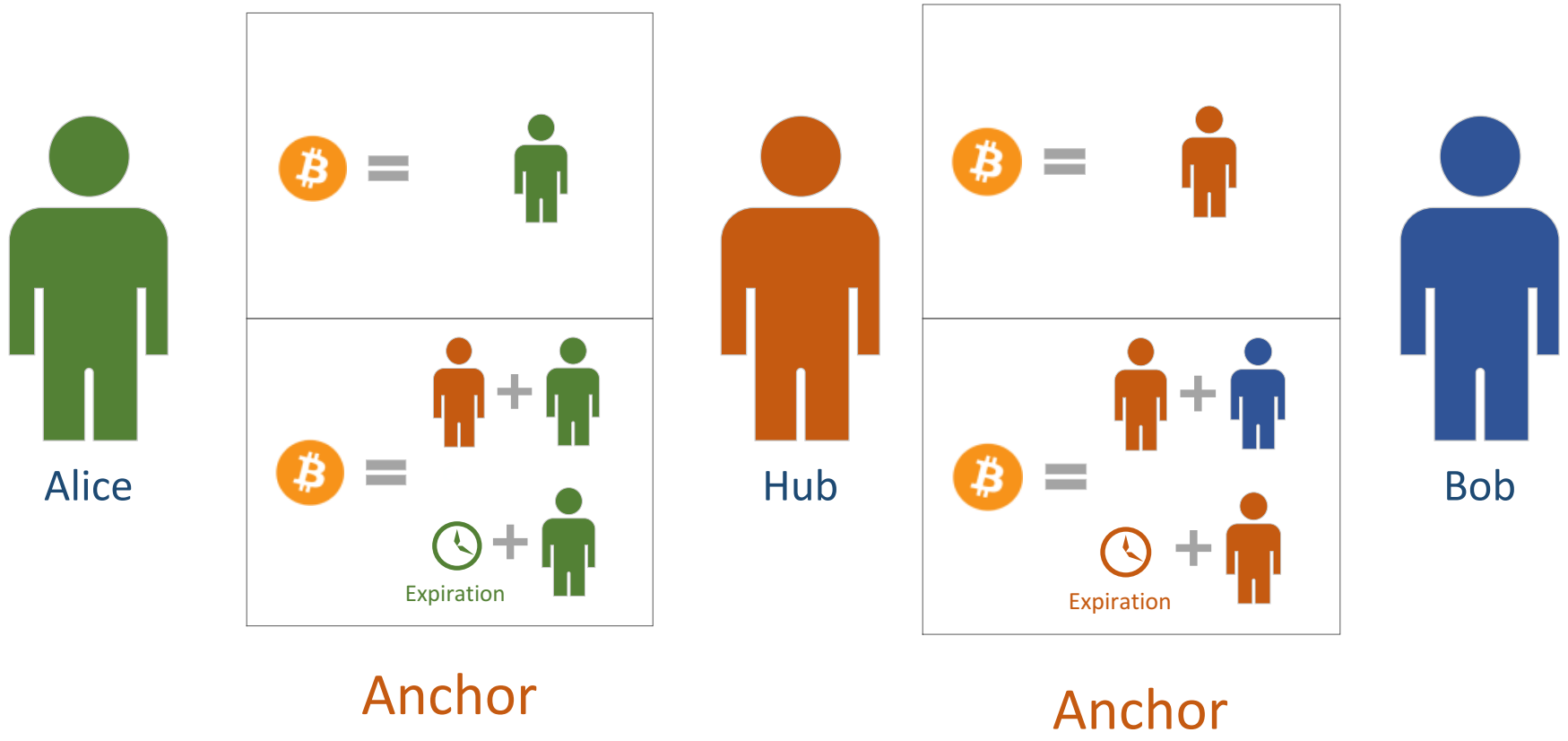
Alice

Hub

Bob

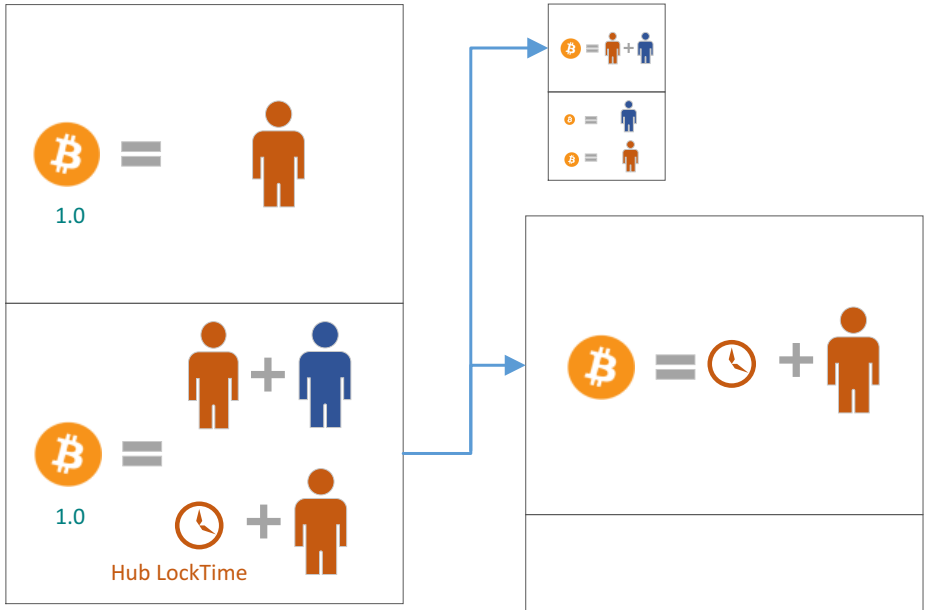
One-Way Payment Hubs in a Nutshell (Channel Setup)

手短に：片道のペイメントハブ（チャネルの設立）



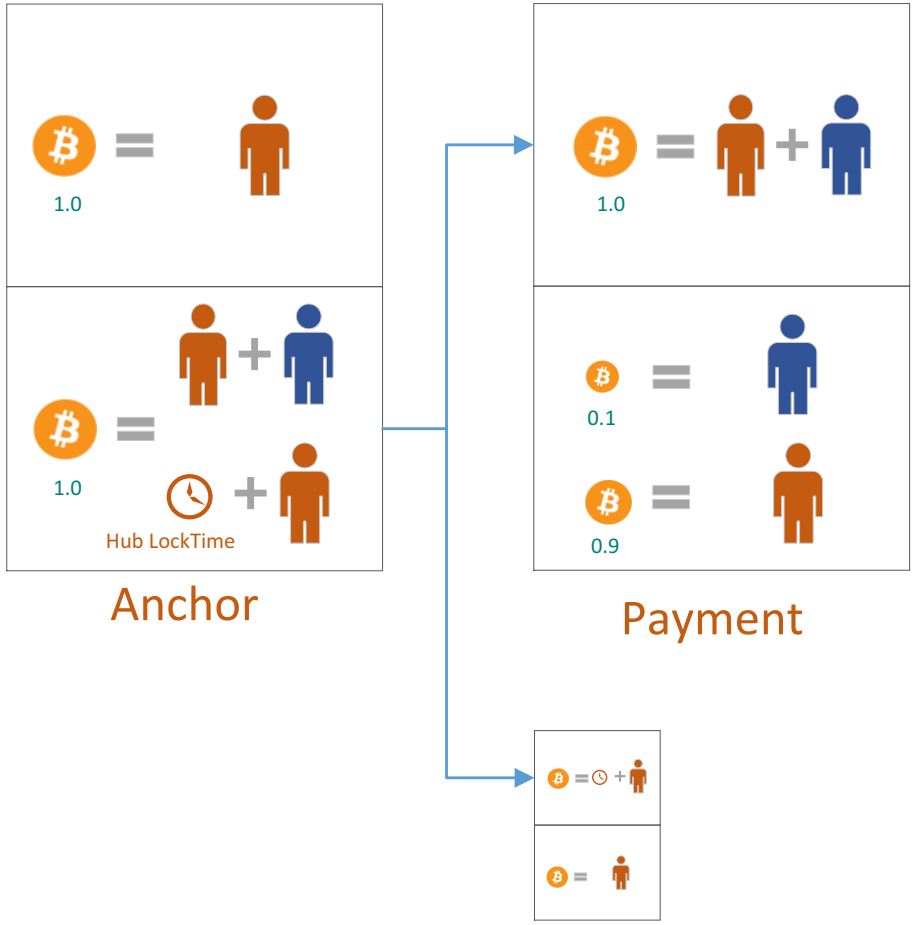
METACO

Bob becomes unresponsive: redeem at timeout
Bobから反応がない：タイムでリディーム



METACO

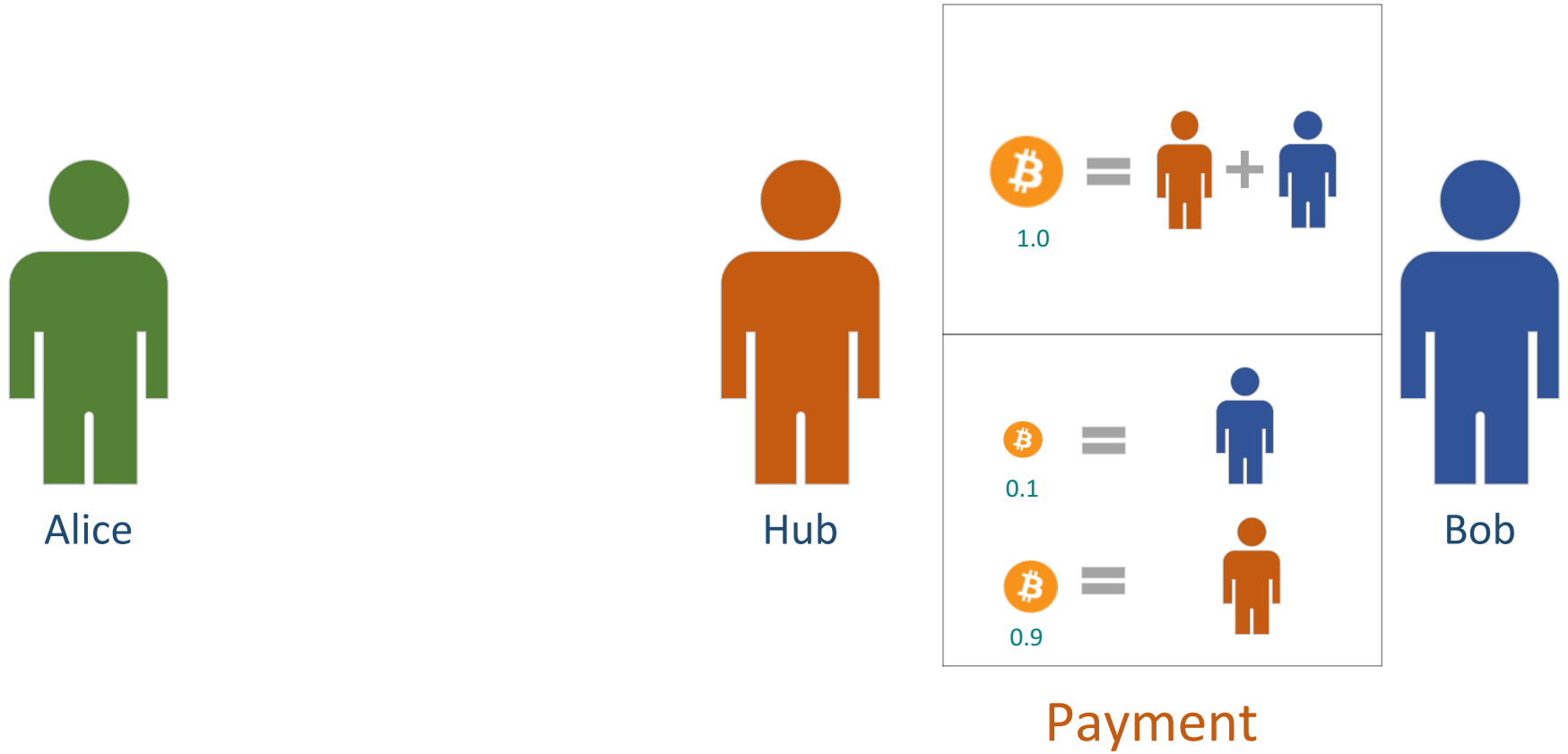
Hub sends money to Bob



METACO

One-Way Payment Hubs in a Nutshell

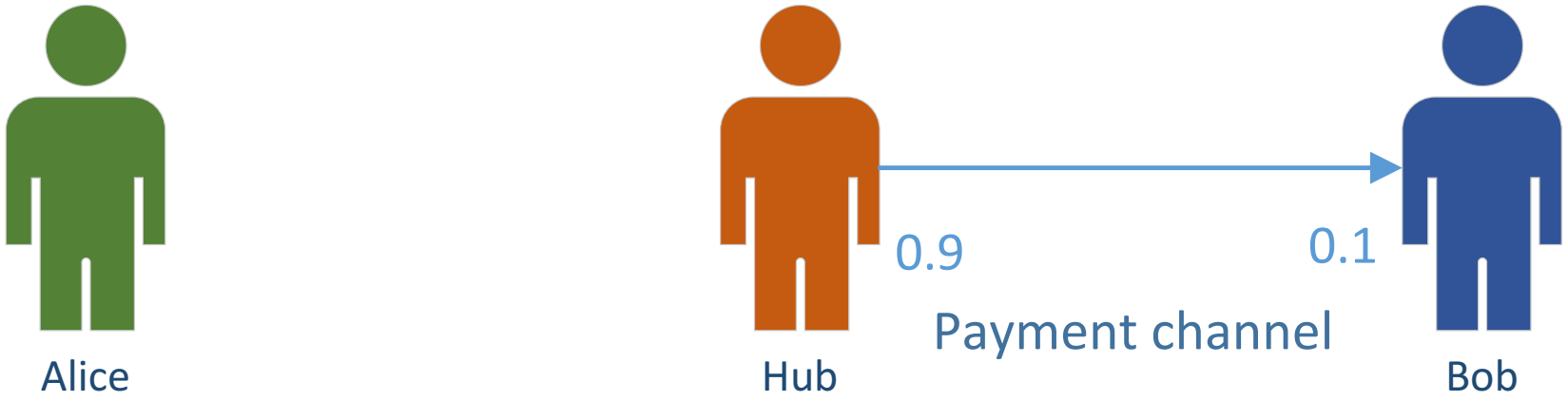
手短に：片道のペイメントハブ



METACO

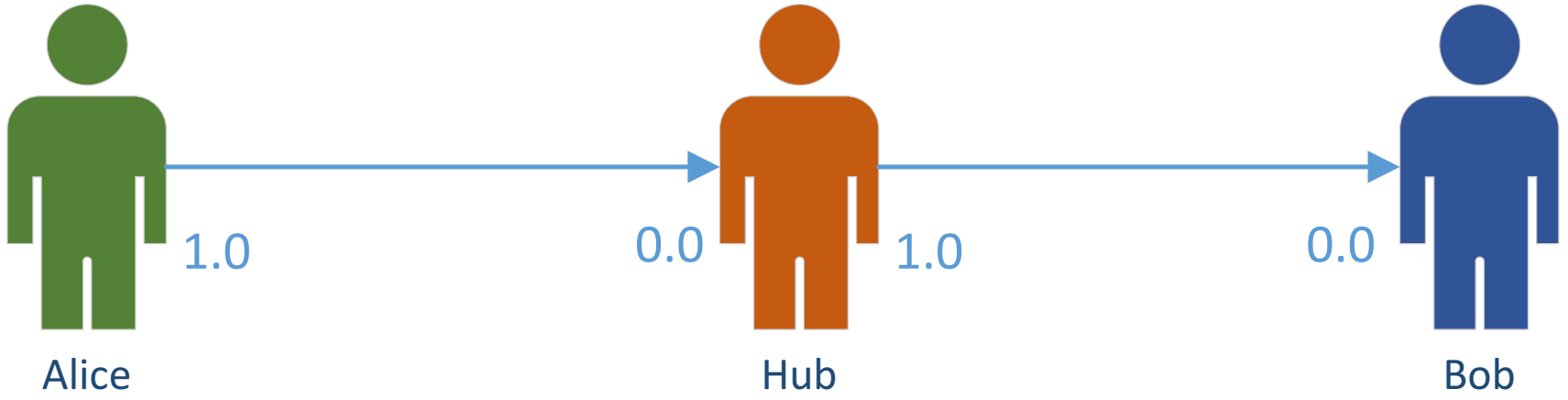
One-Way Payment Hubs in a Nutshell

手短に：片道のペイメントハブ



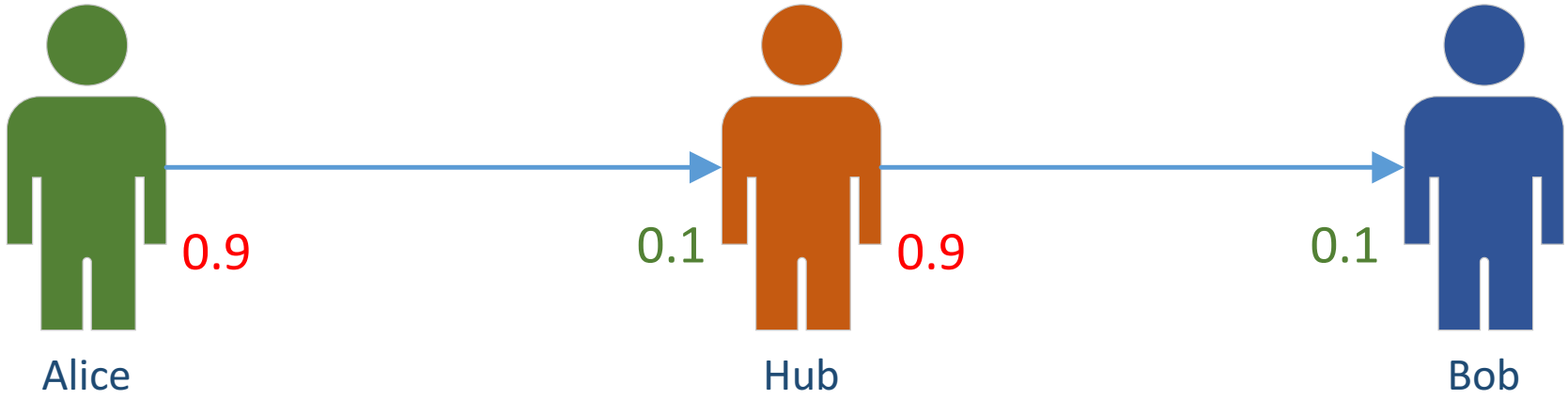
METACO

1. Setup of channel
1. チャネルの設立

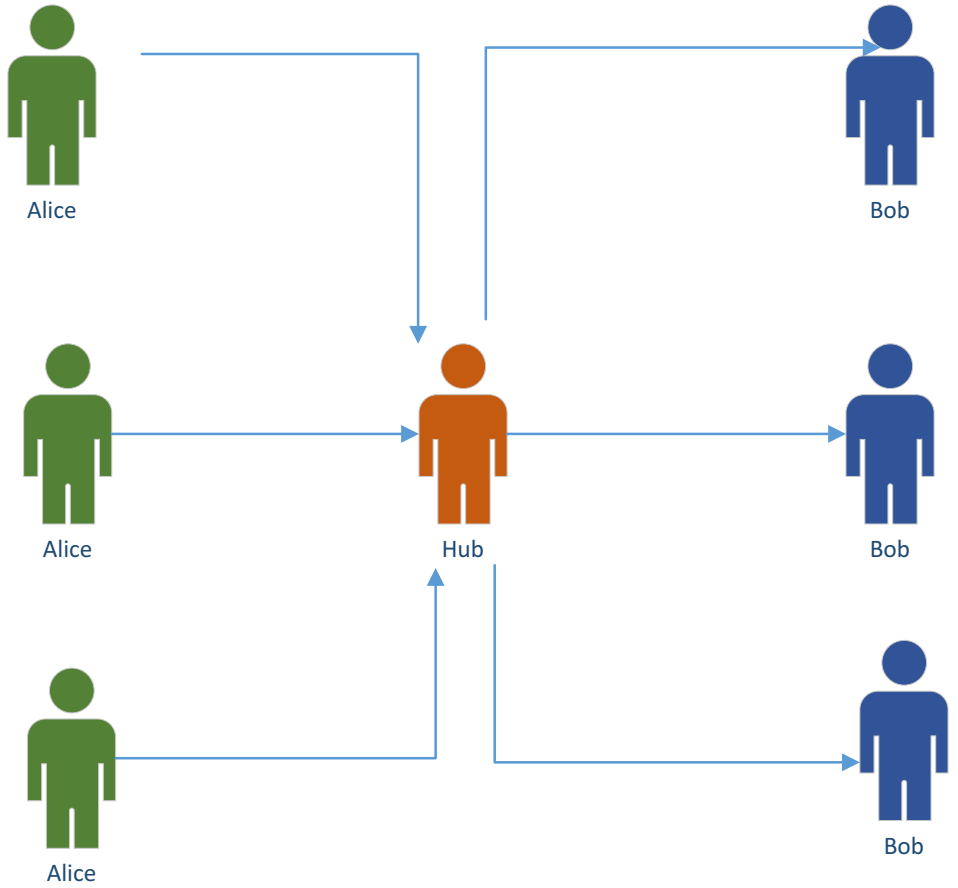


METACO

2. Alice sends to Hub, Hub sends to Bob



All Alices can send money to all the Bobs
全てのAliceが全てのBobに送信出来る



METACO

Problems

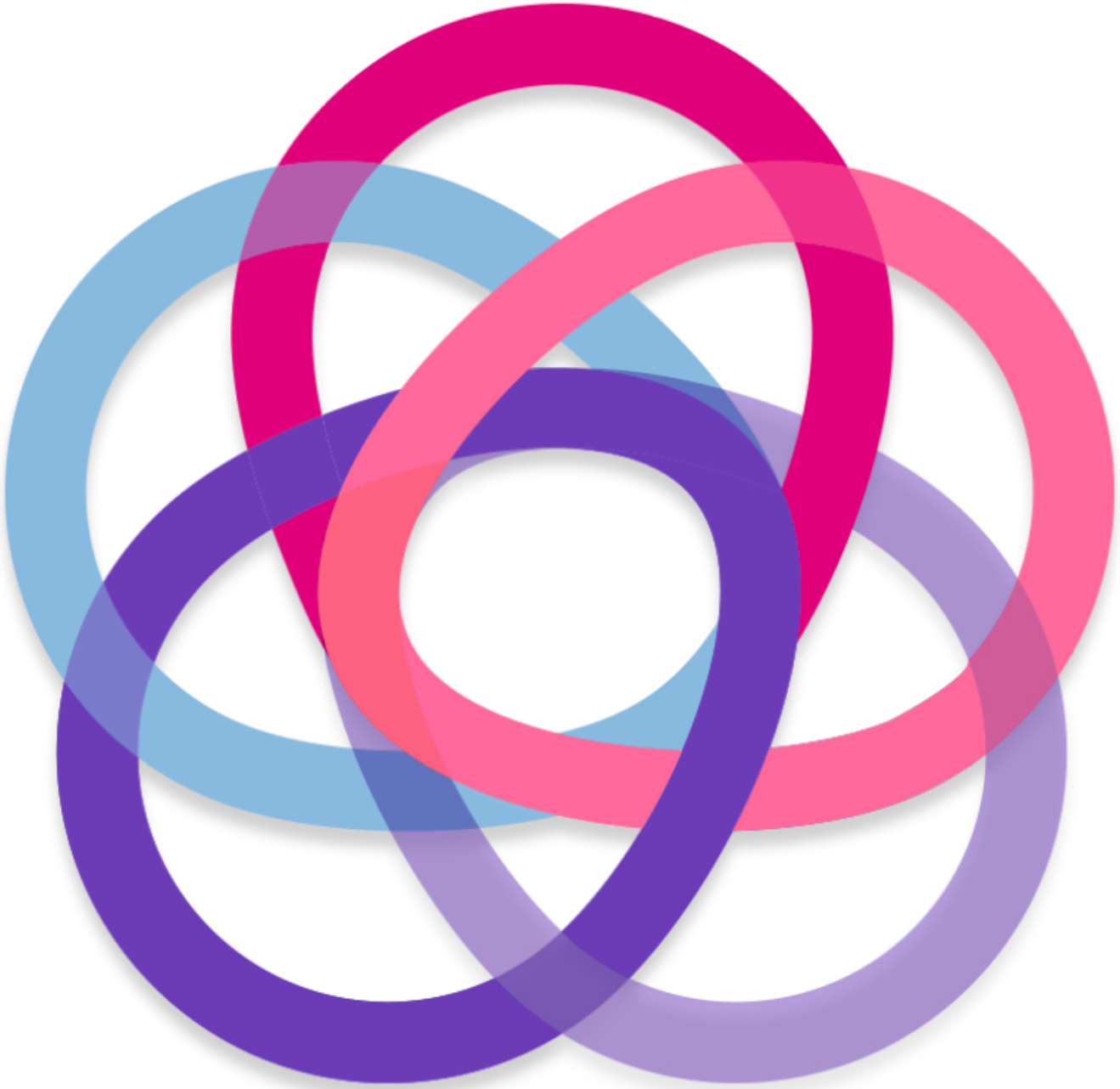
Issues

- Hub can steal money
- Hub knows who sends to who
- Nothing prevents an attacker from creating lots of Bobs so the Tumbler locks all its funds into channels

問題

- ハブがお金を盗める
- ハブは誰が誰に送ったか分かる
- 攻撃者がBobを大量に付けてハブのお金をロック出来る

TumbleBit



METACO

TumbleBit

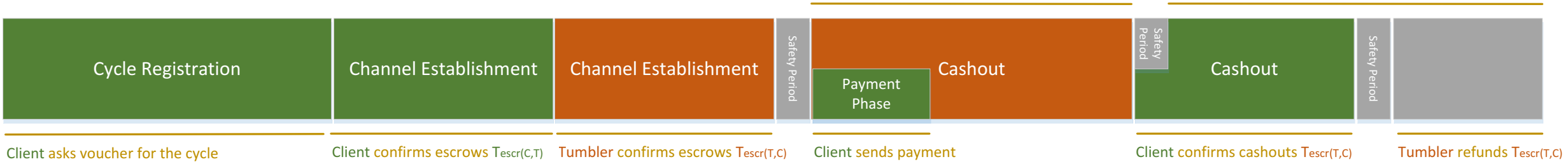
Two modes

- One payment (ie Tumbler Mode)
- Multiple payment (ie Payment Hub Mode)

モードは二つある

- シングルペイメント（タンブラーモード）
- マルチペイメント（ペイメントハブモード）

A Tumbler mode Cycle

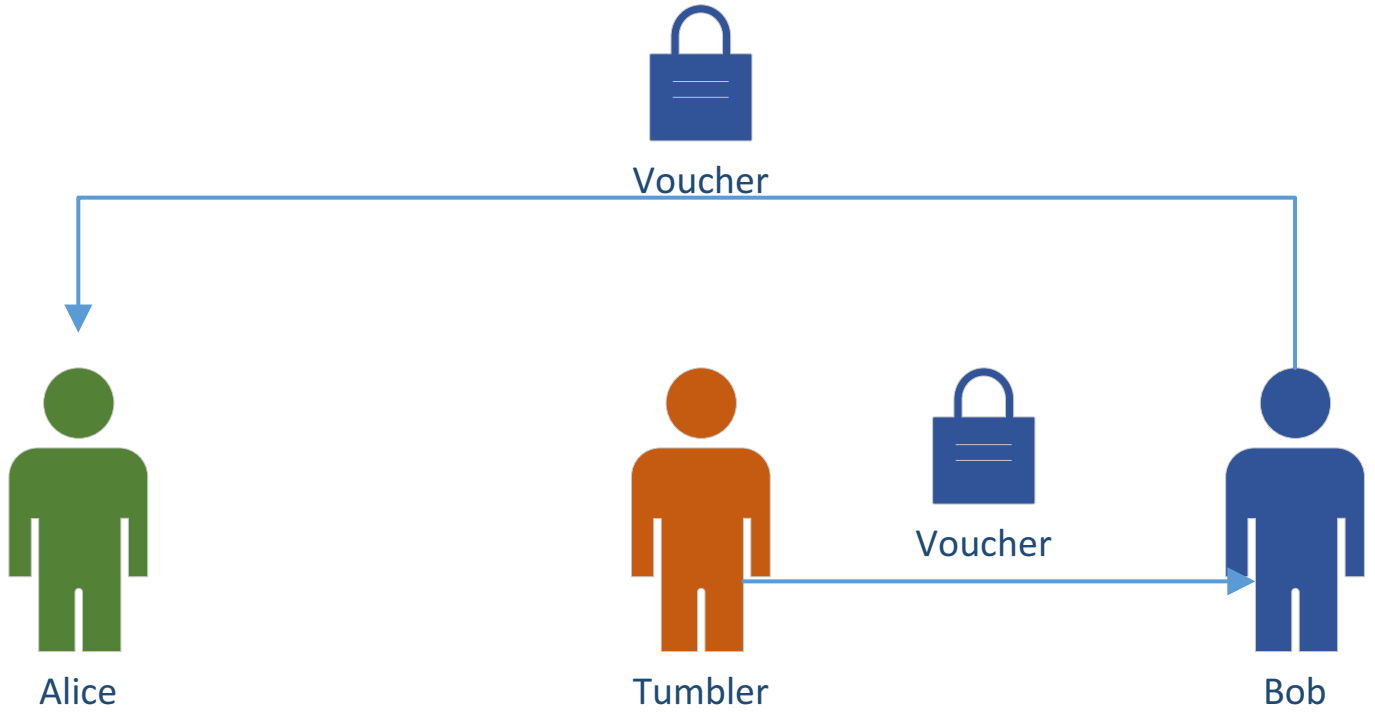


Phases

- Each phase lasts a precise number of blocks.
- Green parts are using the Alice-Tumbler channel
- Orange parts are using the Tumbler-Bob channel

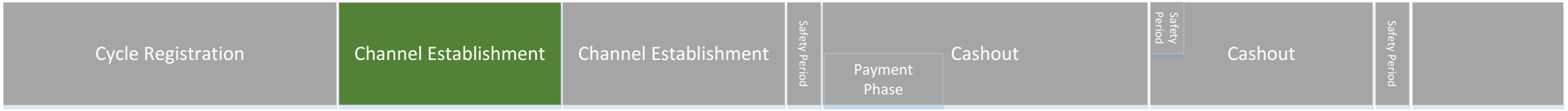
METACO

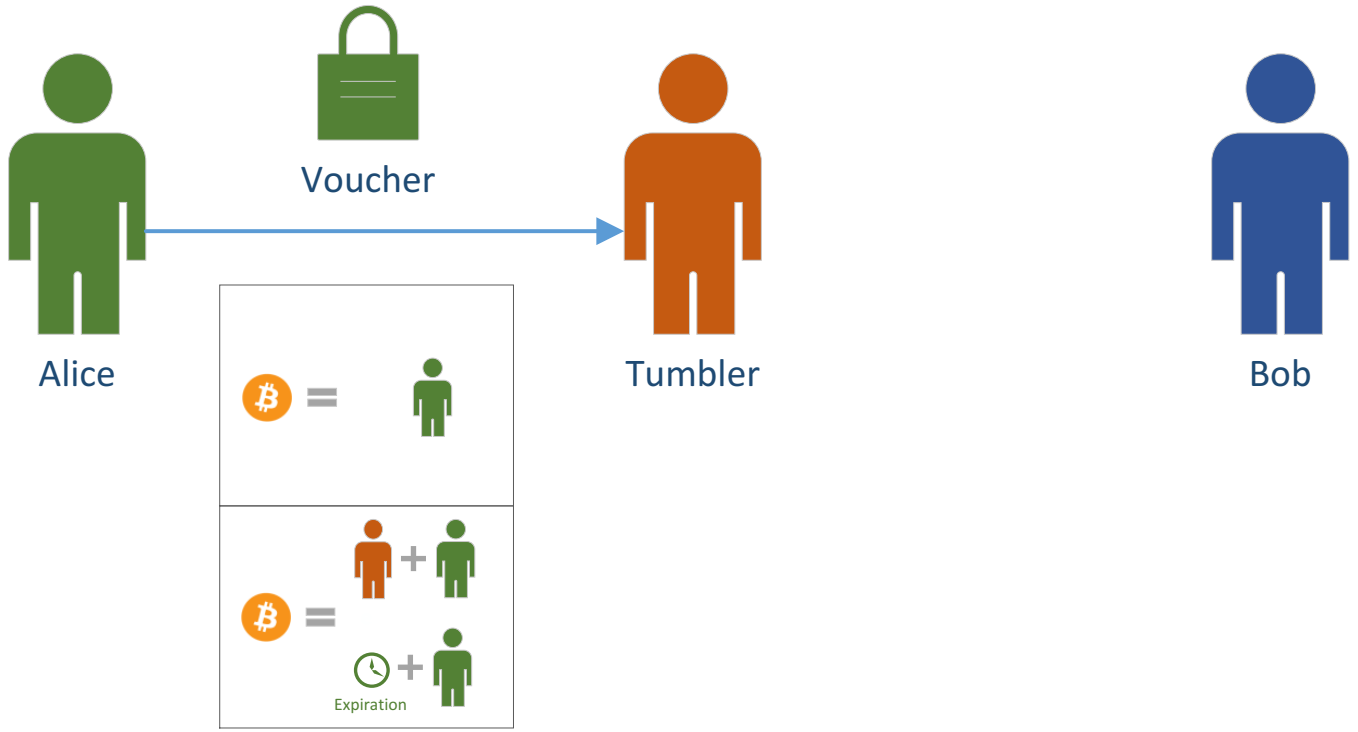
The Registration Phase



METACO

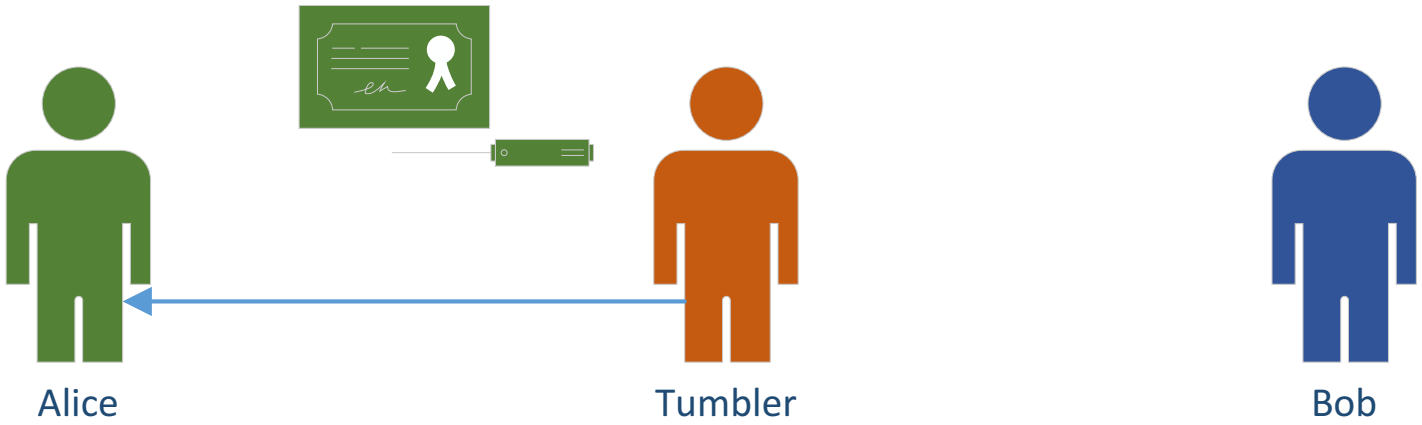
Alice opens channel





METACO

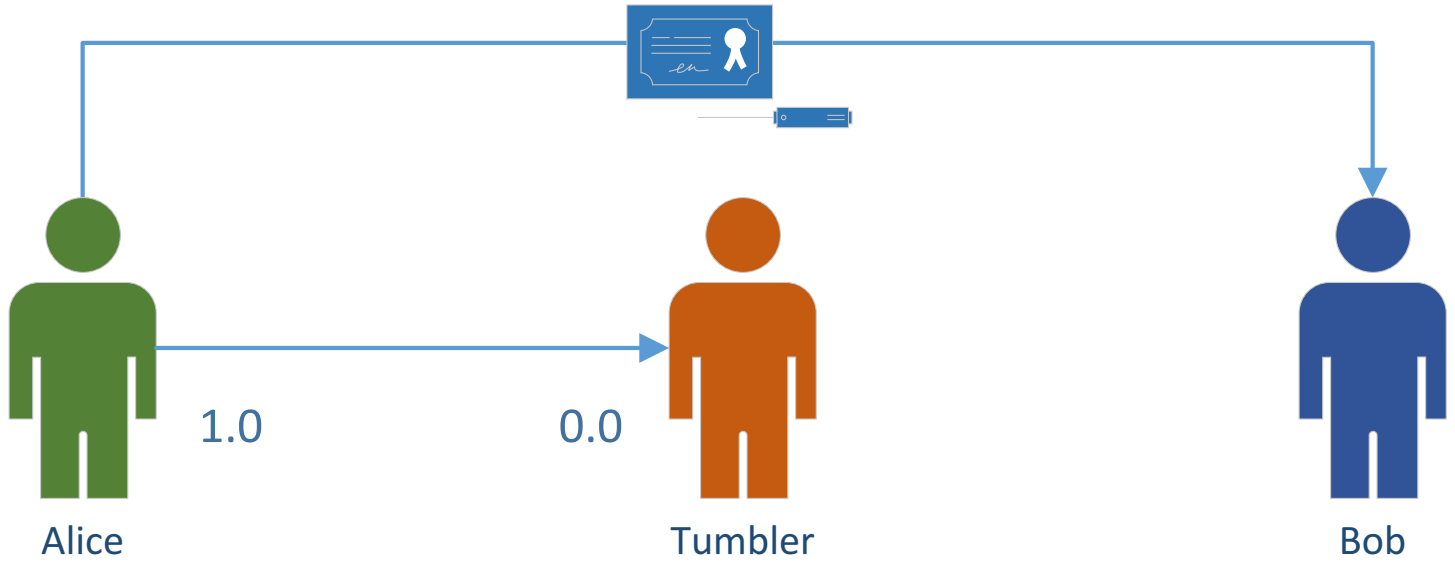
Alice opens channel



METACO

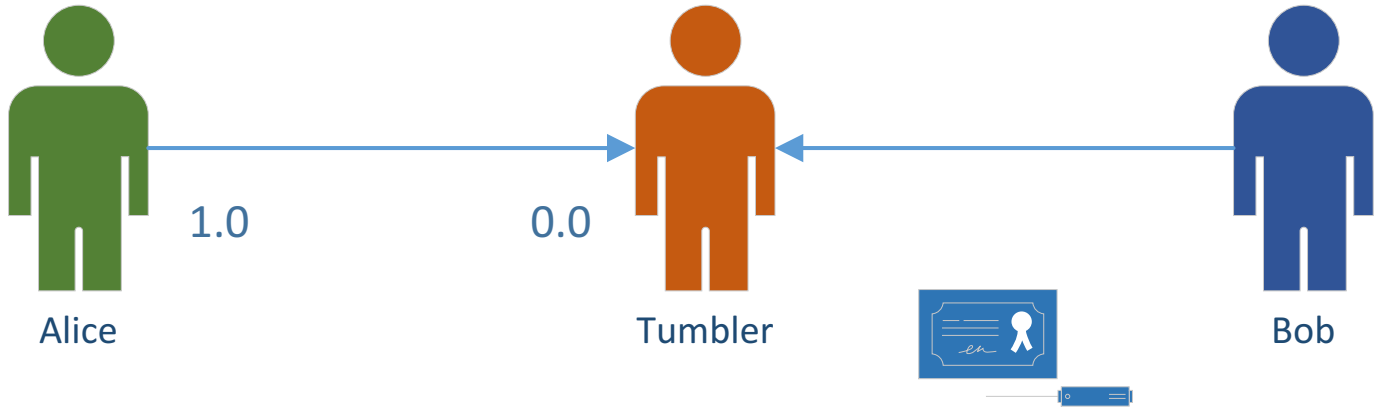
Alice opens channel

Cycle Registration	Channel Establishment	Channel Establishment	Safety Period	Payment Phase	Cashout	Safety Period	Cashout	Safety Period	



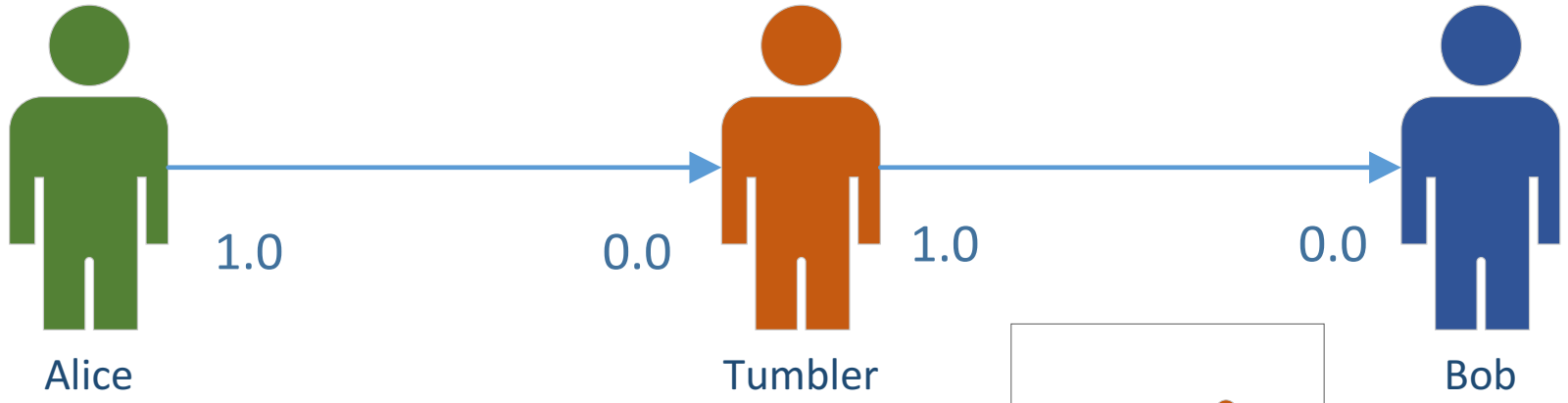
METACO

Tumbler opens channel



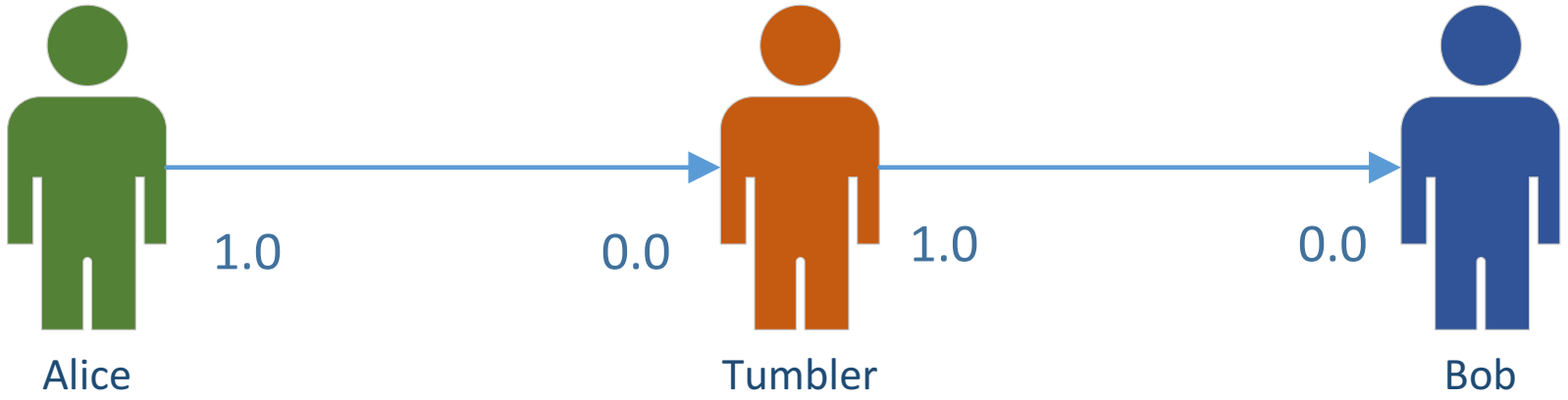
METACO

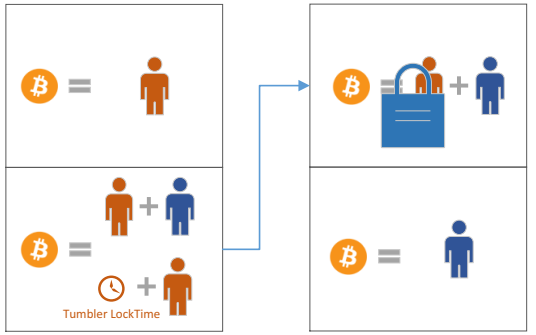
Tumbler opens channel



METACO

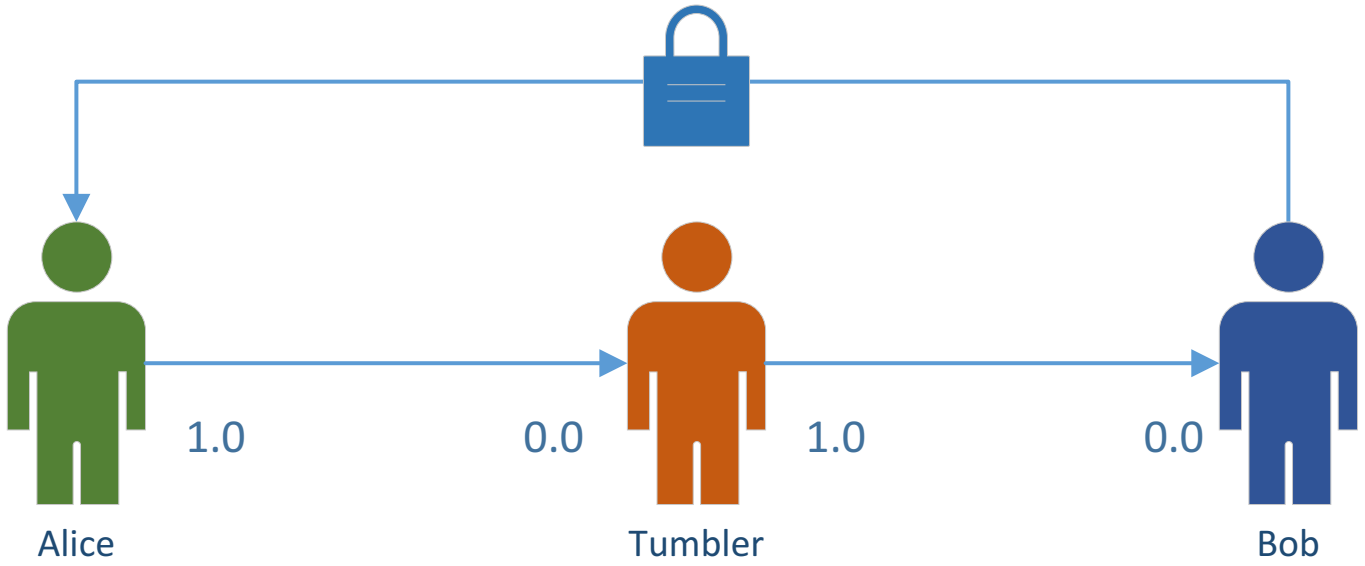
Tumbler opens channel





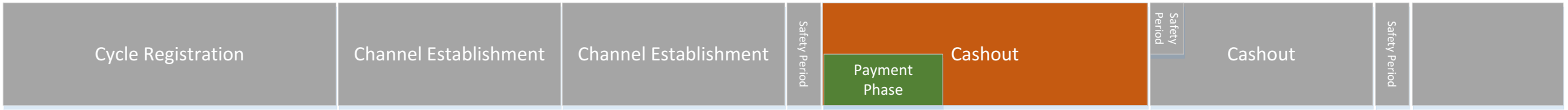
METACO

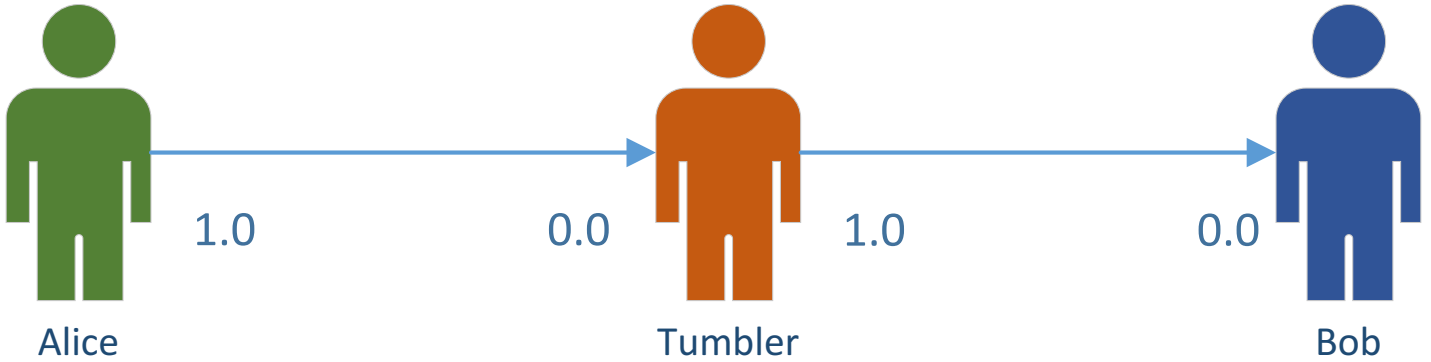
Tumbler opens channel



METACO

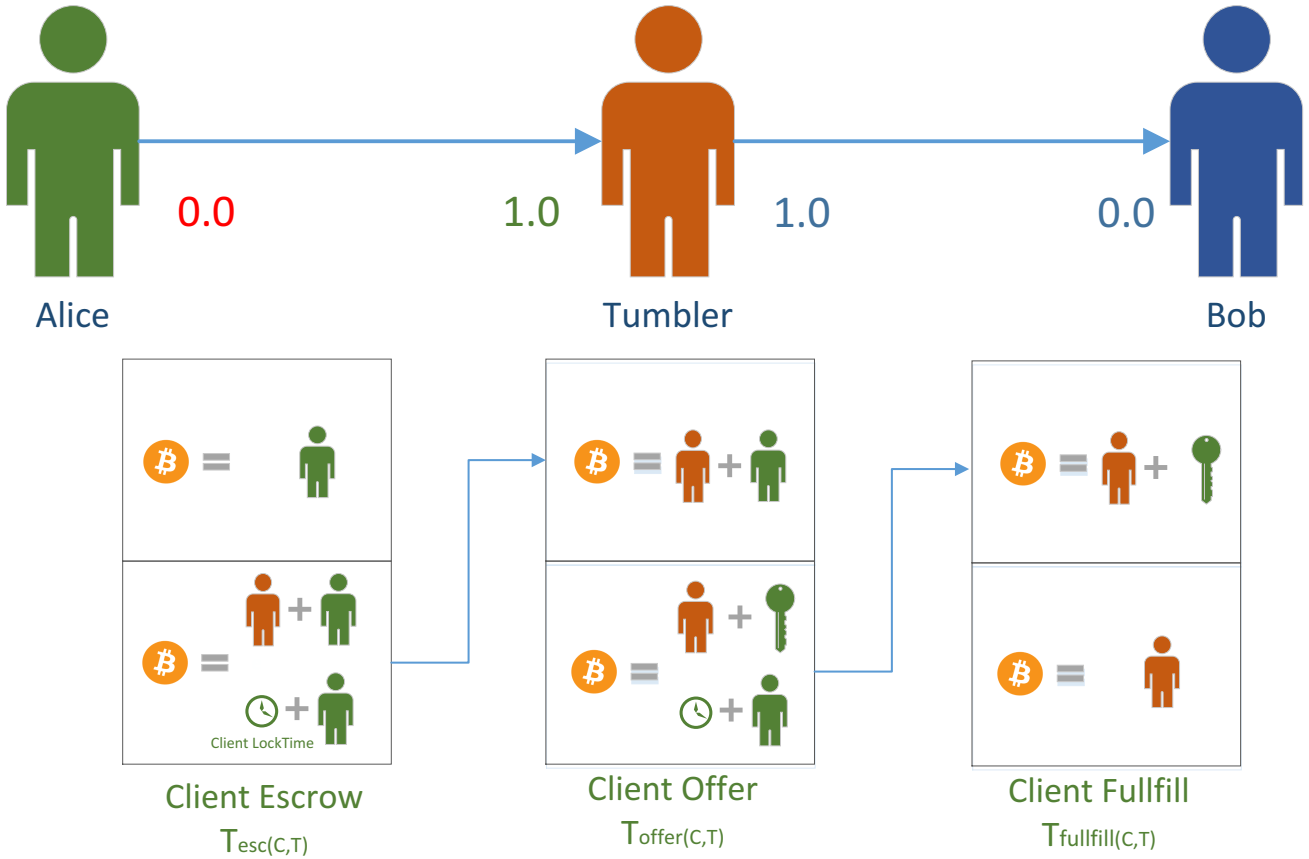
Alice asks payment against the blinded key





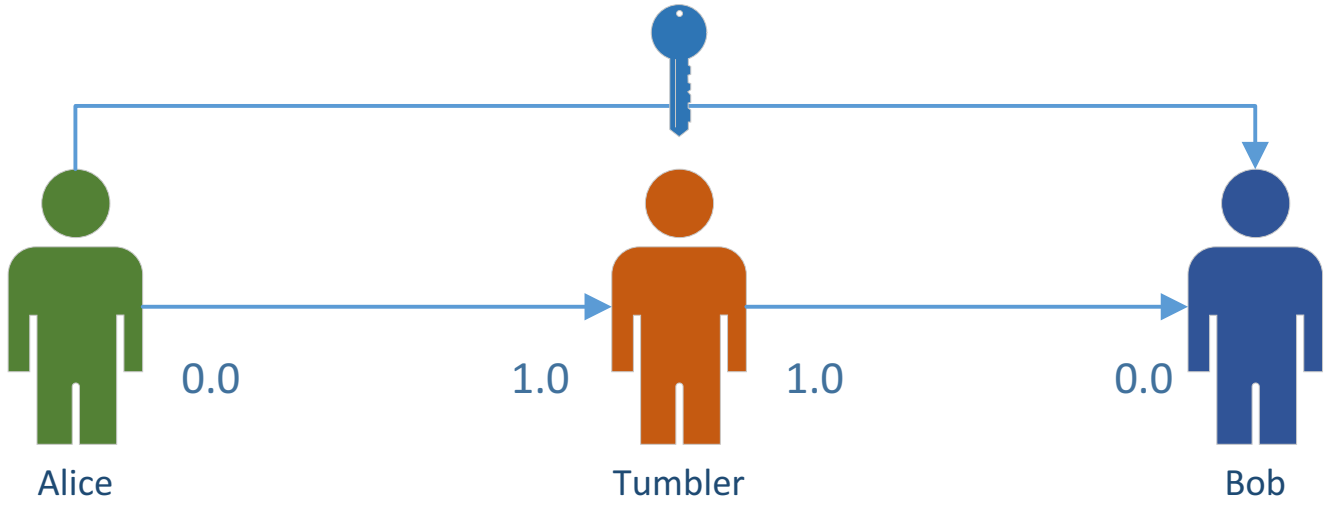
METACO

Alice asks payment against the blinded key



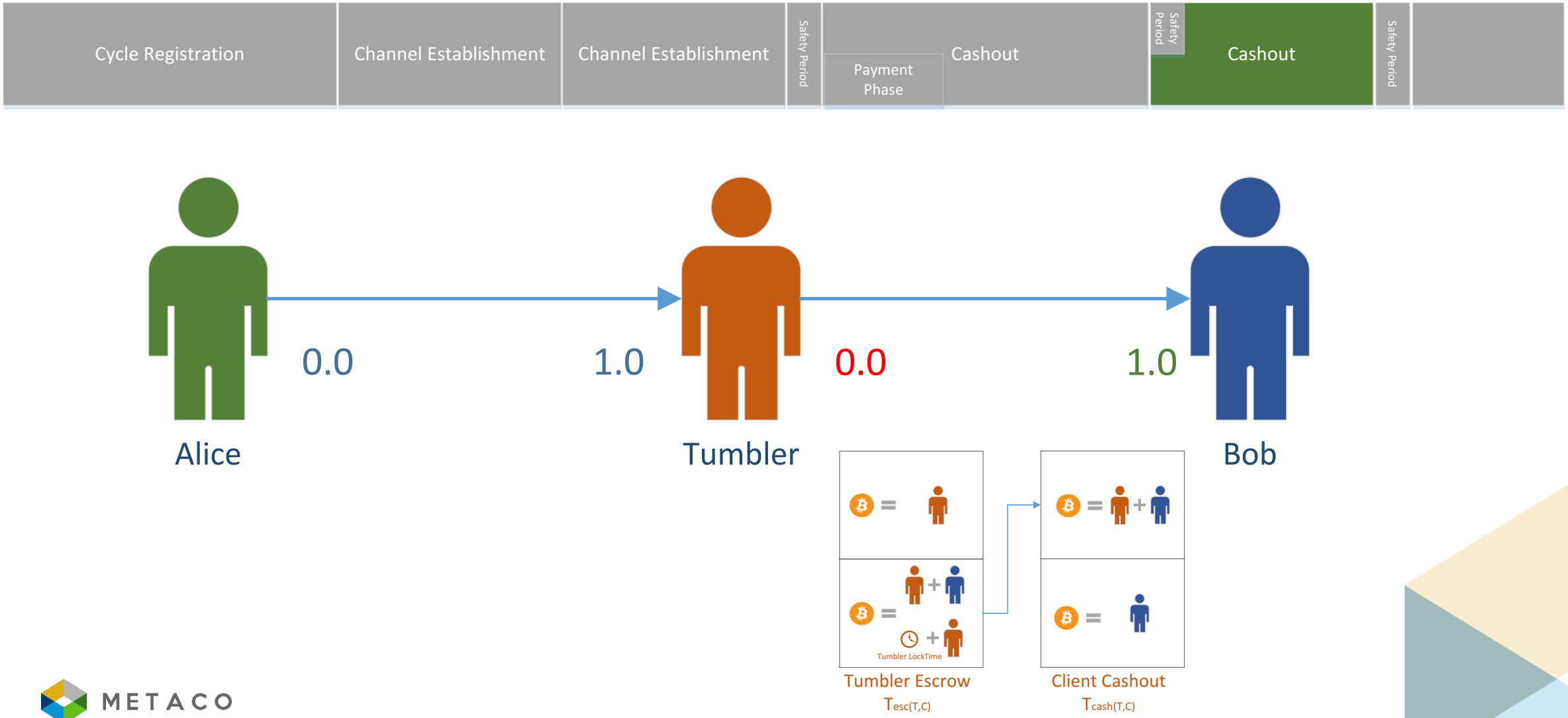
METACO

Alice asks payment against the blinded key



METACO

Bob unlocks the signature with the solution



METACO

TumbleBit

Mystery

- How can Bob be sure that opening the lock will give him access to the Bitcoins?
- How can Alice be sure that the Key she will receive will open the lock?

謎

- Bobがロックを外したらＢＴＣを貰えるということをどうやって確かめる？
- Aliceが貰う鍵でロックを外せるということをどうやって確かめる？

Links

- White paper: https://eprint.iacr.org/2016/575.pdf
- TumbleBit original POC implementation: https://github.com/BUSEC/TumbleBit
- NTumbleBit implementation: https://github.com/NTumbleBit/NTumbleBit
- Blockchain Programming in C#: (also in Japanese) https://www.gitbook.com/@programmingblockchain