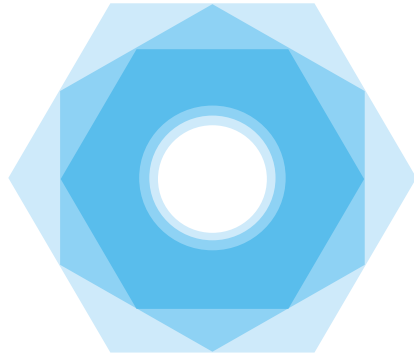
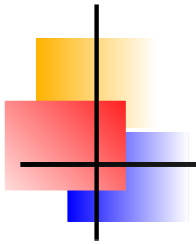


ブロックチェーンにおける識別子と鍵管理

日本銀行 第 1 回 *FinTech* フォーラム

株式会社 Orb / 慶應義塾大学 SFC 研究所

斉藤 賢爾



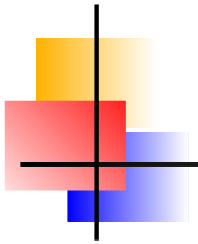
概要

- ビットコインで採用されているいわゆる UTXO

  (Unspent Transaction Output : 未使用の取引出力がコインであるとする)
  データ構造を用いるブロックチェーンにて
  - 識別子と公開鍵を分離して管理し、
  - 秘密鍵を失った際にも鍵ペアをリプレースして利用を継続できる仕組み

  を紹介します
- 同様の考え方で UTXO 構造を持たないブロックチェーンにおける仕様も設計できると考えます

- ご参考 :
  - 特許第 5858506 号, 株式会社 Orb, 「仮想通貨管理プログラム、及び仮想通貨管理方法」, 2016 年 2 月 (発明者 : 斉藤)

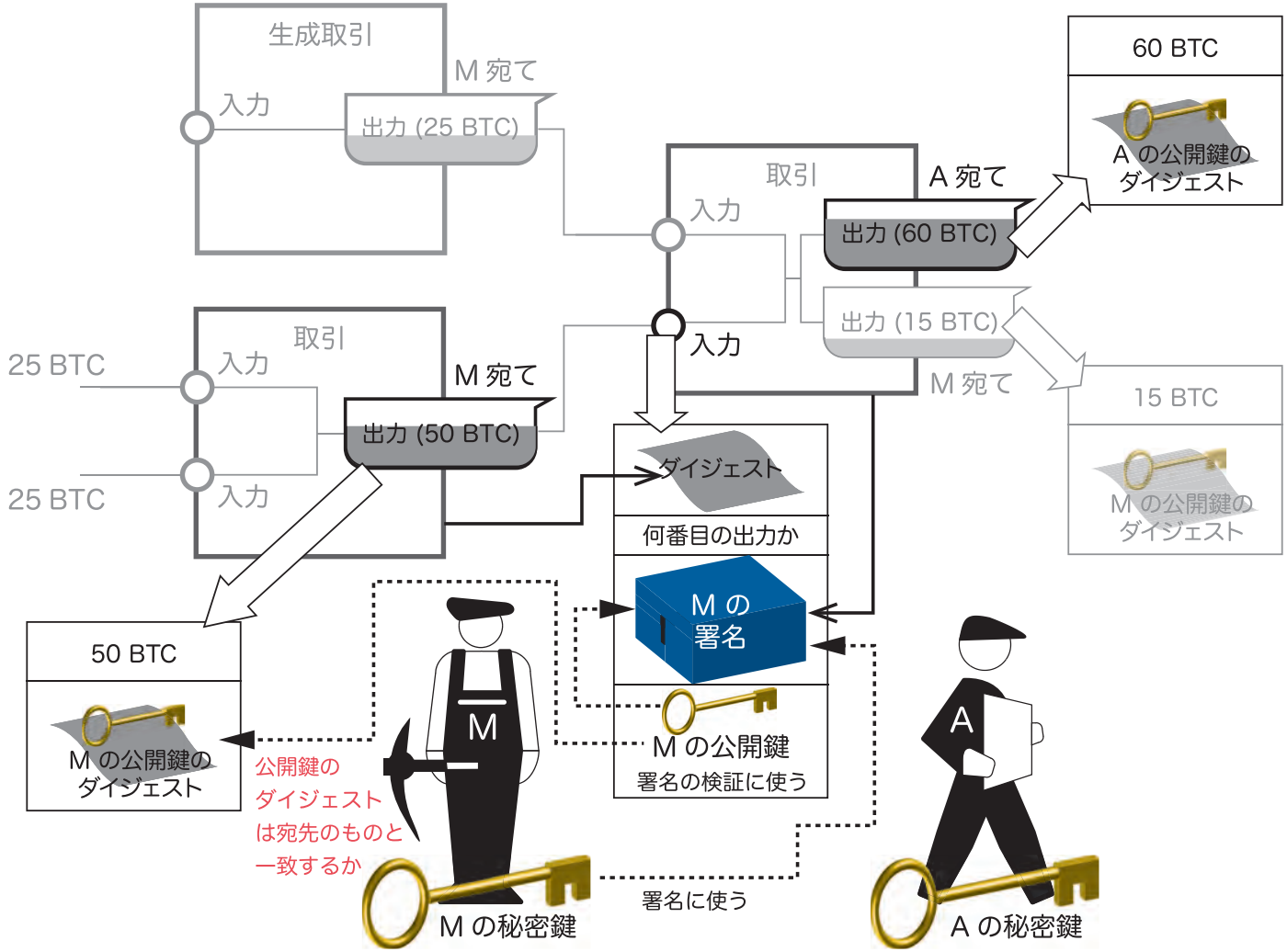


課題と要求

- 課題：
  - 秘密鍵を失うと資産のコントロールを失う
    - 資産の移転の宛先に (概念的には) 公開鍵を指定
    - 対応する秘密鍵を失うと本人の証明ができなくなる

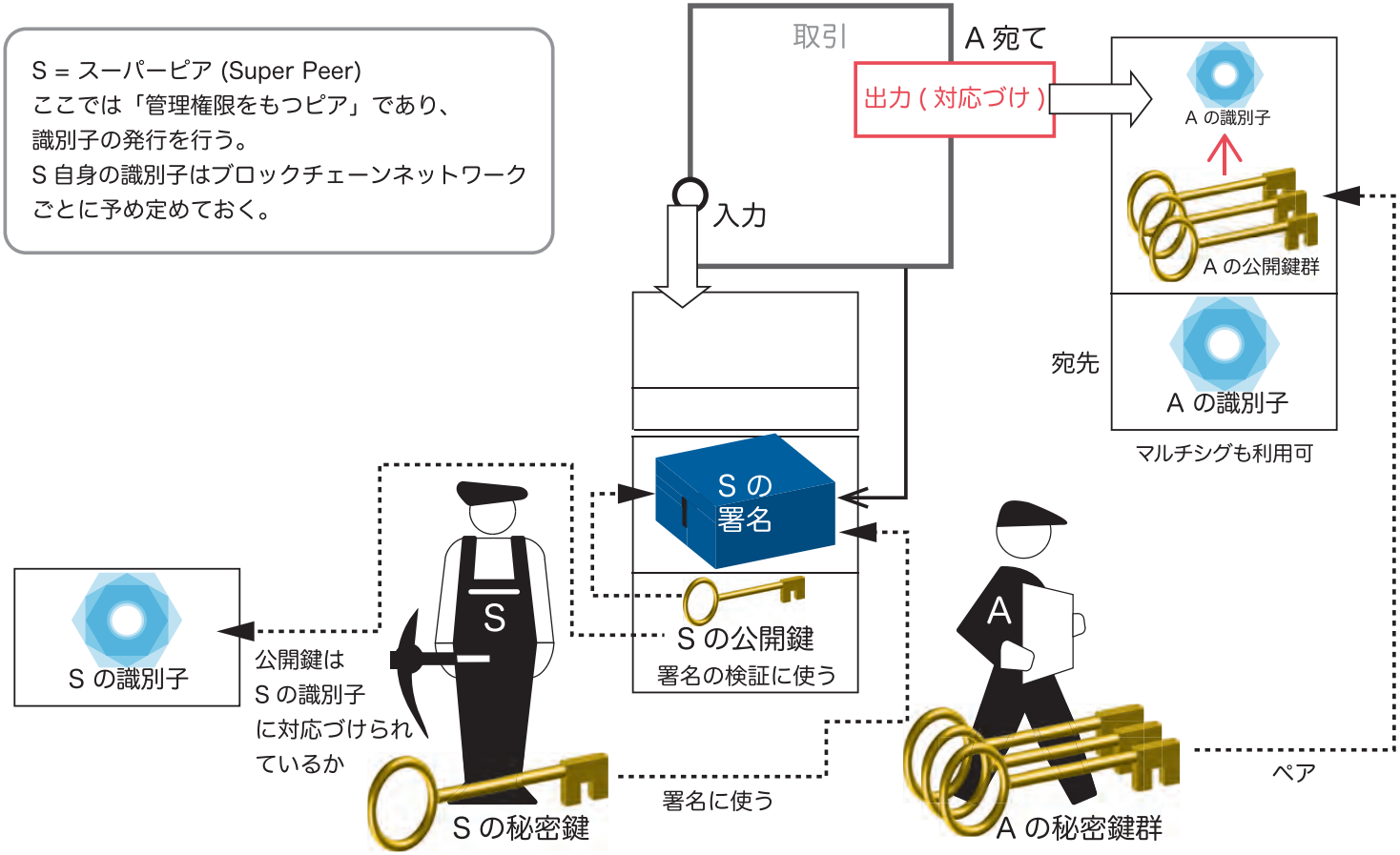
- 要求と実現方針：
  - 識別子を公開鍵と分離する必要がある
    - 資産の移転の宛先には識別子を指定する
    - 識別子と公開鍵の対応づけを別途管理する
      - 新しい鍵ペアをつくり、対応づけを更新することにより リプレースできる
  - 完璧ではないが、はるかに良い

現状の仕組み (UTXO 構造の場合)



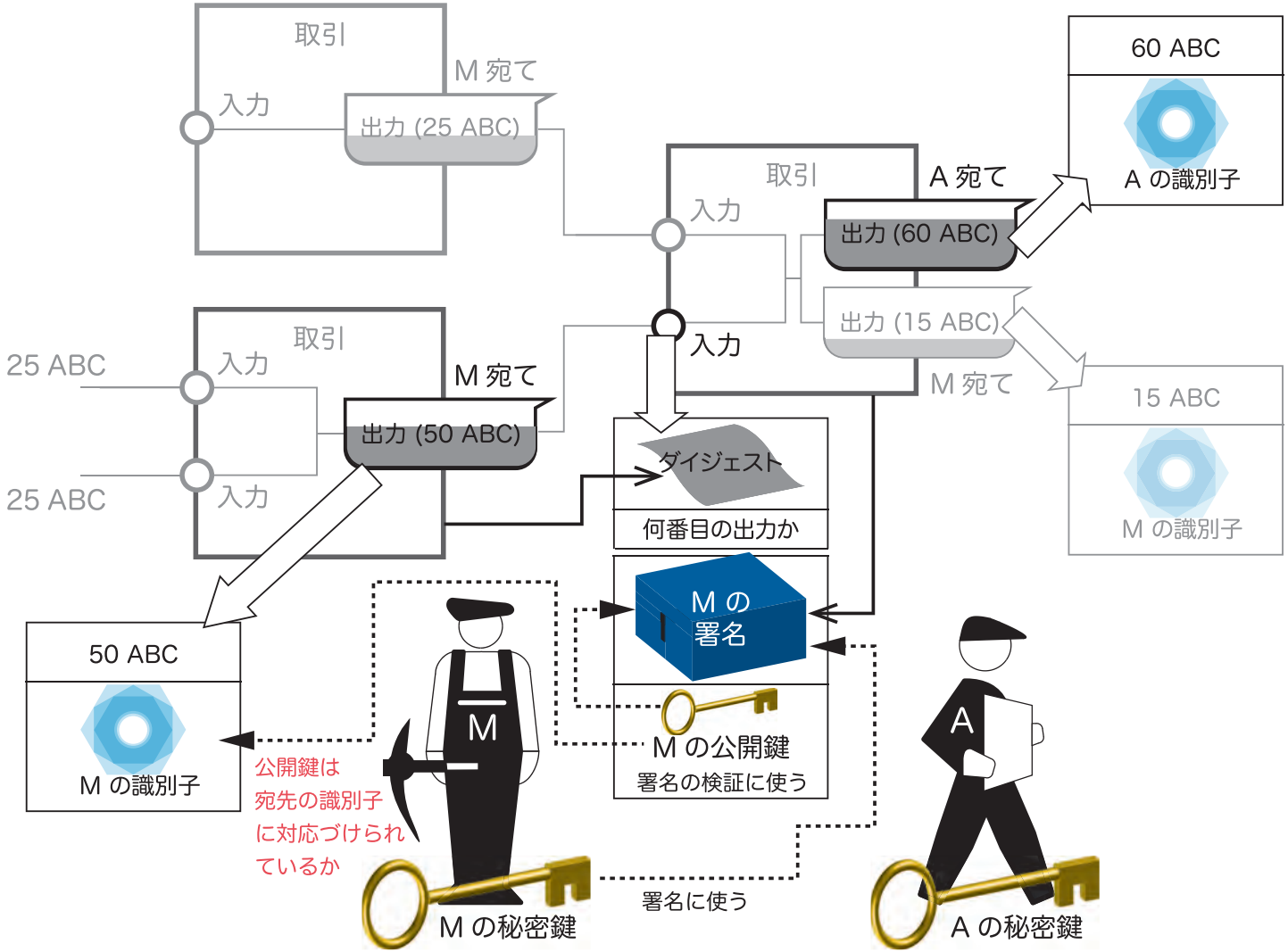
- 提示された公開鍵について計算したダイジェストが宛先と一致することで正当な利用者であることを証明

新たな仕組み 1 (Orb 1 にて実装済み)

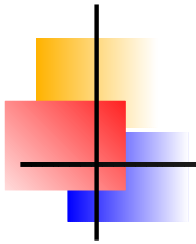


- 識別子は任意の値 (Orb 1 では 160bit)
- 取引は、識別子と公開鍵群の対応づけを出力できる
- それを参照し入力とすることで対応づけは更新できる

新たな仕組み 2 (Orb 1 にて実装済み)



- 提示された公開鍵が宛先と対応づけられていることで正当な利用者であることを証明

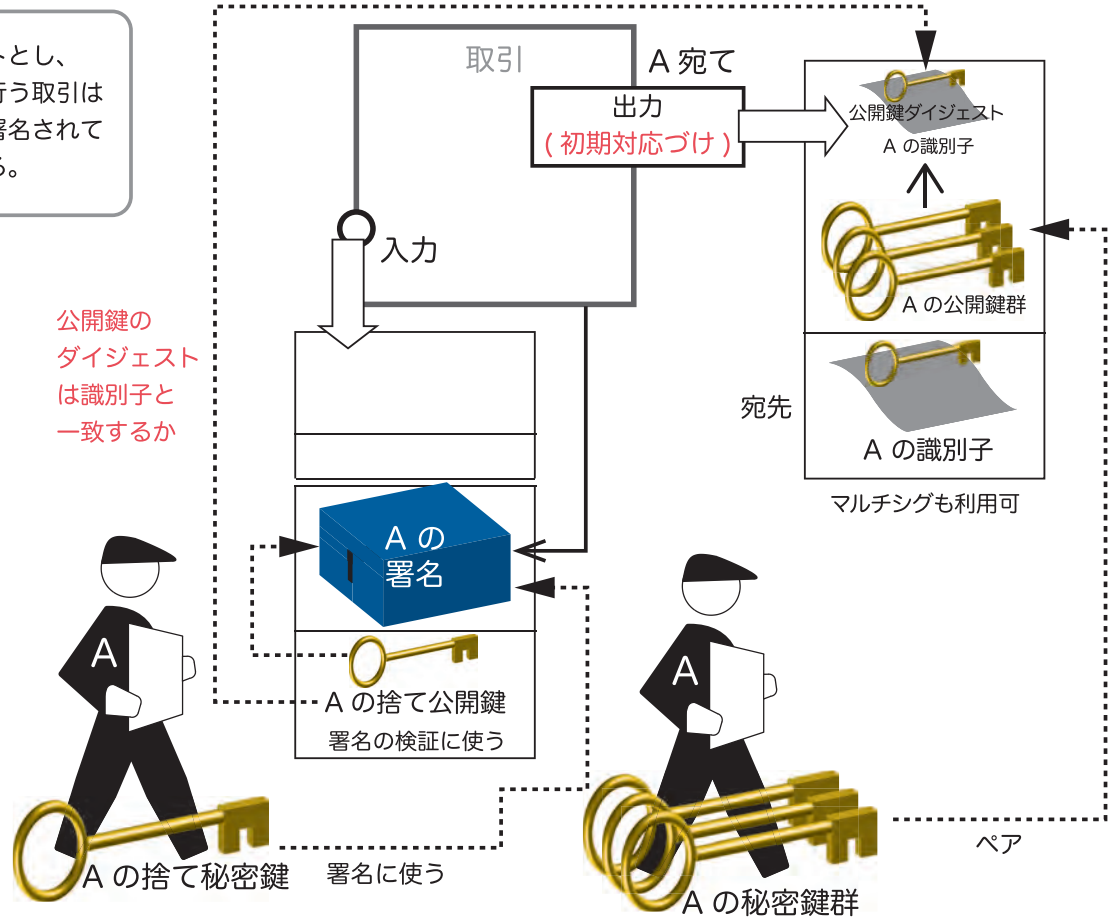


Orb 1 における課題

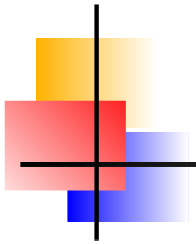
- スーパーピアの存在を前提として設計されている
  - 識別子をスーパーピアが管理する
    - 管理者のいない識別子生成はスクワッティング (使わない識別子を予め (大量に) 確保しておくこと) などの問題を引き起こす
  - スーパーピアの識別子と、公開鍵群との初期対応づけはノードのスタート時に共有されている
- エンタープライズ応用ではスーパーピアの存在は多くの場合適切 (運用の主体が存在するため)
  - スーパーピアは従来の耐故障性技術で保護できる
- とはいえ、ビットコインのようなオープンなブロックチェーンにも適用可能か？
  - スーパーピアがなくても動くようにつくれるか

自律分散的な識別子生成の提案

識別子を公開鍵のダイジェストとし、
公開鍵群との初期対応づけを行う取引は
識別子とペアとなる秘密鍵で署名されて
いなければならないことにする。



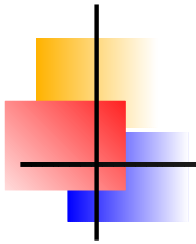
- 識別子の生成においてビットコインと同じ条件であり、
  ビットコインでは識別子のスクワッティングは報告されていない
  - スクワッティングが実際的に可能ならシステムとして破綻



UTXO 構造以外への拡張的適用

- アプリケーションロジックを一般化している (スマートコントラクトを記述できる) システムの多くでは UTXO 構造を用いていない
- その場合でも、資産の移転の宛先を示す識別子がデジタル署名の検証用に提示されている公開鍵とマッピングされていることを実行の条件とするようにスマートコントラクトを記述できるのでは？

- 現在、それができないなら、できるように拡張することを提案したい



まとめ

- 秘密鍵が失われることについて、システムが保護手段をもっていない現状は問題と考えます
- オリジナルであるビットコインブロックチェーンの設計を拡張して、識別子と公開鍵を分離する設計が可能であることを実証しました
- この基本的な考え方は、管理者をもたないオープンなブロックチェーン、および UTXO 構造を持たない、状態遷移記述にもとづくブロックチェーンにも適用が可能と考えられます