Lightning Network
ブロックチェーンを新しいアプリケーションで広げる

Thaddeus Dryja <tdryja@media.mit.edu>

BC2 2017
2017-02-04

ブロックチェーンのスケーラビリティ

- 数億人がどのように、ブロックチェーン（例えば、ビットコイン）を使える？
- 多数のブロックチーンで、どのように交換出来る？

スケーラビリティの問題

- 全ての機械が、全ての取引を保存してる
- インターネットが、一つの無線LANの機械のように、遅くなる
- 全員の同意を得ることは大切だが、非効率的である

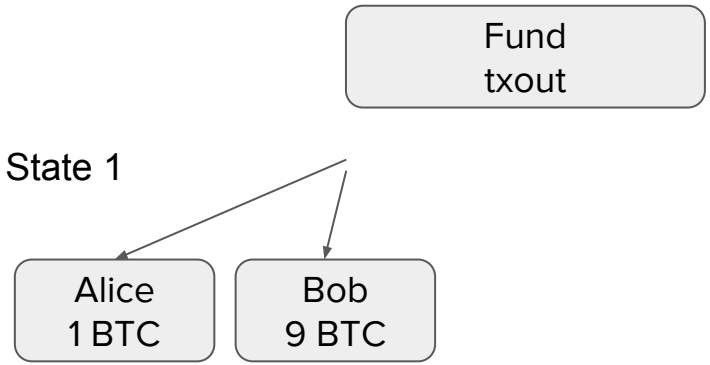
スケーラビリティの問題

- 全ての機械が、全ての取引を保存してる
- インターネットが、一つの無線LANの機械のように、遅くなる
- 全員の同意を得ることは大切だが、非効率的である

スケーラビリティの解決

- システムの通信量を増やす
- 2倍、4倍ぐらいは可能
- 802.11g → n → ac
- ネットワークを分ける (多くのルーター)
- 同じセキュリティ？
- 他のアプリケーションはできる？
  (特に、マイクロペイメント)

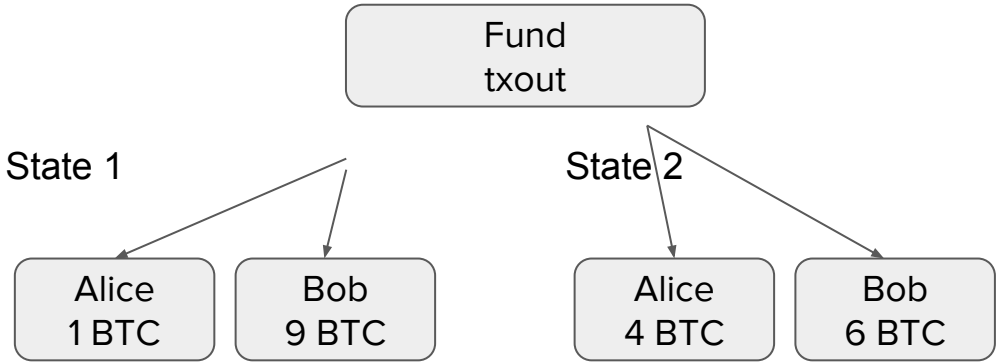
ペイメント　チャンネルとは



Alice と Bob がブロックチェーンに通信せずに、2人で署名を交換する。
チャンネルが開いている間、自分の残高が減って、相手の残高が増えてお金送れる。

いつでも、相手の協力にかかわらずに、チャネルを閉められる。
一番最近の残高をブロックチェーンに送信して、両方の人の最後の残高が決定する。

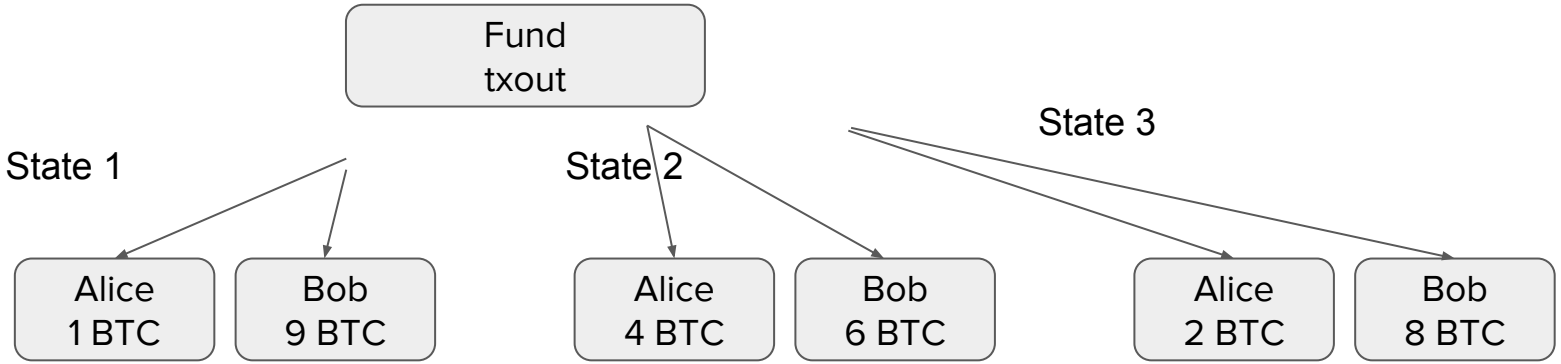
ペイメント　チャンネルとは



Alice と Bob がブロックチェーンに通信せずに、2人で署名を交換する。
チャンネルが開いている間、自分の残高が減って、相手の残高が増えてお金送れる。

いつでも、相手の協力にかかわらずに、チャネルを閉められる。
一番最近の残高をブロックチェーンに送信して、両方の人の最後の残高が決定する。

ペイメント　チャンネルとは



Alice と Bob がブロックチェーンに通信せずに、2人で署名を交換する。
チャンネルが開いている間、自分の残高が減って、相手の残高が増えてお金送れる。

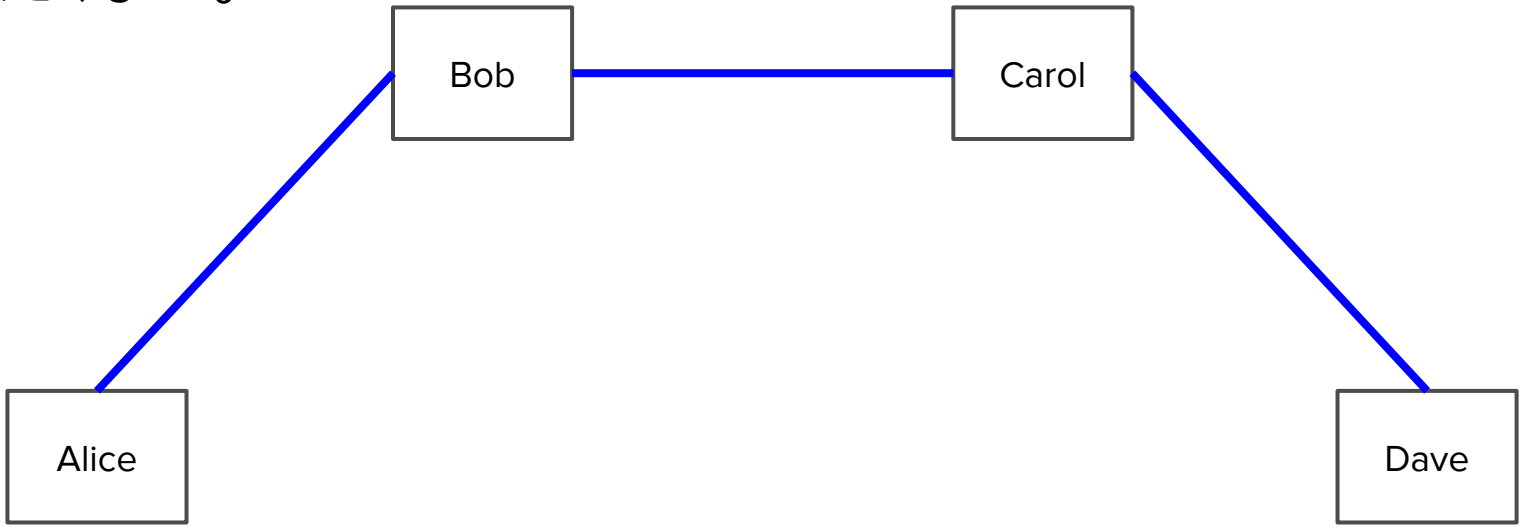
いつでも、相手の協力にかかわらずに、チャネルを閉められる。
一番最近の残高をブロックチェーンに送信して、両方の人の最後の残高が決定する。

複数のチャンルによるネットワーク

- 一つのチャンネルは、２人の人（又は機械）を繋げる。2つのブロックチェーンの取引で、何回もチャンネルで取引出来る
- 多くの取引は、口座を作る必要がなく、１回だけの支払い
- そういう場合に、多数のチャンネルが繋がって、チャンネルネットワークを作る

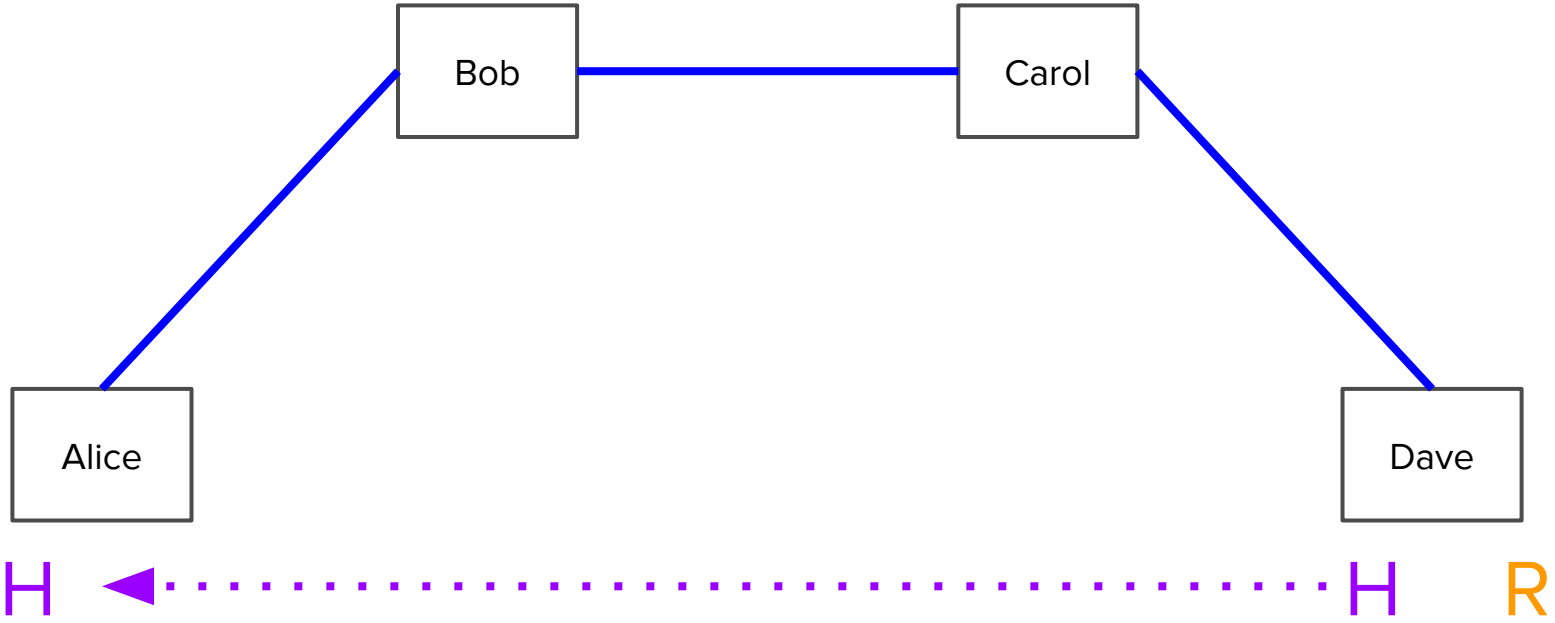
チャンネルネットワークの動き方

Aliceが Daveにお金を送りたい。しかし、新しいチャンネルを作りたくない。



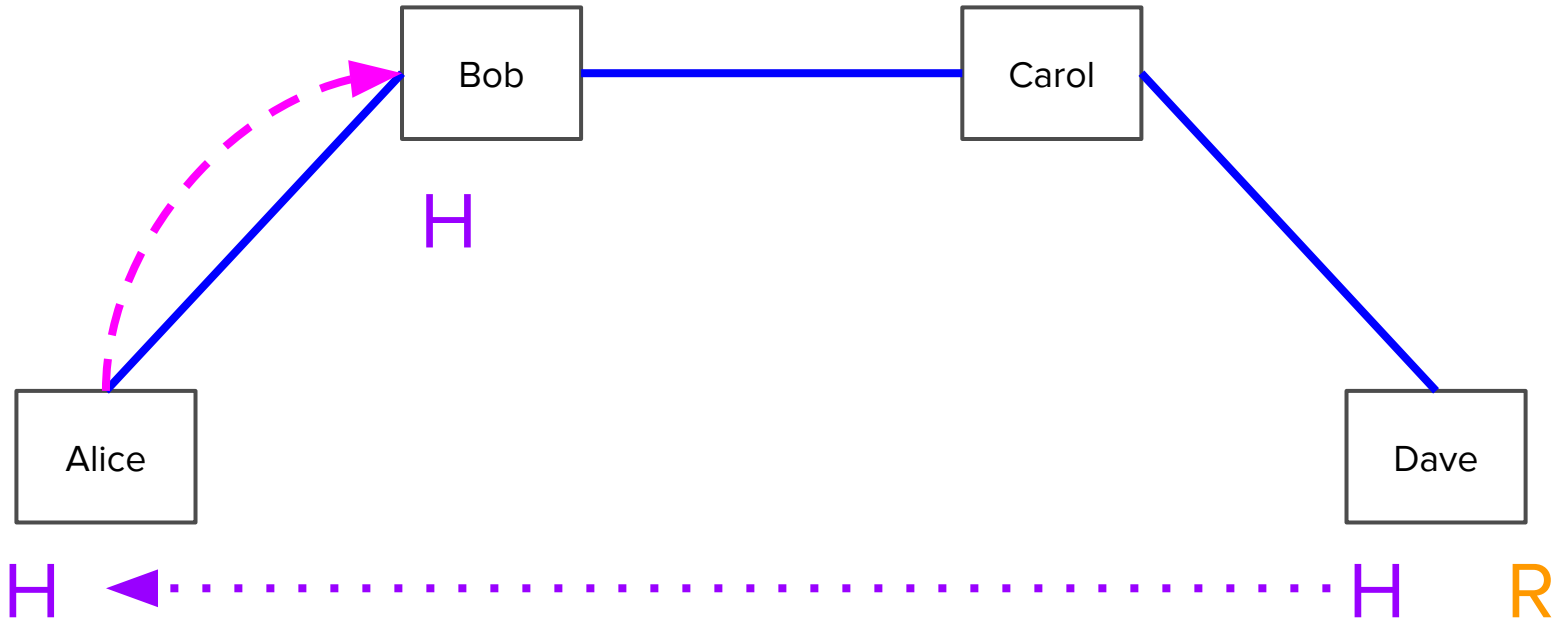
チャンネルネットワークの動き方

まずは、Daveがランダムな数字を作って（R）、その数字をハッシュする（H）
AliceがDaveからHをもらっている



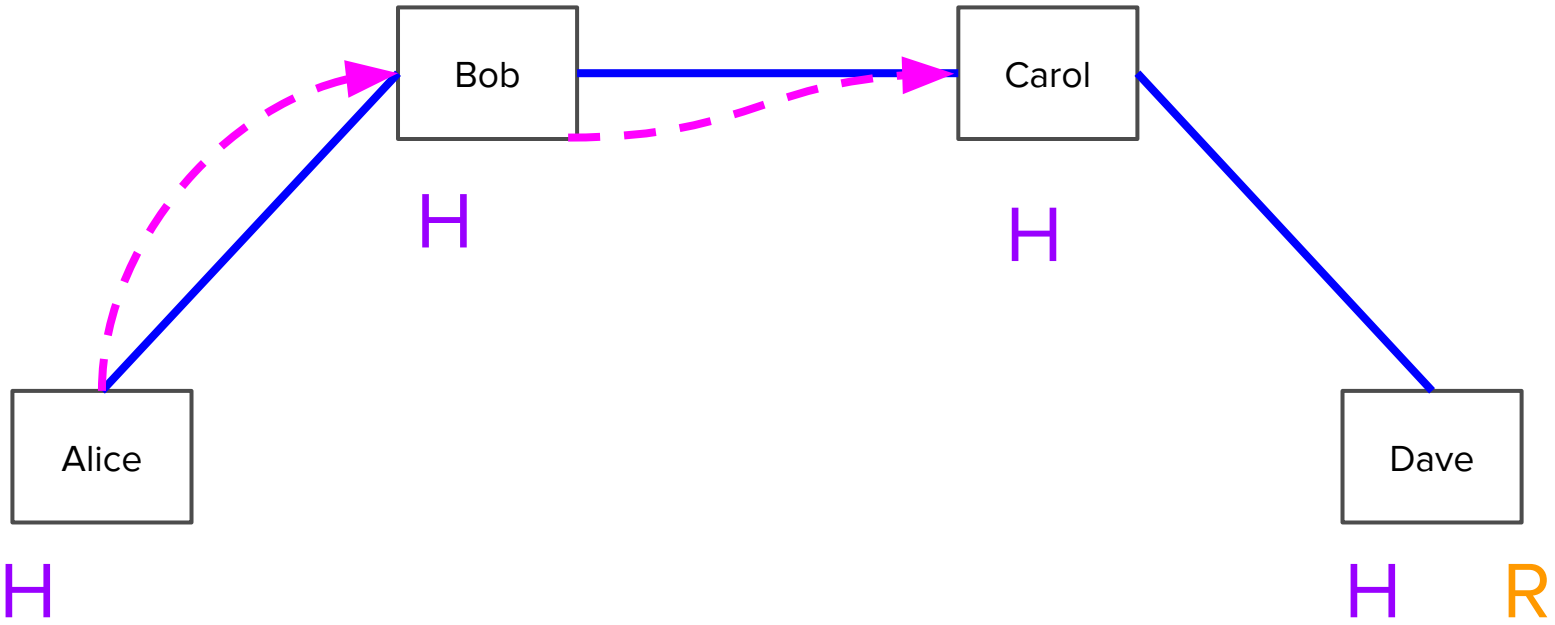
チャンネルネットワークの動き方

Alice が Bobに払う。しかし、BobがRを知らないとお金を貰えない。



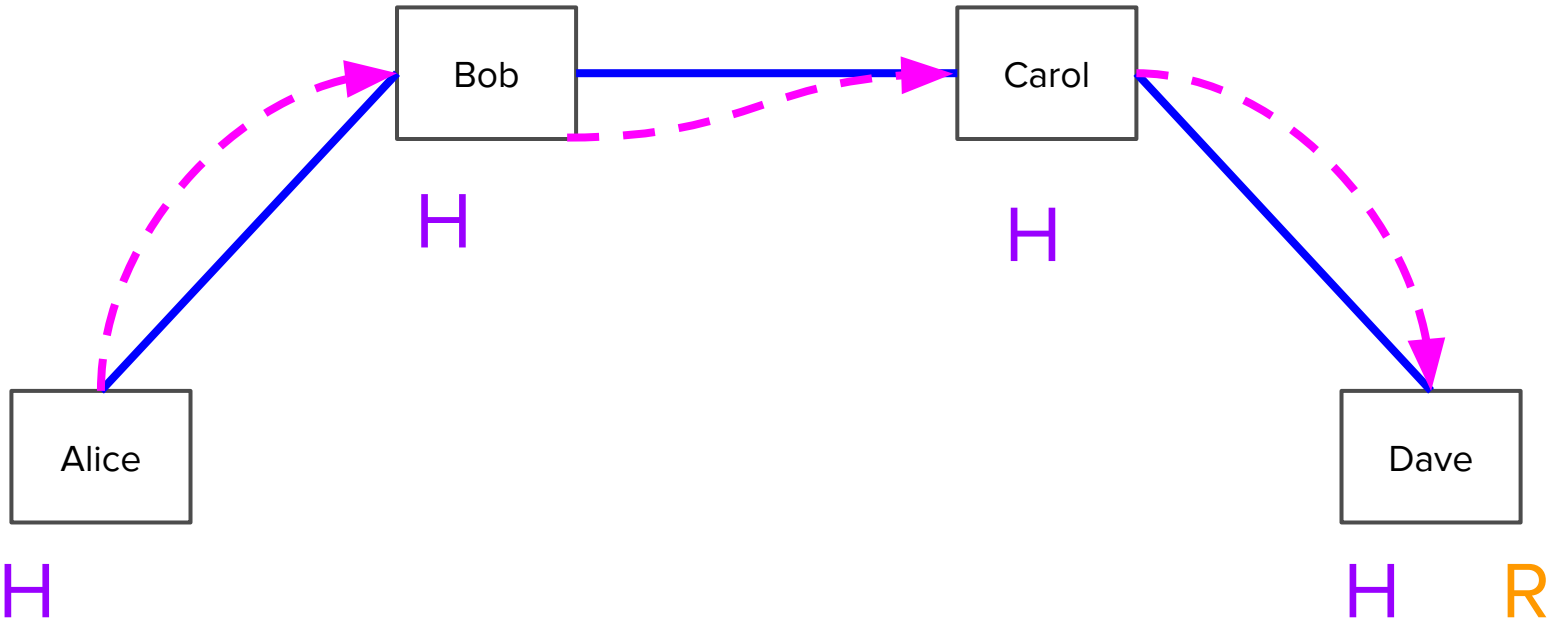
チャンネルネットワークの動き方

同じように、BobがCarolに払う。CarolもRを知らないと貰えない。



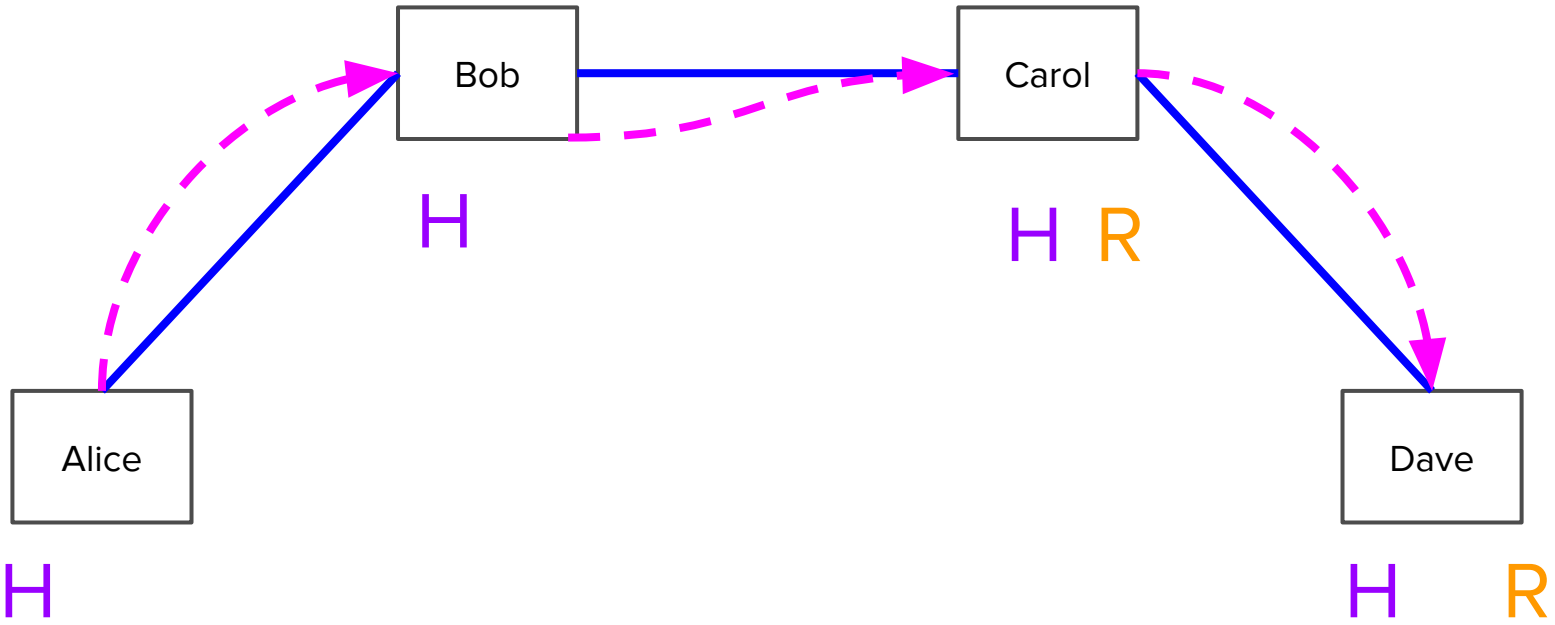
チャンネルネットワークの動き方

Carol が Dave に払う。DaveはRを知ってる（自分で考えたから。）



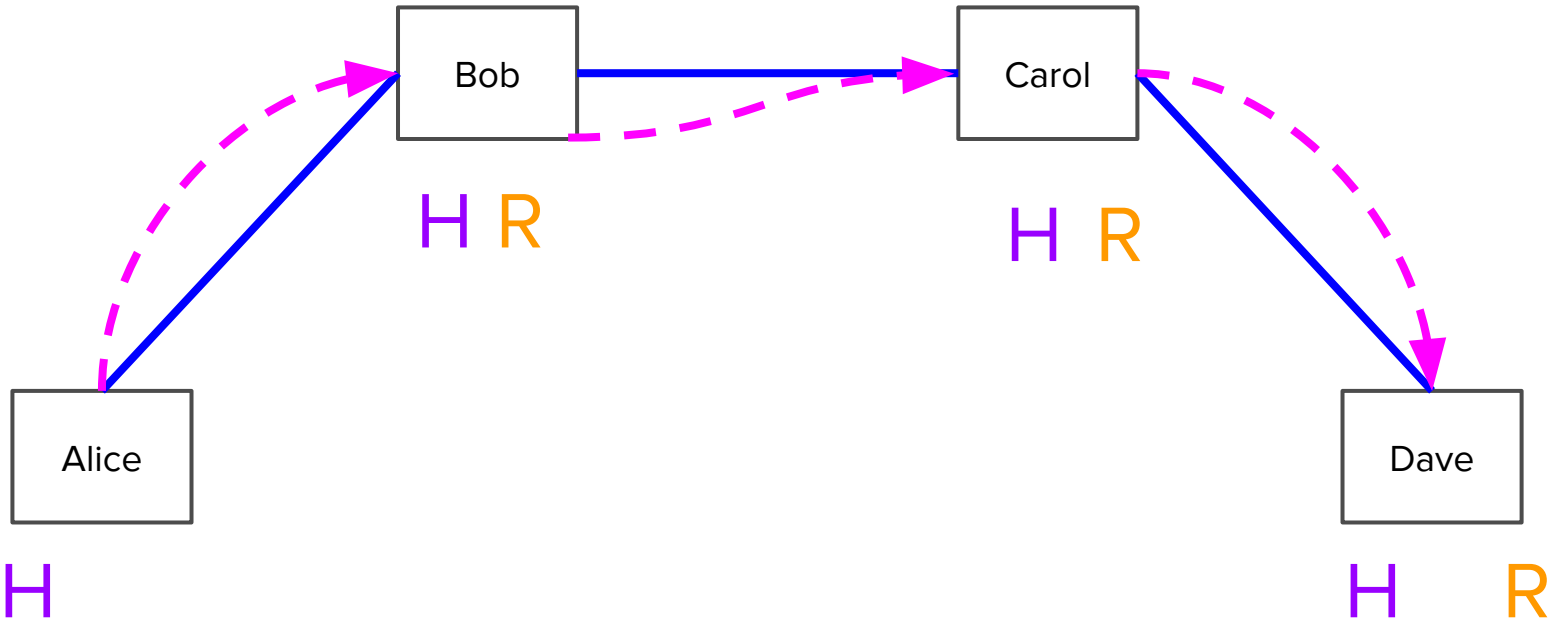
チャンネルネットワークの動き方

Daveが Carol に Rを見せたら、Carolが Bobからお金を受け取れる。



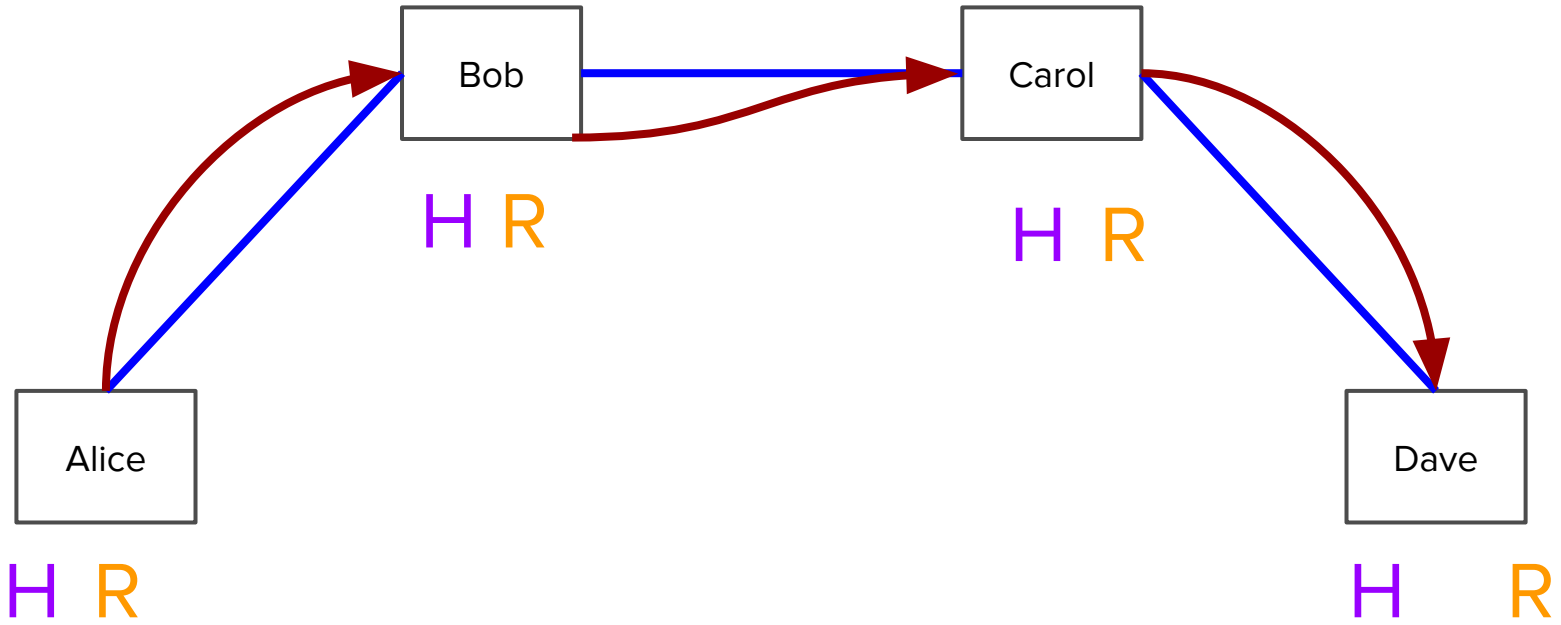
チャンネルネットワークの動き方

Carol が Bobからお金を貰えたら、BobもRが見えて、Aliceからお金が取れる。



チャンネルネットワークの動き方

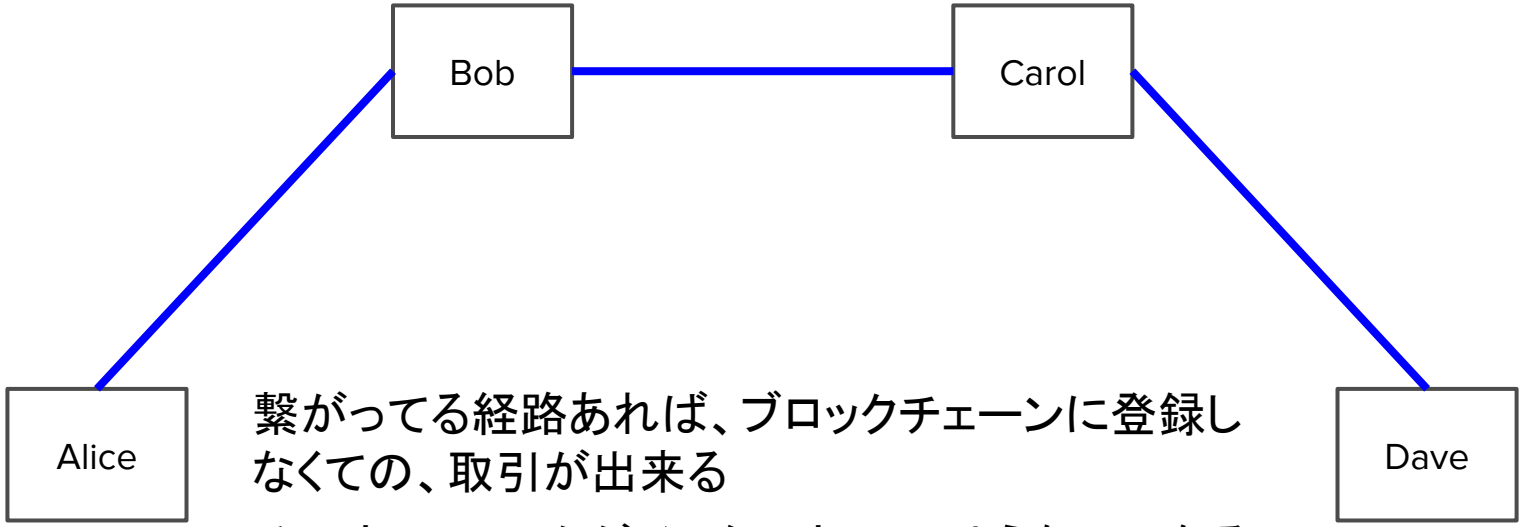
AliceがRを見たら、領収証みたいに、支払いがDaveまで出来ました。



チャンネルネットワークの動き方

このまま、直接のチャンネルが無くても、ネットワークで支払いはできる。

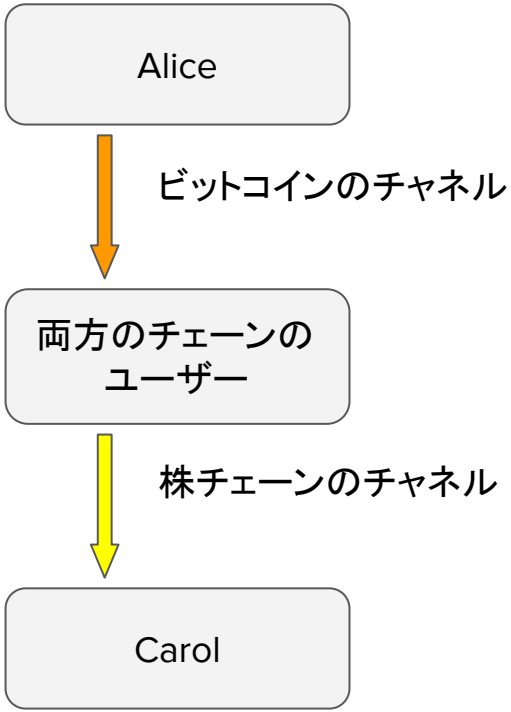
中のユーザーに信用が必要ない。



繋がってる経路あれば、ブロックチェーンに登録しなくての、取引が出来る

そのネットワークがインターネットのような形になる

別のブロックチェーンを繋げる



ネットワークのチャンルが 必ず同じブロックチェーンではない。別のチェーンにまたがっても、同じように動いてる。

Lightning Networkの特徴

- プライベートのブロックチェーンよりも、チャンネルのシステムの方が速い
- 協力するなら、安く、速くなってる
- 同意しないなら、ブロックチェーンのセキュリティーに戻る
- みんな契約いっぱい作るけど、ほとんど裁判所に行かない。（でも裁判が重要）

新しいアプリケーション

- 銀行や株のブロックチェーンがあれば、信用のいらない市場が作れる
- ブロックチェーンのトレードなら、払ったら、必ず貰う
- 信用が必要なければ、誰にでも出来る
- 誰にでも出来れば、コストが非常に下がる

現在のソフト: lit (リット)

- Go言語で書いています linux/mac/win
- SPVワレット付き
- 使いやすい、安全の目的
- Segregated Witness使います （必要）
- マルチホップモードまだ書いてません
- 今日使いましょう

ご注意

- Lit　は完全出来てません、バッグまだいっぱいあります
- 今回は初めの多く人が使ってる。　新しいバッグ発見しましょう！
- 発見したら、ちょっと書いたら嬉しいです
- Githubにissuesも日本語OK

SPV

- SPV (simplified payment verification) は lightning のことじゃないけど、便利です
- 100ギガ以上じゃなくて、約50メガ
- bitcoin-qt以外のワレットはSPV、又はSPV以下のセキュリティ
- SPVはリスクがあります

フールワレットの動き

- ブロックをダウンロードと保存
- 全ての取引を確かめる
- 自分のアドレスを探します
- 自分のアドレス見つけたら、UTXOのDBに入れる
- UTXOが消えたら、DBから消える

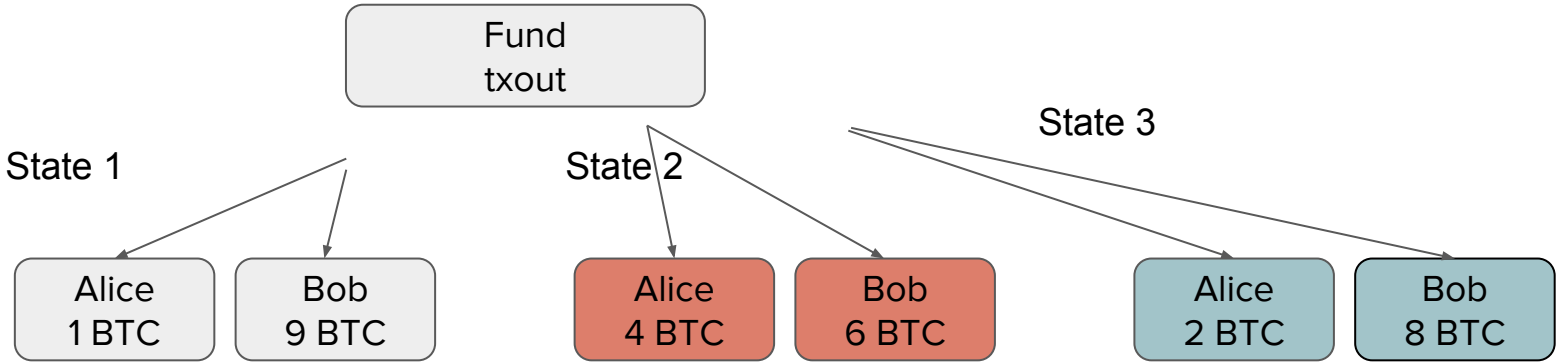
SPVワレットの動き

- 80バイトのheaderだけダウンロードする
- Bloom filterをフールノードに送って
- 自分のアドレスが入ってる取引だけをダウンロードする
- 数メガだけかかる

SPVの問題

- ネットワークのルール守れない
  - 例えば、ルール以上のコインを作る
- デジタル証明を確かめれない
  - 前の取引持ってない；証明と前の鍵が合ってる？
- 繋がてるフールノードが色々分かっちゃう
  - 自分のアドレスなど
- 未確認の取引は全く意味ない

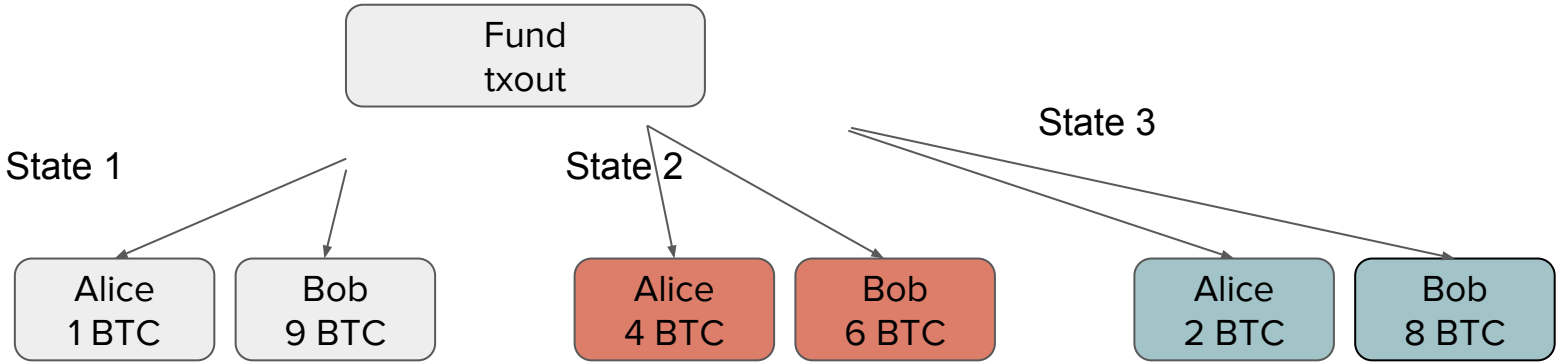
ペイメント　チャンネル



どうやって歴史を消す？

自分のパソコンからデータを消せれるけど
相手が「うん、消したよ！」と言っても、嘘かもしれない
消すの証明は。。。可能？　無理ですね

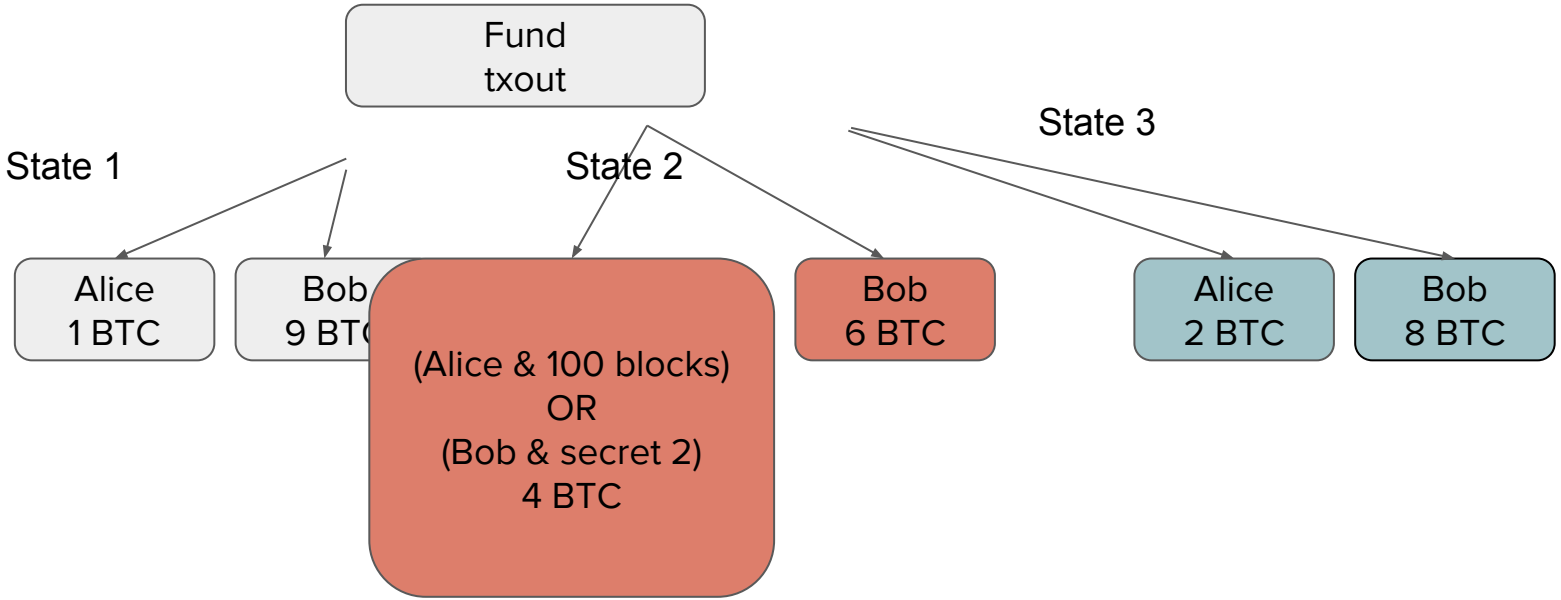
ペイメント　チャンネル



このtxを放送したら、ネットワークには、正しいに見える

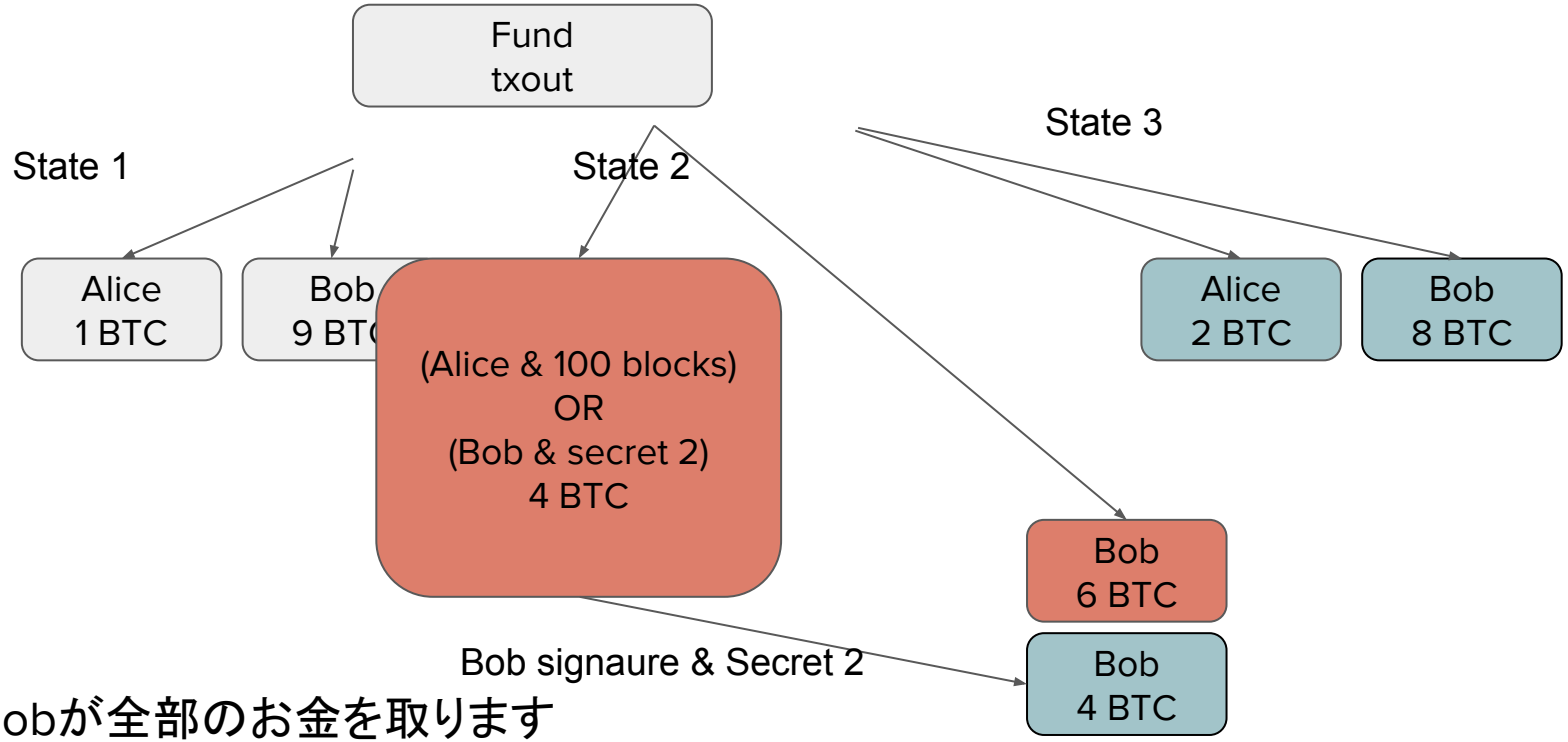
ネットワークが State 3知らないから、Alice が4, Bob が 6

歴史を消す - revoke



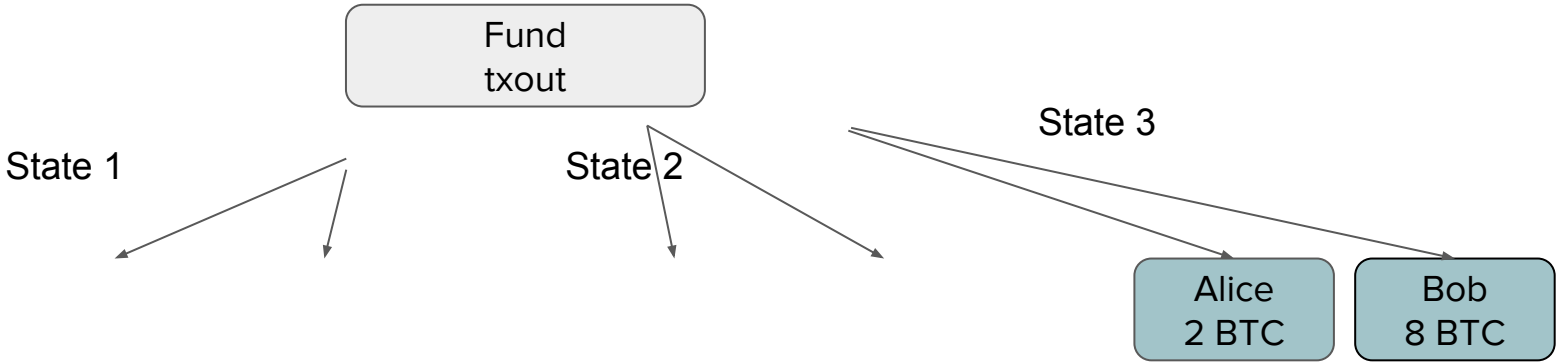
Aliceが放送したら、100ブロック待たないと
Bob が secret#2持ってるなら、すぐ使える

歴史を消す - revoke



Bobが全部のお金を取ります
ありがとう犯罪者Alice! 罰金いただきます！

ペイメント　チャンネル



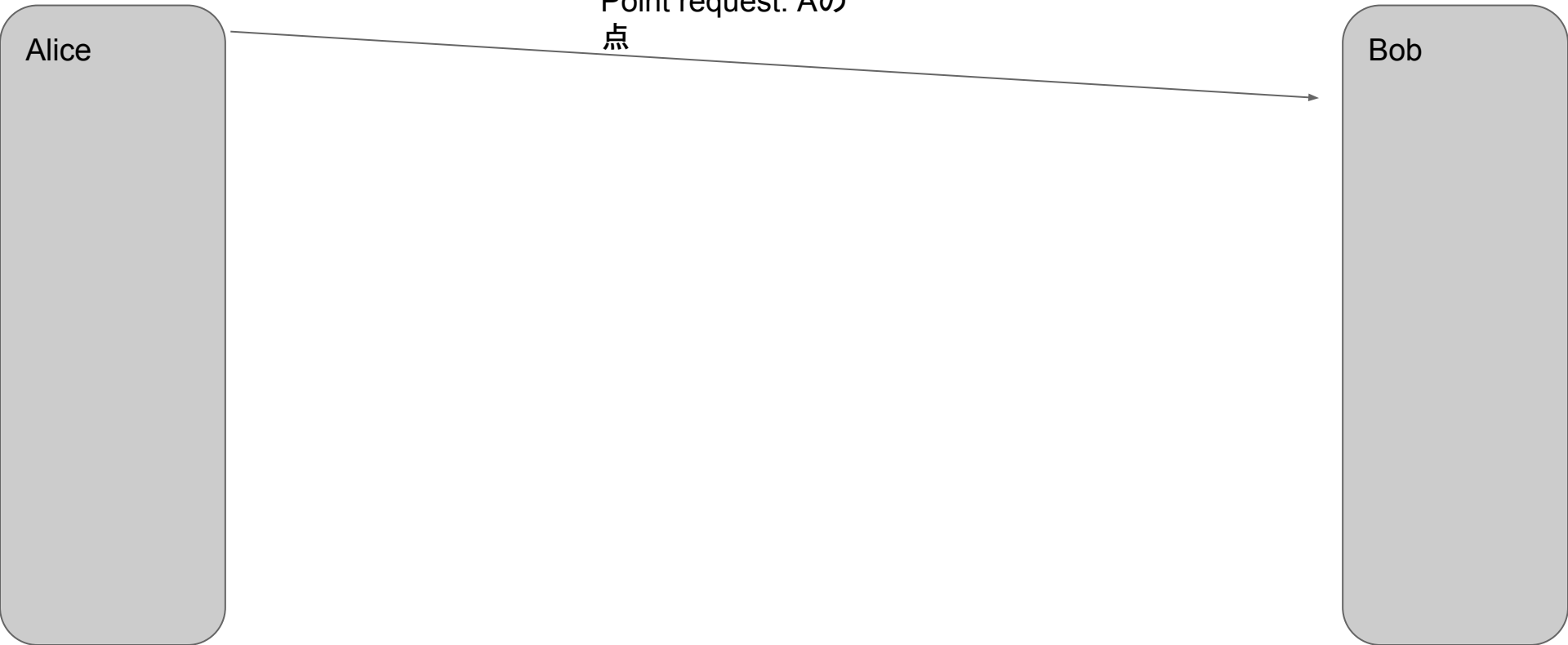
過去のstateを放送したら、相手が全部のお金を取ります！
過去のstateが危険で、新しい stateを作ったら、過去のをすぐ消します。
それで両方の人は同じstateを同意します、チャネルが正しく進んでいます。

Lit のメッセージの流れ: fund

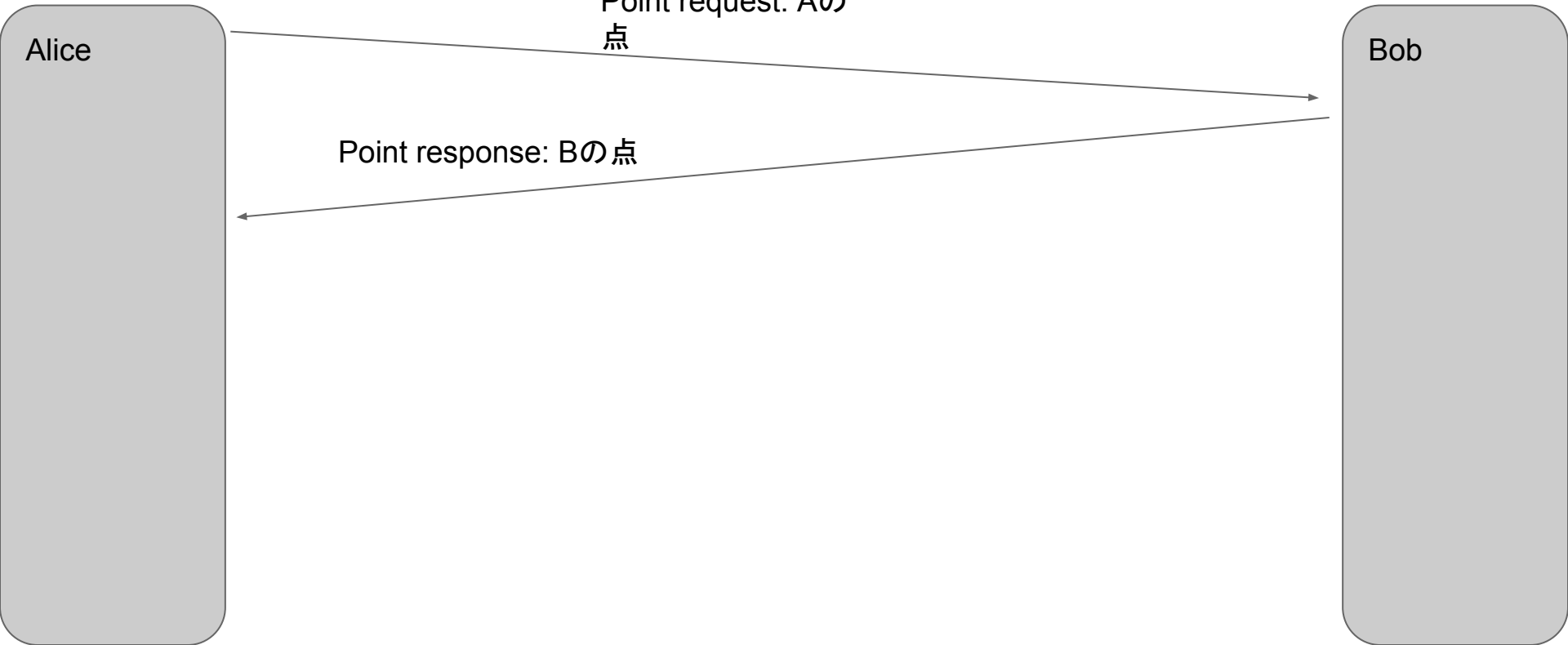
- チャネルを作る方法　qln/fund.go

Lit のメッセージの流れ: fund

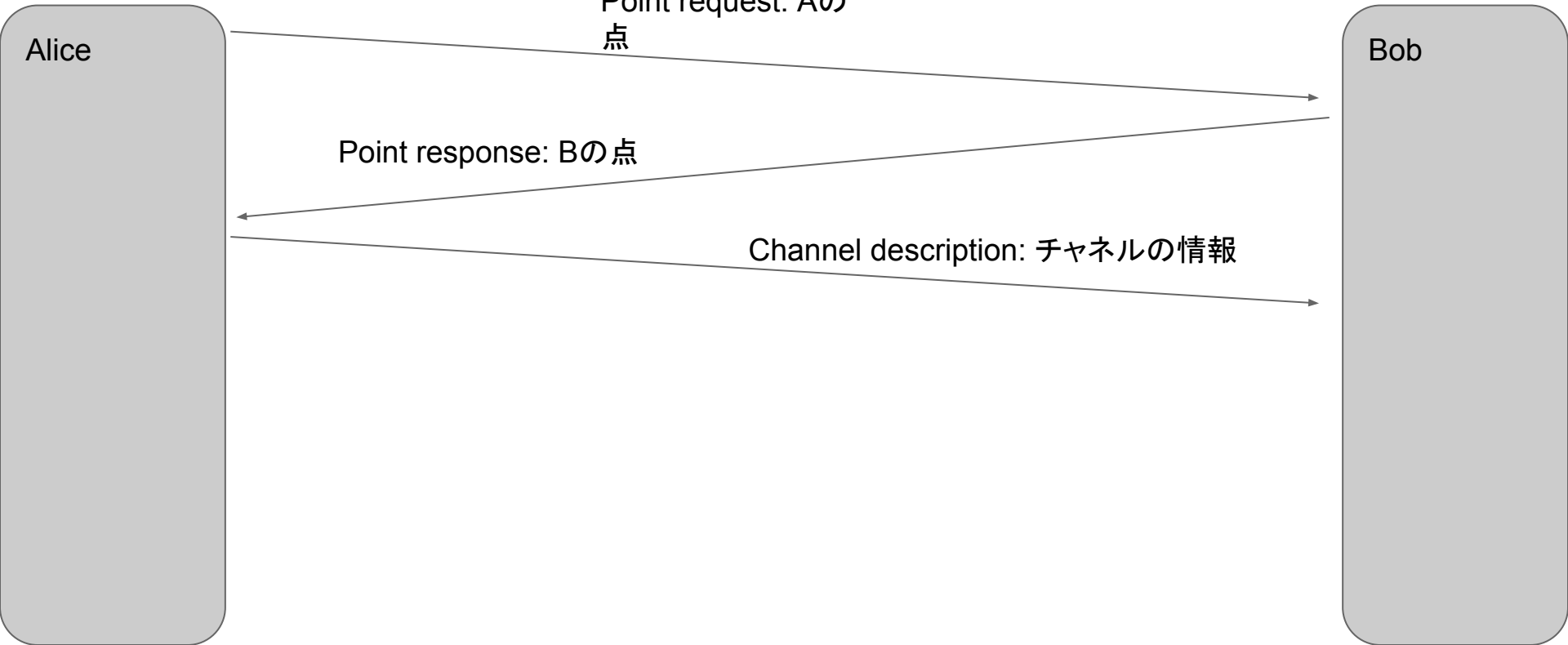
Lit のメッセージの流れ: fund



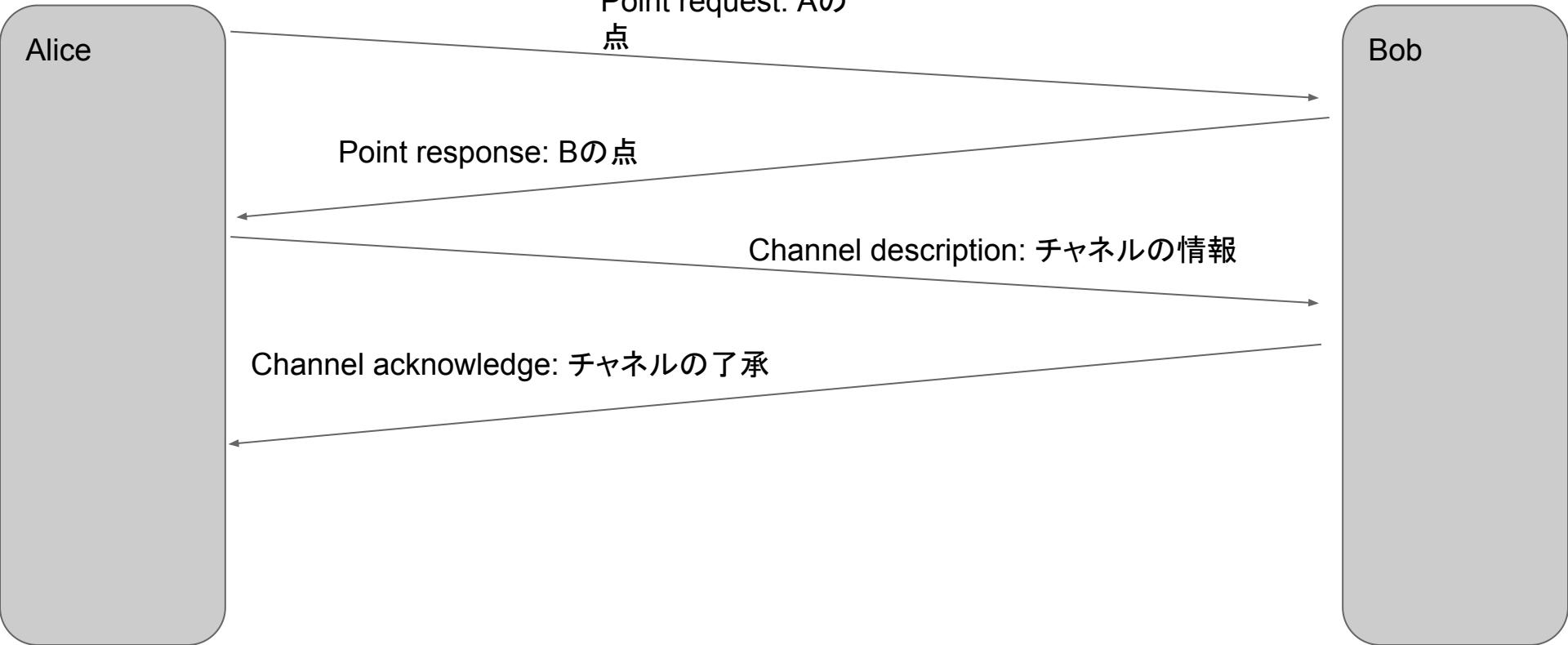
Lit のメッセージの流れ: fund



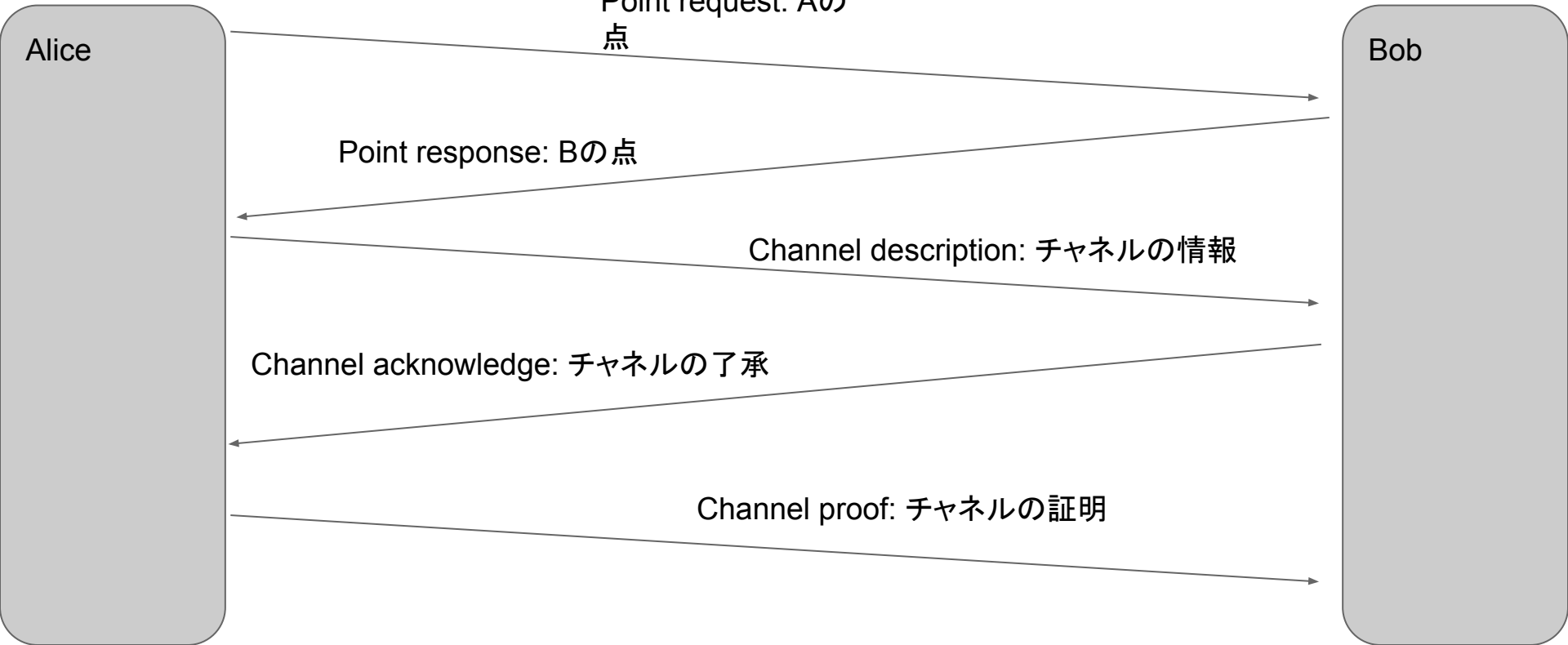
Lit のメッセージの流れ: fund



Lit のメッセージの流れ: fund



Lit のメッセージの流れ: fund



Lit のメッセージの流れ: push

- チャネルを作る方法　qln/pushpull.go

Lit のメッセージの流れ: push

Alice
State: 4
Delta: 0
Amt: 66

Bob
State: 4
Delta: 0
Amt: 25

Lit のメッセージの流れ: push

Alice
State: 4
Delta: 0
Amt: 66

State: 4
Delta: -3
Amt: 66

Bob
State: 4
Delta: 0
Amt: 25

Lit のメッセージの流れ: push

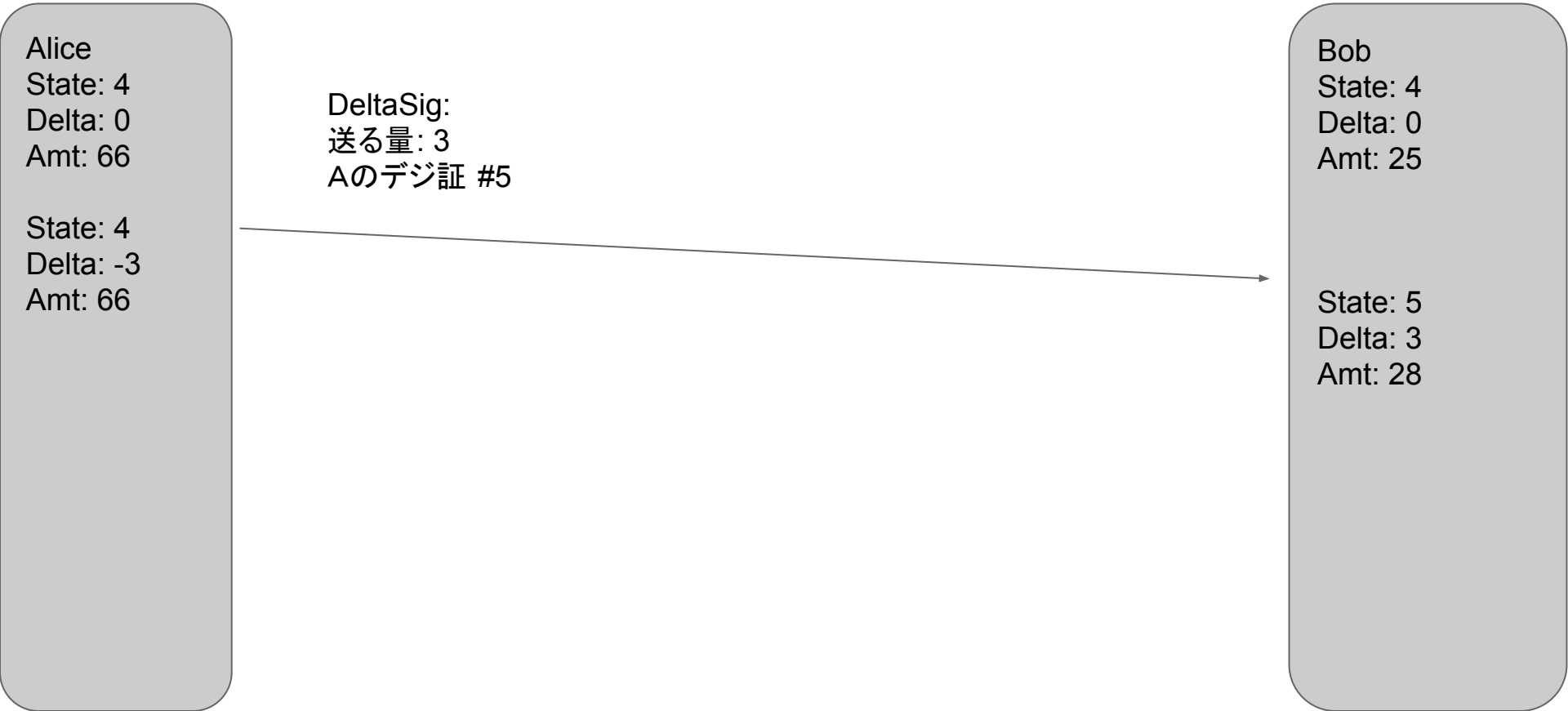
Alice
State: 4
Delta: 0
Amt: 66

State: 4
Delta: -3
Amt: 66

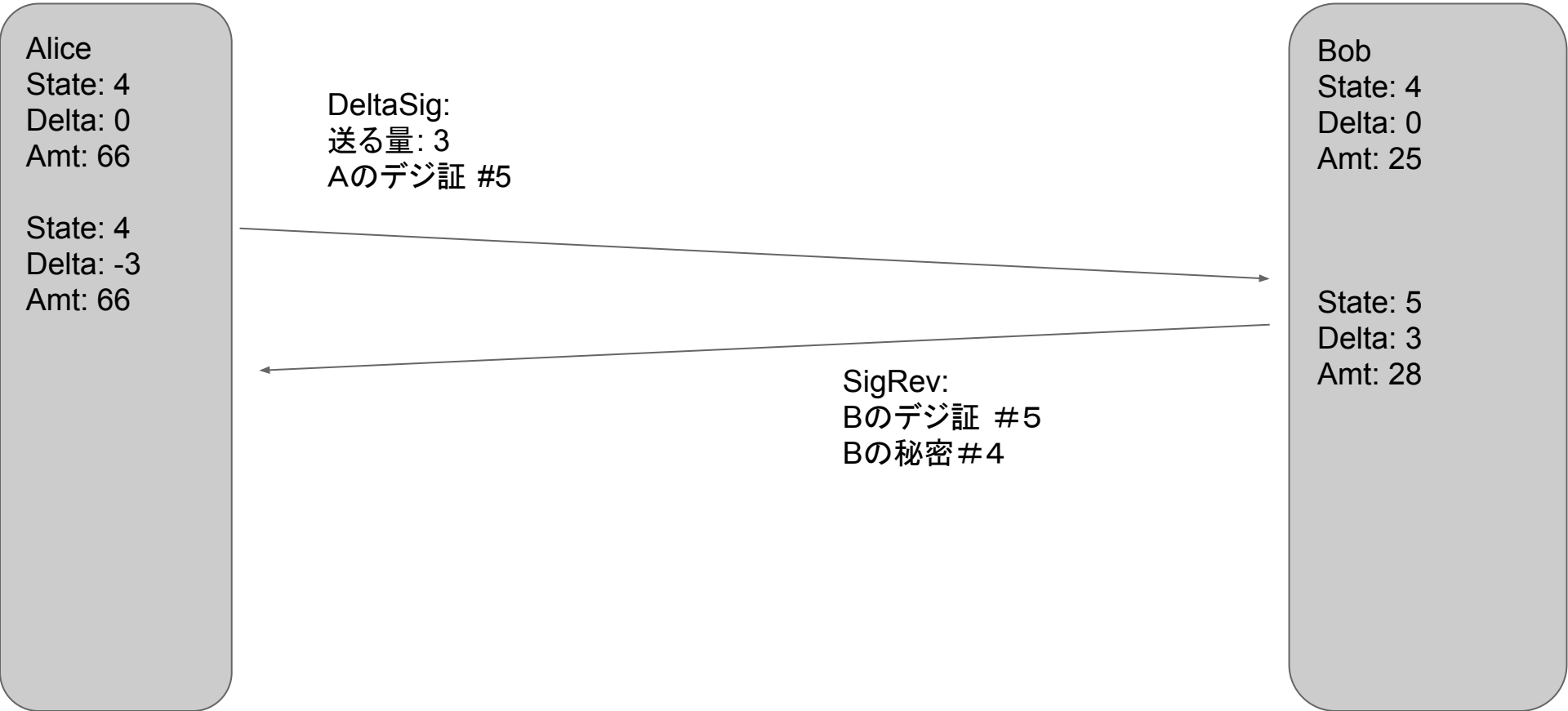
DeltaSig:
送る量: 3
Aのデジ証 #5

Bob
State: 4
Delta: 0
Amt: 25

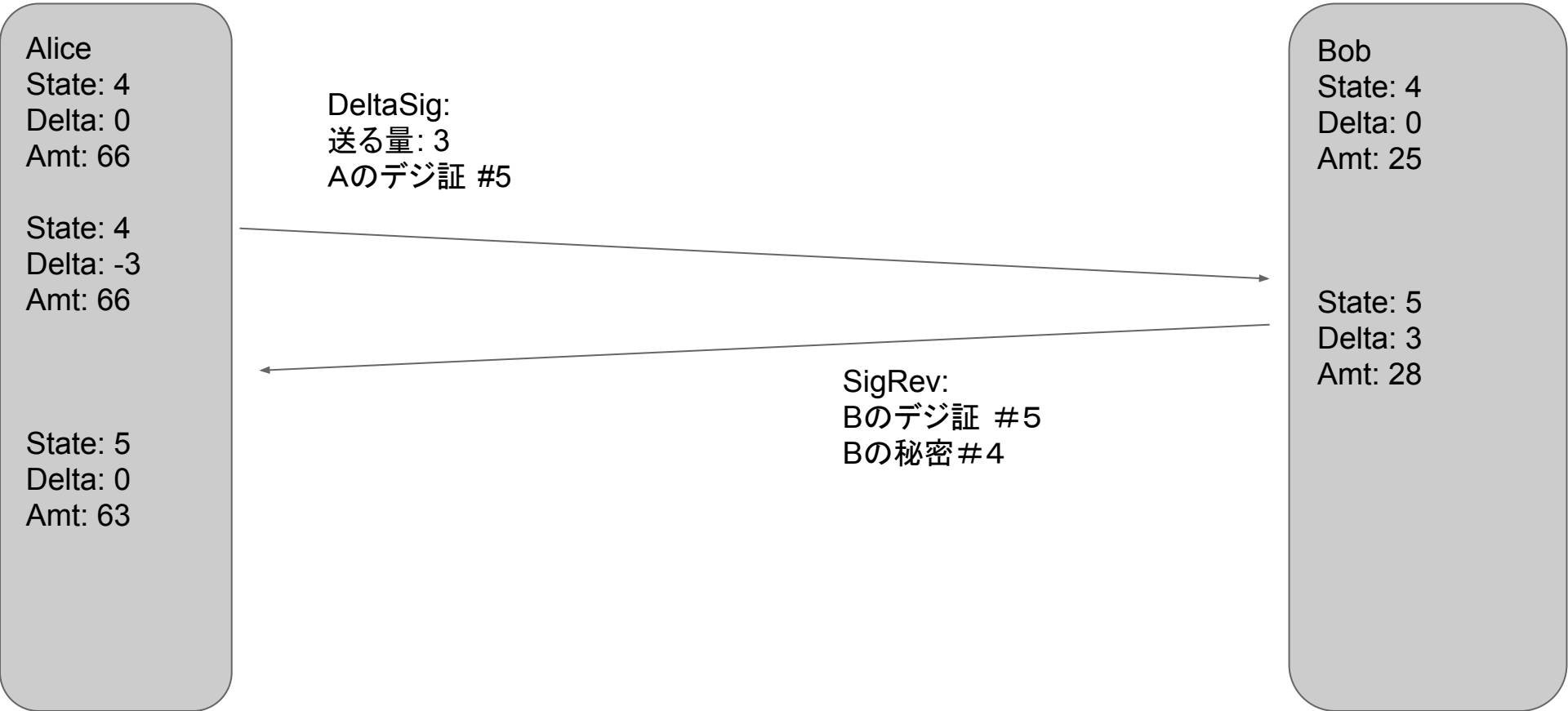
Lit のメッセージの流れ: push



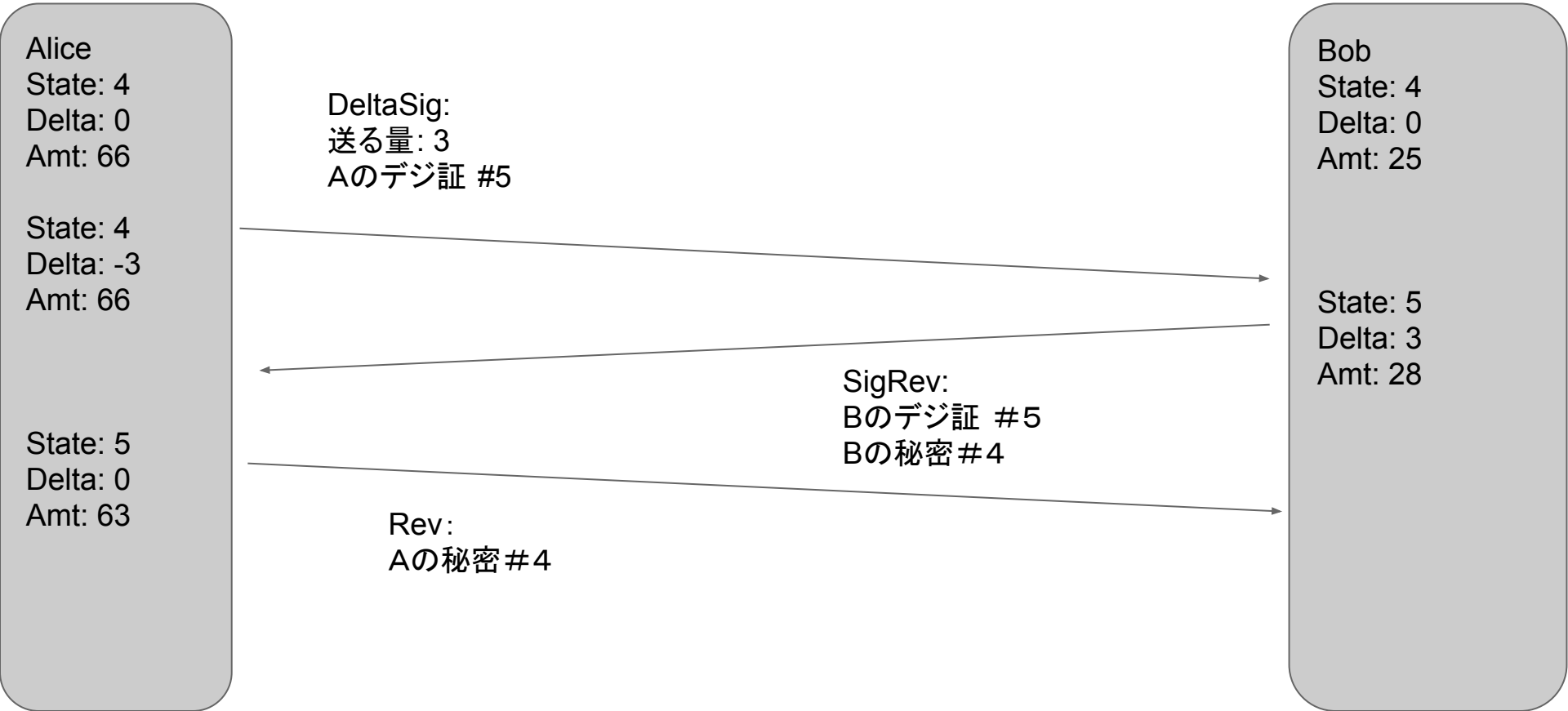
Lit のメッセージの流れ: push



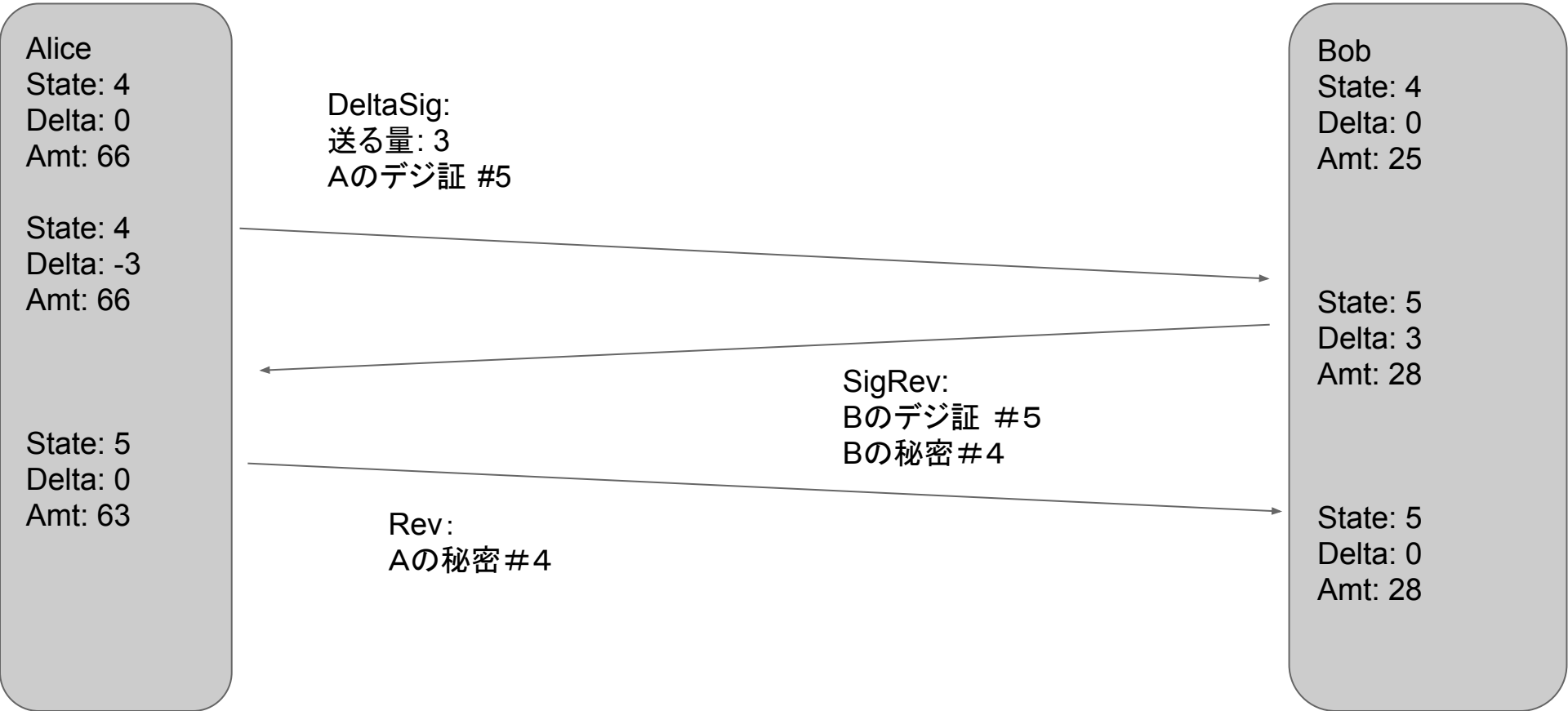
Lit のメッセージの流れ: push



Lit のメッセージの流れ: push



Lit のメッセージの流れ: push



Lit のデモ　チャンネルを作りましょう

- litのbinaryをダウンロードする
  http://172.16.130.201:8000/
- Mac (darwin) と linuxある
- lit:bitcoind, lit-af:bitcoin-cli
- bitcoin-cliでlitのワレットに

Lit のデモ　チャンネルを作りましょう

- `./lit -bc2 -tip 21850`
- `./lit-af`
  - `ls lis con send fund push close break`
- お金を貰う
- segwitアドレスに変わる
- 友達と繋がる
- チャネルを作る

Lit のデモ　チャンネルを作りましょう

- ./lit -bc2
- ./lit-af
  - ls lis con send fund push close break
- お金を貰う
- segwitアドレスに変わる
- 友達と繋がる
- チャネルを作る

Lit のコマンド

ls: ワレットのデータを見る
send: お金を送る
lis: 他のノードが接続出来るポートを開ける
con: 他のノードに接続する
fund: channelを作る
push: チャネルでお金を送る
close / break: チャネルを閉まる
stop: litノードを閉まる

The Bitcoin Lightning Network

質問してください。

ご清聴ありがとうございます!