FUJITSU
shaping tomorrow with you

2018年電気系同窓会 講演資料

# ブロックチェーンのスケーラビリティ技術

2018年10月20日

(株)富士通研究所 ソフトウェア研究所 デジタルサービスPJ
東京大学大学院情報理工学系研究科(松浦研究室)D1
宮前 剛

# 本日の講演内容

- (ブロックチェーンの)スケーラビリティ分析
- (ブロックチェーンの)スケーラビリティ向上技術
  - オンチェーン最適化
  - ブロックチェーン相互接続
  - オフチェーン技術
- オフチェーン技術の紹介
  - 単方向ペイメントチャネル
  - Lightning Network
  - 双方向ペイメントチャネル
  - TumbleBit

# スケーラビリティ分析

# ブロックチェーンのスケーラビリティ

FUJITSU

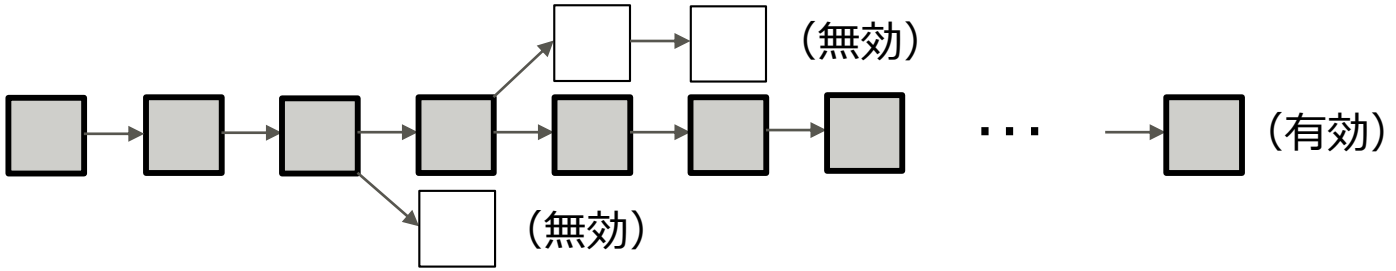
- ブロックチェーンの場合、トランザクション性能のことを「スケーラビリティ」と呼ぶことが多い
- 現状、単一ブロックチェーンのスケーラビリティは極めて低いのが現実
  - 非中央集権性、耐改ざん性などを実現するための性能面のコスト負担
  - VISAが15,000TPS(Transaction/s)に対して、ビットコインは高々7TPS
- パブリックチェーンの場合は、不特定多数の参加者を認めて中央集権を回避する設計思想のため、認証の仕組みを敢えて設けていない
  - その代わりに、シビル攻撃を防止するために、承認権限の根拠としてアカウント数ではなく計算リソースや資産リソースを設定
    - 全ての参加者ができるだけ対等な承認権限を持てるような工夫
    - Proof-of-Work(ビットコイン), Proof-of-Stake(Ethereum), etc.
- コンソーシアムチェーンの場合は、参加者を特定企業に限定することによって(Permissioned)、ブロックの承認プロセスを単純化
  - Hyperledger Fabricでは、Proof-of-Workよりはるかに単純なビザンチン耐性アルゴリズム(PBFT)を適用することにより、1,000TPS程度を実現

# Proof-of-Workのスケーラビリティ

FUJITSU

## Proof-of-Work方式とは

- ハッシュ計算のパズルが解かれたブロックを正式承認されたブロックとみなし、パズルを解いた参加者に報酬を付与
  - このようにして新しいブロックを生成する行為を「マイニング」、生成者を「マイナー」と呼ぶ
  - パズルは全参加者が並列に挑戦するため、ブロック列の分岐が発生し得る
  - ブロック列が分岐した場合は、最長のブロック列のみが有効とみなす（最長ルール）



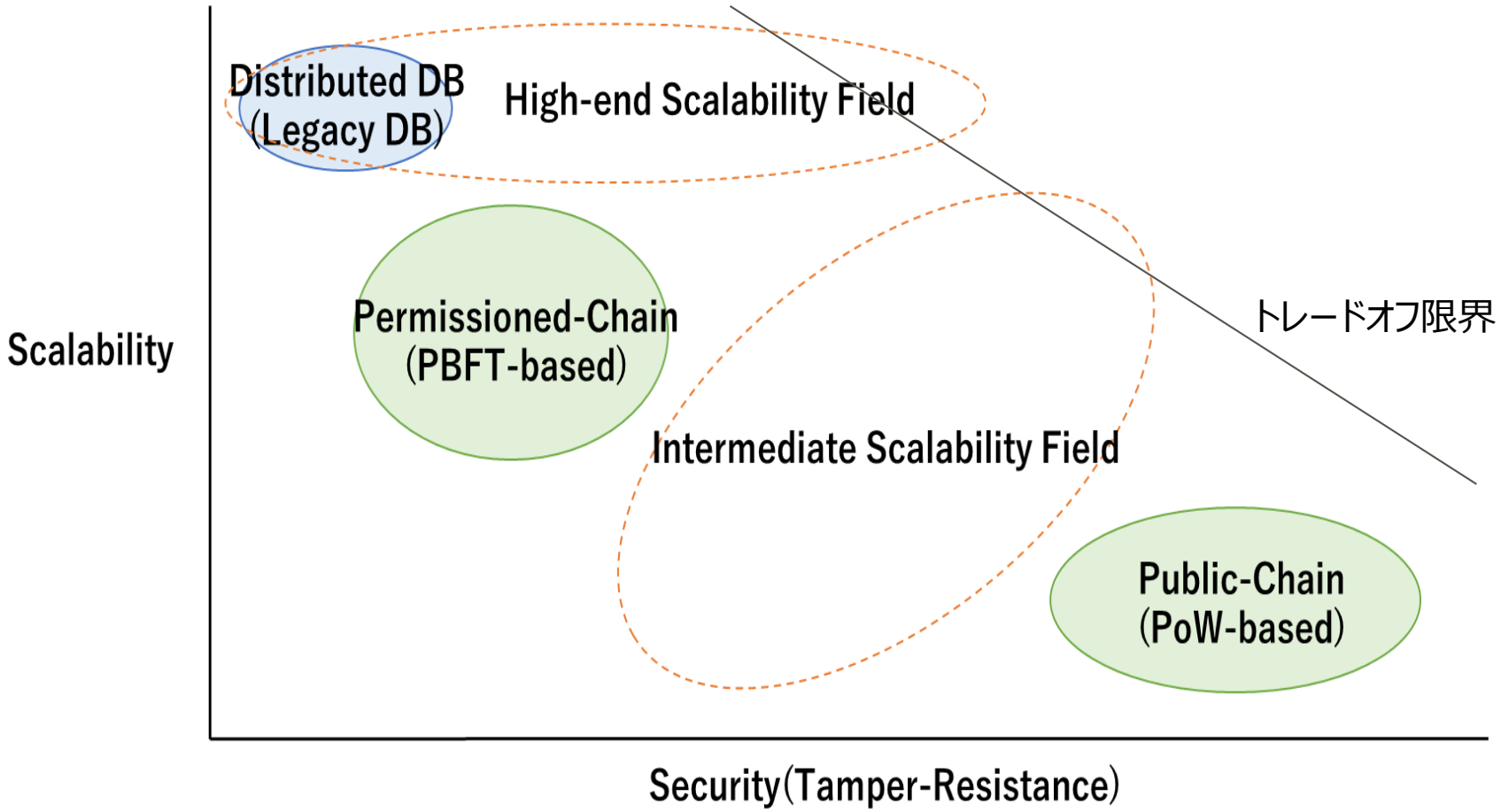

## ブロックの伝播速度

- パズルが解かれたブロックは各参加者にP2Pで伝播されるため、全参加者（ビットコインの場合は1万ノード）へ到達するのに30秒程度必要
- 従って、ブロックの生成間隔は、少なくともこの程度の時間的なオーダーの必要あり
  - 生成間隔がこれより短い場合、ブロック列の分岐確率が上昇（セキュリティ低下）
  - ビットコインのブロック生成間隔は平均10分

# セキュリティとスケーラビリティの関係

FUJITSU

- 両者の間にはトレードオフの関係が存在
  - セキュリティ(耐改ざん性)に応じたスケーラビリティを追求することが重要
  - High-endのフィールドと、PermissionedとPublicの中間のフィールドが未開拓

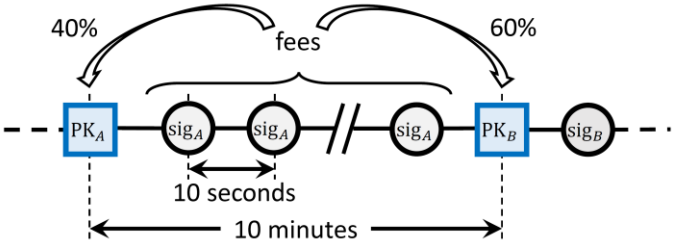


# スケーラビリティ向上技術

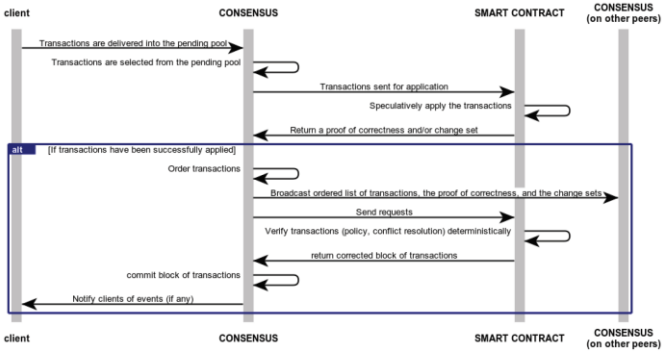
# オンチェーン最適化

- オンチェーン最適化とは
  - ブロックチェーン自身のトランザクション性能を向上させる技術

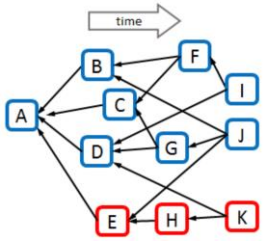
- 有効ブロックの重み付け最適化
  - GHOST
- トランザクション処理効率の最適化
  - Bitcoin-NG, Segwit
- PBFTの性能最適化
  - MinBFT, CoSi(ByzCoin), FastBFT
- トランザクションの投機的並列実行
  - Hyperledger Fabric v1.0
- DAGベースの並列トランザクション
  - IOTA, NANO(RaiBlocks), Byteball, GHOSTDAG



（Bitcoin-NGの論文より引用）



（Hyperledger Fabricのホワイトペーパーより引用）



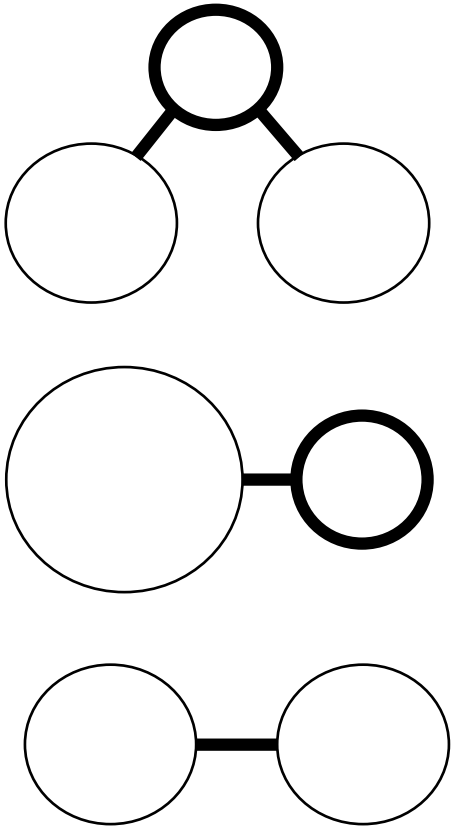
（GHOSTDAGの論文より引用）

# ブロックチェーン相互接続

FUJITSU

- ブロックチェーン相互接続とは
  - 異なるブロックチェーンをまたがるトランザクションをサポートすることにより、全体のトランザクション性能を向上させる技術

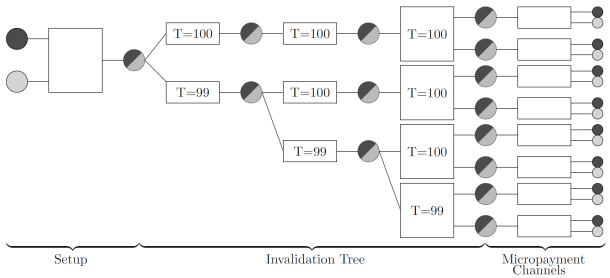
- エスクローベースの相互接続プロトコル
  - Ripple Interledger Protocol (ILP)
  - Fujitsu ConnectionChain
- 分割したチェーン間の相互接続
  - OmniLedger, Ethereum Sharding
- 軽量トランザクションのオフロード
  - Pegged Sidechain(Blockstream)
  - Ethereum Plasma
- チェーン同士の直接接続（クロスチェーン）
  - Atomic Swap



# オフチェーン技術

FUJITSU

- オフチェーン技術とは
  - ブロックチェーンの安全性を根拠に、ブロックチェーンの外で安全にトランザクションを実行する技術
    - ブロックチェーンにトランザクションを書き込まないため、非常に高速
    - ブロックチェーンのトランザクションコストが発生しないため、マイクロペイメントを実現する手段として注目
- ペイメント・チャネル
  - 予めデポジットされた金額の範囲内で、参加者間で未伝播トランザクションを取引
  - ビットコイン系
    - Spilman, Decker, Poon-Dryja, Bolt, Teechan, TumbleBit, eltoo, Channel Factories
  - イーサリアム系
    - Raiden



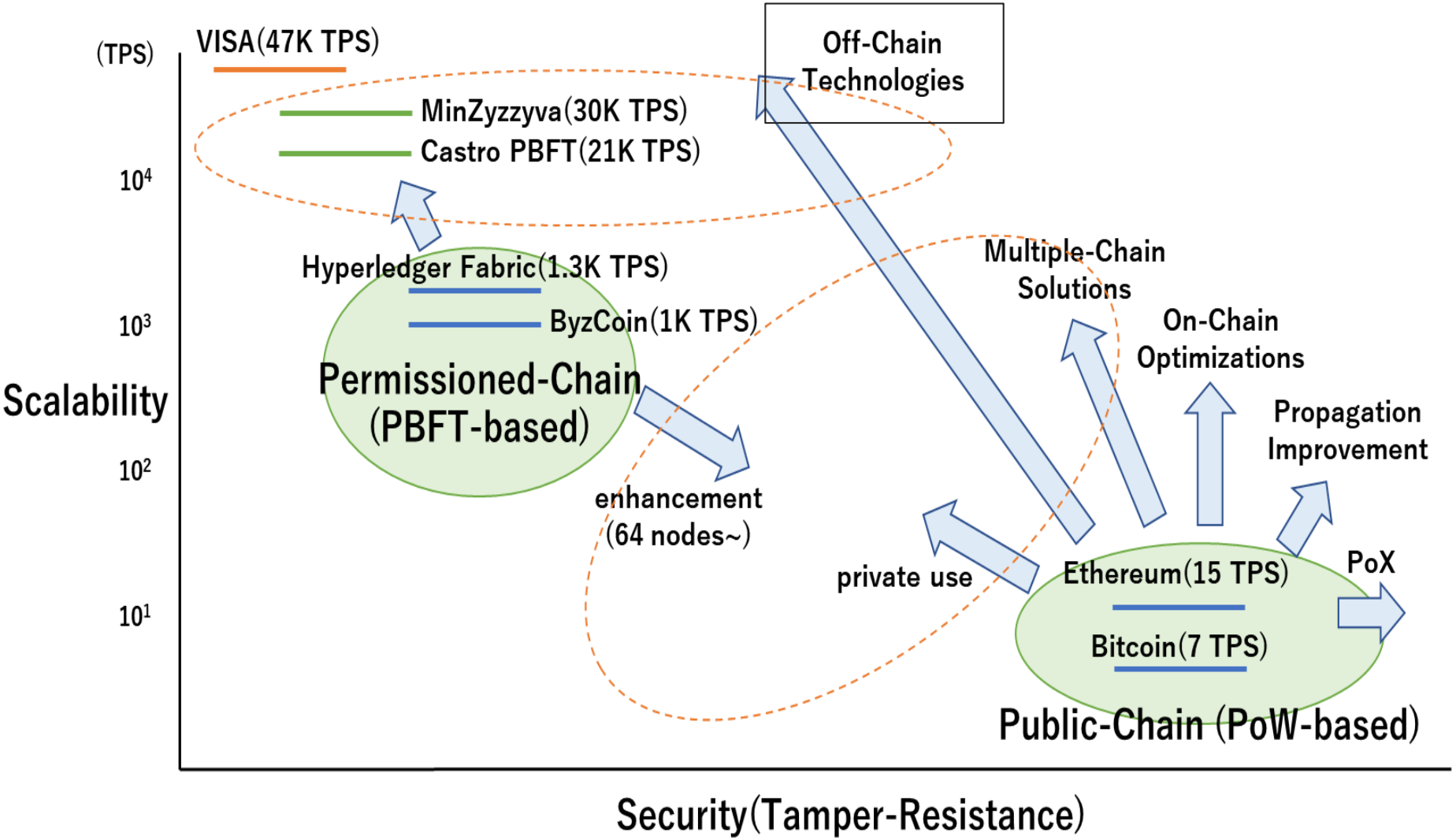
（Deckerの論文より引用）

- ペイメント・ネットワーク
  - ペイメント・チャネルを連結し、ネットワーク上の任意の参加者にオフチェーン送金
    - Lightning Network, Sprites, Fulgor/Rayo

# スケーラビリティ技術が実現する領域

FUJITSU

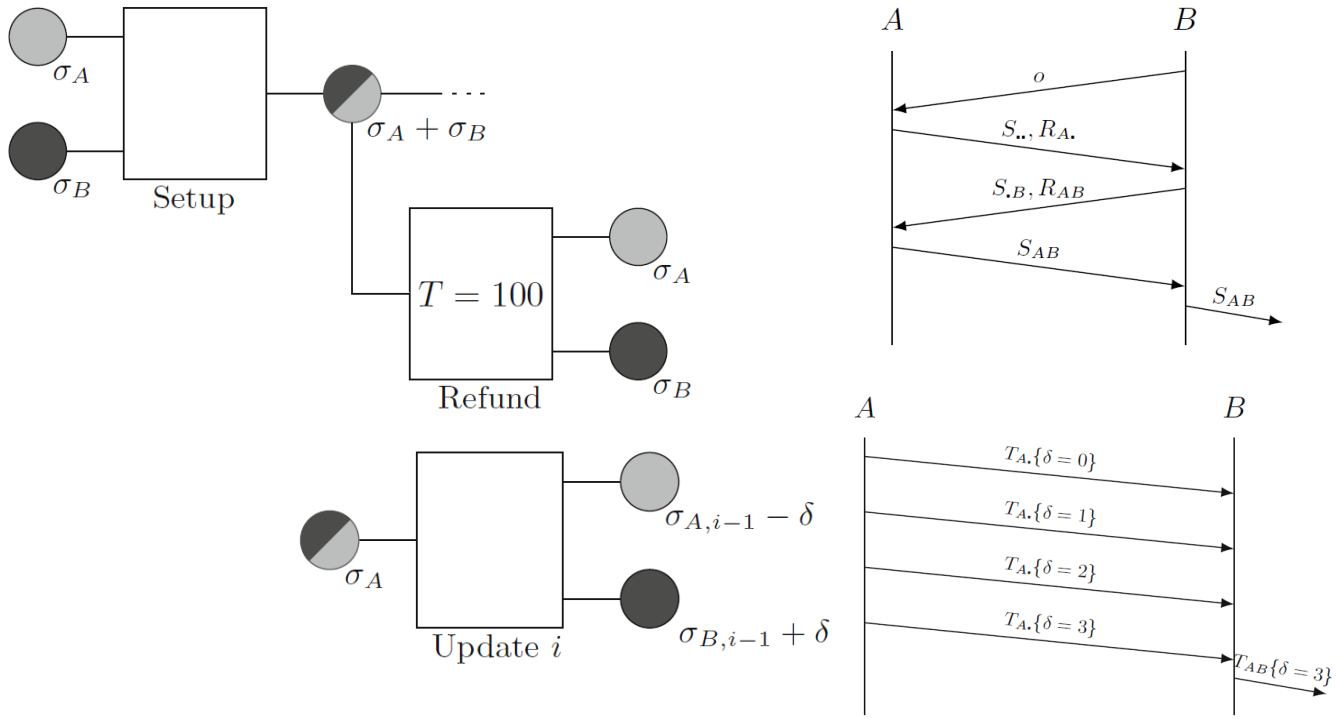
■ 既存のデータベース領域の性能に挑むオフチェーン技術に注目



# オフチェーン技術のご紹介

# 単方向ペイメントチャネル [Spilman, 2013]

- 将来的にブロックチェーン・ネットワークに流すことが可能な未伝播トランザクションデータを、チャネルの当事者のみの間でローカルに取引
  - トランザクションをブロックチェーン・ネットワークに流さないため、即時決済が可能で、かつブロックチェーンの手数料が不要

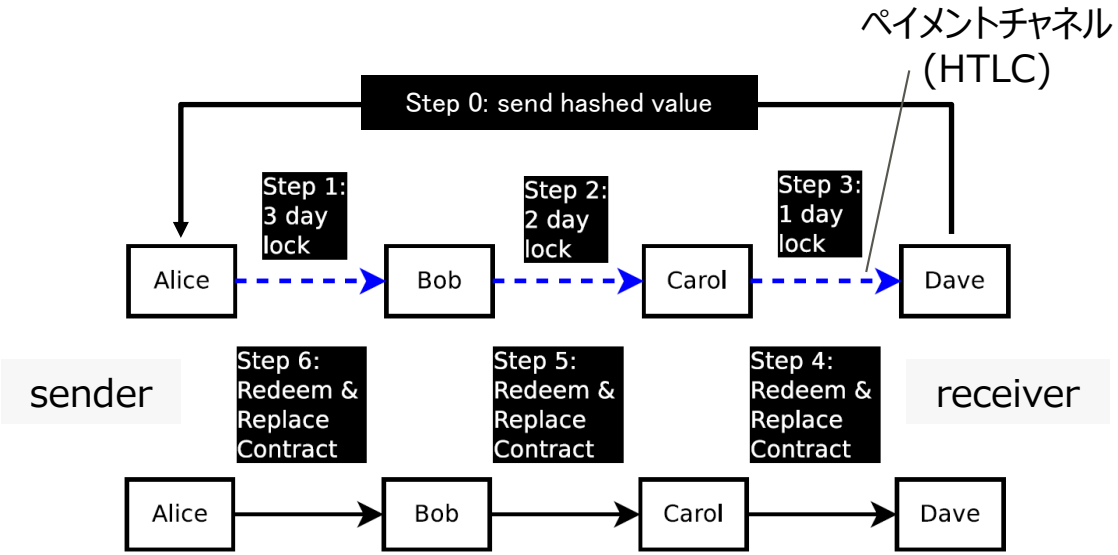



（図はDeckerの論文より引用）

# ライトニング・ネットワーク [Poon and Dryja, 2015]

FUJITSU

- Hashed Timelock Contracts (HTLC)
  - ハッシュ値の元の値を知っていたらビットコインを受け取れるコントラクト
- ルート上の全てのペイメントチャネルで同じハッシュ値のHTLCを締結
- 送金先の参加者がハッシュ値の元の値を開示
  - 全てのHTLCが有効になり、送金元から送金先への送金と同等の結果を得る
  - これにより、直接ペイメントチャネルを張っていない相手とのオフチェーン取引が可能

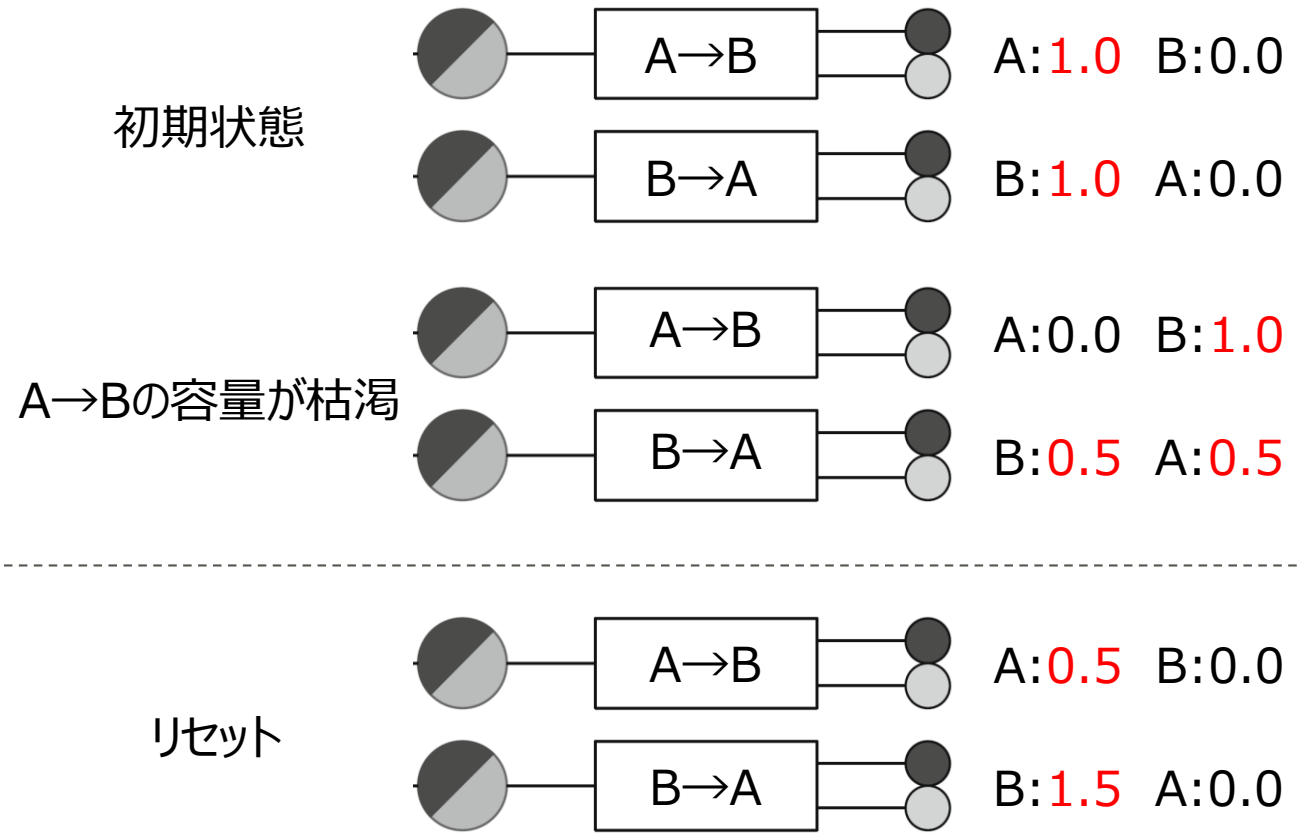



（Poonの論文の図を一部加工）

# 双方向ペイメントチャネル (1/2) [Decker and Wattenhofer, 2015]

FUJITSU

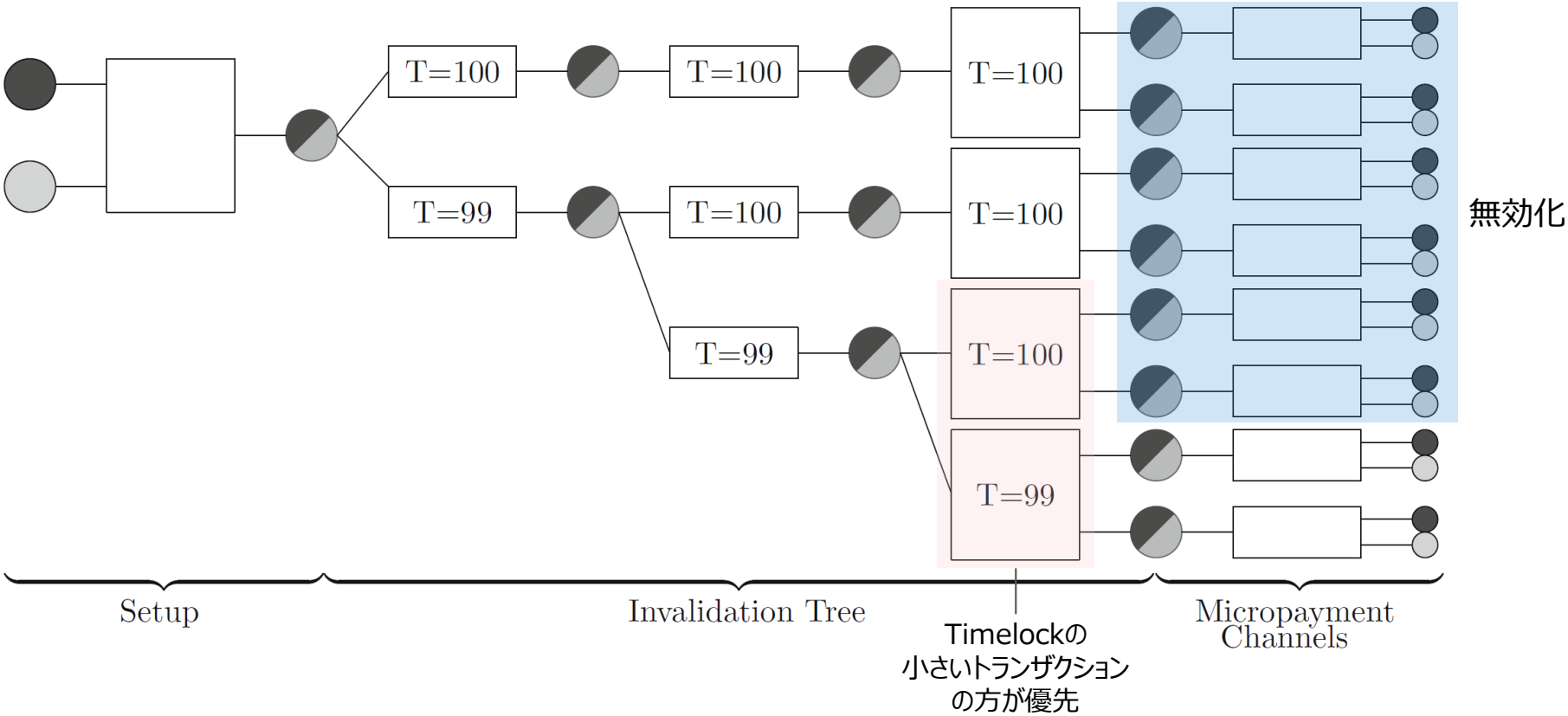
- 普通に単方向ペイメントチャネル x 2 で構成しても、リソースが2倍必要になるだけなので、あまり嬉しくない
  - しかし、片方の単方向ペイメントチャネルの容量枯渇時に、コスト0でペイメントチャネル・ペアの残高調整（リセット）が行えると、状況はかなり改善



# 双方向ペイメントチャネル (2/2)

FUJITSU

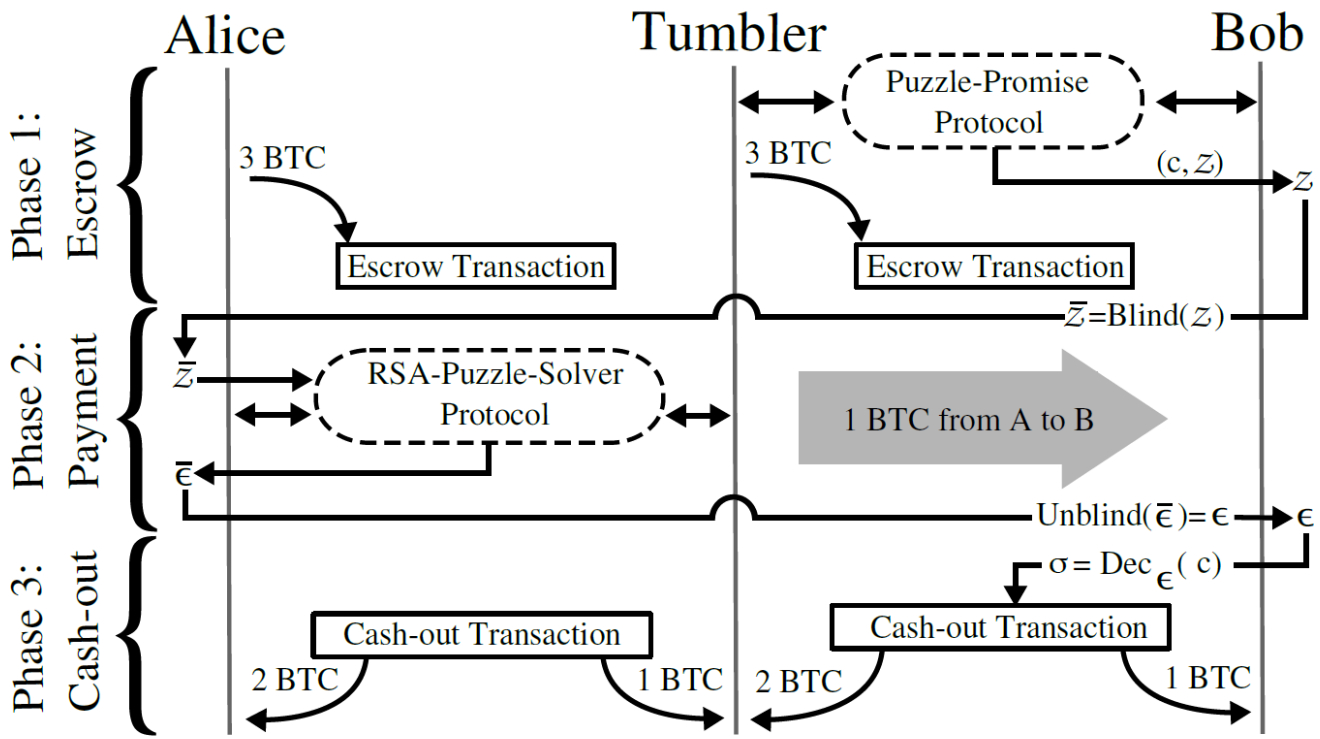
- Timelockを利用して、古い単方向ペイメントチャネル・ペアをコスト0で無効化
  - 結局、ブロックチェーンのトランザクションはチャネルのセットアップとクローズの2回
  - 環状のライトニング・ネットワークのルートを使ったリバランシングで、ほぼ永久機関化



# TumbleBit [Heilman, et al., 2017]

FUJITSU

- 送金元と送金先の間にTumblerが入り、取引を仲介
  - パズルの答えを媒介として、送金元から送金先へ間接的に資金移動
  - ブラインディング（暗号技術）により、送金元と送金先の関係をプライバシー保護（Relationship Anonymity）



FUJITSU

shaping tomorrow with you