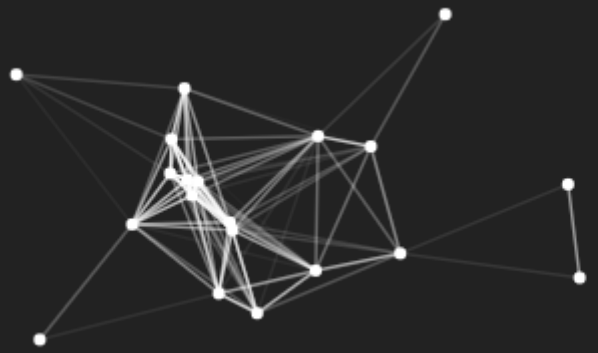
SECRET SHARING DAO



目次

1. BlockChainのプライバシー
2. Secret Sharing Dao
3. 変化予測

自己紹介

9月からブロックチェーンエンジニアをやります。
セキュリティに興味があります。

BLOCKCHAINのプライバシー

情報それ自体へのアクセス権（読み込み）をブロックチェーンライクな仕組みで管理する方法を提供することは可能なのでしょうか？

広義にブロックチェーンといっても、その種類は多岐にわたっています。 特に、現在は細分化の傾向が大きくなっています。

整理のため、今回話すプライバシーがどの領域の特徴なのかを定義します。

		トランザクション履歴	
		公開	非公開
合意形成	trustless	BTC, ETH	Enigma
	trusted	Ripple	HyperLedger

今ポイントした箇所は、経済面でのプライバシーという点で現行の預金と比較して非常にユニークな特徴を有しています。
発行主体が存在しないので、日銀券とは違う仕組みでプライバシーを担保しています。

SECRET SHARING DAO

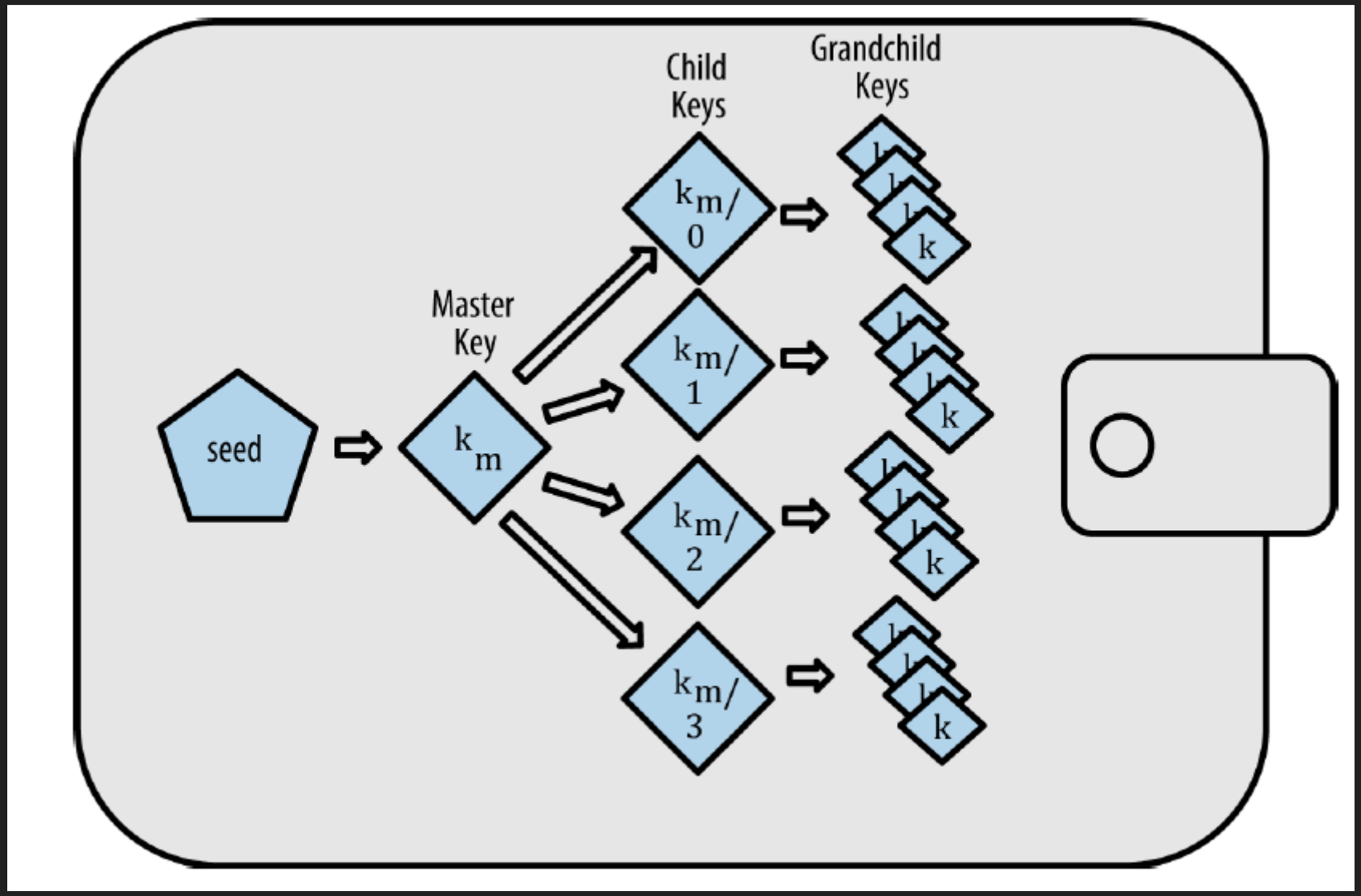
プライバシーの問題を解決するEthereumのソリューションであり、 Enigma等の最新のプログラムの基礎になっています。

2つの特性がビットコインをそれぞれ反対方向に引っ張っています。

- 物理的アイデンティティの秘匿
- トランザクションの公開

仕組み上はEthereumも同じですが、現実には異なる事情が生まれています。

ビットコインは貨幣としての使用を想定しており、本質的に代替可能なものです。

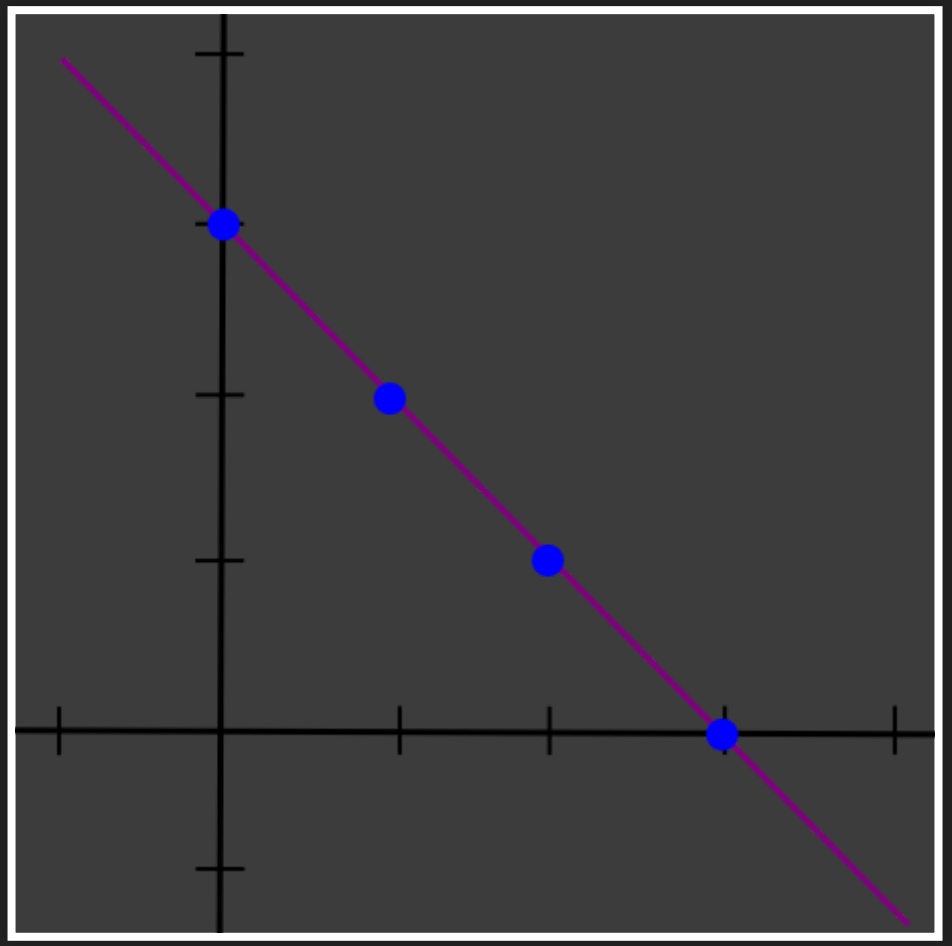


Ethrereumの場合、「アカウントに紐付けられた(account-based)」情報であるため、
単一の参加者が複数のアカウントで活動を行うには複雑な管理が必要になります。

本当にプライバシー保護が必要になった場合、どのように需要を満たすべきか、という問題が強調されます。

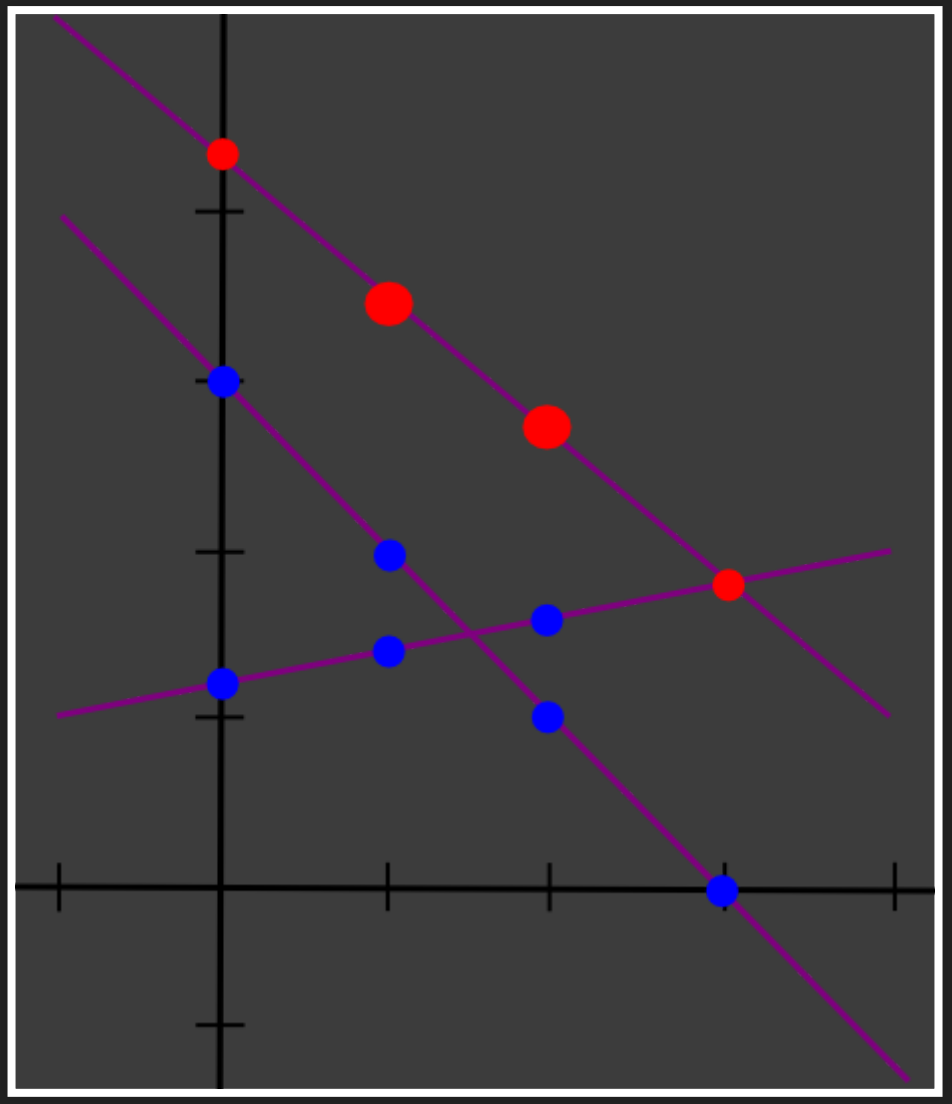
- 秘密分散

N人の参加者がデータを分割して保持し、そのうちK人が協力すればデータを完全に復元できますが、K-1人では何の情報も得られないようなデータの分割方式です。



- SMPC

参加者全員が計算後のデータのみを手にし、途中でいかなるデータも単一のノード上で復元されることはないアルゴリズムです。



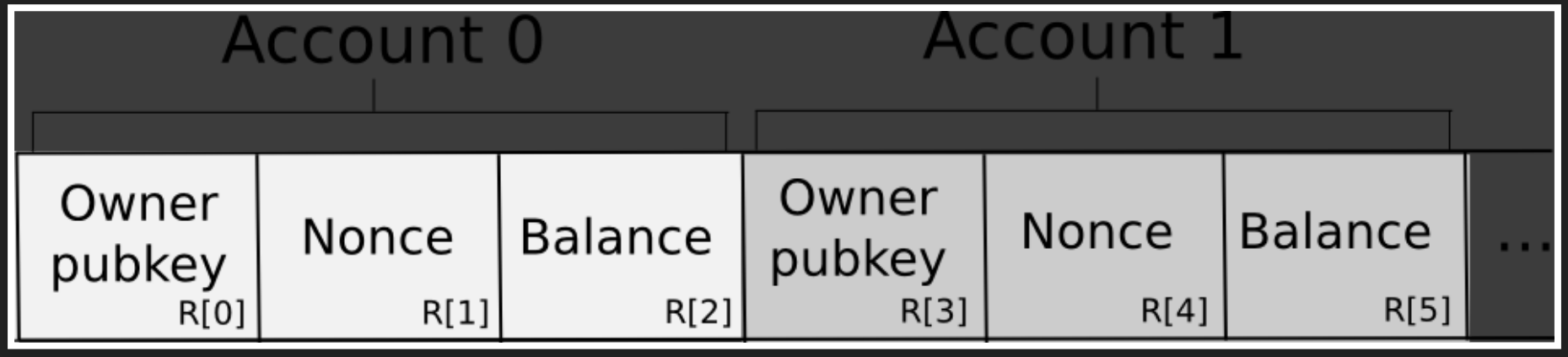
秘匿情報の（同一のx座標における）合計値は、合計値の秘匿情報と等しい。
これはより高次元の場合にも成り立つので、aの秘匿情報とbの秘匿情報からa, bのいずれをも再構成することなくa+bの秘匿情報を計算することができます。

ブロックチェーンアクセスへの適用

ブロックチェーン自体には秘匿性がないので、ユーザーがブロックチェーンに送ることのできるトランザクションは下記がイメージできます。

```
APPLY(STATUS, TX) = new STATUS
TXs = REQUEST(ACCOUNT)
```

データベースは下記を想定します。



各要素(R[0...])についてSMPCで取得することが可能ですが、上記の単純な形式でさえ、データ量が増えると計算量は膨大です。

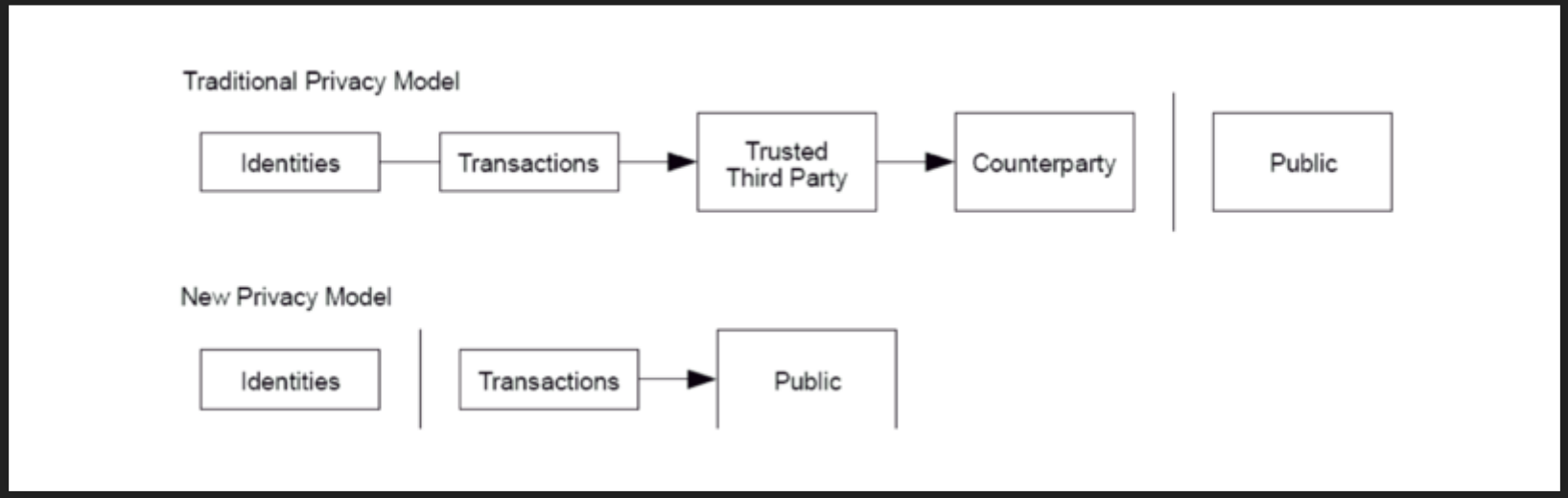
変化予測

Secret Sharing Daoにより、プライバシーを手に入れることができますが、大きなアプリケーションを構築するのは不可能です。

一部のプライバシーが非常に重視される領域（医療情報、評価）等への適用が期待できます。
秘密鍵管理、という案もあるでしょう。
ただし、世界で最もオープンなシステムであるという性質は失われます。

公開鍵を匿名にするのである。ある額を誰かが誰かに送金したことは全参加者に知られるが、誰が取引に関わったかは見抜かれない。

-- Satoshi Nakamoto



この特徴を利用し、コインチェックの580億盗難事件の際にはツールを作りました。

もし、犯罪的行為が助長されるということが判明し反感を買った場合、善意のボランティアハッカーでさえもがこのシステムを落とそうとするかもしれませんし、それが正当とみなされる可能性もあります。