Discreet Log Contracts
ビットコインの見えないスマートコントラクト

Thaddeus Dryja <tdryja@media.mit.edu>

BC2 part 2
2017-08-02

intro

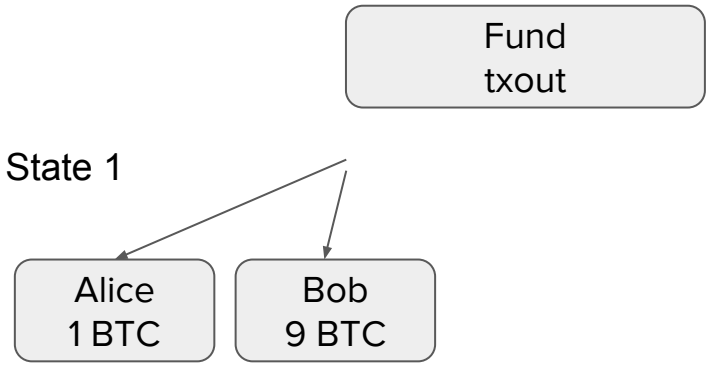
- DLC は今まで発表しなかった。 世界初！
- このアルゴリズムとデザインはまだ研究級
- ビットコインの上にスマコン
- ブロックチェーンに入っても、コントラクトが見えない。 内容だけじゃなくて、コントラクトがあったかどうか見えない

オヤジギャグすみません、discreet は「目立たない」 discrete は「分離」

ライトニングのまとめ

- 以前に説明したけど、少し繰り返します
- 多数のブロックチェーンに入っていない取引が使って、最新の取引しか放送出来ない。

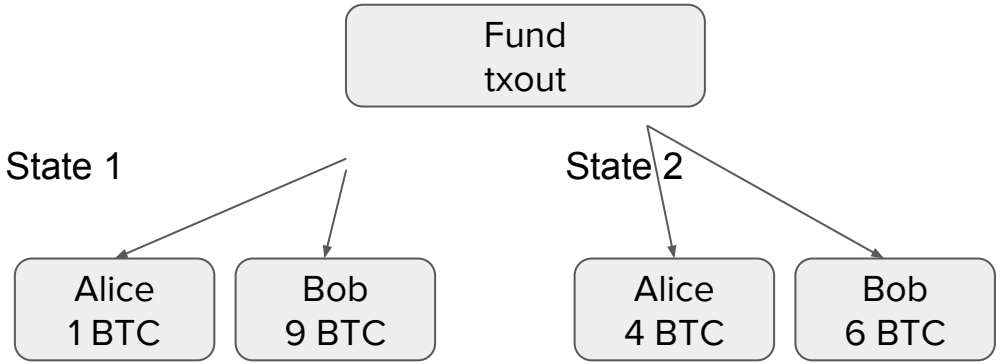
ペイメント　チャンネルとは



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。

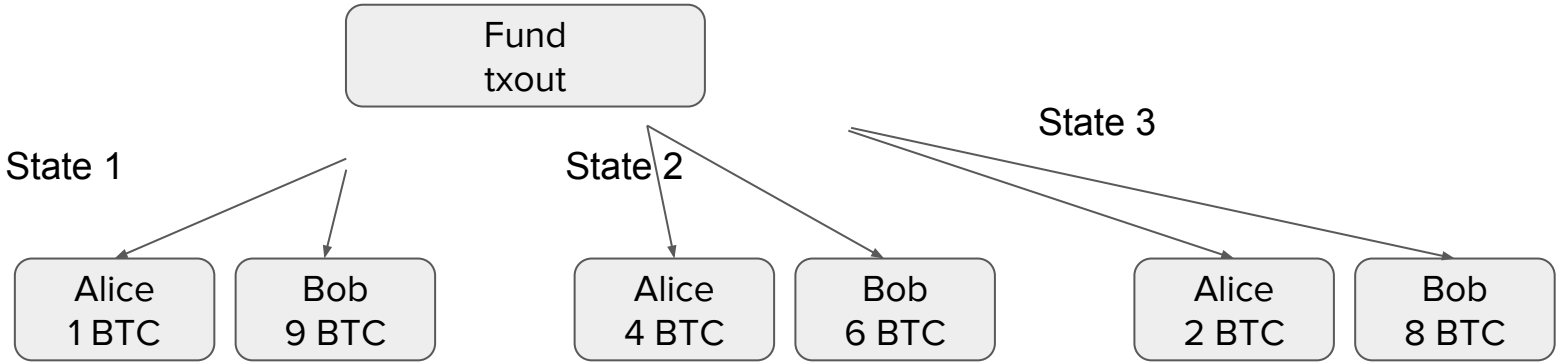
ペイメント　チャンネルとは



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。

条件着き支払い

- 基本のスマートコントラクト：イベントでお金の動きが決める
- 例えば、明日の天気。雨が降ったら、Alice に1BTC.　晴れなら、Bobに1BTC
- 問題：ブロックチェーンは天気知らない

Oracle

- 晴れか雨、だけが決める？
- ２の２のmultisigなら、喧嘩したら、お金が停まっていた
- 第三者のOracleが必要
- ２の３multisigとoracle

2 of 3 multisig oracle

- 3つの鍵： Alice, Bob, Olivia
- 雨ならAlice, 晴れならBob, Olivia が決める
- AliceとBobが同意したら、Oliviaに頼まなくていい。 喧嘩したら、Oliviaが誰が貰うを決める。
- 問題：AliceがOliviaに
  「雨に決めたら、0.5BTC上げるよ」

Interactive oracle

- ２の３multisig のoracleはinteractive;コントラクトを全部見える
- Oracle がコントラクトを見えないほうがいい、でもどうやって？

Schnorr signature

- 小さい文字 = scalar（普通の数字）
- 大文字 = point（楕円曲線の点）
- カーブに、Generator G
- 秘密鍵 a <- $
- 公開鍵 A = aG
- h() はハッシュ関数
- m はメッセージ

Schnorr signature

a <- $; 公開鍵 A = aG

メッセージ m; k <- $; R = kG

サインする: s = k - h(m, R)a

署名:(R, s)

確かめる: sG = kG - h(m, R)aG

= R - h(m, R)A

Fixed-R Schnorr signature

公開鍵 A　　署名:(R, s)

DLC:

公開鍵　(A, R)　　署名: s

まだ使えるけど、1回しか使えない

k-collision

署名1　$s_1 = k - h(m_1,R)a$

署名2　$s_2 = k - h(m_2,R)a$

$s_1 - s_2 = k - h(m_1,R)a - k + h(m_2,R)a$

$= h(m_2,R)a - h(m_1,R)a$

$= (h(m_2,R) - h(m_1,R))a$

$a = (s_1 - s_2) / (h(m_2,R) - h(m_1,R))$

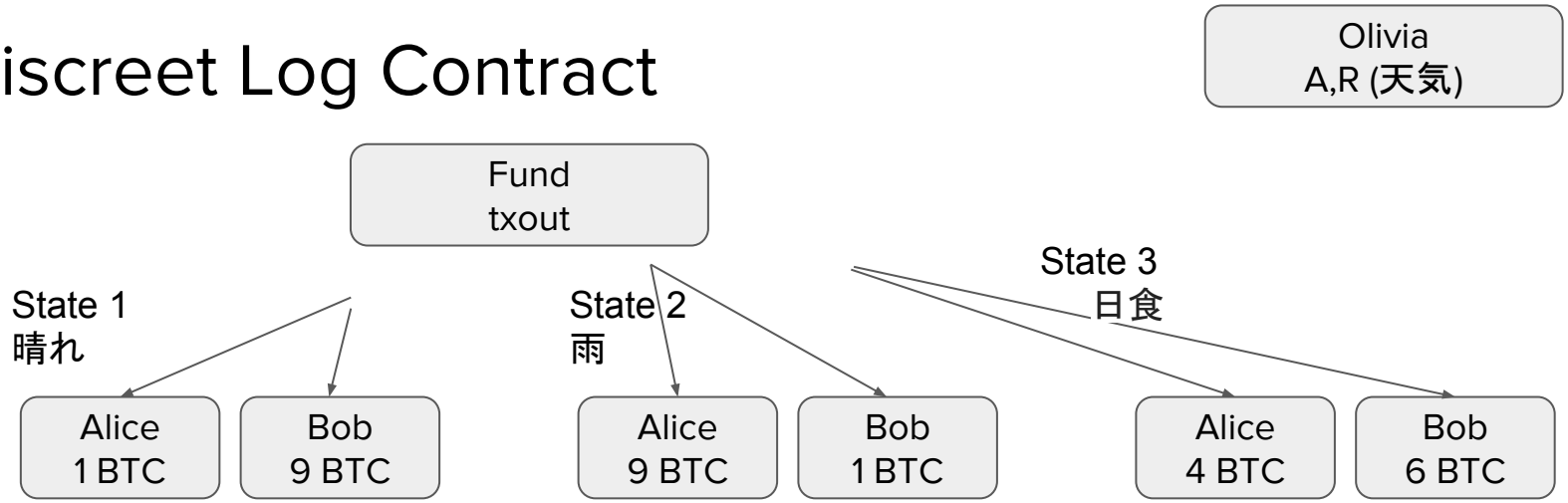
ちなみにこれプレステ3の秘密鍵バレる問題

Anticipated Signature

公開鍵(A, R)が知ってる　署名:s 知らない

でも sG = R - h(m,R)A
何でものメッセージの署名を計算できる！
でも sG 出来る. Sは計算出来ない
(EC Discrete log problem)

Discreet Log Contract



Alice と Bob が賢い契約（スマコン、スマートコントラクト）を作ります
LNと似てるけど、LNは順番で1個ずつ作って、正しいのは最新のだけ。
DLCの場合には、正しい取引は Oliviaが決める
Oliviaはスマコン見ないので、Oliviaの署名で正しい取引を決める

署名　＝　秘密鍵

- Olivia の s は秘密鍵にする
- sG は公開鍵にする

署名 ＝ 秘密鍵

Olivia の s は秘密鍵にする
sG は公開鍵にする
Alice と Bobの公開鍵に混ぜる

$$pub_{alice} + sG = pub_{contract}$$
$$priv_{alice} + s = priv_{contract}$$

Example

3つの結果: $m_{晴}$ $m_{雨}$ $m_{食}$

3つのsigKeys: $s_{晴}G = R - h(m_{晴},R)A$

$AlicePub_{晴} = AlicePub + s_{晴}G$

$BobPub_{晴} = BobPub + s_{晴}G$

$AlicePub_{雨} = AlicePub + s_{雨}G$

$BobPub_{雨} = BobPub + s_{雨}G$

ライトニングのscript

PubR OR (PubT AND 時間)
ライトニングに使ってるのは、正しいのは PubT と op_csv
駄目の取引のは、PubR がすぐ取れる (秘密鍵の半分が表す

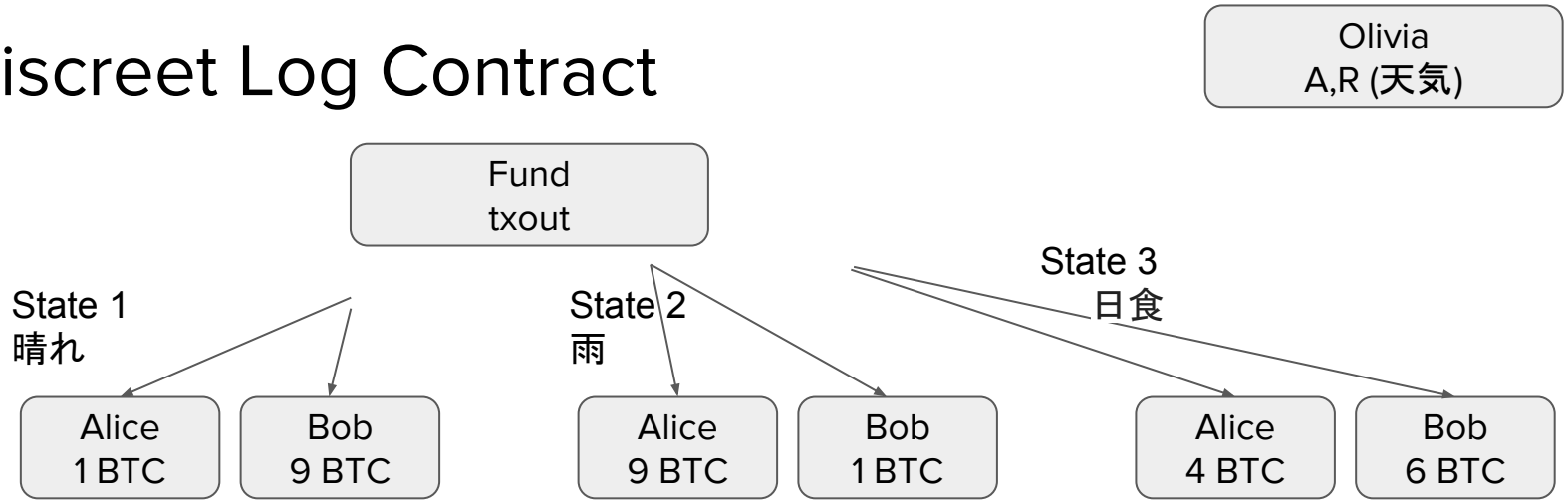
```
OP_IF PubR OP_ELSE delay OP_CSV OP_DROP PubT OP_ENDIF OP_CHECKSIG
```

ライトニングとDLCの2つの鍵

PubX OR (PubY AND 時間)
PubY はピュアー、PubX はpart1+part2

Lightning: PubY が正しい PubXは間違え
DLC: PubY が間違え PubX が正しい

Discreet Log Contract

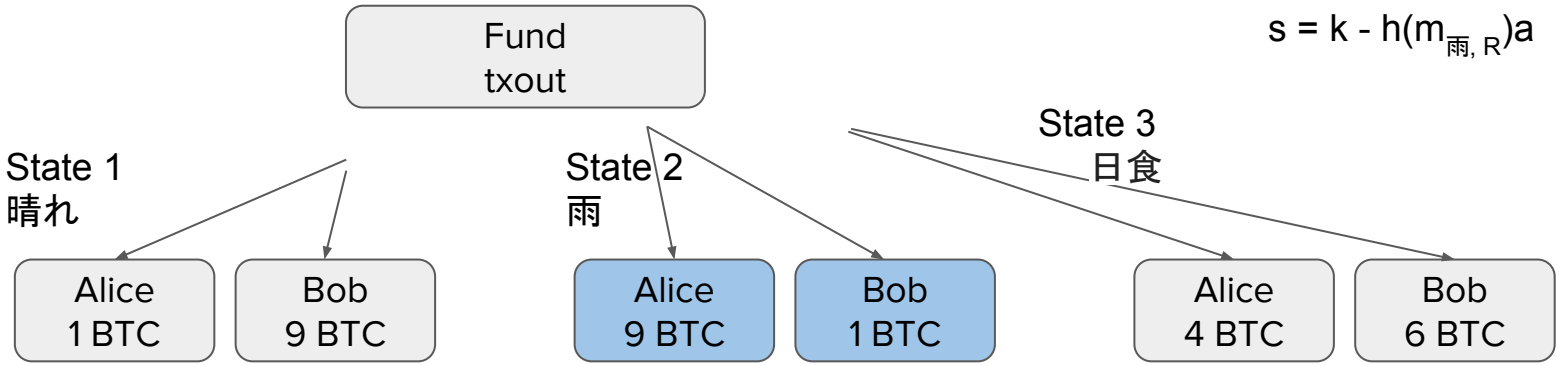


雨が降ってきた
Oliviaは 「雨」というメッセージをサインします

Discreet Log Contract

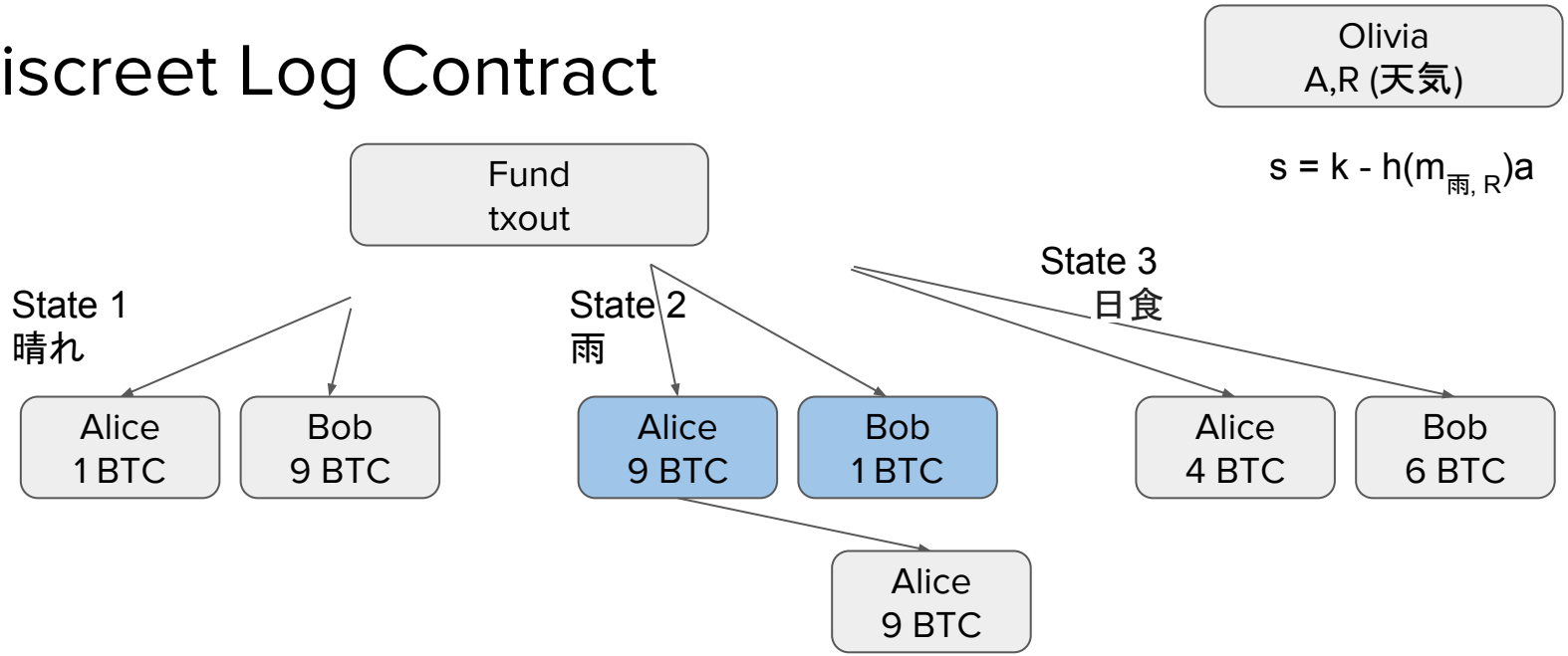
Olivia
A,R (天気)

$s = k - h(m_{雨, R})a$



$s_{雨}$ は署名。 そして、秘密鍵。
State2 が正しいから、AliceがState2 を放送する

Discreet Log Contract



Aliceがその青いoutputの秘密鍵持っています。Aliceの個人の秘密鍵とOliviaの$s_{雨}$の混ざってる秘密鍵 。

Alice はすぐ、そのState2のoutputを払って、自分のピュアーなアドレスに送ります
そうしないと、明日Bobがその9BTC取れる

DLCと時間

Lightningの場合には必ずネットワークを見る

違反の取引が見つけたら、そのコインをすぐ取らないと

DLCには、自分の放送した取引のoutputをすぐ取らないと。それのほうが楽。
(ソフトには、同じ時に両方のtxを放送する)

No surprises

駄目Olivia

Oracleが駄目だっと、正しくないoutcomeが起こられる。

　一つのoutcomeしか出来ない（2つサインしたら、秘密鍵がバレる）

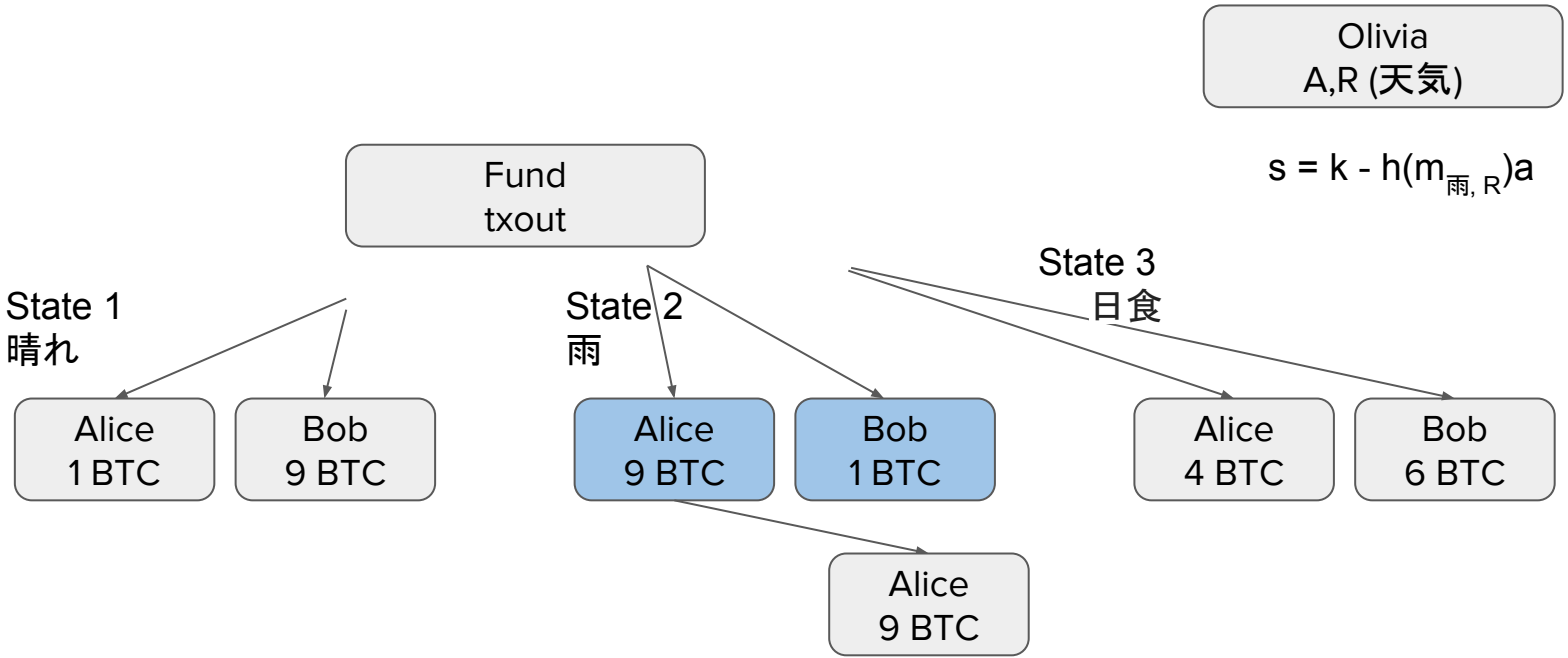
　正しくないoutcomeサインしたら、みんな見える

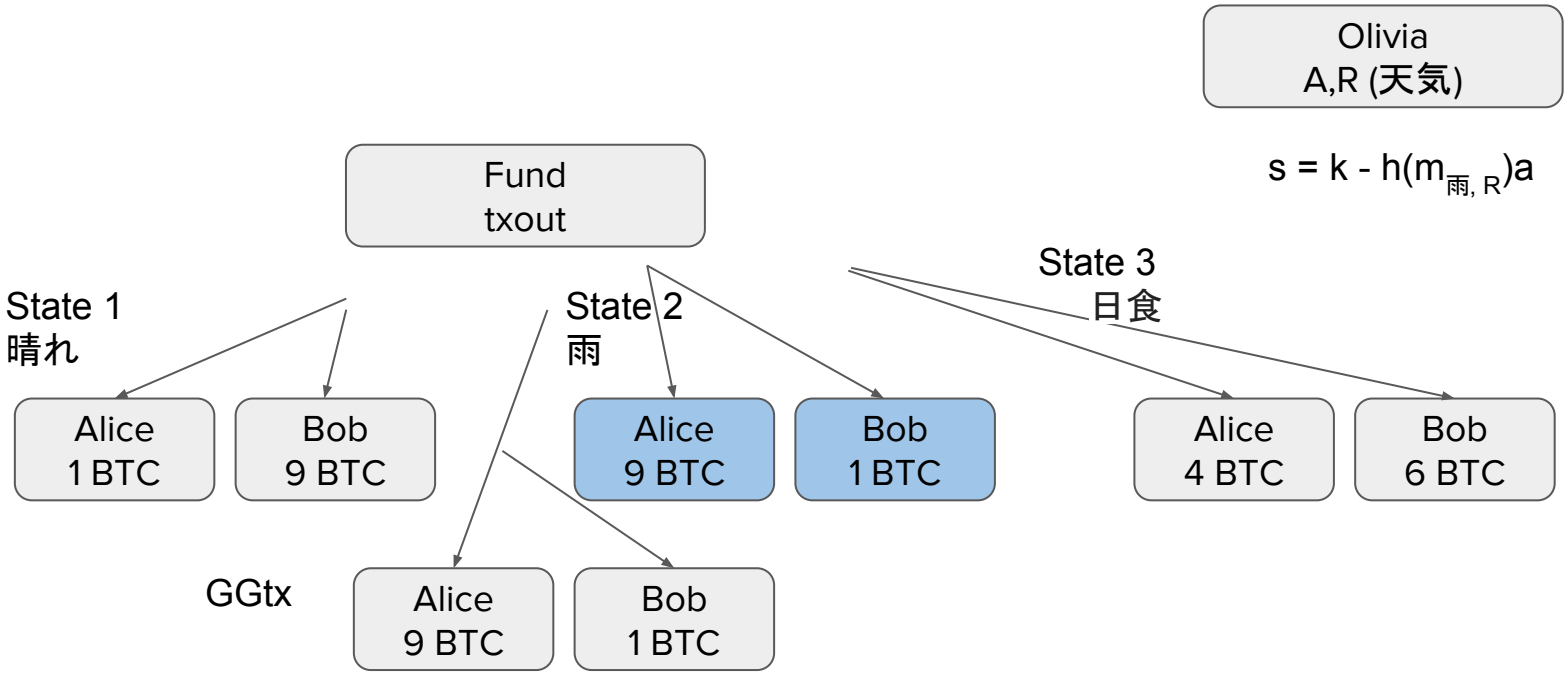
そして、Oliviaは誰がsを使ってるか知らない

DLCとscalability

スマコンは3つの取引

みんな同意するなら、2つの取引になる

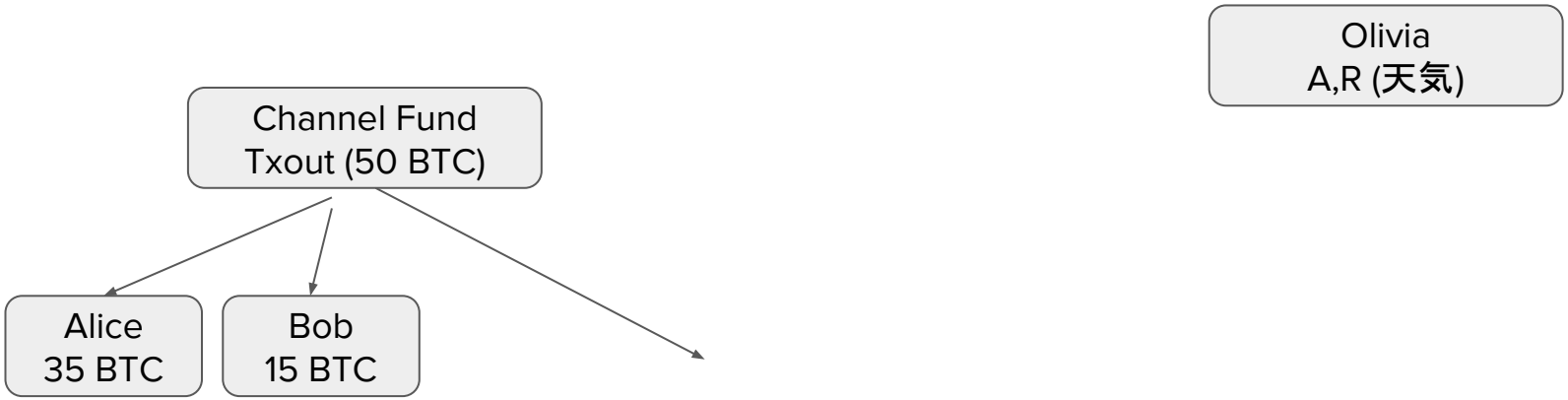

Olivia
A,R (天気)
s = k - h(m雨, R)a
Fund
txout
State 1
晴れ
State 2
雨
State 3
日食
Alice
1 BTC
Bob
9 BTC
Alice
9 BTC
Bob
1 BTC
Alice
4 BTC
Bob
6 BTC
Alice
9 BTC



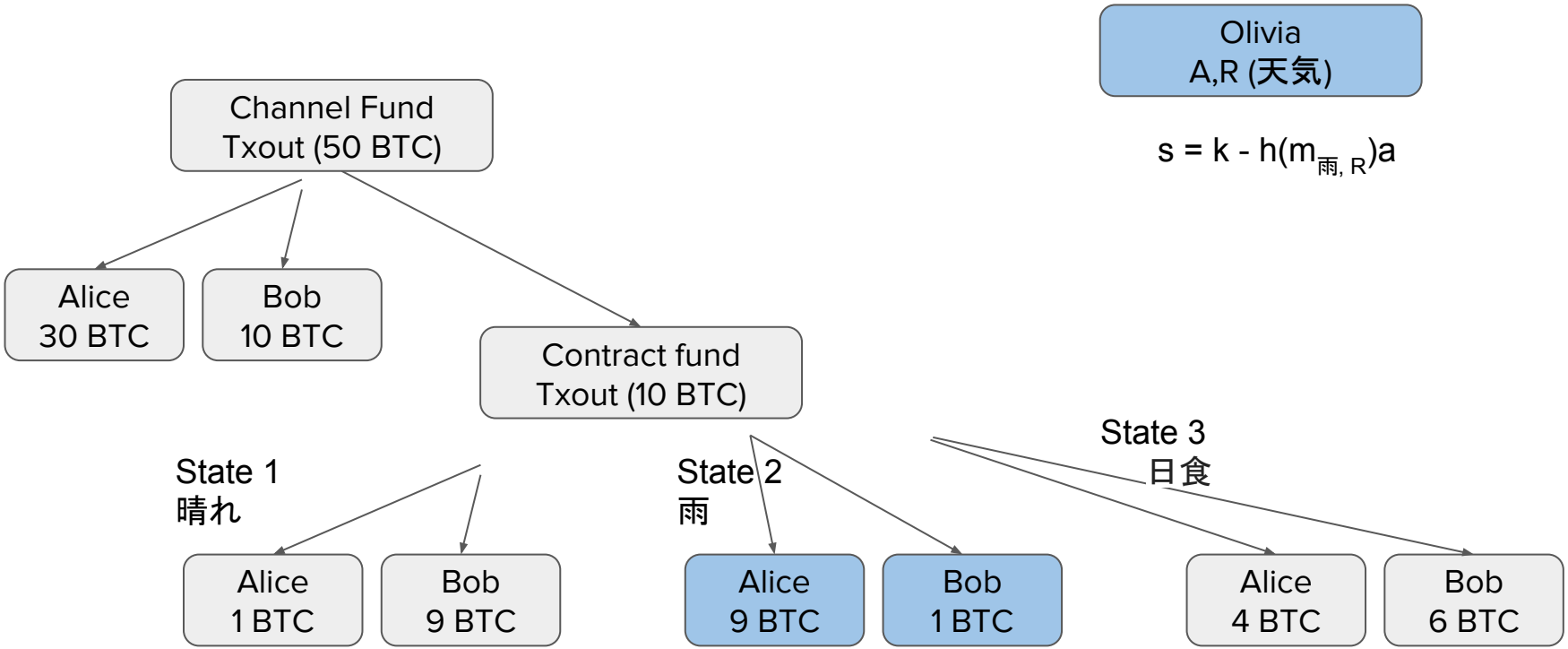
GGtx　みんな同意するから、負ける人が直接の txをサインします

チャンネルとDLCのscalability

LNのチャネルの中に、DLCのスマコン
協力すると、スマコンがOtx

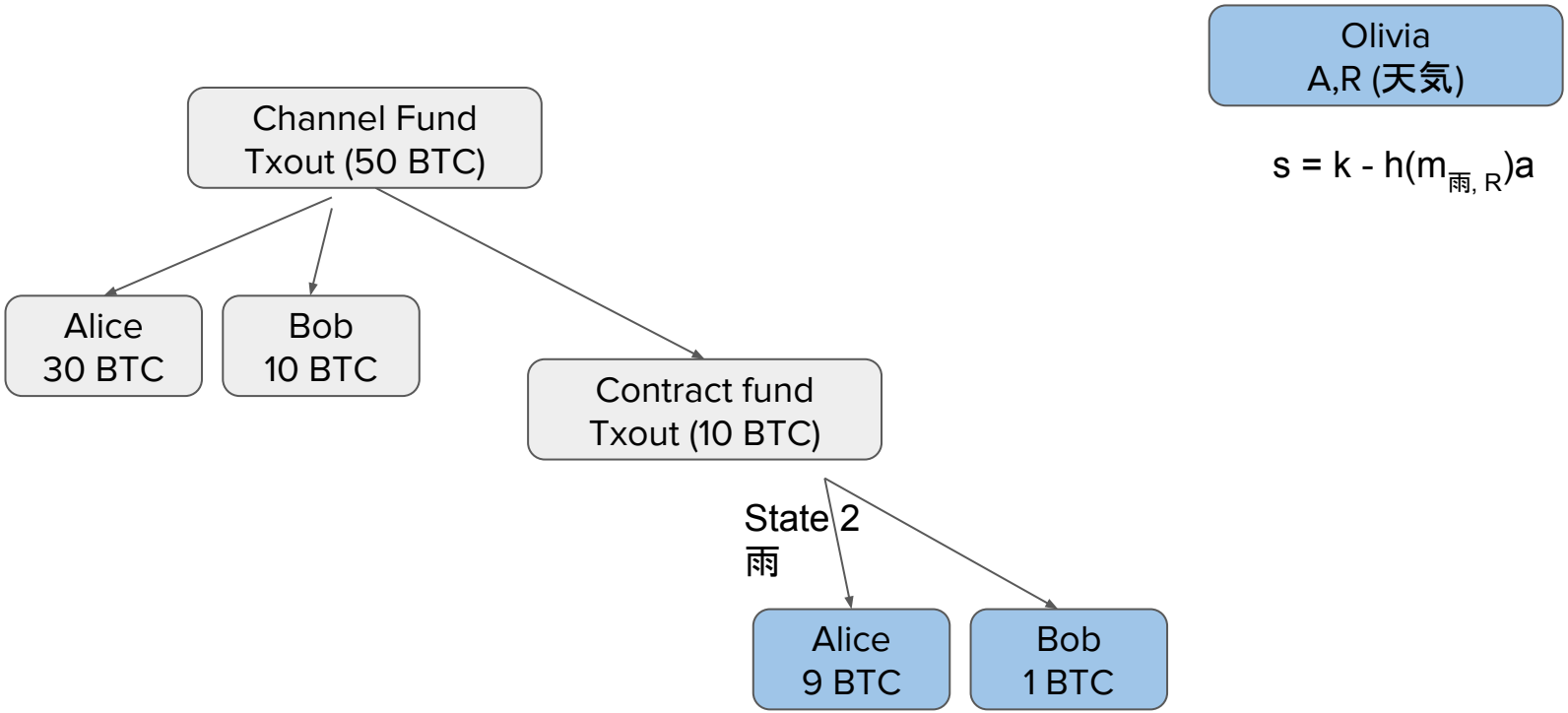


普通の lightningのチャネルに



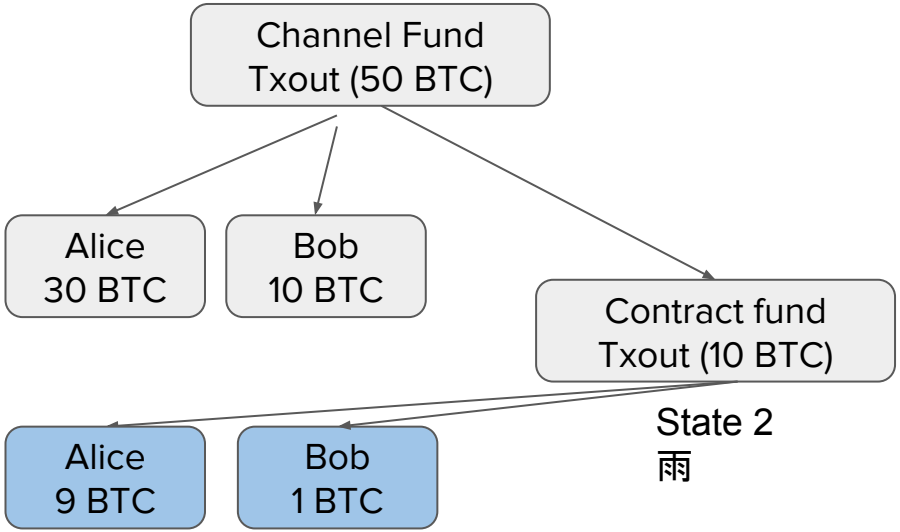
Olivia の $s_{雨}$が出って、State2のが正しい

チャンネルもスマコンもclose出来るけど



Olivia の $s_{雨}$が出って、State2のが正しい

チャンネルもスマコンもclose出来るけど

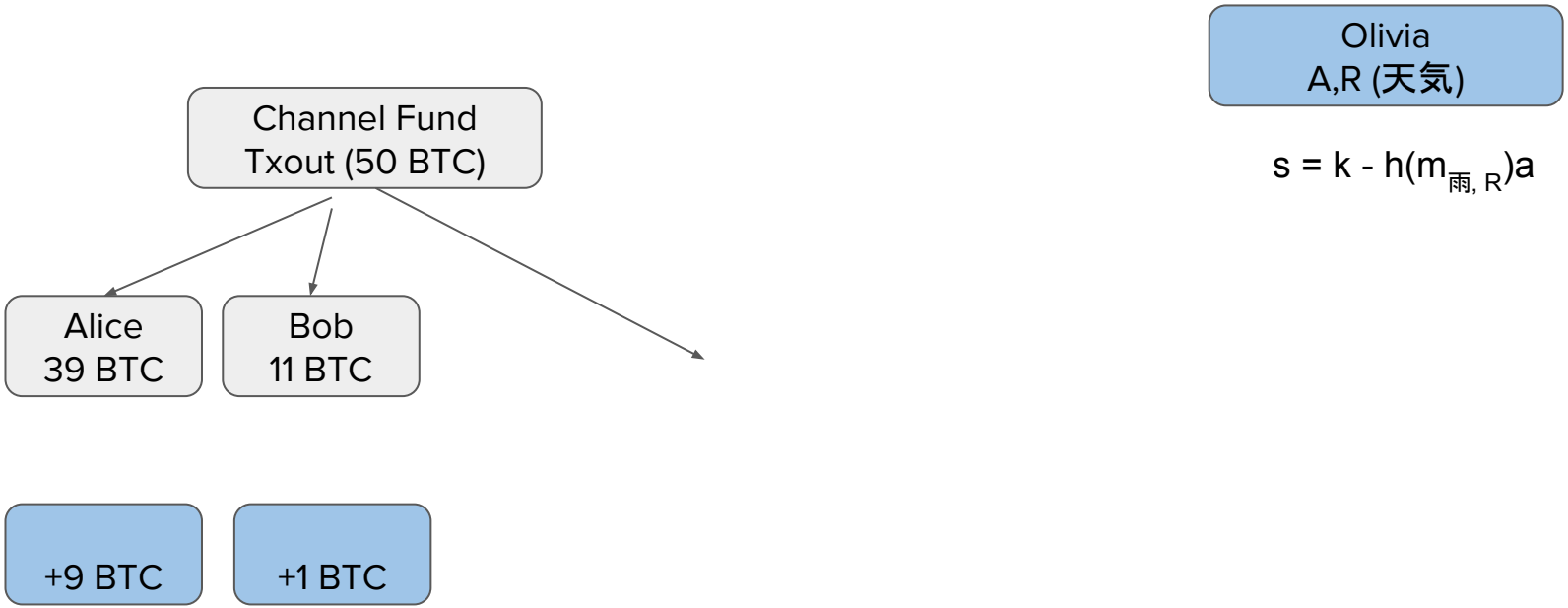


Olivia
A,R (天気)

$s = k - h(m_{雨, R})a$

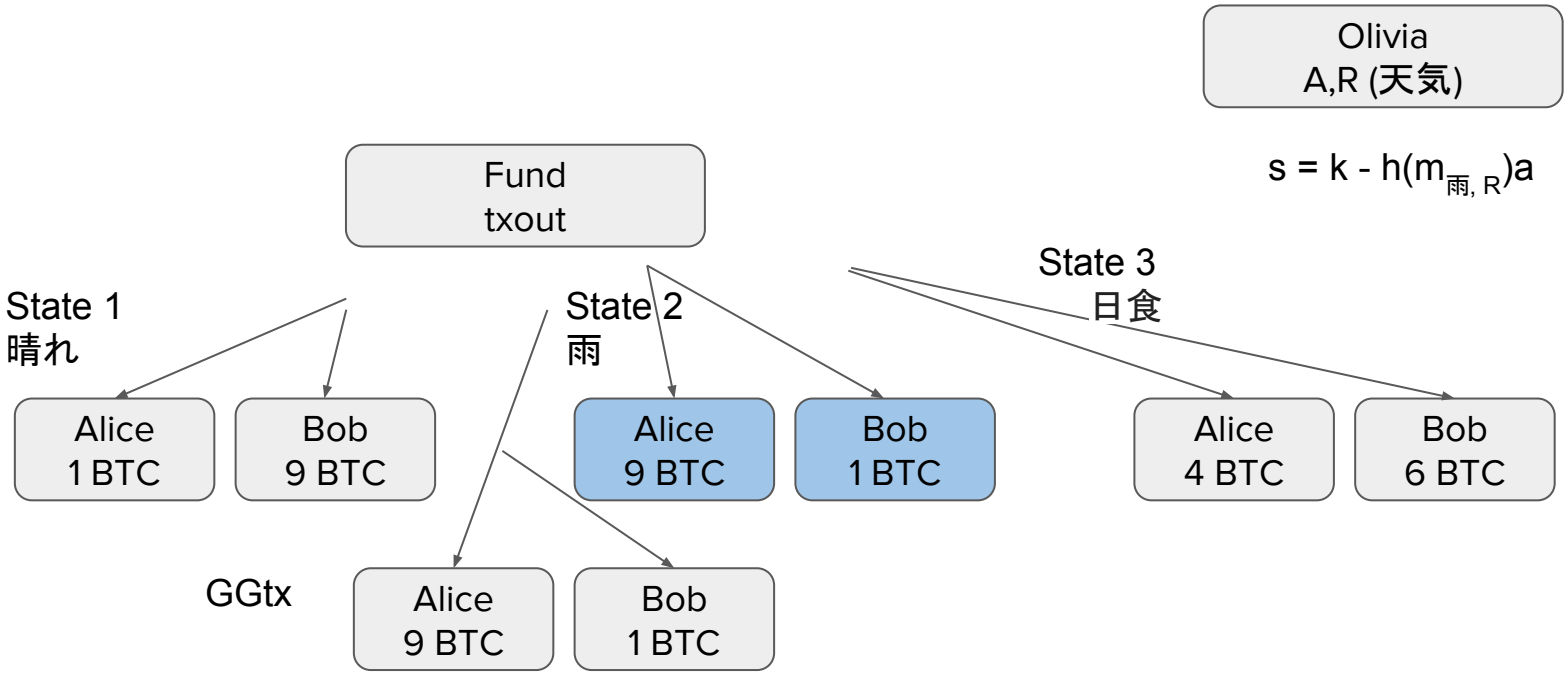
Olivia の $s_{雨}$が出って、State2のが正しい

チャンネルもスマコンもclose出来るけど



Bobが協力したら、チャネルの残高を Alice に9BTCを増やす、そしてスマコンの output を消す

それなら、0txのスマコン



GGtx　みんな同意するから、負ける人が直接の txをサインします

DLCのdiscreet

チャネル内のスマコンなら、相手だけが見える

ネットワークに全部放送しても、公開鍵はoracleのsGと関係見えない。

スマコン？または、LNのチャネル？同じ見た目

天気はいいけど

２つ、３つの結果じゃなくて、みんな使いたいのは、値段

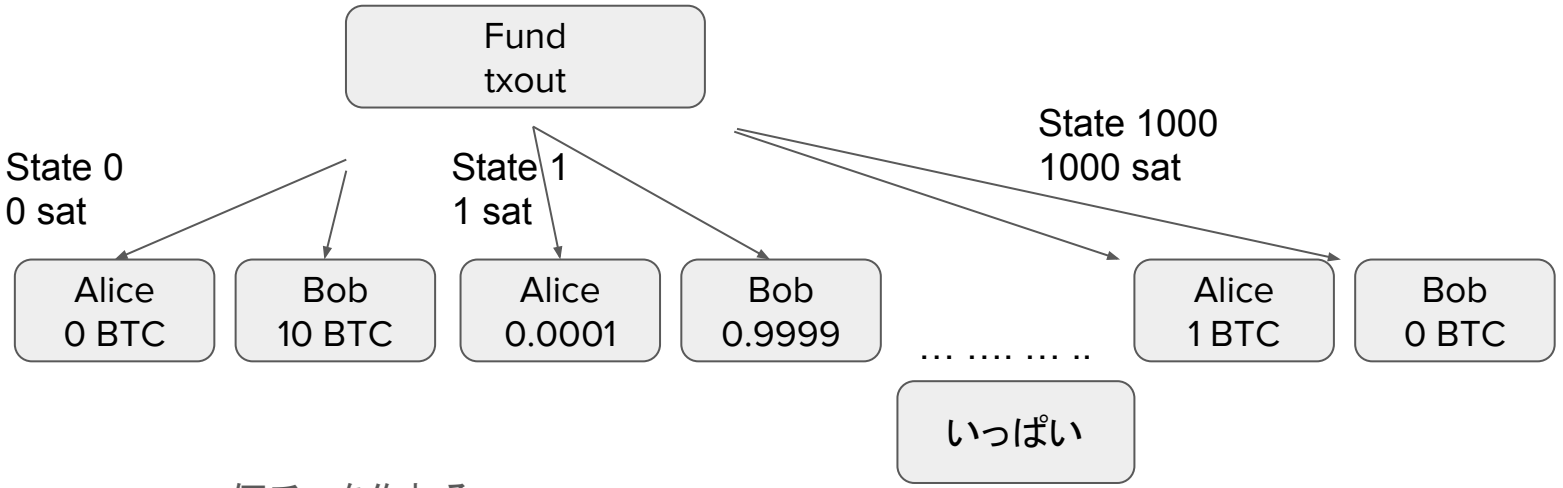
m = 値段(satoshi)なら、出来ます

現在、１円は 330sat

数百取引作れる

Price Data

Olivia
A,R (日本円)



何千txを作れる

1 tx は　～100B
1万tx は 1MBぐらい

off-chainの scalability

数万の別の結果が可能なら
(例えば6桁の値段)
10MBとかになる
悪くないけど、もっと小さく出来る

off-chainの scalability

2つのR, そして2つのs

$R_{exponent}$と$R_{mantissa}$

$R_{exp} = 3, R_{mant} = 43$

$price = 4.3 * 10^{3} = 4300$

ダブルR

結果が変わらない範囲に、R_{exp}だけを使う
例えば値段が 1000、4000、8000でも、Alice が全部貰うなら R_{exp}のsGだけを使う。
結果が大切の範囲に、R_{exp}+R_{mant}を使う

それで、スマコンのサイズは1MB以下に出来る

マルチオラクル

2つのoracle は簡単に使えます

$s_aG + s_bG = s_mG$

ただ色んなoracleのsGポイントをたす

n of n サイズ変わらない

(m of nも出来るけどスマコンのサイズがでかくなる)

DLCの用途

天気？　ヴァーチュアル円、ドル、株

スポーツなど

保険

Prediction marketみたい

非常に残念ながら、ICOやってない　泣

Disctreet log contracts

質問してください。

ご清聴ありがとうございます!