HITACHI
Inspire the Next

第1回ブロックチェーンセキュリティワークショップ(BWS2021)

暗号通貨とゼロ知識証明

株式会社日立製作所
長沼健

目次

- ゼロ知識証明とは？
- 暗号通貨でどうやってゼロ知識証明を使うのか？
- zk-SNARK方式の紹介
- さらなる応用：プライバシーを超えて
- まとめ

目次

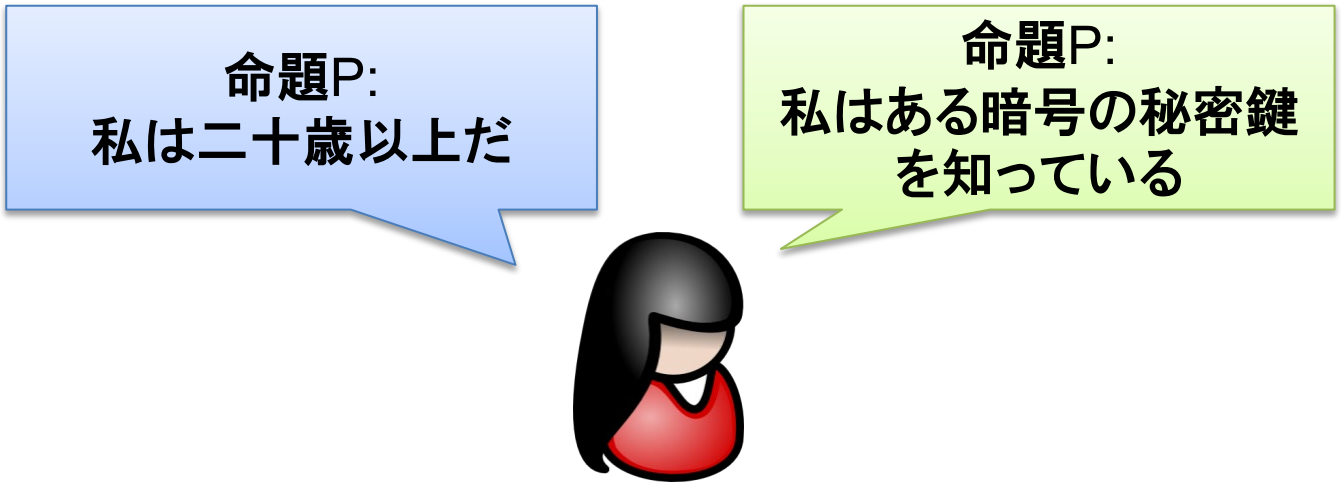
HITACHI
Inspire the Next

- ゼロ知識証明とは？
- 暗号通貨でどうやってゼロ知識証明を使うのか？
- zk-SNARK方式の紹介
- さらなる応用：プライバシーを超えて
- まとめ

ゼロ知識証明とは？

HITACHI
Inspire the Next

ゼロ知識証明(zero-knowledge proof)とは、証明者(Prover)が検証者(Verifier)に、
自分の持っている命題が真であることを伝えるのに、真であること以外、
何の知識も伝えることなく証明できるような対話(非対話)知識証明プロトコルである。

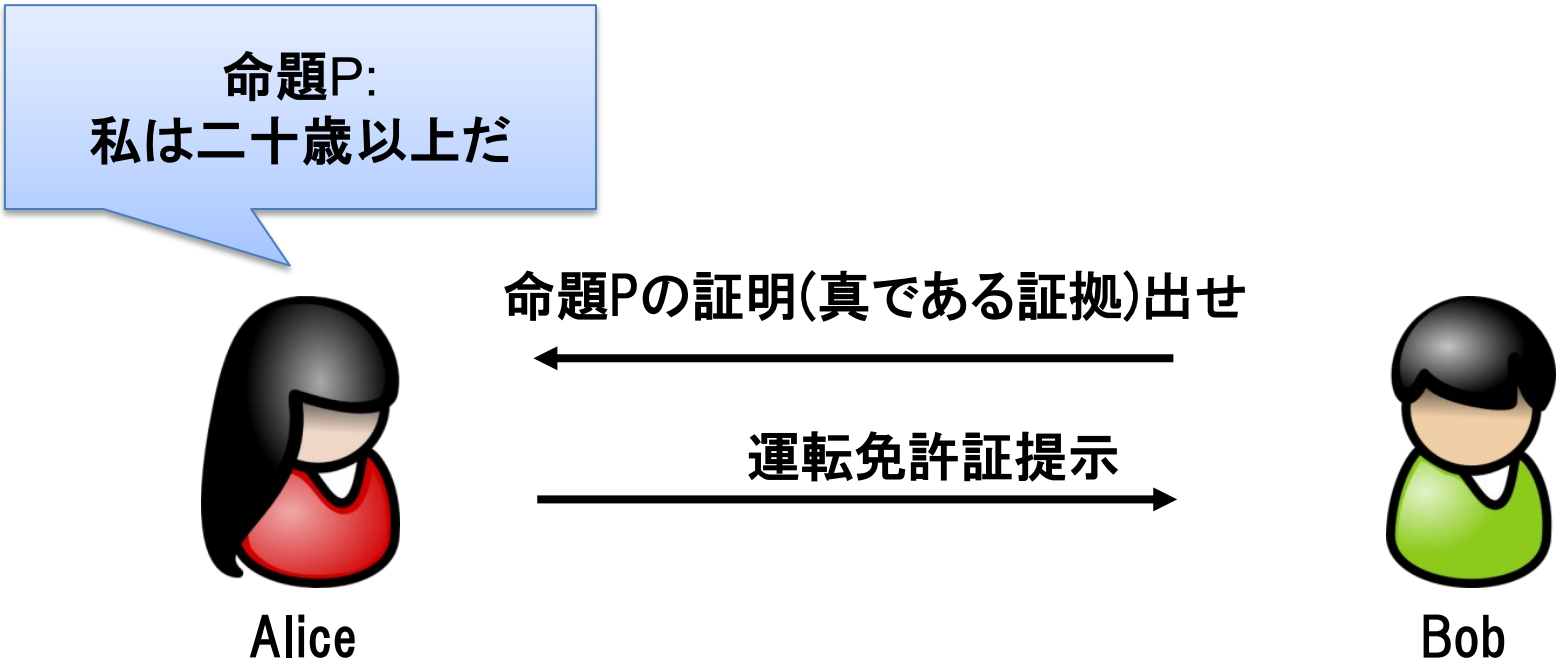


Alice (Prover)は命題Pが真(True)である事を誰かに証明したい

ゼロ知識証明とは？

HITACHI
Inspire the Next

Alice (Prover)は命題Pが真(True)である事をBob(Verifier)にゼロ知識証明したい



運転免許証提示でAlice (Prover)は命題Pが真(True)である事をBobに証明できるが**ゼロ知識ではない**。生年月日から年齢などが漏れている。
どんなものがゼロ知識証明と言えるのか？

ゼロ知識証明とは？

HITACHI
Inspire the Next

Alice (Prover)は命題Pが真(True)である事をBob(Verifier)にゼロ知識証明したい

命題P:
私は公開鍵[pk]に対する
秘密鍵を知っている

Enc(pk, r)

r

乱数[r]を生成

秘密鍵を知っているのでEnc(pk, r)
を復号化して平文[r]を計算可能

Bob(Verifier)は自分で生成した乱数[r]を貰うだけなので、
対話終了後に秘密鍵に関する知識を得ていない⇒**ゼロ知識**

目次

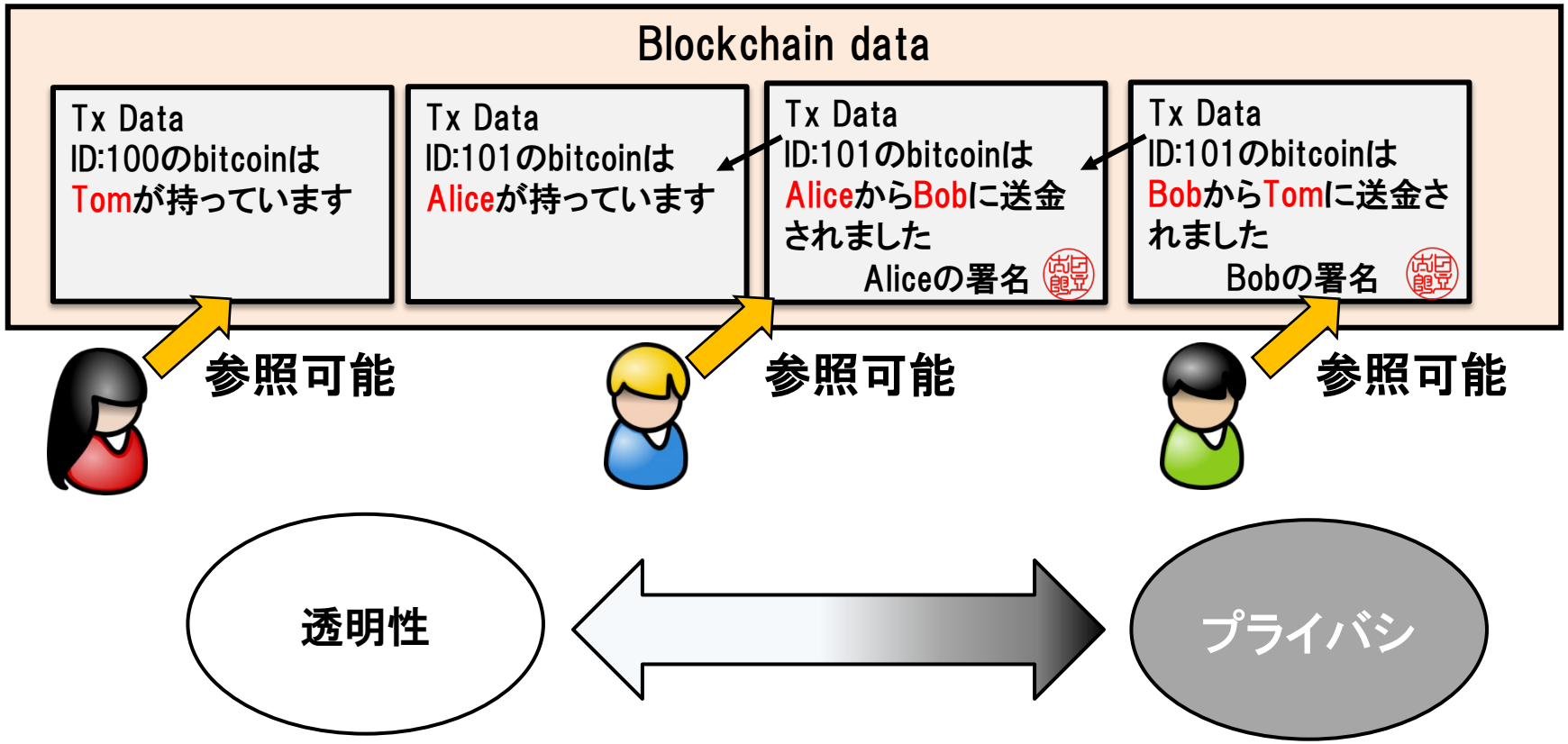
HITACHI
Inspire the Next

- ゼロ知識証明とは？
- **暗号通貨でどうやってゼロ知識証明を使うのか？**
- zk-SNARK方式の紹介
- さらなる応用：プライバシーを超えて
- まとめ

プラバシー vs 透明性

HITACHI
Inspire the Next

Public Blockchainの台帳データはネットワーク上の誰でも参照可能
⇒透明性が高いがプライバシーは無い

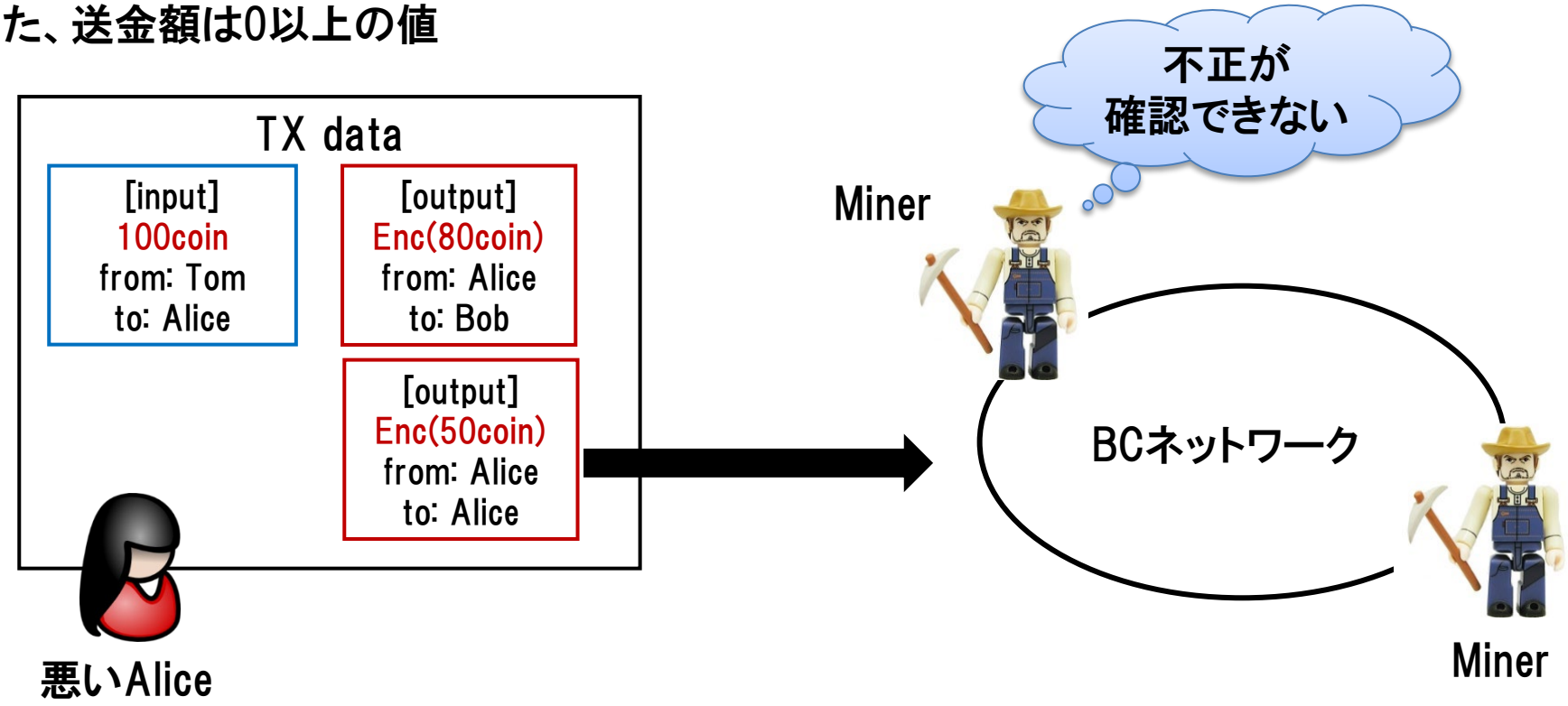


トランザクションデータを暗号化(or hash)したら、プライバシーは保たれるが、
マイナーがトランザクションの**正当性を確認不能**になる

もしトランザクションが暗号化されていると・・・

HITACHI
Inspire the Next

プライバシ保護のためUTXOで送金額が暗号化されたとすると・・・
[inputの金額の合計]=[outputの金額の合計]（手数料は0とする）
また、送金額は0以上の値



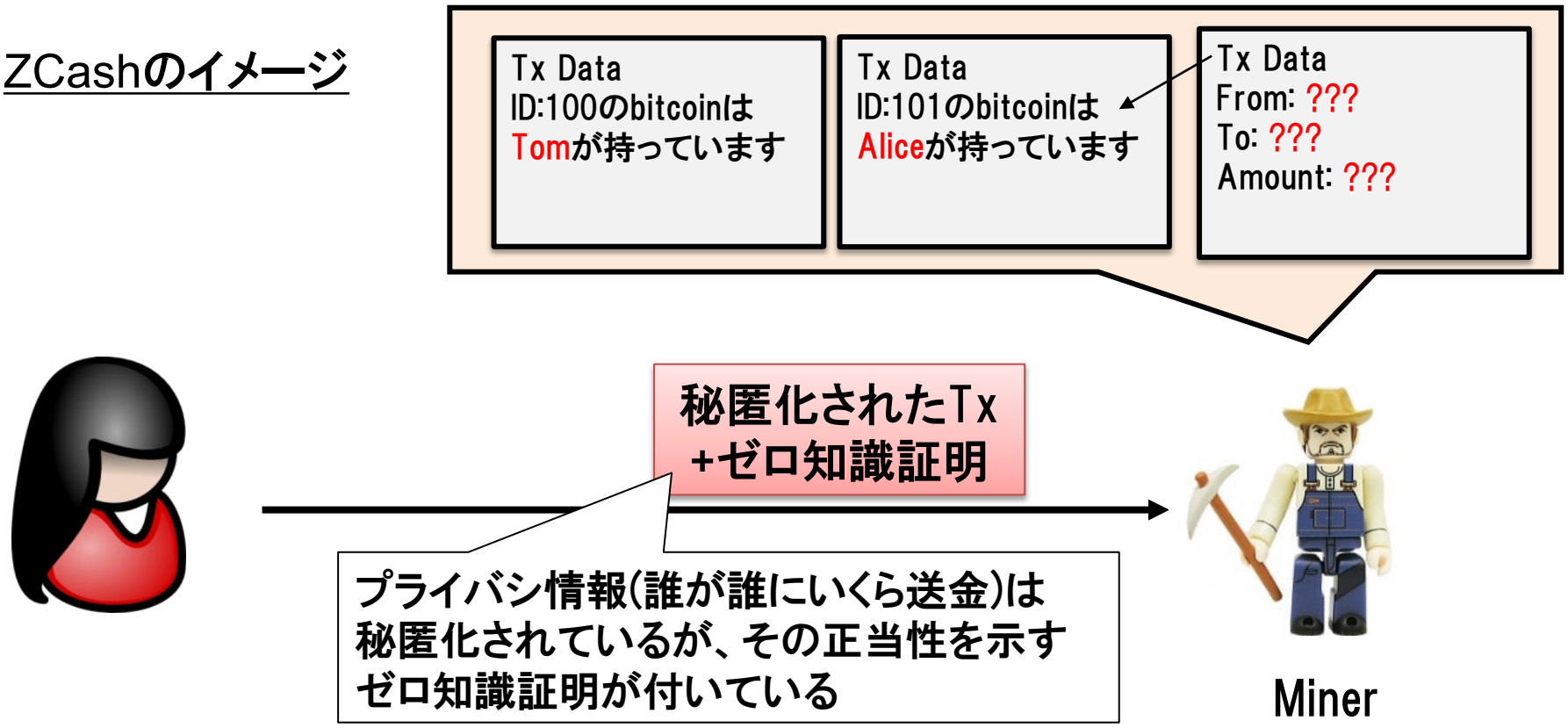
Aliceは100coin分のunspent transactionのうち80をBobに送金、20をAliceに送金(おつり)するが、送金額が暗号化されている事をいいことに、おつりを50に不正に変更。
マイナーは復号化鍵をもっていないので金額の不正に気付かない！

暗号通貨とゼロ知識証明の関係

HITACHI
Inspire the Next

一般的なゼロ知識証明の使い方
トランザクション内のプライバシ情報を秘匿化した際に正当性をゼロ知識で与える

ZCashのイメージ



暗号通貨でのゼロ知識証明の利用方法

HITACHI
Inspire the Next

ブロックチェーンの台帳情報は誰でも閲覧可能
なのでプライバシの観点で問題あり

プライバシ情報は暗号化しましょう

暗号化したらマイナーが正当性を確認できません

正当性を証明するゼロ知識証明を付けましょう！
プライバシーと透明性の良いトレードオフ

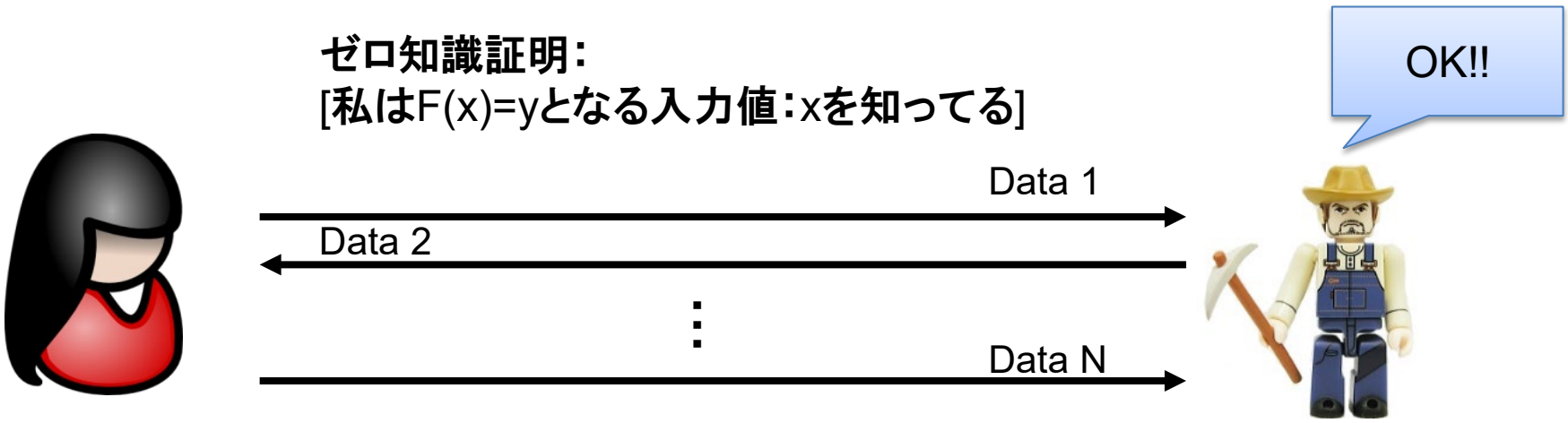
目次

HITACHI
Inspire the Next

- ゼロ知識証明とは？
- 暗号通貨でどうやってゼロ知識証明を使うのか？
- zk-SNARK方式の紹介
- さらなる応用：プライバシーを超えて
- まとめ

zk-SNARKとは？

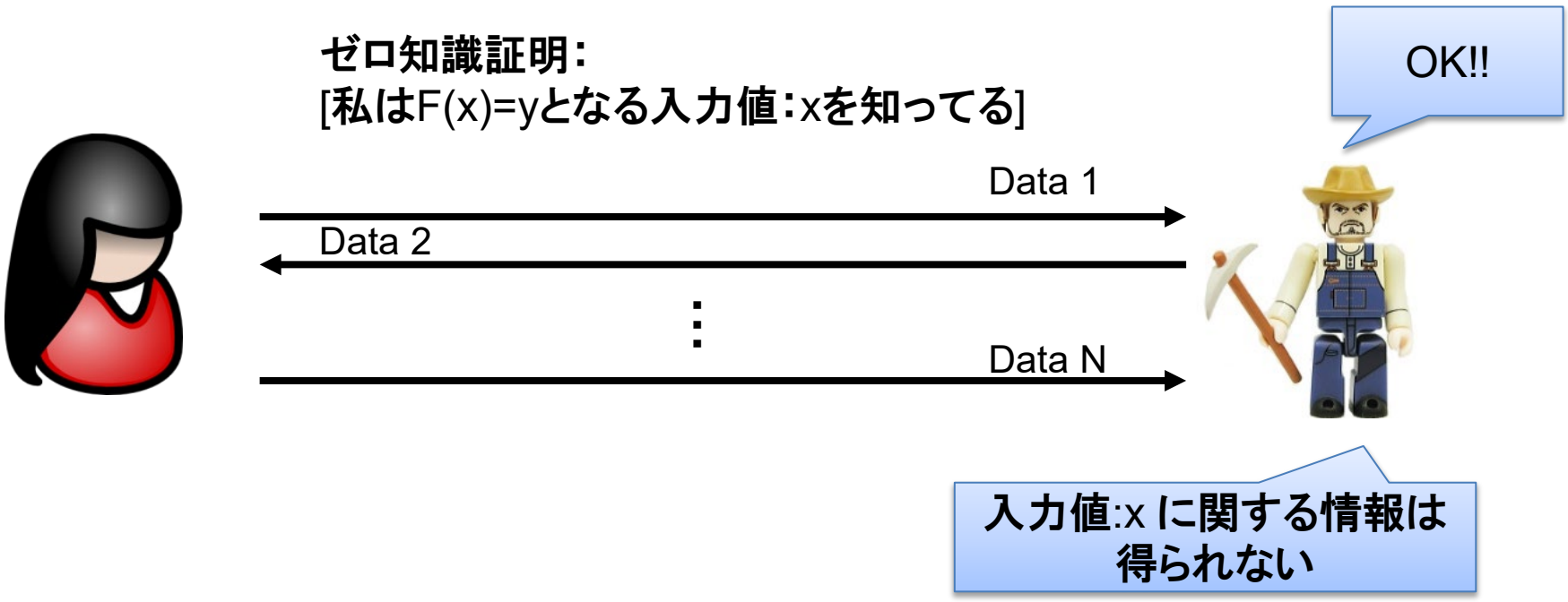
zk-SNARK・・・
zero-knowledge Succinct Non-interactive ARgument of Knowledge



パブリックな関数:F(-)とその出力値:yに対して
Aliceは命題P:私はF(x)=yとなる入力値:xを知っているをマイナーに証明できる。

zk-SNARKとは？

zk-SNARK・・・
zero-knowledge Succinct Non-interactive ARgument of Knowledge



パブリックな関数:F(-)とその出力値:yに対して
Aliceは命題P:私はF(x)=yとなる入力値:xを知っているをマイナーに証明できる。

zk-SNARKとは？

zk-SNARK・・・
zero-knowledge Succinct Non-interactive ARgument of Knowledge

ゼロ知識証明：
[私はF(x)=yとなる入力値：xを知ってる]

Data 1

マイナーからの
データ送信はない

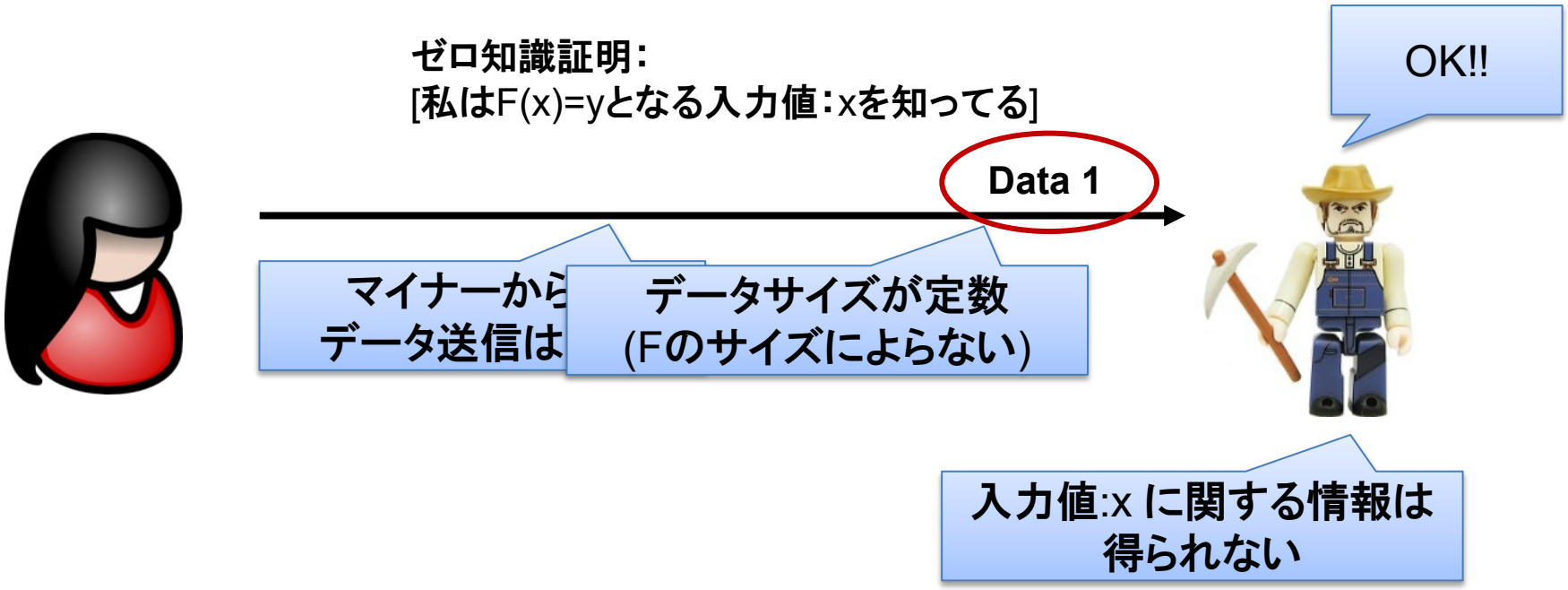
OK!!

入力値:x に関する情報は
得られない

パブリックな関数:F(-)とその出力値:yに対して
Aliceは命題P:私はF(x)=yとなる入力値:xを知っているをマイナーに証明できる。

zk-SNARKとは？

zk-SNARK・・・
zero-knowledge Succinct Non-interactive ARgument of Knowledge



パブリックな関数:F(-)とその出力値:yに対して
Aliceは命題P:私はF(x)=yとなる入力値:xを知っているをマイナーに証明できる。

zk-SNARKの既存方式と課題

HITACHI
Inspire the Next

様々なzk-SNARKがブロックチェーンで利用されている。

古い世代のzk-SNARKs(関数Fが固定)
Pinocchio方式、Groth16方式・・・Zcashなどで利用

新しい世代のzk-SNARKs(関数Fが任意)
PLONK方式、Marlin方式・・・Ethereum 2.0で利用予定

既存方式の課題1
量子計算機耐性を有していない

既存方式の課題2
Setup時に信頼できる第3者(TTP) or Ceremonyを必要とする

日立製作所での研究活動
量子計算機耐性, TTP or Ceremony less Marlin方式を作成

目次

HITACHI
Inspire the Next

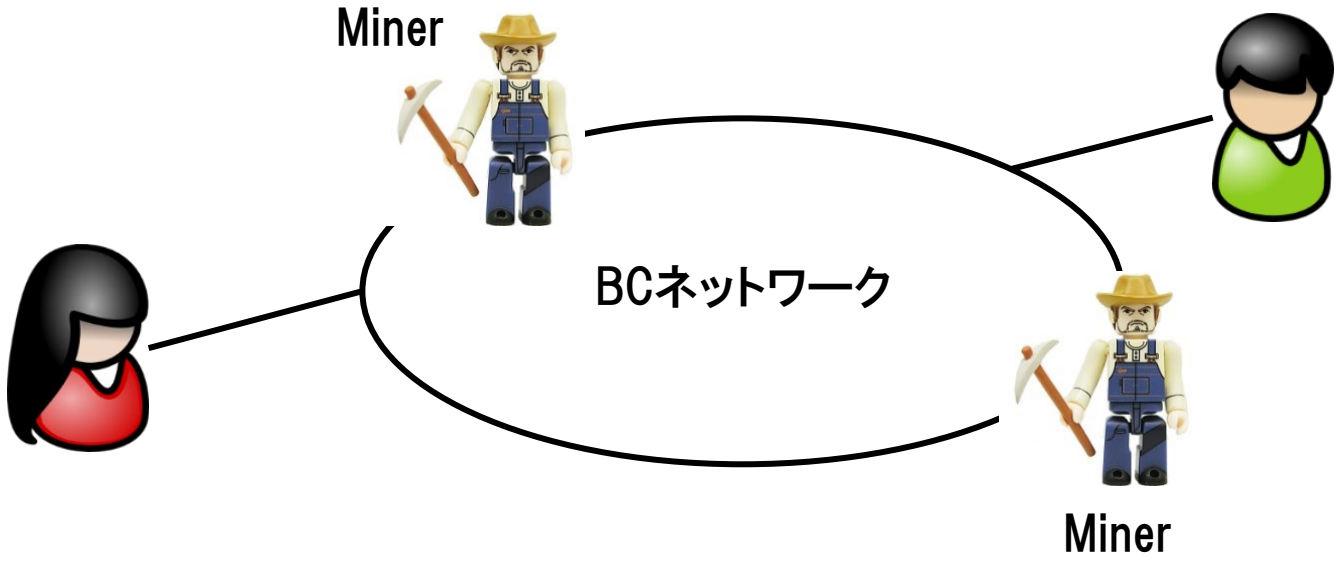
- ゼロ知識証明とは？
- 暗号通貨でどうやってゼロ知識証明を使うのか？
- zk-SNARK方式の紹介
- **さらなる応用：プライバシーを超えて**
- まとめ

暗号通貨の課題とゼロ知識証明

HITACHI
Inspire the Next

暗号通貨が実際に通貨として利用されるためには、まだまだ技術課題も多い

暗号通貨が抱える課題
・スループットに関する課題(スケーラビリティ)
・安定性に関する課題

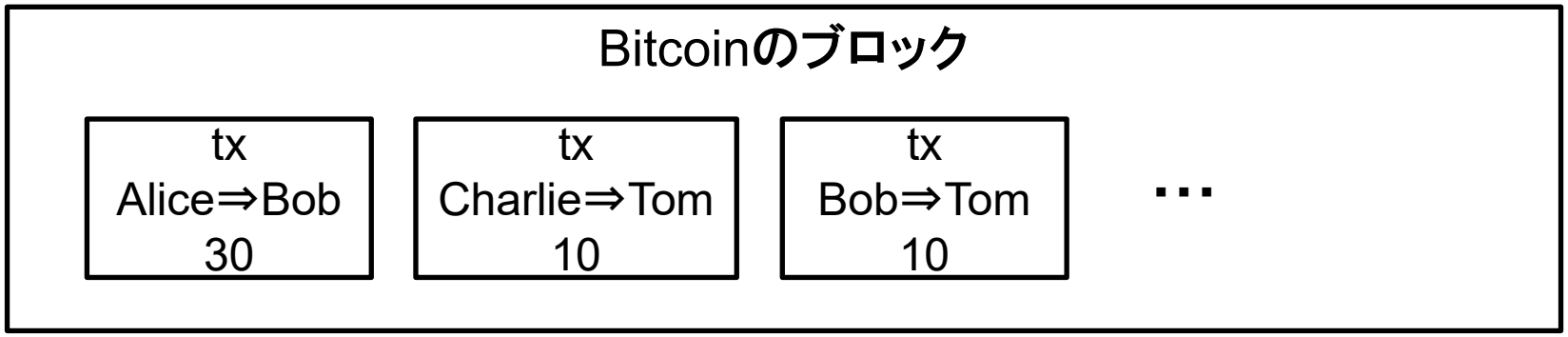


スループットに関する課題

HITACHI
Inspire the Next

Bitcoinのトランザクションは約4tps (理論上は7tps)
Ethereumのトランザクションは約15tps
取引が活発になるとトランザクション詰まりが発生する(手数料増加)

1ブロックのデータ容量は1MB、約10分に1ブロック生成される

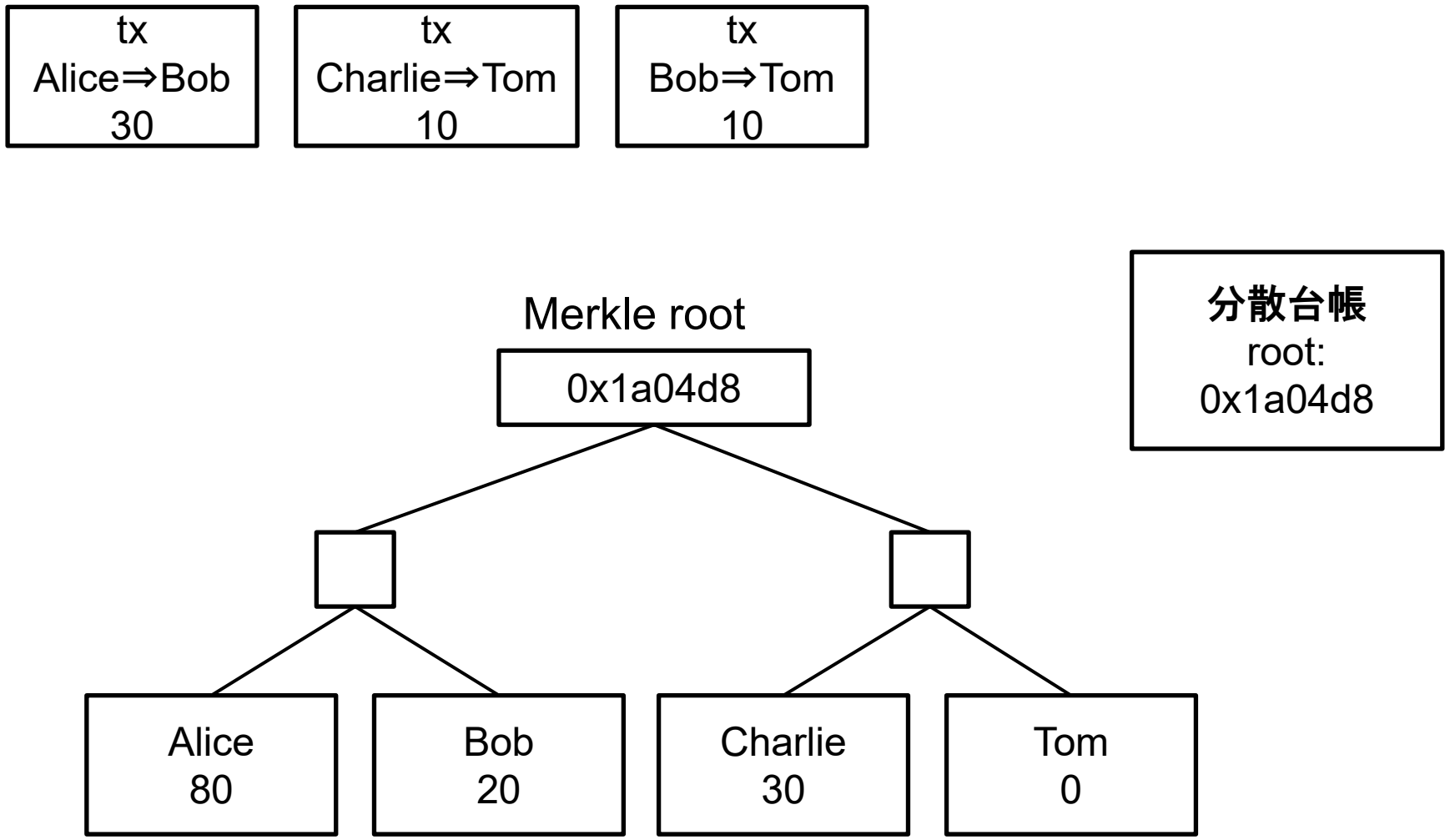


解決方法:
トランザクションはオフチェーンで検証処理し、ブロックチェーンには記載しない
最終結果だけをブロックチェーンに記載する
⇒ゼロ知識証明を使ったRollup

ゼロ知識証明を使ったRollup

HITACHI
Inspire the Next

Rollupのイメージ



ゼロ知識証明を使ったRollup

HITACHI
Inspire the Next

Rollupのイメージ

tx	tx	tx
Alice⇒Bob 30	Charlie⇒Tom 10	Bob⇒Tom 10

Merkle rootの更新処理を
Minerが行う(オフチェーン)
その際に正しく更新が
行われた事を示す
ゼロ知識証明を付ける

分散台帳
root:
0x1a04d8

Merkle root

0x947c3b

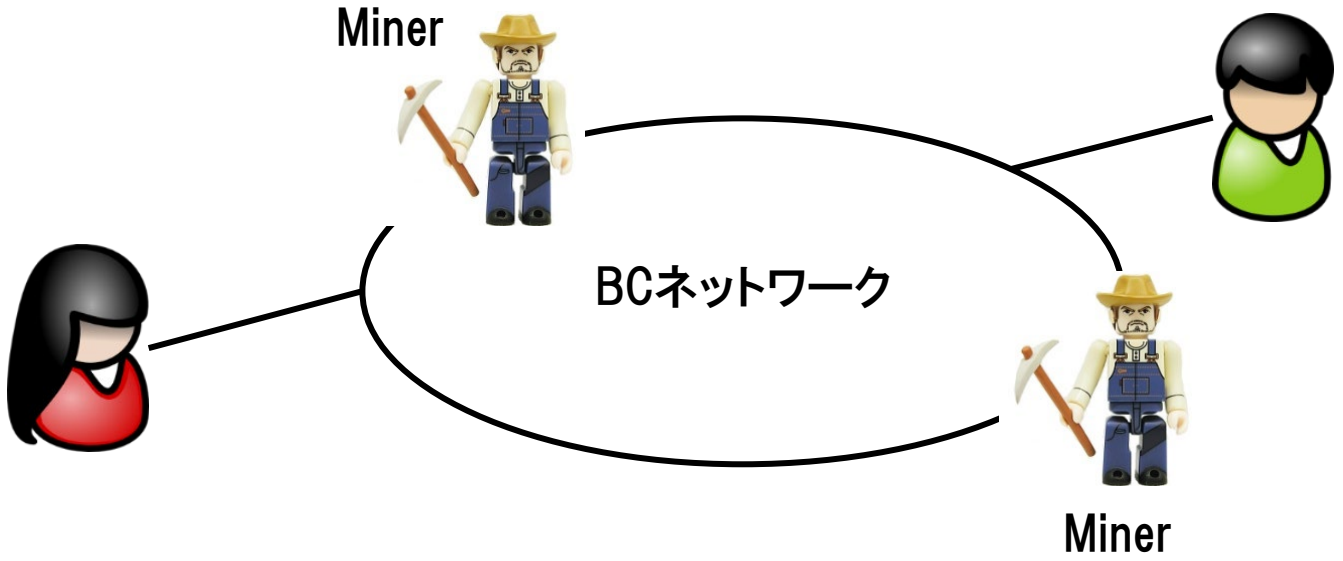
Alice	Bob	Charlie	Tom
50	40	20	20

暗号通貨の課題とゼロ知識証明

HITACHI
Inspire the Next

暗号通貨が実際に通貨として利用されるためには、まだまだ技術課題も多い

暗号通貨が抱える課題
・スループットに関する課題(スケーラビリティ)
・安定性に関する課題



安定性に関する課題

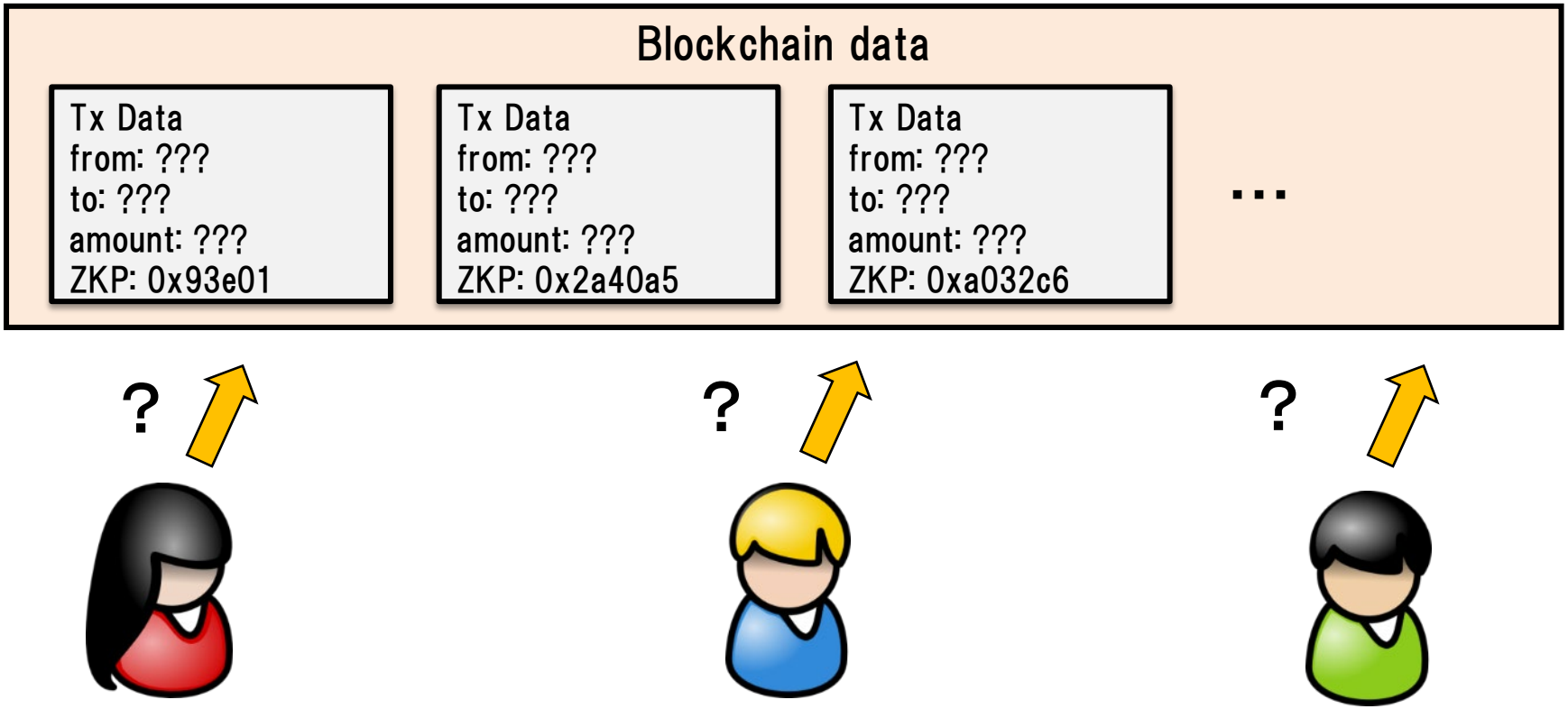
HITACHI
Inspire the Next

2021年初頭からElon Musk氏の動向によりBitcoinの価格は乱高下した
※twitterでの発言、暗号通貨の投機ブームなどの複合的な要因もある
⇒通貨として利用するためには不安定

安定性に関する課題

HITACHI
Inspire the Next

ゼロ知識証明を使った解決方法
⇒匿名送金(誰がいくら持っているか秘匿)にすることで、
誰が誰にいくら送金しているか、誰がいくら持っているか分からない
⇒投機的な動きが見えづらくなる



目次

HITACHI
Inspire the Next

- ゼロ知識証明とは？
- 暗号通貨でどうやってゼロ知識証明を使うのか？
- zk-SNARK方式の紹介
- さらなる応用：プライバシーを超えて
- まとめ

まとめ

HITACHI
Inspire the Next

ゼロ知識証明では、情報を秘匿したまま、その情報の正当性を証明できる
⇒プライバシーと透明性のちょうど良いトレードオフを与える
⇒暗号通貨では匿名送金等に利用されている

ゼロ知識証明のプライバシー以外のユースケース1
暗号通貨のスループット向上(スケーラビリティ)
⇒オフチェーンバッチ処理を実行、その際正しく実行されたことを証明する

ゼロ知識証明のプライバシー以外のユースケース2
暗号通貨の安定性向上
⇒送金、ウォレット情報を秘匿することで、投機的な動きを抑制する

技術課題
信頼できる第3者が必要、量子計算機耐性、ゼロ知識証明生成の処理性能