技術資料

NEMscription Platform - OPEN EXPERIMENT

この資料は、パブリックブロックチェーンNEM(Symbol)を利用した、Subscription課金システムの
プロトタイプ（原理試作システム）を用いた公開実験についての技術資料です。

今後、必要に応じて、以下のページで最新の情報を公開していきます。

技術情報の公開（NEMscription Platform - OPEN EXPERIMENT） - https://kitsutsuki.tokyo/technical-information-nemscription/

システム動作の概要

今回の実験では、「BCCC2EE01677A923」という名前のキーを利用することして、対象アドレスが
値の部分の数値（194640）のブロック高までサービスを利用していることを証明することとしている。
※ 有効期限が切れたら、また申し込んでみてください。値を更新するTxが発行されます。

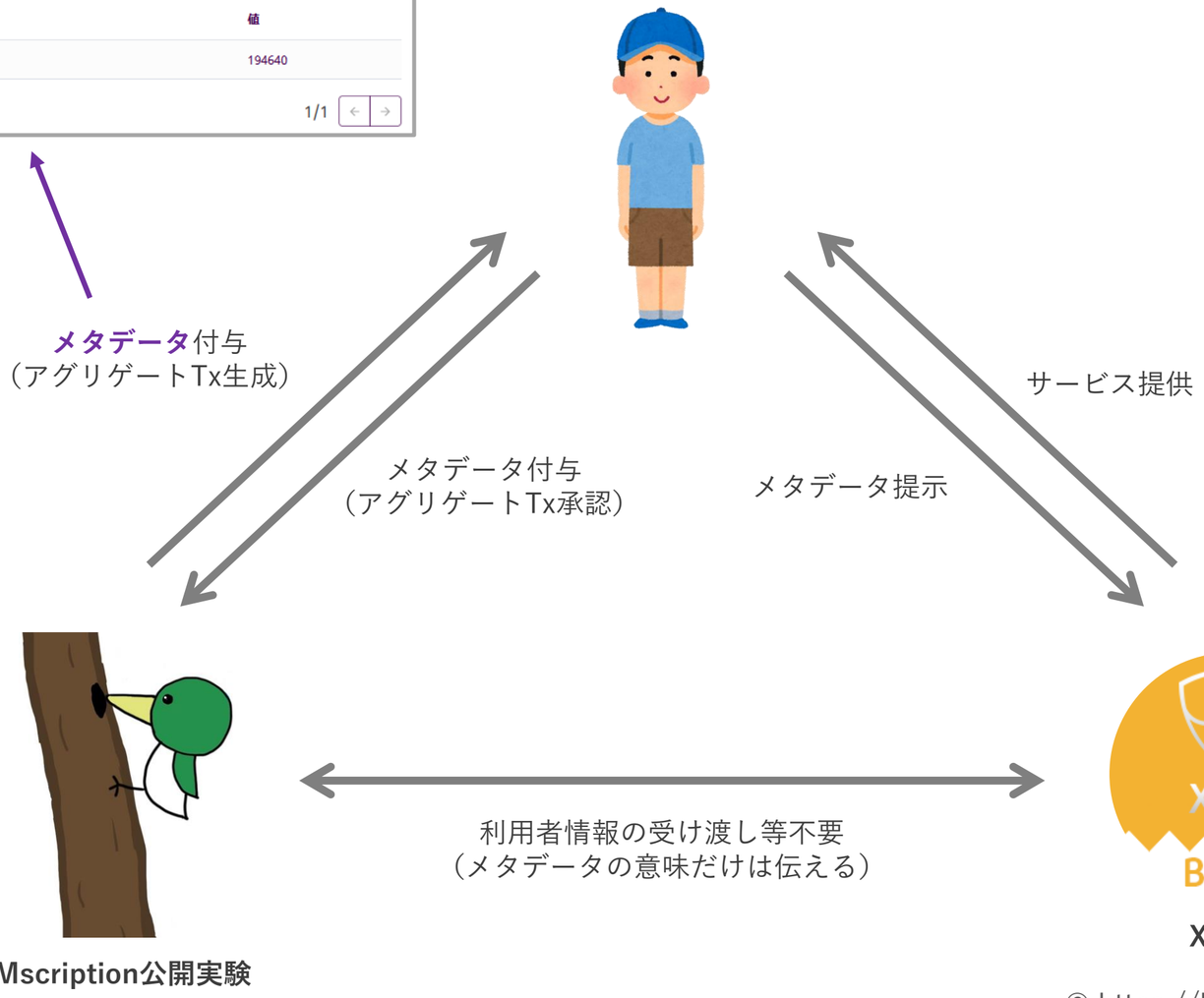
メタデータエントリ　Recent

スコープメタデータキー	対象アドレス	値
BCCC2EE01677A923	NASQMLD67T3RBZU6A4XZ77D5H3R2JNJUK4NE63Y	194640

1/1

メタデータは、エクスプローラから対象アドレス
（自分のアドレス）を見ることで確認できます。

http://explorer.symbolblockchain.io/



メタデータエントリ

Recent

スコープメタデータキー	対象アドレス	値
BCCC2EE01677A923	NASQMLD67T3RBZU6A4XZ77D5H3R2JNJUK4NE63Y	194640

↓ 実験参加アドレスを表す。

↑ 今回の実験に紐づくメタデータであることを表すキー

サービスの有効期限（ブロック高）を表す値 ↑

1/1

1つのアカウント（アドレス）で複数のメタデータを持つことも可能。

メタデータエントリ

Recent

スコープメタデータキー	対象アドレス	値
CEFDEEF67E477F98	TDT4DDLD2RX5NIGERHXNIK24IJVJO45362ACW6A	12333
BCCC2EE01677A923	TDT4DDLD2RX5NIGERHXNIK24IJVJO45362ACW6A	123

ワクチンパスポート用のキー

ワクチン接種を受ける人のアドレス

未接種（0） or 接種日(年月日)

1/1

↑ たとえば、このようなデータを付与することでワクチンパスポートのような仕組みも構築可能。

メタデータを利用したワクチンパスポートシステムの例

アグリゲートTxを利用してメタデータを付与するので、
一方的にメタデータの生成や偽造が出来ない。
※ 公的機関のアカウントとパスポート利用者の双方の秘密鍵で署名が必要。

第三者に秘密鍵を贈与してしまわないような仕組みは必要
例：生体情報で本人確認など

国民

PASS パスポート生成

メタデータ**付与**
（アグリゲートTx生成）

メタデータ**承認**
（アグリゲートTx承認）

パスポートの**正当性確認**し、サービス提供（入店許可）
→　メタデータが確かに公的機関のアドレスから
　　付与されていることを確認

メタデータ提示
（パスポート提示）

PASS

公的機関

飲食店

社会

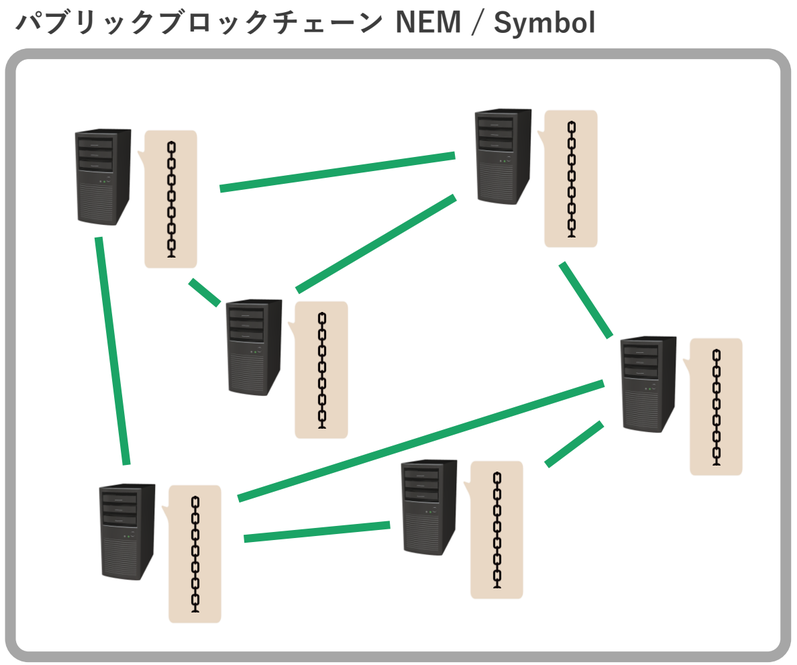
広く社会に対して、
・ 公的機関で使用するアドレス
・ メタデータの仕様
を公開

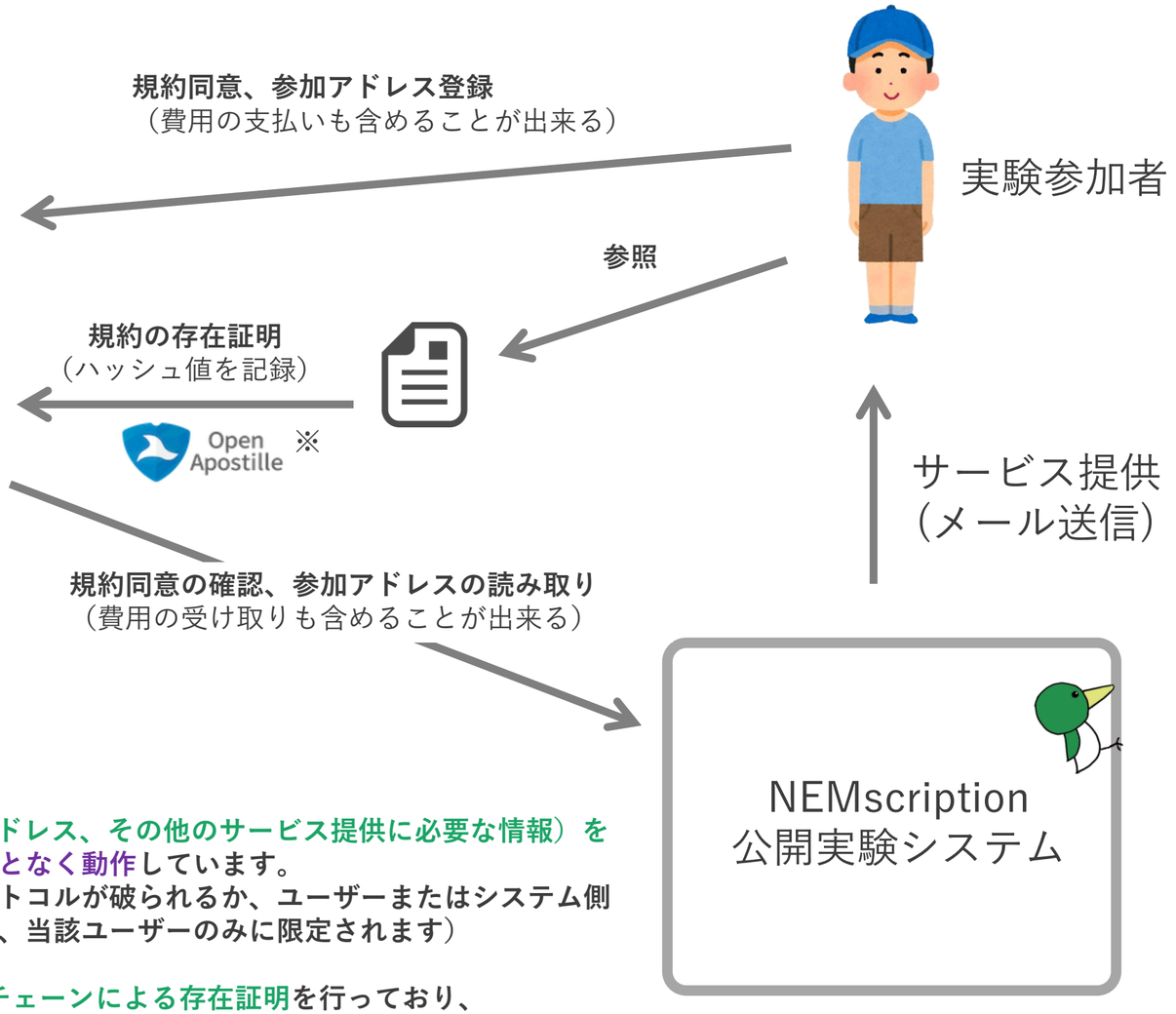
その他の様々なサービス

この公開情報に従って、提示されたメタデータを確認すれば、
あらゆるサービスでワクチンパスポートが利用可能。

システム動作の概要（バージョン１）

※ OpenApostilleは @DaokaTrade 氏が提供する、パブリックチェーンを利用した存在証明サービスです。
ただし、現状はSymbol版ではなくNIS1版のみ提供。（ https://www.openapostille.net/ ）

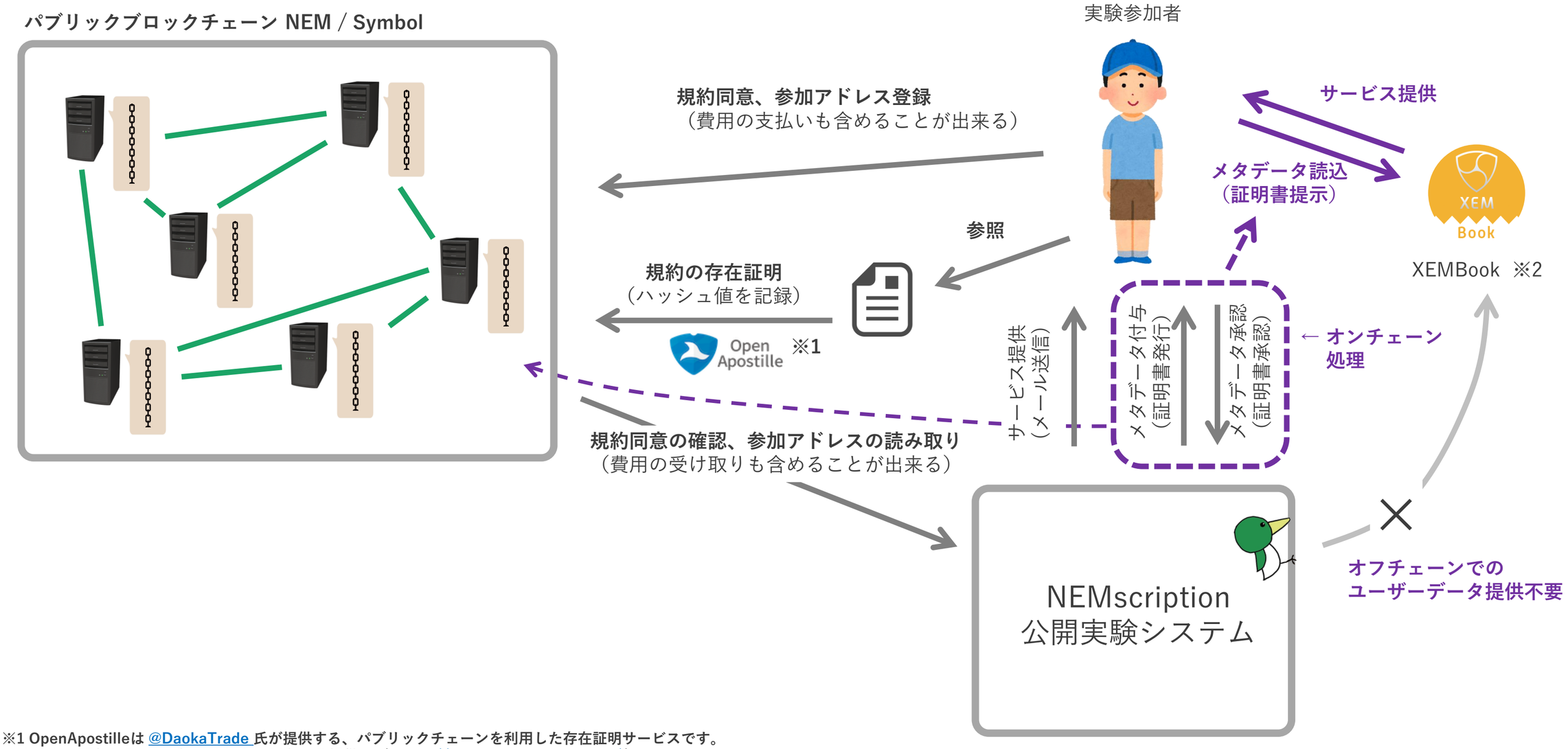




NEMscription システムでは、**すべてのユーザー情報（規約への合意意志、メールアドレス、その他のサービス提供に必要な情報）をパブリックブロックチェーン上に記録**することで、**自前のデータベースを用意することなく動作**しています。
なお、ユーザー情報は暗号化された状態で記録されており、ブロックチェーンのプロトコルが破られるか、ユーザーまたはシステム側の秘密鍵が漏洩しない限り安全に守られます。（ユーザーの秘密鍵漏洩の影響範囲は、当該ユーザーのみに限定されます）

また、**規約については外部サービスであるOpenApostille※を利用して、パブリックチェーンによる存在証明**を行っており、
その**規約へのユーザーの合意意志もブロックチェーン上に、事実上、削除不可能な形で残り**続けます。

システム動作の概要（バージョン２）

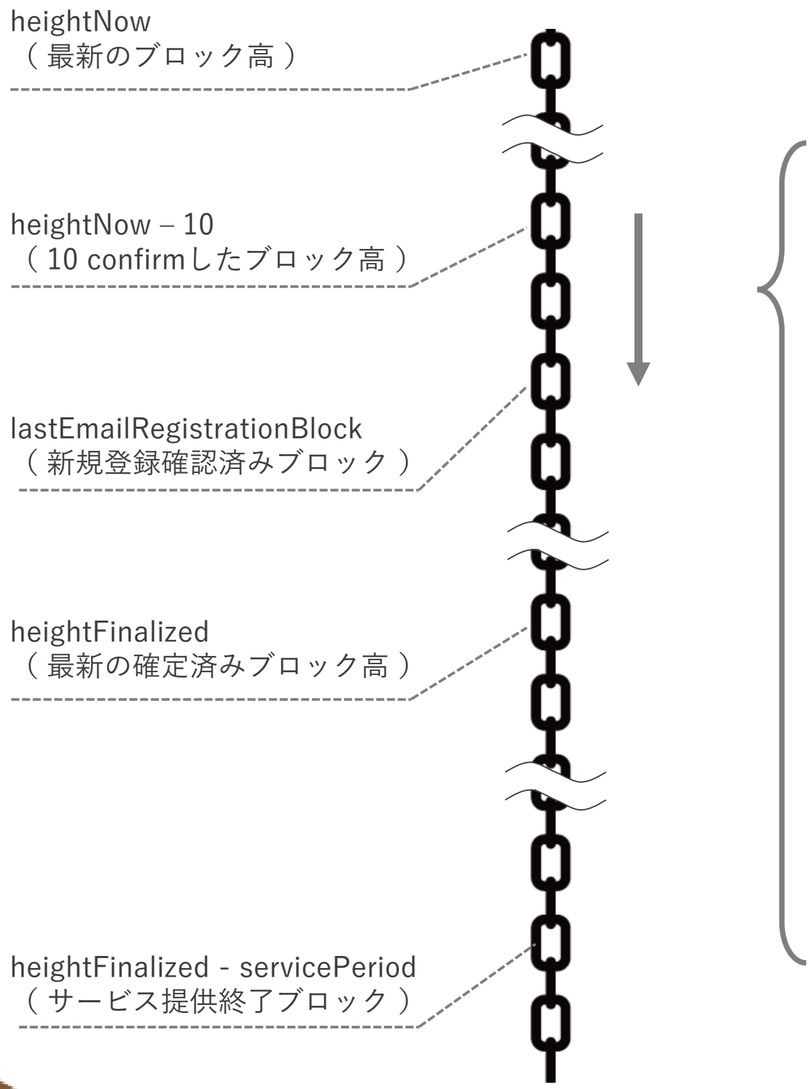


※1 OpenApostilleは @DaokaTrade 氏が提供する、パブリックチェーンを利用した存在証明サービスです。
ただし、現状はSymbol版ではなくNIS1版のみ提供。（ https://www.openapostille.net/ ）

※2 XEMBookは @xembook 氏が提供する、アカウント情報（残高、送金履歴など）閲覧ツールです。
（ https://xembook.github.io/xembook/ ）

新規登録メール送信の動作イメージ

このループを定期的に実行
（公開実験では１回/分に設定）



1 ： サーバに保存したテキストファイルから、前回のループで
新規登録メール送信処理を行った最後のブロックを読み取り。

2 ： 10confirmしたブロックから、前回のループで新規登録メール送信を
を行った最終ブロックの間で指定アドレスに届いたTxを抽出。※

3 ： agreeメッセージ（サービス登録依頼）を抽出

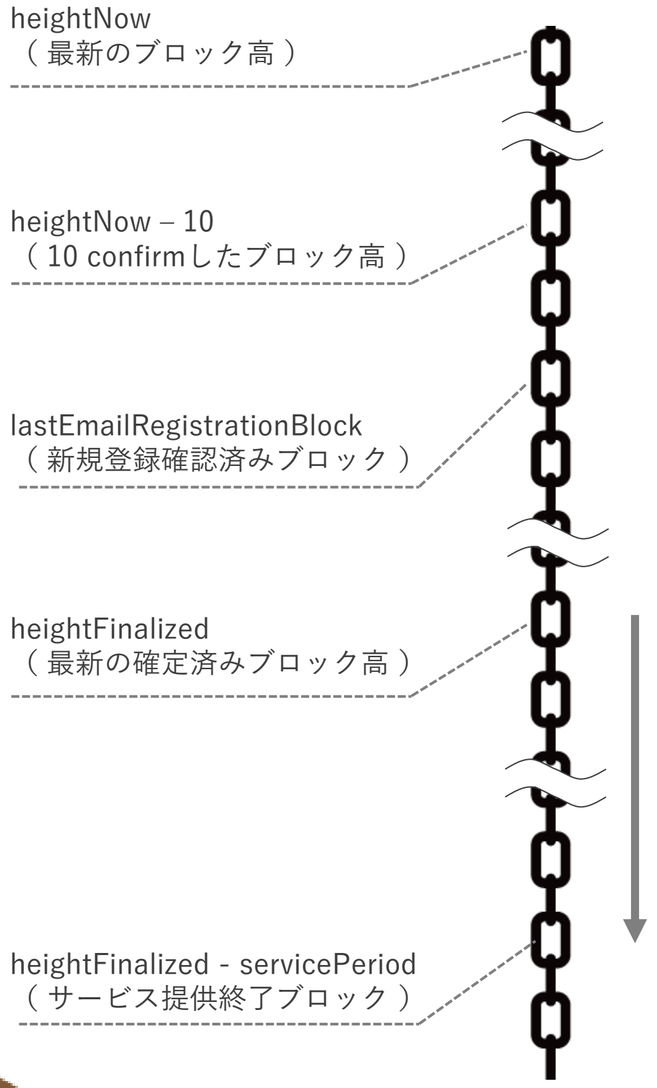
4 ： 正しい書式のメッセージに対して、新規登録メールを送付

5 ： 新規登録メール送信処理を行った最新ブロックを、
サーバにあるテキストファイルに記録。

※ 今回の公開実験ではユーザーの利便性を重視して10confirm(約5分)で登録確認メールを送信した。
よりシステムの堅牢性を重視する場合には、Finalizedされてから送信する手もある。

ノード監視サービスの動作イメージ

ブロックチェーンデータ



このループを定期的に実行
（公開実験では３回/日に設定）

1 ： サービス提供期間に指定アドレスに届いたTxを抽出

2 ： rejectメッセージ（登録解除依頼）を抽出

3 ： rejectアドレスを配列に格納

4 ： agreeメッセージ（サービス登録依頼）を抽出

5 ： rejectアドレスに該当しないagreeメッセージに対して
サービス（ノードの状態監視と結果のメール報告）を実行。※

6 ： rejectアドレスを格納した配列を初期化
（記憶したメールアドレスを削除）

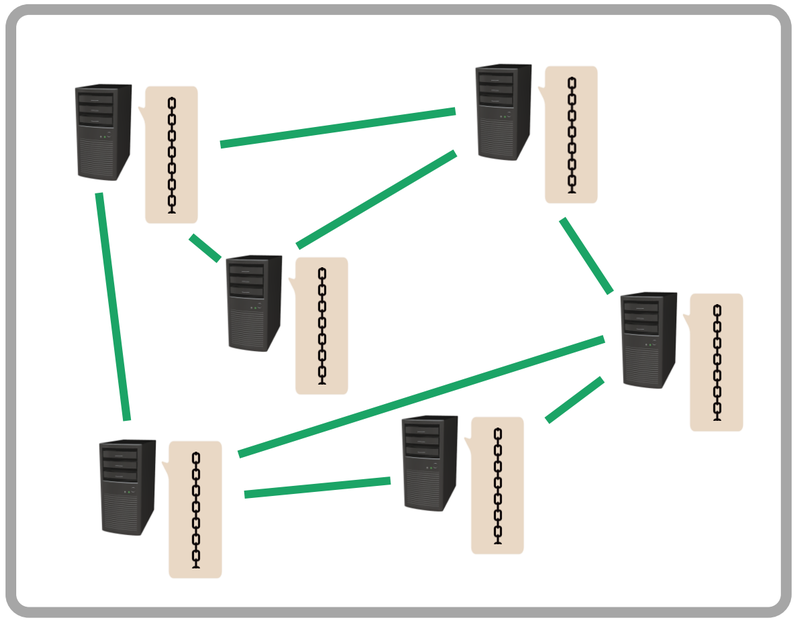
※ 今回の公開実験では無償サービスとして提供したが、サービス提供対象を
「正しい書式のメッセージが届いている」かつ「指定以上の金額の送金をしている」
という条件で絞り込めば、**簡単にサブスクリプションサービス化**できる。

システムの特徴（オンチェーン側/オフチェーン側の特徴）

オンチェーン側

非中央集権 / 強い耐改竄性 / トラストレス

パブリックブロックチェーン NEM / Symbol

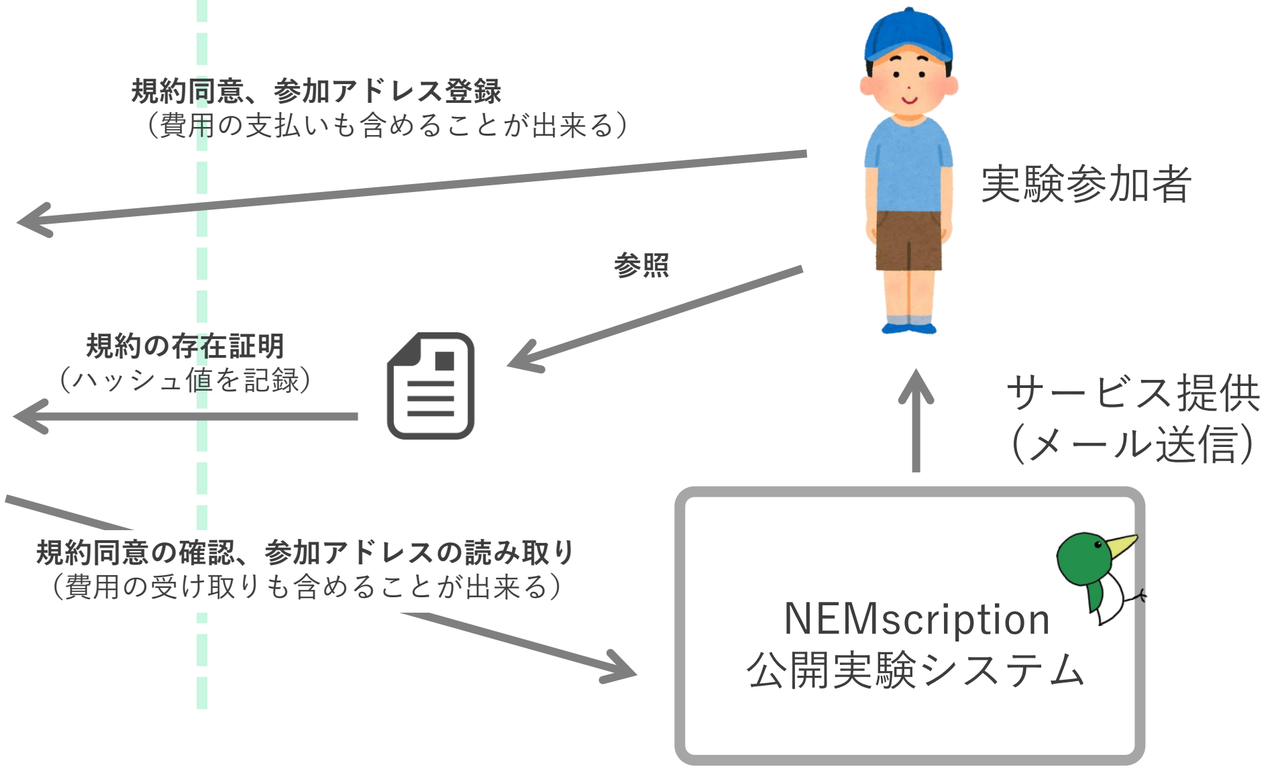


一度、データがパブリックチェーンに取り込まれると、
事実上、（誤記訂正を含む）書き換えも削除も不可能となる。

強力な**耐改竄性を持つ一方で、柔軟性に欠け**る。

オフチェーン側

中央集権 / サービス提供者による書き換えが容易 / トラストが必要



管理者の一存で、システムの書き換えが可能。
バグ対応が容易になる一方で、実験参加者視点では、本当にサービスが
提供されるのかは**実験主催者側をトラスト（信頼）する必要**がある。

どこまでをオンチェーン化して、どこまでをオフチェーン運用とするのかの線引きは、考え甲斐のある課題

システムの特徴（送金関係）

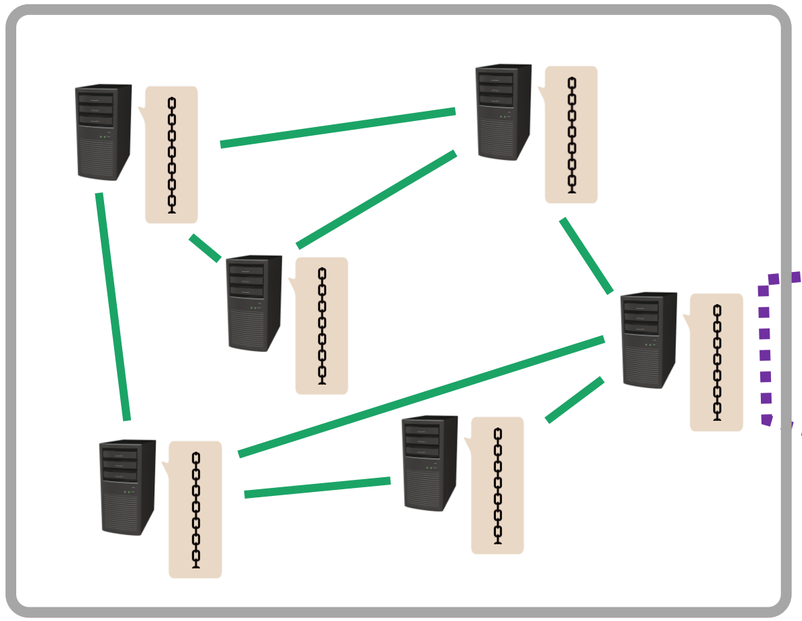
オンチェーン側

非中央集権 / 強い耐改竄性 / トラストレス

オフチェーン側

中央集権 / サービス提供者による書き換えが容易 / トラストが必要

パブリックブロックチェーン NEM / Symbol



実験参加者

送金の流れ

サービス提供
（メール送信）

NEMscription
公開実験システム

今回の公開実験は無償で提供していますが、課金を行う場合の流れは、破線のようになります。

クレジットカード会社などを経由する必要がないため、導入のハードルが低く、手数料も低く抑えられます。
また、氏名やカード番号などの個人情報がなくても安全な送金が可能なため参加者側視点で「怪しいサイトにクレカ番号打ちたくない」のような
心理的なハードルを下げることができます。
（技術的には、システム側と参加者側の2者間で完全匿名取引も可能です。ただし、国家権力であれば取引所の出金データなどから個人特定を出来る可能性が高いので、
くれぐれも悪用しようなどとは考えないでください。また、匿名取引の実施にはマネロン対策視点での注意も必要と思います。）

技術的課題

以下、今回のシステムを作ってみての雑感です。
「こうすればいいんじゃない？」とか、「他にもこんな課題あるね？」とか、「ここどうなってるの？」とか、フィードバックもらえると嬉しいです。

今回の実験システムを応用して、何か面白いことができないか？
（たとえば、飲食店が来店客の情報を記録して、コロナ発生時に通知するシステムとか、ちょっと工夫すれば作れる気がした。
　ただし、「それブロ（それブロックチェーンでやる必要あるの？）」って言われそうｗ あと、実用を前提とした信頼性が必要とされると、経験がなくてハードル高い。）

実用の為には、万が一にも、ユーザーがメッセージの暗号化を忘れてTxの送信をすることがないように、専用のインターフェイスを用意する必要がある。

現状よくある「□規約に同意します」にチェックを入れる形式でも、世の中的に特に問題が起こっていないように見えるが、わざわざブロックチェーンを利用して規約文面の存在証明をすることや、同意意思を改竄不可能な形でブロックチェーンに残すことにたいして、果たして実利的な意味があるのか？

ユーザー側の秘密鍵漏洩の影響は、当該ユーザーのみに限定されるが、システム側の秘密鍵が漏洩すると、全ユーザー情報が閲覧可能になってしまう。
（目指せ北海道さん方式（どこかで書いてたと思うんだけど見つけられず）で、ユーザー情報は別の場所に保管し、　ユーザー情報に紐づく文字列をメッセージ化する方法も考えられるが、別途、データベースを用意する必要がある。データベースからの情報漏洩リスクと、秘密鍵漏洩リスクをどのように評価するか？）

実験主催者側視点では、実験参加者が、規約に同意したことや、参加申込内容、（有料サービスとする場合には送金の受け取り）をほぼ絶対的と言える確度で証明可能となる。
一方、実験参加者側視点では、本当にサービスが提供されるかは、実験参加者側へのトラストが必要。
（トークン化できるサービスであれば、アグリゲートTxでお互いにトラスト不要と出来るが、このようなサービスで参加者側がトラストしなければならないコストを低減できないか？）

ユーザーが新規登録直後に、登録内容に誤りがあることに気づき、すぐにrejectメッセージ（登録解除依頼）を送信。その直後に、あらためて新規登録依頼を行ったとする。
これらの3TxがFinalizedされる順序が、ユーザーがTxを作成した順序と前後した場合、システム側ではユーザーの正しい意図を把握することができない。

通常の、ユーザー側が自発的に解約しないと継続課金されるサブスクリプションとは異なり、このシステムでは、ユーザーが定期的に送金をしないとサービスが継続されないという動作であるため、事業者側視点では、ユーザーの離脱率が高くなるデメリットがあります。
言い方を変えれば、ユーザーの解約忘れを狙うようなことなく、ユーザーに「定期的に支払いを行ってでも使いたい」と思ってもらわないと成立しない健全なビジネス形態であるという見方も出来るかもしれません。（支払い忘れで、意図せず解約されてしまって、クレームになるリスクはある。）