ブロックチェーンスパム対策

Blockchain

村井研
Term発表

Login name : yukijuki
Research group : Bcali

親 Shigeya & Chike

WALT DISNEY

発表項目

01 **What is blockchain**

ブロックチェーンとは何かについて共有します

02 **The problem I am solving**

概要をお話させてもらいます

03 **The key idea for how I solved it**

解決方法の提案

04 **Success of my solution**

具体的解決策

発表項目

05 Key results
実験結果

06 How this impacts the world
社会に対する貢献

07 Evaluation
評価

08 Next action
卒論に向けて

What is blockchain

ブロックチェーンとは？

Blockchain とは？

ブロックチェーンとは、
中央に管理者が存在せず、
参加者によって運営されている
分散型のデータベースです。

なにが
従来と違うの
→

その特徴は、誰でもネットワークに参加し、取引台帳の記録と承認ができます。

また、その非中央集権的な管理は透明性を担保することを可能にしました。

そして、ブロックチェーン上では自分が送りたいデータをいつでも自分の好きに送信することをだれも止めれません。

The problem I am solving

概要について

What’s the problem

今回僕が解決する問題は...

自分が送りたいデータをいつでも自分の好きに送信することがだれも止められないことで起きる問題

メッセージ送信
スパムや嫌がらせメール、広告など

イメージ送信
広告など、刺激的な画像、卑猥な画像

What`s the problem

ブロックチェーンであるからには、

中央集権的な管理はできない。

ブロックチェーンは、みんなのメール受信先（アドレス）が常に公開されているため、勝手に変なメッセージを送りつけることが可能である。

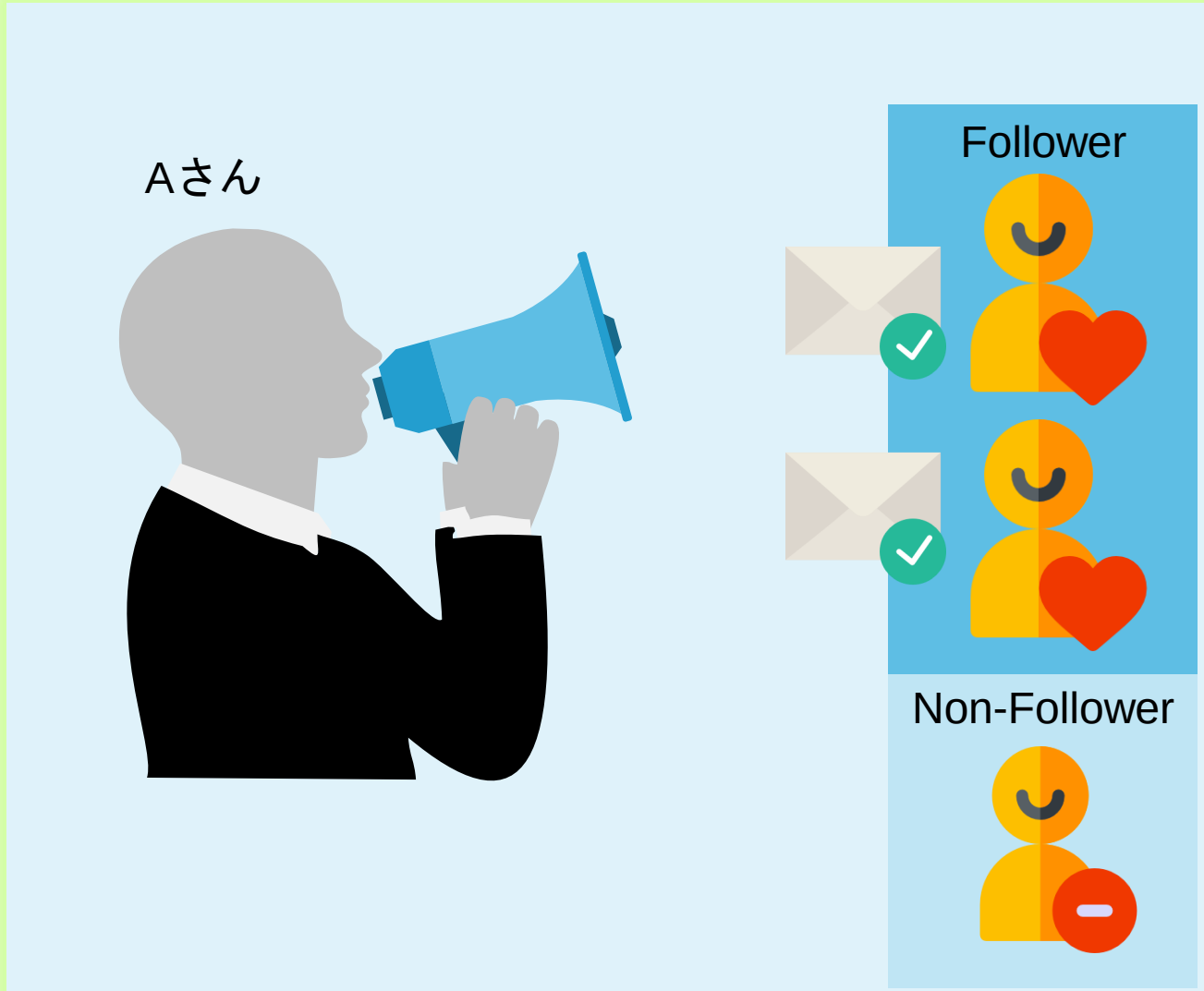
ユーザーが、メッセージや画像を受け取る際に自分で受信先を選ぶようなシステムが求められる。

The key idea for how I solved it

解決方法の提案

First I built something like this

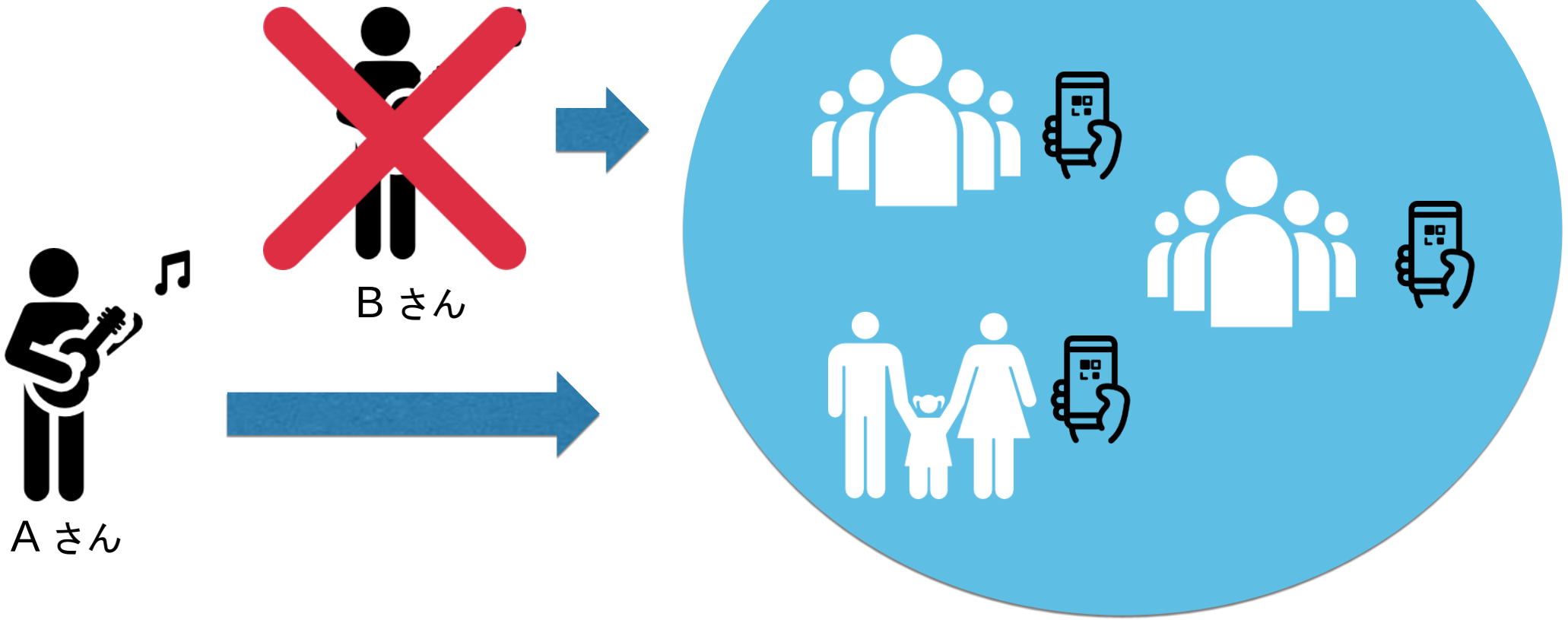
ツイッターのフォロー機能を真似し、受信者が指定した受信先だけを認識し受信できる仕組みを作ってみた。



その際に、こういった攻撃が考えられる。

NEW Point
アドレス以外の方法で
受信先を指定

Aさんいっぱい、ファンを持っているから彼のアドレスをフォローしているファンにメッセージを送ろう



Success of my solution

具体的解決策

Bさん

特定の送信者から受信する

誰かをフォローするには、
フォローしたい人のアドレスに対
しトランザクションを発行します。
follow項目を
（フォローするならTしないならF）
にして送信します。

```
Tx_1 = {
sender : A's pubkey
recipient : B's pubkey
amount : number
follow : T
}
```

```
Tx_2 = {
sender : B's pubkey
message : "hello"
}
```

if sender = A & follow = T,
retrieve recipient.
Retrieve message that recipient
is the sender.

UTXOをかき集めるときに、自分がフォローした人のメッセージを引っ張てくる

Aさん

メッセージを送信する

フォローしてくれた人にメッセージを送信したい場合、宛先なしにメッセージ送信します。

Protocol

Transaction type Protocol

・通常送金
・フォロー送信
・メッセージ送信

この形以外のトランザクションは、ノードのメモプールによってはじかれる検証を設けます。

通常送金 = {
　　Sender : sender pubkey
　　Recipient : recipient pubkey
　　Amount : float
　　Signature : hexdigest
}

フォロー送信 = {
　　Sender : sender pubkey
　　Recipient : recipient pubkey
　　Follow : T or F
　　Amount : float
　　Signature : hexdigest
}

メッセージ送信 = {
Sender : sender pubkey
Message : string
Signature : hexdigest
}

Get message Protocol

自分が発行した、トランザクション中で”follow”項目がTになっているものを引っ張てきます。

そのトランザクションの”recipient”のアドレスがsenderであるトランザクションを引っ張てきます。

そのトランザクションの”message”項目をすべて引っ張て来て、戻り値に設定します。

Key results

実験結果

Key Results
実験結果

結果、自分の指定した受信先の送信のみ受け取ることができました。
パブリックチェーン上で、僕のアドレスを特定し送信することは可能ですが
僕は、指定した受信先以外からはメッセージを受け取ることはありませんでした。

How this impacts the world

どのように応用できるか？

How this impacts the world

**世界では、ブロックチェーンベースの
チャットアプリやSNSがあります。
これらの発展に寄与できる。**

ブロックチェーン上でのスパムメッセージや嫌がらせ対策が今後必要とされるのかと思います。

Evaluation

評価

Evaluation

従来のブロックチェーンでは、アドレスがパブリックチェーン上に常に
公開されており、知らない人から迷惑メールやスパムを
もらい続ける（対策がない）という潜在的な問題があったが、

新しい受信の仕方を発見することによって、
アドレスが公開されていても、スパムや嫌がらせといった行為を
防ぐことが可能になったことを評価してほしい。

Next Action

卒論に向けて

Next Action

卒論に向けて

この機能は、ブロックチェーン上で受信するメッセージで起こりうるスパムや嫌がらせ問題に対する解決策の一つであり、その問題解決をするにはまだまだ改善の余地がある。

01

フォロー機能の解除

フォローした人がもし、悪意な人に成り代わった場合データが消せないブロックチェーンではどのようにフォローしているという事実をなくすことができるのかについて研究する。

02

1対1個人間のメッセージでも同じように受信先を絞れるようにしたい。

現在では、1対N間メッセージでの対策なので、1対1も可能にできるのかを研究する。