Layer 2 Technology :
スマートコントラクトを活用したブロックチェーン連携

The 2nd Workshop Basing Blockchain

日本電信電話株式会社
NTTサービスエボリューション研究所
渡邊　大喜

自己紹介

- 渡邊　大喜（わたなべ　ひろき）
  - NTTサービスエボリューション研究所　研究員
  - 2015前半より, ブロックチェーン応用研究に携わる
    - BitcoinCoreを使ったDRMシステムの検討
    - Ethereum, Hyperledger Fabric 上の秘匿化方式の検討

ブロックチェーン技術入門, 森北出版, 2017
岸上 順一, 藤村 滋, 渡邊 大喜, 大橋 盛徳, 中平 篤

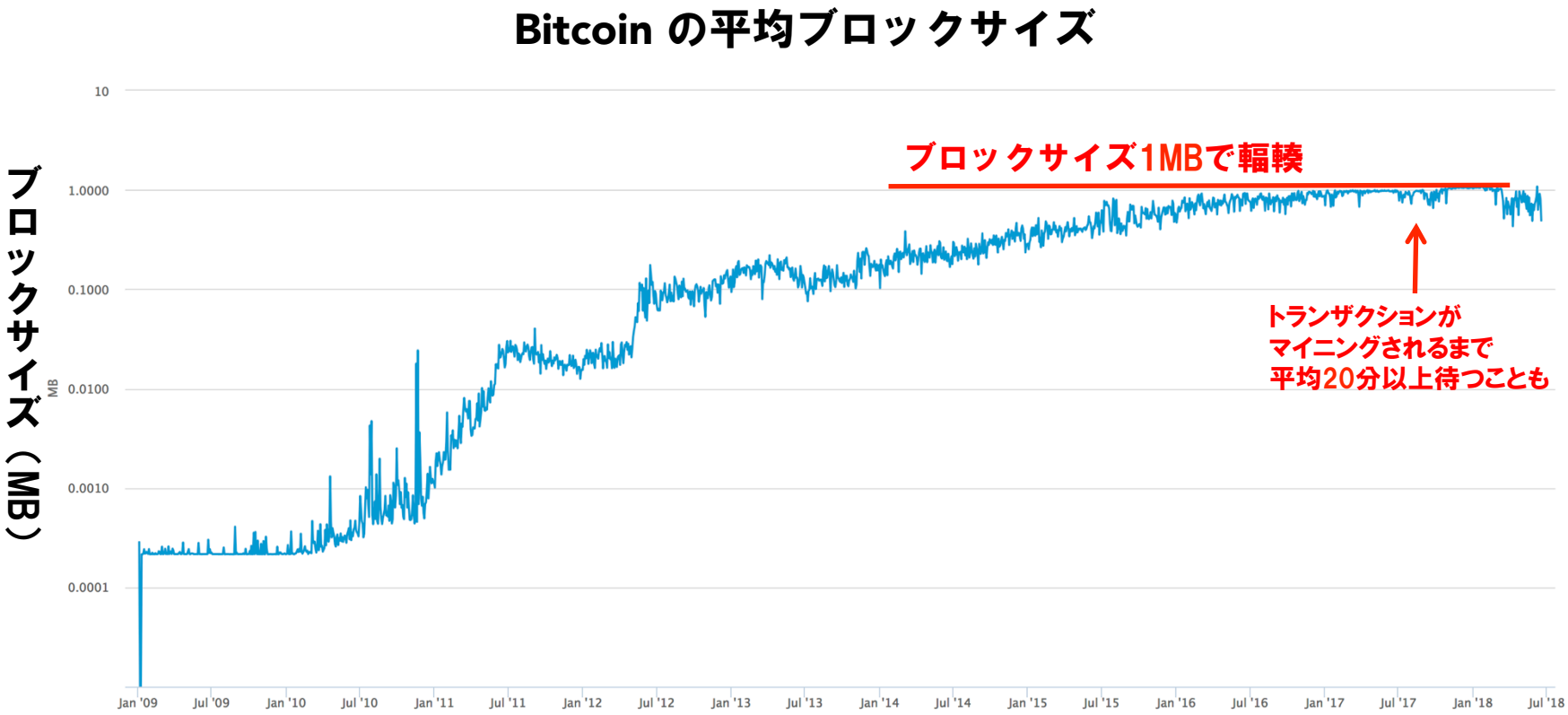
  - 主に、ブロックチェーンの「応用技術」について研究しています
    - Watanabe, H., et al., “Blockchain contract: A complete consensus using blockchain,” IEEE GCCE, 2015.
    - Watanabe, H., et al., “Blockchain contract: Securing a blockchain applied to smart contracts,” IEEE ICCE, 2016.
    - Watanabe, H., et al., “Niji: Autonomous Payment Bridge between Bitcoin and Consortium Blockchain,” IEEE Blockchain, 2018（開催予定：2018.7.30-2018.8.3)←NEW
  - 仮想通貨は買っていません（笑）

今日お話しすること

1. Layer2テクノロジの概要と要素技術

2. Payment Channelを使ったブロック連携方式 Niji
（提案技術）

Scalability問題

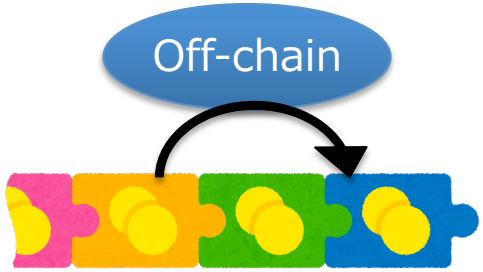


Source: blockchain.info

2つの解決策

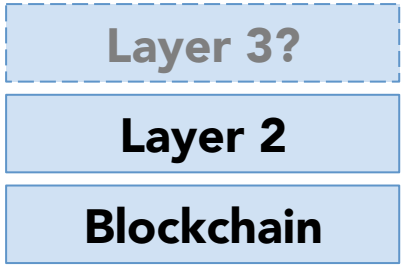
- プロトコル自体の変更
  - 署名の分離（Segwit），ブロックサイズ変更など
  - 果てしない論争の末，自然とブロックサイズは縮小していった…
    （Bitcoinから投資熱が他の通貨に移った？）

- オフチェーン取引
  - ブロックチェーンの外側でスケーリングし、
    最終残高のみをチェーンに記録する
  - 特に，基盤となるブロックチェーンを第一層とし，
    第二層（Layer2)で高効率な処理を行う
    Lightning Networkに注目が集まる



Layer2の定義

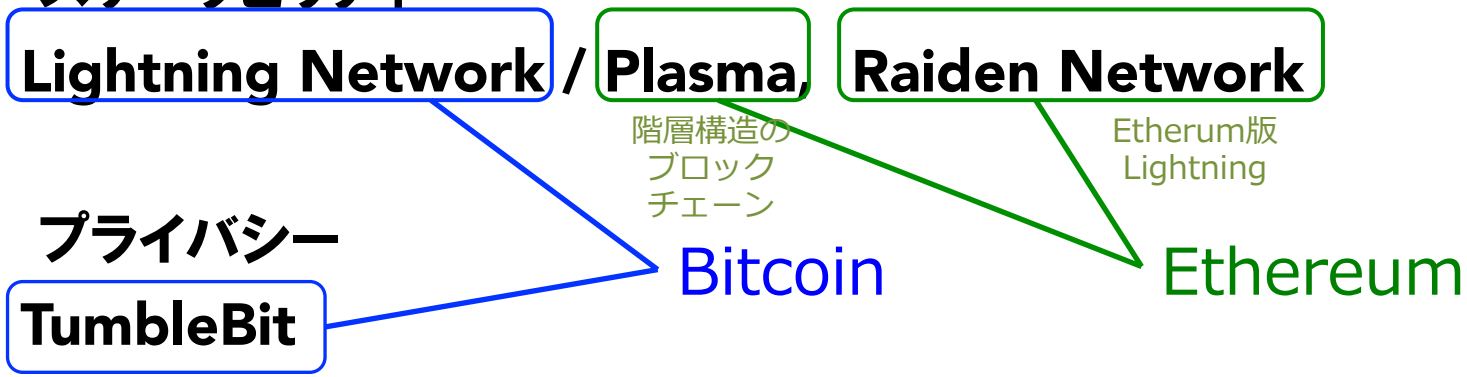
- 厳密なLayer2定義は見当たらず・・・
  - HTTP on TCP/IPのアナロジー
  - 「スケーラビリティの向上やプライバシー保護のため，
    オフチェーンで動作するネットワーク層」
  - 「チェーン上と**同様の**セキュリティ保護を受ける」
    - 単一のエンティティに支配されない
    - Double spendingが成立しない



様々なLayer2の提案

現在では，Layer2に相当する多様なプロトコルが提案されている

- **スケーラビリティ**



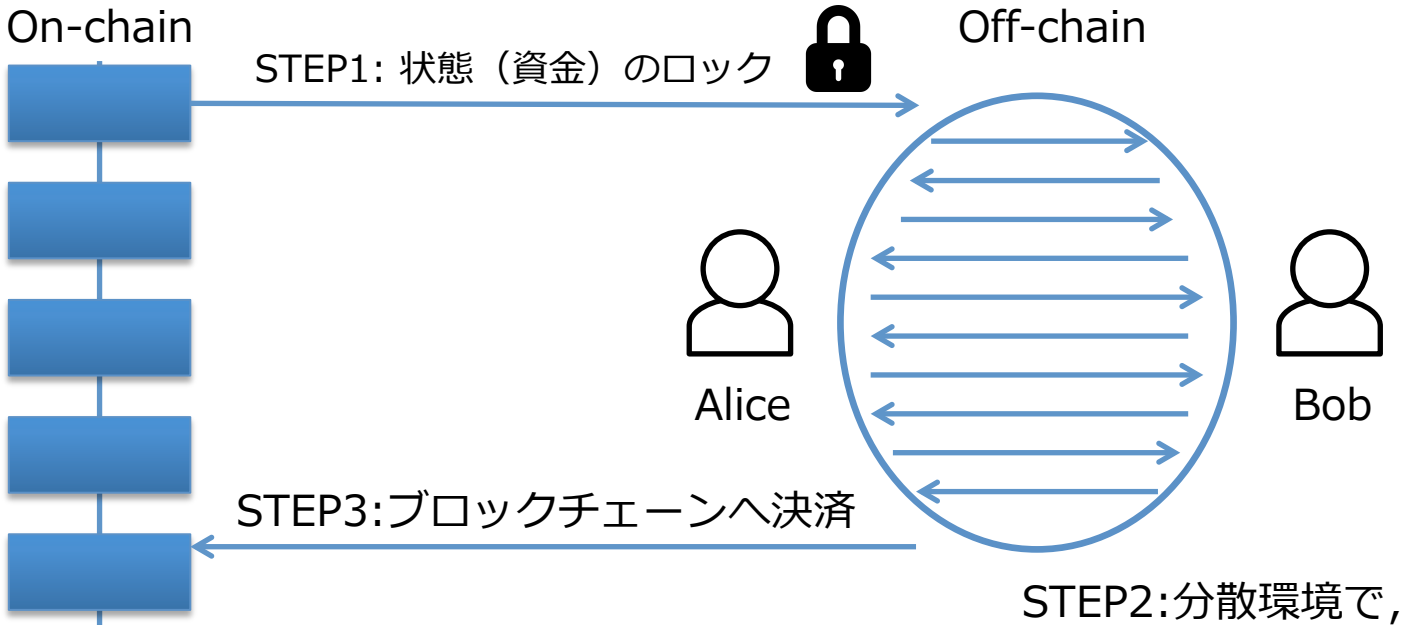
- **プライバシー**

- **相互運用性** Inter-blockchain

  Cosmos / Polkadot ブロックチェーンを仲介するブロックチェーン

Layer2を実現する3ステップ

- **Layer2技術は，概して3つのステップから成る**



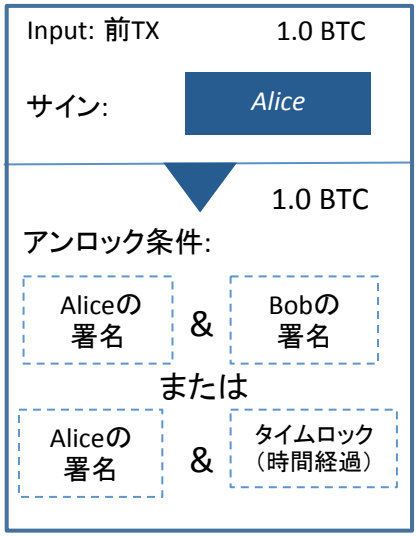
要素技術：Payment Channel (Bitcoin)

- 2者間において取引の“チャネル”を構築し，
  ブロードキャストせずに，複数回取引を更新できるテクニック

- Bitcoinのスクリプティングを利用し，資金の移動に制限をかける

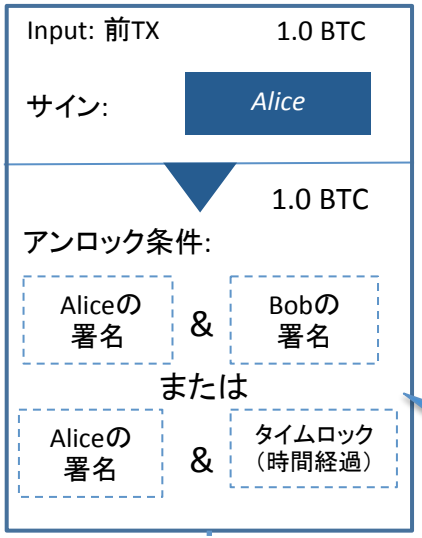
Simple payment channel

「Alice」から「Bob」への単方向チャネル



Simple payment channel

「Alice」から「Bob」への単方向チャネル



Bitcoin NW

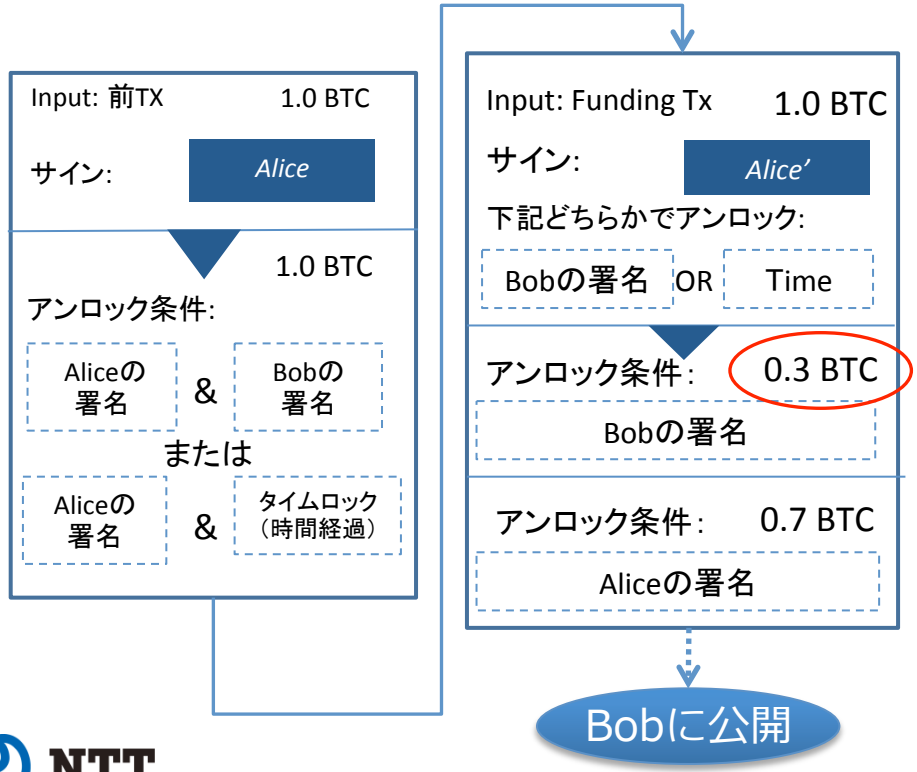
STEP1：資金のロック（ON-chain)

Aliceはタイムロック付きの
Bobとのマルチシグに入金する
これはネットワークにブロードキャスト

AliceとBobの署名
or
一定時間経過すると
Aliceのみの署名でアンロック

Simple payment channel

「Alice」から「Bob」への単方向チャネル



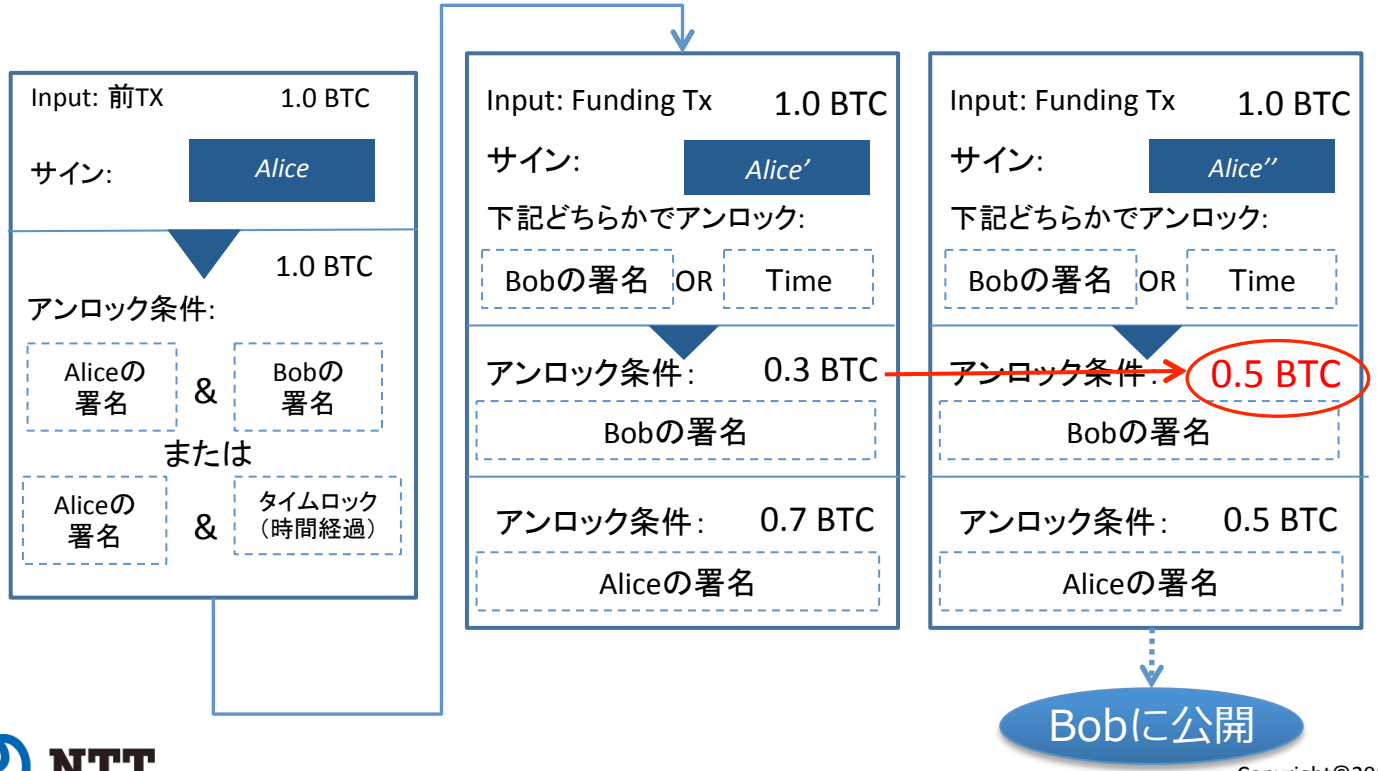
STEP2：取引（OFF-chain)

先のトランザクションを入力とし，
AliceはBobに0.3BTC支払うTXを作り，
Aliceのみ署名する
（Aliceのみなので
不完全なトランザクション）

これをBobに公開し，
BobがAliceの**署名を検証し正しければ**
取引成立

Simple payment channel

「Alice」から「Bob」への単方向チャネル



STEP2：取引（OFF-chain)

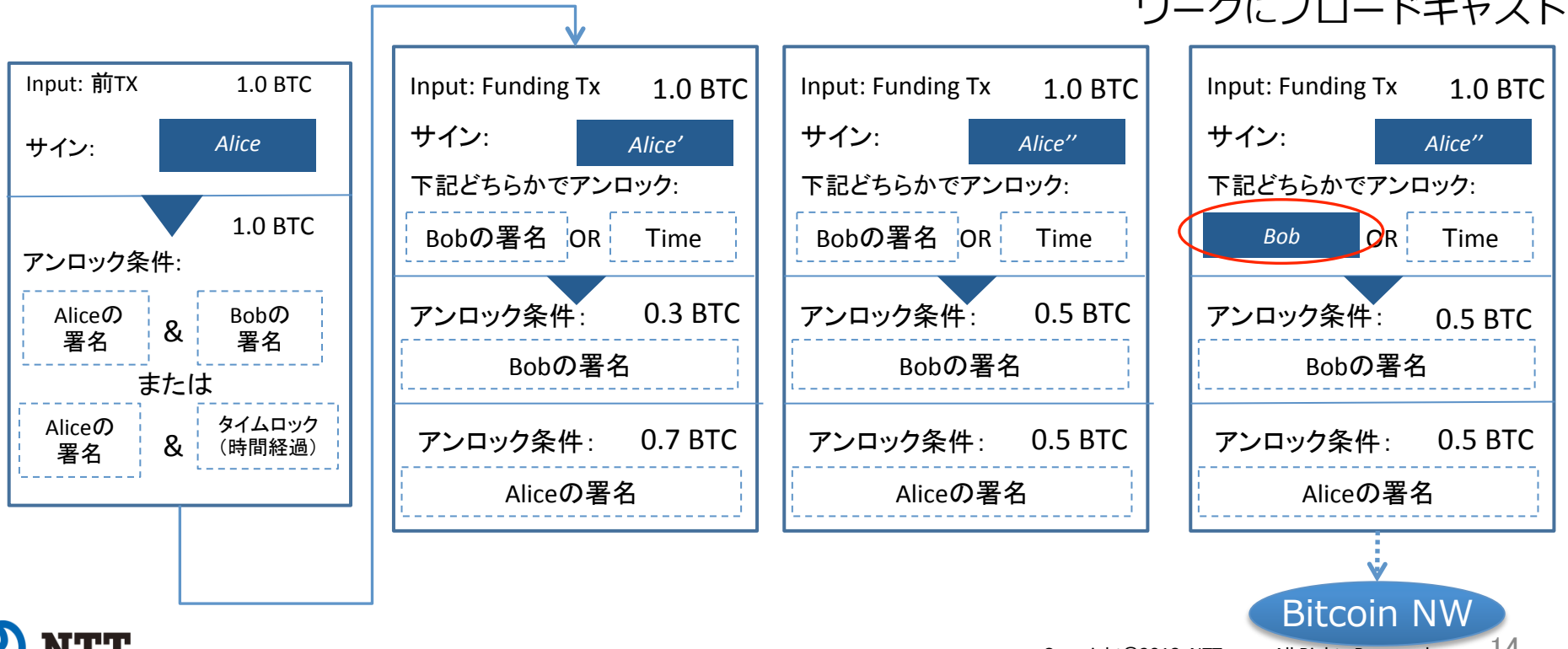
不完全なトランザクションのまま送金額を書き換え署名をつけて更新

Bobが検証して取引成立

Simple payment channel

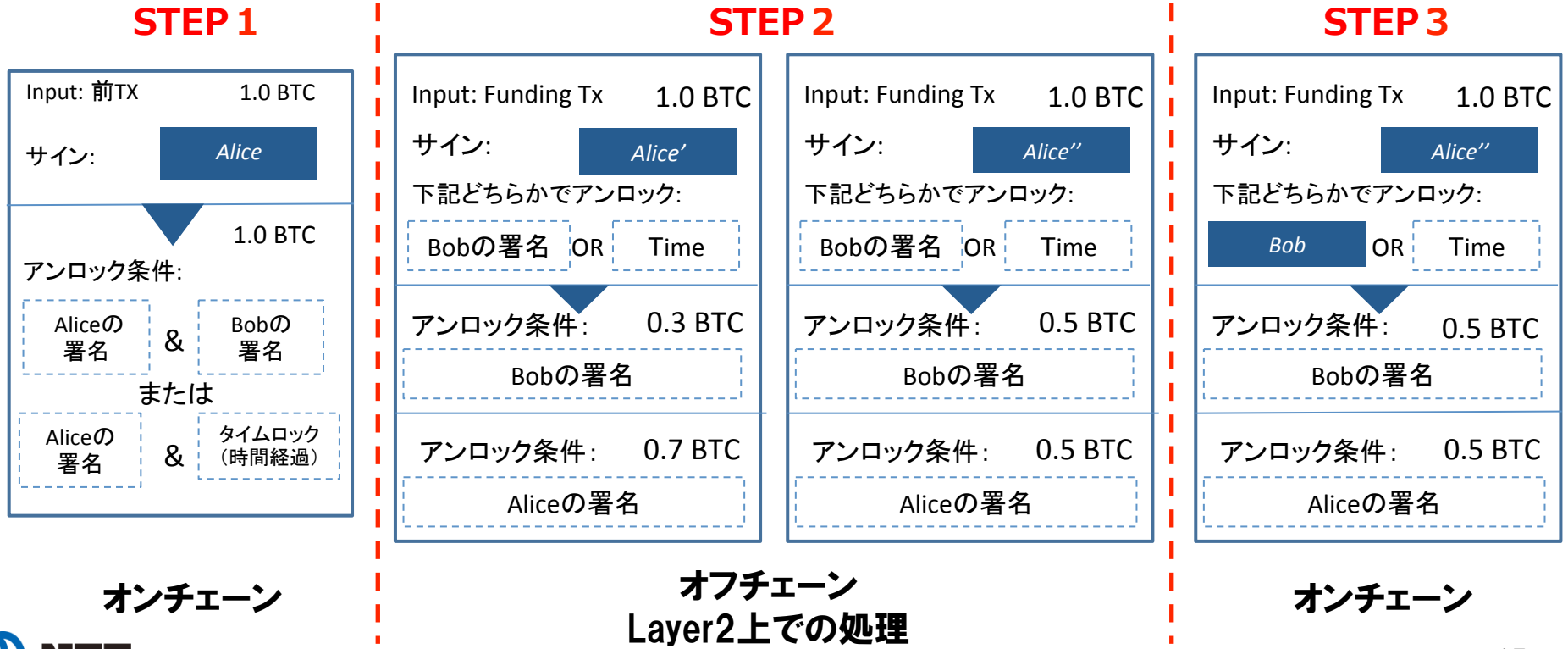
「Alice」から「Bob」への単方向チャネル

STEP3：決済（ON-chain）
Bobが最終的に署名してネットワークにブロードキャスト



Simple payment channel

「Alice」から「Bob」への単方向チャネル



様々なPayment Channelの設計

Innovative R&D by NTT

単方向チャネル（A→B）

- **Spillman-style payment channels (= Simple payment channel)**
  Jeremy Spillman, “Re: Anti DoS for tx replacement, bitcoin-development mailing list”, 20 April 2013
- **TumbleBit (Payment Hub)**
  Ethan Heilman, Leen AlShenibr, Foteini Baldimtsi, Alessandra Scafuro and Sharon Goldberg, “TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub”, 2016

双方向チャネル（A→B，B→A）

- **Duplex payment channels**
  Christian Decker, Roger Wattenhofer, “A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels”
- **Lightning Network payment channels**
  Joseph Poon, Thaddeus Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”

NTT

様々なPayment Channelの設計

Innovative R&D by NTT

単方向チャネル（A→B）

- **Spillman-style payment channels (= Simple payment channel)**
  Jeremy Spillman, “Re: Anti DoS for tx replacement, bitcoin-development mailing list”, 20 April 2013
- **TumbleBit (Payment Hub)**
  Ethan Heilman, Leen AlShenibr, Foteini Baldi… …aron Goldberg, “TumbleBit: An Untrusted Bitcoin-Compatible Ano…

Payment Channel
＋
暗号パズルを使った
匿名化

双方向チャネル（A→B, B→A）

- **Duplex payment channels**
  Christian Decker, Roger Wattenhofer, “A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels”
- **Lightning Network payment channels**
  Joseph Poon, Thaddeus Dryja, “The Bitcoin Li… …-Chain Instant Payments”

ペナルティを導入した
Payment Channel
＋
マルチホップや
ルーティング

NTT

Layer2の概念と要素技術 ここまで

Innovative R&D by NTT

Layer2のイメージをざっくり
捉えていただけたら幸いです

NTT

今日お話しすること

1. Layer2テクノロジの概要と要素技術

2. Payment Channelを使ったブロック連携方式　Niji
（提案技術）

背景

- **Layer2技術において，Bitcoinコミュニティとしては，「スケーラビリティ」「プライバシー」を特に強く意識**

- **一方，産業界としては，PublicなBitcoin（仮想通貨）よりも，ブロックチェーンそれ自体が何に使えるかに興味あり**
  - ブロックチェーンを利用したSI案件，実証実験の増加
  - 最大の強みは，非中央集権的なサービスが作れること

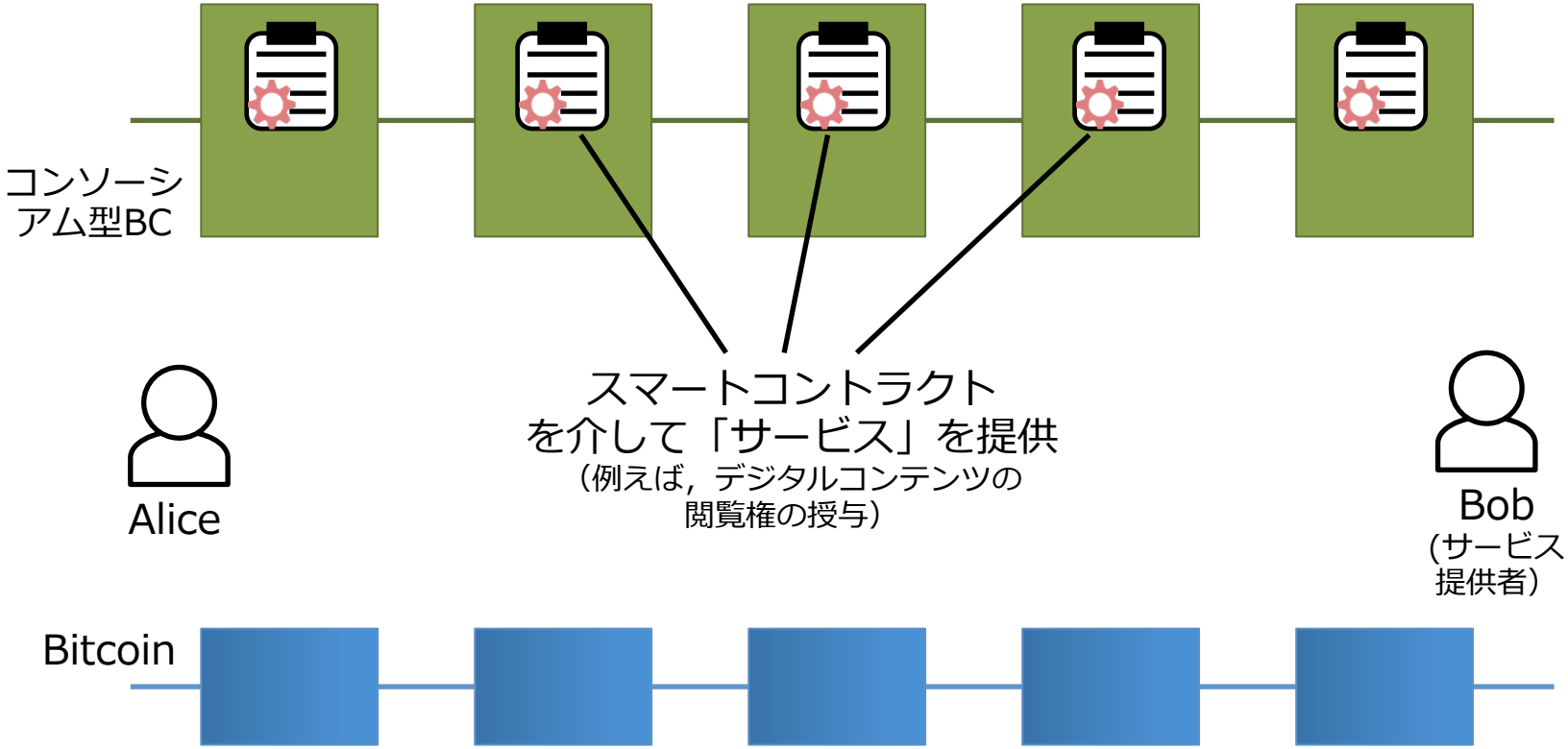
- **コンソーシアム型Blockchain基盤の開発も活発に行われている**
  - Hyperledger, R3 Corda, Ethereum Enterprise Alliance

研究の着眼点

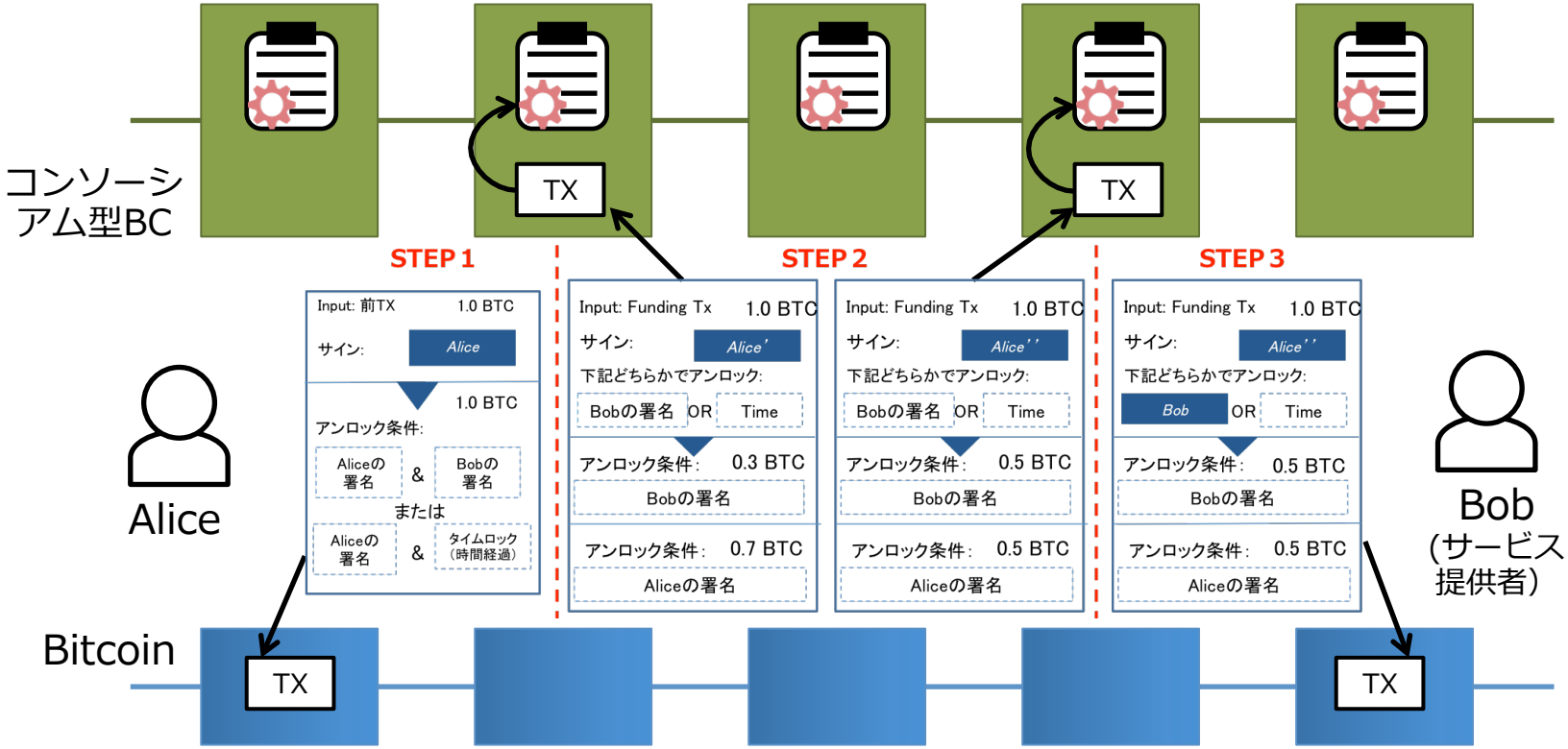
- **コンソーシアム型BCでは，多くの場合**
  “トークン”は市場価値を持たず，決済手段の導入が難しい
  - ICOによる価値獲得も行われているが，草コインに対する攻撃が後を絶たたず、リスク高
  - 提供したサービスの対価は，誰がどのように決済責任を負うか？
    （e.g., P2P電子書籍の販売）
  - 分散と集権化のバランス設計することは極めて難しい

仮想通貨の支払いはBitcoin,
サービスの提供（Smart Contract）をコンソーシアムチェーン,
といった具合に、役割を切り分けて連携できないか

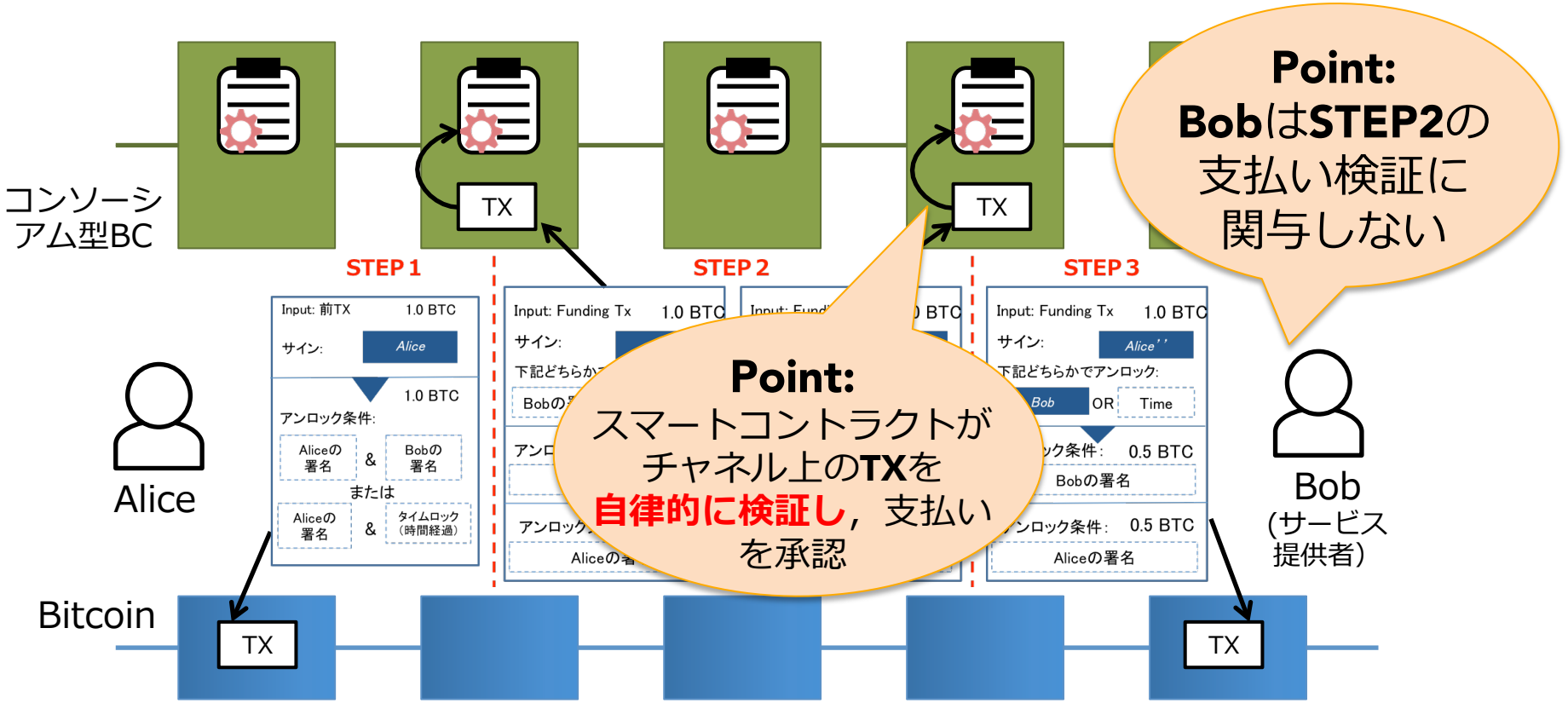
基本となるアイディア



基本となるアイディア



基本となるアイディア



どのコントラクト実行環境を用いるか？

- コンソーシアム型BCの各基盤に互換性はない
- コントラクト実行環境の選択がプロトコル設計に影響
  - Chaincode container (Hyperledger Fabric)
  - Etherum Virtual Machine (EVM) (Ethereum)

どのコントラクト実行環境を用いるか？

- コンソーシアム型BCの各基盤に互換性はない
- コントラクト実行環境の選択がプロトコル設計に影響
  - Chaincode container (Hyperledger Fabric)
  - Etherum Virtual Machine (EVM) (Ethereum)

    【メリット】
    - 移植性が高く，Ethereumのみならず，多様なBC基盤（Hyperledger, Quorum)でも展開が進む
    - Publicなチェーンで安全性の検証が進んでいる

    【デメリット】
    - 計算コストの制約（gasの仕組み）
    - (ネイティブに比べて）貧弱なオペコード

Point:
制約の多い**EVM**に合わせた
プロトコル設計とすることで
他基盤への展開も視野に

EVMで動作可能な汎用プロトコル(Niji)

- **EVMで動かすための3つの課題**

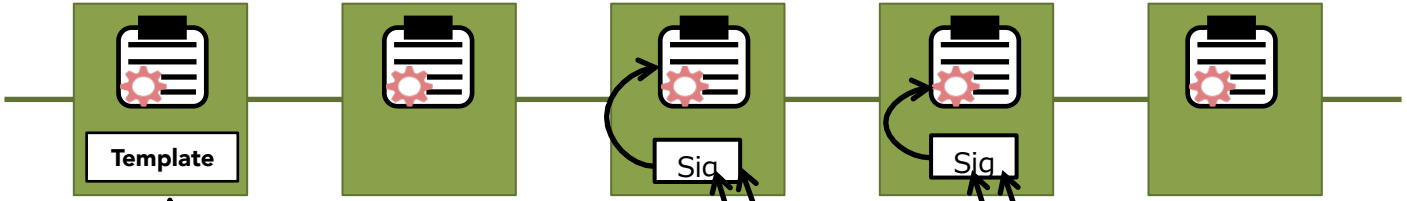
  1. 計算コストをEVMの制約内に抑える
  - コントラクトをセキュアに保つためには
    gasの制約内に収め，EVM側の改造は行わない

  2. Bitcoin署名をEVM上で検証する
  - 通常のオペコードではBitcoinの署名検証は高コスト

  3. 双方向チャネル化(bi-directional)
  - 支払いのキャンセルなどには双方向チャネルが必要
  - (現在検討中)

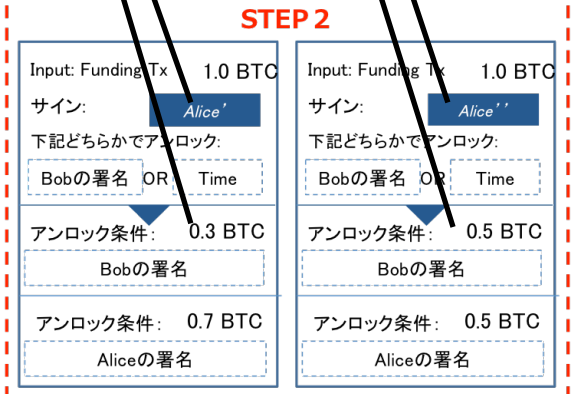
1. 計算コストをEVMの制約内に抑える

解決策：
トランザクションのテンプレート（雛形）を
事前にコントラクトで管理し，差分情報（署名や金額）のみを提出させる



STRUCTURE OF TRANSACTION TEMPLATE

Field		Value
Version		2
Input count		1
Input [0]	Previous output	<funding tx hash>
	Index	<index of previous output>
	Script	only <redeemScript of previous output> **(no signatures)**
Output count		2
Output[0]	Value	**nil**
	Script	contains <service provider's pubkey hash>
Output[1] (change given back to user)	Value	**nil**
	Script	contains <user's pubkey hash>



2. Bitcoin署名をEVM上で検証する

- **BitcoinとEthereumの署名(ECDSA)では，同じsecp256k1曲線を使用していることに着目**
  - ただし，BitcoinではDERフォーマット，Ethereumでは(v, r, s)パラメータで表現されている

$$Sig_{DER} \rightarrow (v,r,s)$$

  - EVMではEthereumの署名値とメッセージからアドレスを出力する特殊な関数（Precompiled contracts)が存在する

```
ecrecover(bytes32 hash, uint8 v, bytes32 r,
    bytes32 s) returns (address)
```

上記はSolidityで規定のインタフェース，メッセージ（hash）は署名前TXにsha256dして算出

  - さらに，Bitcoinの公開鍵を仮想的にEthereum形式のアドレスに変換することにより，署名検証可能

3. 双方向チャネル化(bi-directional)

- ここまでの解決策1と2は単方向チャネルでは成立
- ただし，実用には双方向チャネル化も必要(キャンセル時)
  - Lightning Networkのチャネルが**適用ができない**
    - 更新毎に双方の合意が必要
    - 相手の裏切りを監視するため，常にオンラインであることが推奨
  - (現在方式検討中)

評価（単方向チャネルのみ）

- Bitcoin testnet & go-ethereum(4nodes, PoA consensus)
- 一般的なEVMのスマートコントラクトのgasの範囲に収まることを確認
- 実験条件下で，平均2.5秒前後のレスポンスタイムで支払い完了
  （うちコンソーシアムのコンセンサスが1秒，プロトコル部分は実質1.5秒）

TABLE II
GAS COST OF COMPUTATIONAL WORK

Operation	Gas cost (gas)
Deploy bridging contract	1,785,044
Set deposit information	245,922
Set transaction template	285,183
Update payment	455,355
Close channel	46,626

ブロック上限
(8百万Gas)
に収まる

Publicでは
高すぎる程度
のGas量

TABLE III
TIME ANALYSIS OF OPERATIONS IN PAYMENT STEP.

Task	Mean	Maximum	Minimum	Std. Deviation
Get transaction template	677	793	632	20.7
Update payment	1817	2663	1124	353
Total	2493	3359	1770	352

まとめ： 本方式(Niji)がもたらす効果

- **コンソーシアムチェーンでの仮想Bitcoin払い**
  - Dollarization(自国でドルを公的通貨として認める)
    ならぬ”Bitcoinization”
  - ICOを行わなくても**分散＆セキュアな支払い手段**を獲得
  - 資金はPayment Channelによって保護され，
    決済スピードはコンソーシアムチェーンによってスケール可能
  - プロトコル自体は，柔軟に多様な基盤と接続可能（**緩い連携**）
- **一方で・・・**
  - コンソーシアムチェーンの不正（例えば二重払い）が発生したとして，
    親チェーンが強制的に状態を巻き戻すことはできない
  - Ethereumの「Plasma」なら可能（**堅い連携**）