Fungibility/Security Issues, ビジネス応用

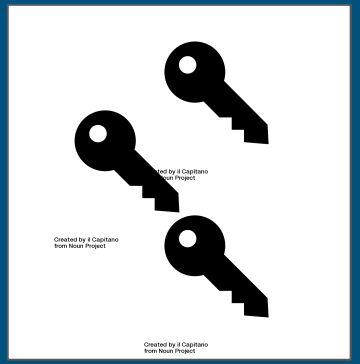
@DG Lab Anditto Heristyo

今回の話

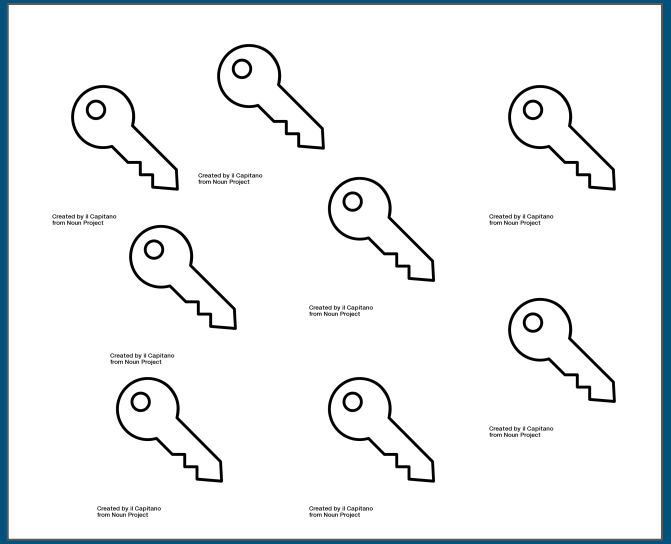
1. Bitcoinのプライバシーについて
2. Confidential Transactions (CT)
3. Confidential Assets (CA)
4. DG Lab の CA 実例

Bitcoinのプライバシー

Bitcoinとは



自分の秘密鍵
「財布」



Bitcoinのデータベース

データベースの中から、どのトランザクションに入っている公開鍵が自分の持っている秘密鍵とペアになっているのかという紐付けを手がかりに新たなトランザクションを作成することで価値の移転を表現するシステム。

単純なビットコインのトランザクション

インプットは別の前のTxのアウトプットから

インプット	アウトプット
自分 10 BTC	A 8 BTC
	B 1.999 BTC
	手数料

アウトプットは後のTxのインプットになる

:秘密鍵

:公開鍵

自分の財布

自分の鍵

他の人はこのTxデータを見て:

1. ちゃんと鍵が合ってるか？
2. インプット金額 ＝ アウトプット金額？

セキュリティに対する大事な条件

1. 関わっている人の承認

   → 公開鍵暗号

2. インプットとアウトプット（合計）は等しい

   → システム内のコインは増えてない？

(パブリック)ブロックチェーンの強み

人 / サーバーを信用しなくても大丈夫

→ データがOKであれば、承認出来る

その効果:全部の情報を公開するべき

→ Bitcoinの場合はトランザクションの流れと金額

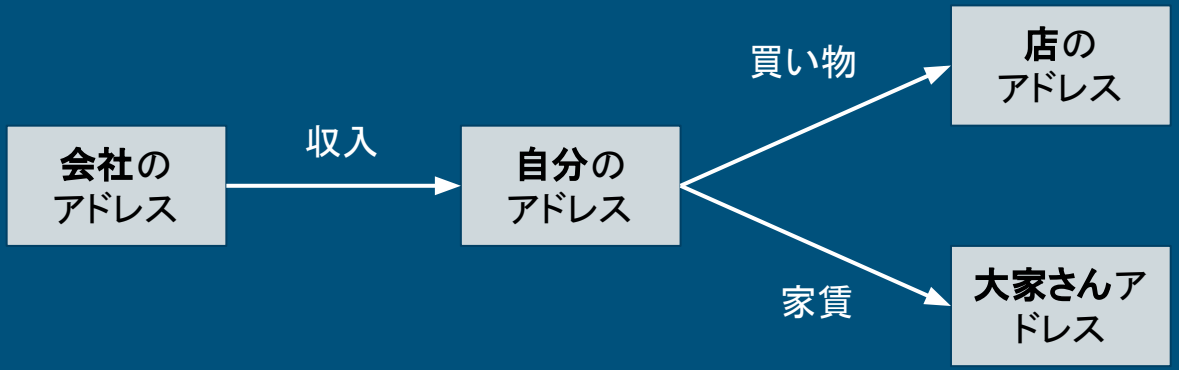
でも

誰がどの鍵を持っているか分からないから、なんとなくプラバシーはありそうだけど、トランザクションを作成するたびに1つずつバレてしまう。

→ 実はBitcoinは完全にanonymousというわけではない。

例えば

- 会社からBitcoinで給料をもらう。
- 給料（Bitcoin）を使って、買い物、家賃などを支払う。



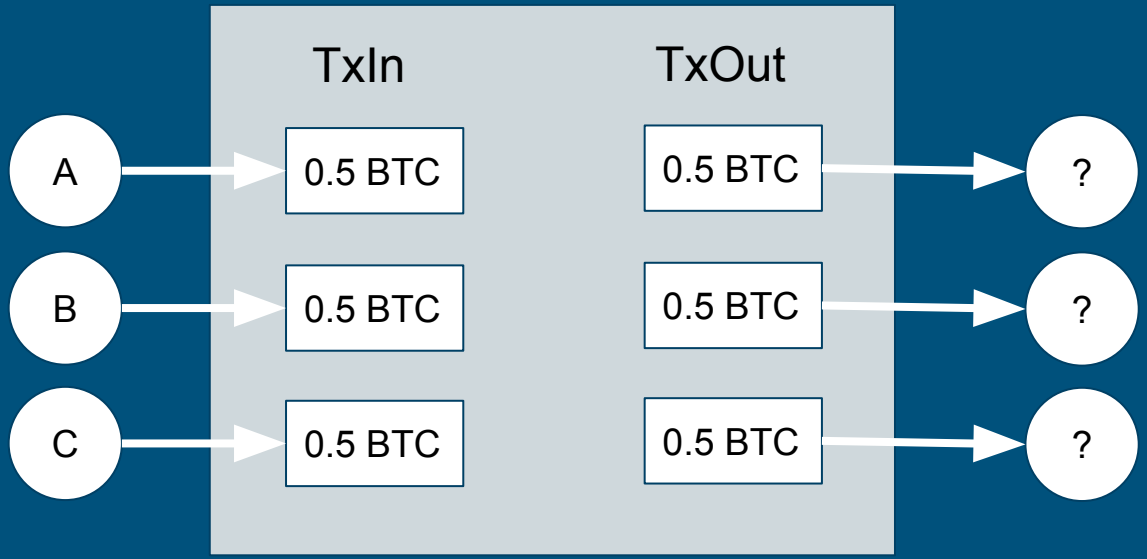
- 店と大家さんからはあなたの収入が見えちゃう。
- 会社からもあなたの給料の使い道が見えちゃう。

ビジネスの応用の場合

同じく、色々な情報がバレてしまいます：

- 会社のキャッシュフロー
- クライアント情報
- 営業のボリューム
- とか。。

解決方法 - Mixing / CoinJoin



もっと詳しくは Ethan & Nicolas のセッションで話す。

まだ問題は残っている

全部金額が統一じゃないとだれがどれを持つかの解決ができる。

Mixingをする人の信頼性と匿名性。

→ TumbleBit で解決できる

結論：トランザクションの金額を隠したら良い。

Confidential Transactions

最初のアイデア

Adam Back (Blockstream 社) - 2013年

“bitcoins with homomorphic value (validatable but encrypted)”

準同型金額のBitcoin（検証できるが暗号された）

https://bitcointalk.org/index.php?topic=305791.0

参考 : https://ja.wikipedia.org/wiki/準同型暗号

Confidential Transactions (CT)

Greg Maxwell (Blockstream社)によるハイレベルの説明:

https://people.xiph.org/~greg/confidential_values.txt

数学の詳しい説明:

https://github.com/AdamISZ/ConfidentialTransactionsDoc

数学が分からなくても理解しやすい使い方の説明:

https://elementsproject.org/elements/confidential-transactions/

Elements Project

https://elementsproject.org/

オープンソースの Bitcoin のフォークである。プラス新しい機能：CT、CA、Sidechain、など。

もっと詳しくは Greg & Mark のセッションで話す。

効果

1. 金額を公開せずに、トランザクションのバランスを承認できる。

   → ブロックチェーンの強みを活かせる

2. 一部公開することができる。

   → 例：社外監査に blinding_key を共有して、支払能力を証明する

3. CoinJoinとTumblebitと同様に使える。

   → プライバシーをもっと強化する

トレードオフ

1. トランザクションのデータサイズが大きくなる

   → 帯域幅が 15x~20x になる

2. 承認にはもっと時間かかる

   → 承認のコストが 30x~60x になる

3. アドレスの長さが長くなる

   → 2x になる

Confidential Assets

Confidential Assets (CA)

Confidential Transactions のアイデアを拡張して、複数の

アセットタイプをブロックチェーンに載せる。

参考:

https://blockstream.com/2017/04/03/blockstream-releases-elements-confidential-assets.html

http://fc17.ifca.ai/bitcoin/papers/bitcoin17-final41.pdf

CAの実例

問題点

ポイントカードのシステム：

マイレージ、ロイヤリティプログラム、など。

例えば：

問題点 - ユーザの視点

- ポイントカードが多すぎて、管理は難しい。
- 残高がバラバラ。
- 使い道がバラバラ、あるいは限られてる / 難しい。

AIRSKY

いっぱい持ってるけど、飛行機チケット中心

Melon

電車とコンビニ中心

MONECRE

連携サービスにしか使えない

問題点 - ポイント発行会社の視点

- ロイヤリティプログラムに参加しない
  - ポイントの価値を高めたい
- ポイントがユーザにいっぱい分配されて、使われてないのでもっと消費して欲しい

解決提案

オープンなブロックチェーンで、アセットの交換は出来るが：

- 会社のトランザクションがバレる
  - 金額、ボリューム、など
- ユーザーの情報もバレる

→ Confidential Transactions & Confidential Assets

この前の公開したデモ

ポイント・エクスチェンジのシナリオ、ちょっと古いElementsに動いている。

興味がある人は：

https://github.com/ElementsProject/confidential-assets-demo

ポイントエクスチェンジのシナリオ

登場人物:

Alice (A) → ポイントを使いたいユーザー

Bob (B) → 他のユーザー

Charlie (C) → ポイント交換を提供する会社

Dave (D) → コーヒー屋さん

Fred (F) → ポイント発行会社

ポイントエクスチェンジのシナリオ

1. **Alice (A)** は AIRSKY ポイントをいっぱい持っている。
2. **Dave (D)** は珈琲屋さんで、コーヒーを売ってる。
3. **D**はとあるキャンペーンで MELON ポイントでコーヒー買うことが出来る。
4. **Charlie (C)** はポイント交換プロバイダーで、AIRSKY→MELONの交換を提供している。
5. **A**はアプリで自動的にポイントを交換し、コーヒー代を支払う。
6. **Bob (B)** は他のユーザであり、これらのトランザクションの詳細が見えない。
7. ポイントの発行者（AIRSKYとMELON）は自分が関わるトランザクションの詳細が見える。

https://github.com/ElementsProject/confidential-assets-demo

今回のBC2に使われるもの

BC2 - Elementsのネットワーク:

- 自分のパソコンにインストールするノード
- iOS / Android アプリ
- ランチのPOS → Day 2に使って見ましょう！


BC2
Blockchain Core Camp


DG
LAB