

web3 無償の愛 dapp

(トヨタ、KEY3 web3 ハッカソン作品)

2023.3.14 宮電株式会社 佐藤作成

1. 概要

2023 年 3 月に行われたトヨタ、KEY3 主催のハッカソンへの応募作品
任意のアドレスを指定して任意のメッセージを送れる web アプリ。メッセージを送るごとに愛トークン（ポイント）が取得できるというゲーム性を持っている。

2. デモ

スマートコントラクトはアスターのテストネットである shibuya ネットにデプロイしている。
Client のファイルを xdomain（無料）のサーバーにアップロードしてあるので、そこにアクセスする場合を示す。Metamask がインストールされているブラウザで以下のサイトにアクセスする。

<http://eidensato.html.xdomain.jp/hasoto/index.html>

3. プログラム

<https://github.com/EidenSato/web3toyota>

にプログラムは公開されている。各プログラムの概要について次に紹介する。

3- 1 contracts/5_hasoto.sol

ソリディティで書かれたスマートコントラクト。

メッセージ、自分のアドレス、相手のアドレス、送信時の時刻、取得したポイントをブロックチェーンに記録すると共に、相手のアドレス毎に mapping にて最新の送信時刻をブロックチェーンに記録し、この時刻の情報を元にポイントを計算している。（※ポイント計算の為にデータをすべて検索するのは時間がかかるのと高額なガス代につながるため mapping を利用した。）

以下の関数を実装している。

•[Write] postLetter(address _to,string _text)

あて先アドレスとメールの内容を引数に指定してブロックチェーンに書き込む関数。

•[Read] lastTime(address)

アドレスを引数に指定することにより、そのアドレス宛に送られたメッセージの最新の送信時間が読み出せる。

•[Read]letters(uint256)

ブロックチェーンに記録されたメッセージを読み出すための関数。引数は記録された順番で最初に記録されたメッセージは 0 番。メッセージ、自分のアドレス、相手のアドレス、送信時の時刻、取得したポイントを読み出すことができる。

•[Read]timePoints(address _adr)

アドレスを指定することにより、そのアドレスにメッセージを送った時に取得できる予定のポイント数を取得できる。

•[Read]totalLetters()

ブロックチェーンに記録されたメッセージの総数。この数未満を引数に指定して letters(uint256)にてブロックチェーンのメッセージを読み込むことができる。

•[Read]totalPoints(address _adr,uint256 startNumber)

その人（アドレス）の総ポイント数を計算して値を返す。startNumber でメッセージの何番から集計を行うのかを設定できる。

※このスマートコントラクトにはいろいろ問題があるが、現時点では問題を解消する為のコードの実装は一切行っていない。4 章にて紹介する。

3- 2 client/index.html

ソリディティにアクセスするための web アプリ。

jQuery および Bootstrap を利用している。jQuery を利用し JAVA を簡単なコードで動くようにしており、また、Bootstrap を利用して見た目を整えている。またスマートコントラクトにアクセスするための web3.js のライブラリを読み込んでいる。

3- 3 client/abi.js

ソリディティのプログラムへのアクセス方法を記載している ABI（contract Application Binary Interface）ファイル。基本部分はソリディティのプログラムをコンパイルすることにより自動生成されるので、それを利用し作成する。デモのコンパイルは Remix を利用した。

3- 4 client/address.js

メッセージを頻繁にやり取りする人同士の名前と対応するアドレスが書かれたリスト。

あくまでデモ用のサンプル。

3- 5 client/pic1.png および pic2.png

女の子のイラスト。通常は pic1.png が表示されているが、メッセージの送信が成功すると pic2.png が表示される。

4. 問題点

スマートコントラクトで余計な制限をかけていないこと、また、ゲームとしてはいろいろとチートができてしまうなどの問題点があるが、ブロックチェーンの本質を理解するためにあえて制限をかけない方がデモとしては面白いと判断して現状は何も制限をかけないことにした。

(1) 誰でもメッセージを送ることができる。

パブリックのブロックチェーンにデプロイすることにより、誰もが任意の相手にメッセージを送れてしまうということになる。誰でも参加できるというメリットがある一方、匿名のアドレスを利用して送信主が分からないように匿名で悪口のメッセージを送ることもできてしまう。もちろん、ネットワークへのアクセスを解析することで、匿名のアドレスから誰かばれる可能性もあるので、全くの匿名が保たれるとは限らない。

解決方法としては、スマートコントラクトにてオーナーのみが変更可能な参加者リストを作成して、メッセージを送り合えるメンバーを限定する方法があると考えられる。

(2) ポイントを無限に送り続けられる

ゲームとしては、メッセージの送信回数に制限を設けていないので、同じ人に対して何度もポイント送ったり、自分が持っている別のアドレスから自分宛てにメッセージを送ってポイントを取得することができる。解決方法としては、スマートコントラクトで一度メールを送った後は一定期間メールが送れなくなる機能を実装する方法が考えられる。

(3) 何ポイント得られるかを把握できる

web アプリからはあえてメッセージを送った時に取得できるポイントを見るためのインターフェースは用意していないが、ブロックチェーンを直接覗いたり、スマートコントラクトの関数にアクセスすればポイント数がどれくらい取得できるか簡単にわかってしまう。解決方法としては、時間情報をブロックチェーン外に持ち、アクセス制限を設けるなどが考えられるかもしれない。

(4) ブロックチェーンに書いたり読んだりするスピードが遅い

ネットワークのブロックチェーンのファイナリティのスペックに依存するが、ネットワークによってはかなり本 web アプリのレスポンスが遅いと感じるかもしれない。

(5) 得点の集計期間の設定が web アプリ側

特にポイントの不正が行えるというわけでないが、得点の集計期間の設定は web アプリ側から設定することになっている。スマートコントラクトにてオーナーが自動的に設定出来たり、あるいは、スマートコントラクトが自動的に集計期間を設定出来るようにすることも可能と考えられる。

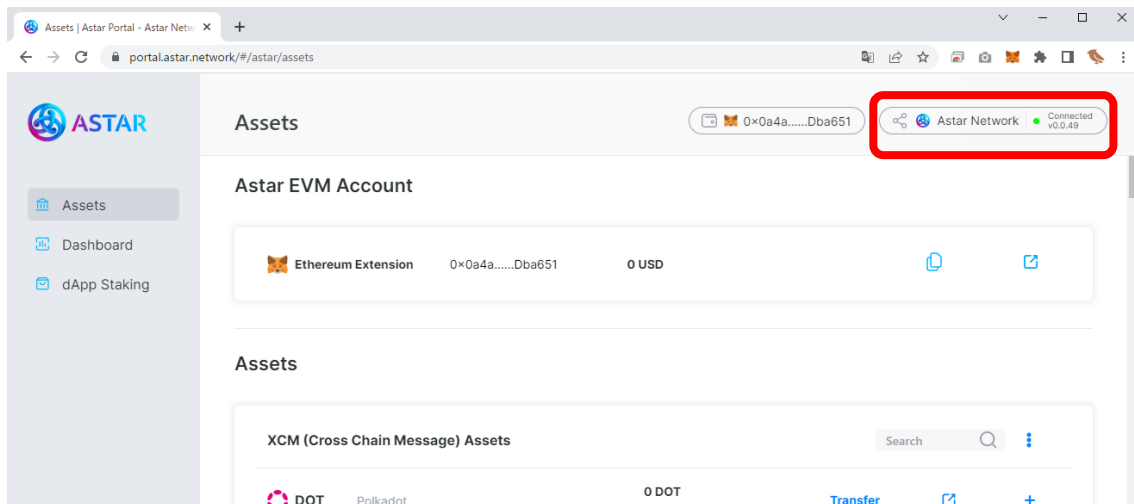
5. デモ実行

5- 1 Metamask の設定

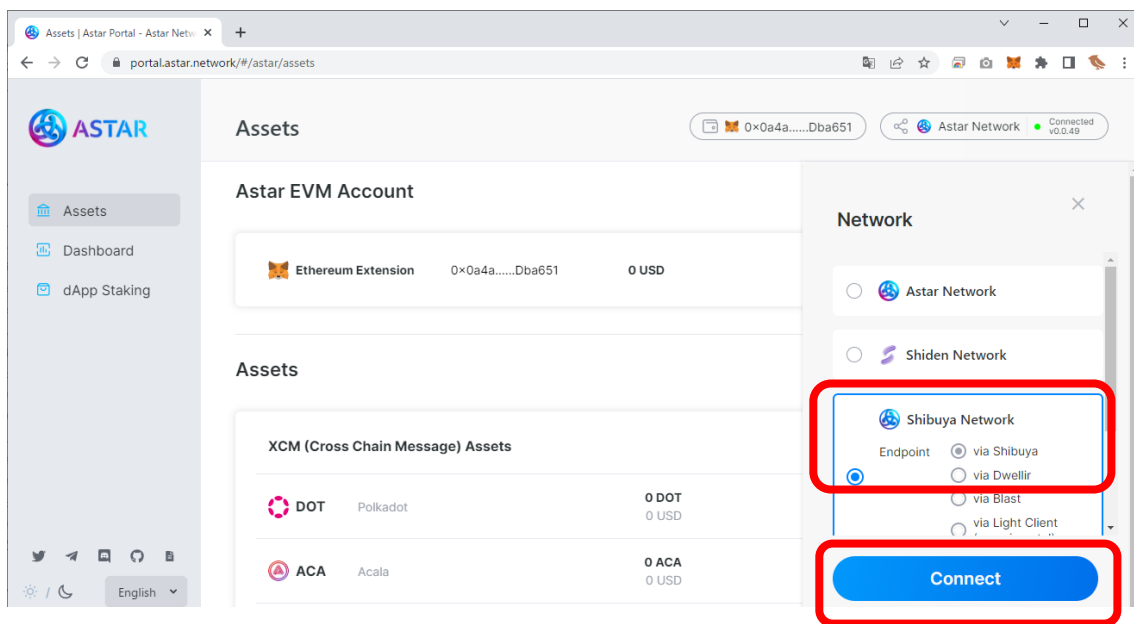


メタマスクを

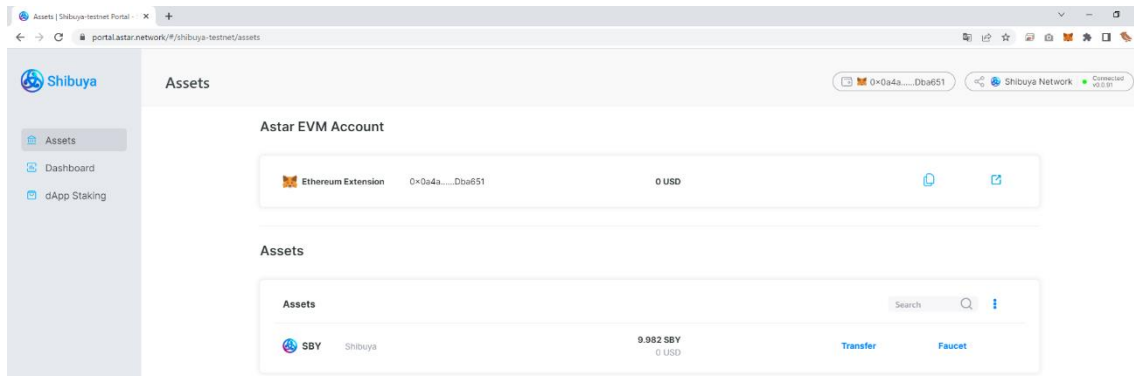
ネットワークを“Shibuya Testnet”に設定するとともに、SBY の残高がある事を確認する。
もし、“Shibuya Testnet”が存在しない、残高が無い場合はアスターのサイトにアクセスする。
<https://portal.astar.network/#/astar/assets>



右上の“Asetr Network”をクリックすると以下の画面が出てくる。“Aster Network”に○がついているので、画面を下にスライドして、“Shibuya Network via Shibuya”を選択する。

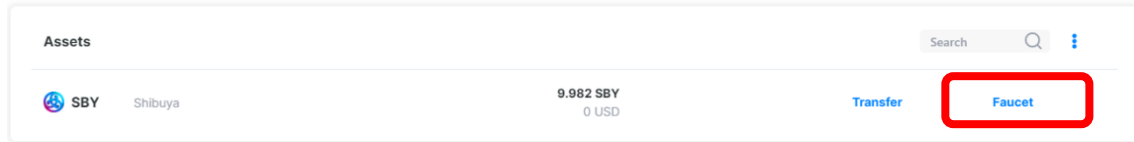


“Shibuya Network via Shibuya”を選択した後、Connect ボタンを押す。と Metamask が起動しネットワーク切替等のメッセージが出た後、次のような Shibuya ネットワークの画面になる。



ここで、Assets 内の“Faucet”をクリックする。

Assets



Faucet のダイアログが出る。ここで私はロボットではありませんにチェックを入れ、“Confirm”ボタンをクリックすることで、10SBY もらえる。Metamask に 10SBY が入金されたことを確認して次の作業に行く。

Faucet


What is faucet and how does it help you?

There is a small fee for each transaction, and this is paid using SBY tokens. If you have no SBY in your account, you cannot send any tokens. Faucet sends enough SBY to cover the transaction fee.

Faucet Balance: 118,987.527 SBY

You will receive
10 SBY

☐ 私はロボットではありません

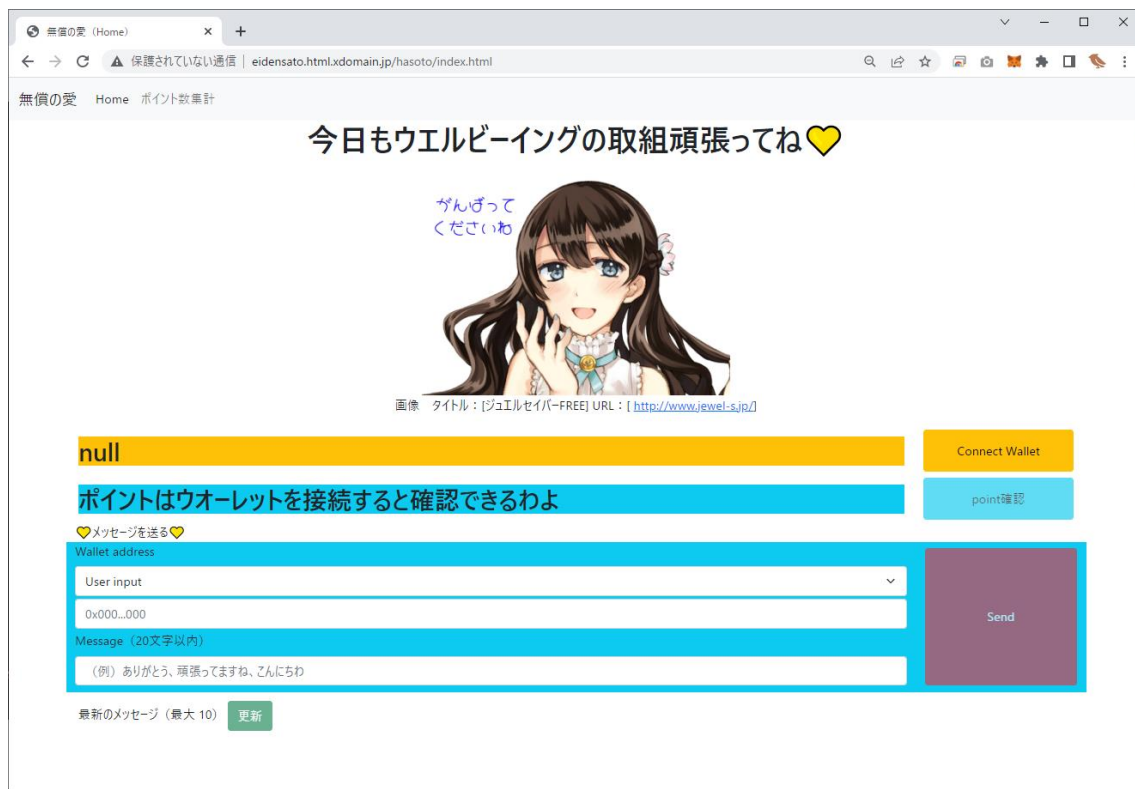

reCAPTCHA
プライバシー - 利用規約

Confirm

5- 2 デモサイトへのアクセス

Metamask のネットワークが“Shibuya Testnet”、SBY の残高がある状態で以下のサイトにアクセスする。

<http://eidensato.html.xdomain.jp/hasoto/index.html>



5- 3 ウォレットの接続

“Connect Wallet”ボタンを押し、成功するとアドレスが正常に表示される。

また、ポイントと送受したメッセージが表示される。

メッセージの青丸は自分が相手に送ったメッセージ。黄丸は相手からもらったメッセージ。丸の中の数字が取得したポイント。



5- 4 メッセージの入力（メンバーリストからの選択）

メッセージを送るフォームの右側をクリックする。

♡メッセージを送る♡

Wallet address

User input

0x000...000

Message (20文字以内)

(例) ありがとう、頑張ってますね、こんにちは

リストが出るので、メッセージを送りたい相手を選ぶ。

♡メッセージを送る♡

Wallet address

User input

User input

佐藤 総一

大山 茂

三上 さやか

尾崎 常道

濱田 淳

内山 貴可

Wallet address に選択した相手が表示されていることを確認（アドレスの数字は自動的にセットされ変更できません）して、メッセージを入力する。

無償の愛 (Home) x +

← → C 保護されていない通信 | eidensato.html.xdomain.jp/hasoto/index.html

無償の愛 Home ポイント数集計

今日もウェルビーイングの取組頑張ってるね♡

がんばって
くださいわ

画像 タイトル: [ジュエルセイバー-FREE] URL: [http://www.jewel-s.jp/]

0x0a4ab49cb3a71263bb3881799f50c32af0dba651

Connect Wallet

あなたのポイントは 25 ポイントよ

point確認

♡メッセージを送る♡

Wallet address

濱田 淳

0x18769354a755Bc3AEa18E324d669b86DDfb585C

Message (20文字以内)

こんにちは

Send

最新のメッセージ (最大 10) 更新

To: 大山 茂 2

Message: [2023/3/10-18:27:24]頑張ってる

5-5 メッセージの入力（アドレス直接入力）

メッセージを送りたい人のアドレスとメッセージを直接入力する。

無償の愛 (Home) × +

← → ↺ 保護されていない通信 | eidsato.html.xdomain.jp/hasoto/index.html

無償の愛 Home ポイント数集計

今日もウェルビーイングの取組頑張ってるね♡

がんばって
くださいわ

画像 タイトル: [ジュエルセイバー-FREE] URL: [<http://www.jewel-s.jp/>]

0x0a4ab49cb3a71263bb3881799f50c32af0dba651

Connect Wallet

あなたのポイントは 25 ポイントよ

point確認

♡メッセージを送る♡

Wallet address

User input

0xb27Ef6bB58F12EC2Ce17C1913A9e7a8e9c32aFe2

Message (20文字以内)

こんにちは

Send

最新のメッセージ (最大 10) 更新

To: 大山 茂 2

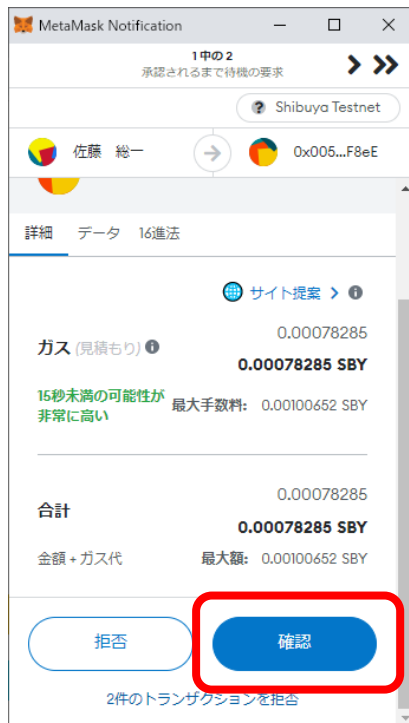
Message: [2023/3/10-18:27:24]頑張ってる

5- 6 メッセージの送信

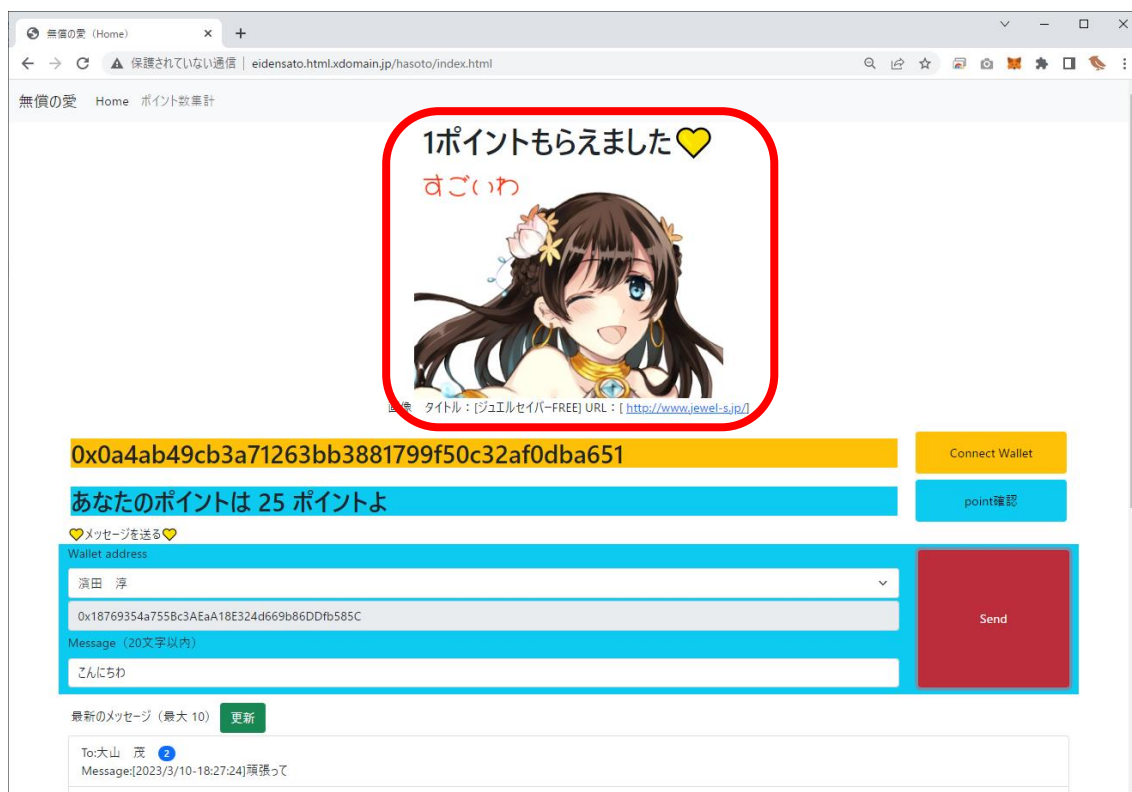
Send ボタンを押す。



メタマスクが起動するので確認ボタンを押す。



正常にメッセージが送られると、タイトルにもらえたポイントが表示され、絵も変わります。



ポイント数、メッセージは自動更新されませんので、“points 確認”ボタン、メッセージの“更新”ボタンを押すとそれぞれ最新の状態に更新されます。

6. 使用素材

無償で利用できる、

タイトル：[ジュエルセイバー-FREE] URL：[http://www.jewel-s.jp/]

の絵を利用している。※利用申請済み。

以上