CRYPTREC Symposium 2024, Tokyo, Japan

暗号資産の鍵管理

IIJ
Internet Initiative Japan

須賀祐治 0x613851AfC21Cb290Cc60a0Fb9FfeC319074cfeCa

2024-09-02

Ongoing Innovation

□に不等号記号を入れなさい

128 □ 256

[2024 CRYPTREC]

□に不等号記号を入れなさい

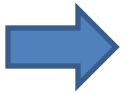
56 □ 64

[1976 NIST]

本格的にFinancial securityに関わるきっかけ

Backgrounds: Too many incidents

- Japan is one of top countries which suffered from cryptocurrency/cryptoassets incidents.
  - (We should have learned from past incidents)



Date	Victim	Value of coin loss
Feb 2014	Mt.GOX (Japan)	$450 Million
Jan 2018	CoinCheck (Japan)	$535 Million
Sep 2018	Zaif (Japan)	$ 59 Million
Jul 2019	BitPoint (Japan)	$ 32 Million

General policy

C G T F | CRYPTOASSETS GOVERNANCE TASK FORCE

https://cgtf.github.io/

Neutrality

We will address this issues from multiple perspectives, including academic and security experts as well as crypto asset exchanges.

Transparency

By publishing the documents and minutes to be developed by CGTF, we aim to ensure transparency in the management of the TF.

Effectivity

We aim to create documents that are useful in practice by reflecting the knowledge of domestic and international experts in standardization organizations.

History in 2018

Feb.8. 2018	1st TF Meeting.
July. 2018	Security WG deliverable "General Security Considerations for Cryptoassets Custodians" submitted to **IETF** as an internet draft.
Oct. 2018	Public Draft: Japanese edition “General Security Considerations for Cryptoassets Custodians” (received > 100 comments)
Oct. 2018	Activity Report on the Scaling Bitcoin Tokyo.
Dec. 2018	Members were dispatched to the Technical Committee of **JVCEA** (the Japan Virtual Currency Exchange Association, established in March 2018, as a self-regulatory organization accredited by the Japanese Financial Services Agency (JFSA) on October 24, 2018)

CGTFからのアウトプット

『暗号資産カストディアンのセキュリティ対策についての考え方 第5版』

2024/4/12

Cryptoassets Governance Task Forceは、『暗号資産カストディアンのセキュリティ対策についての考え方 第5版』を公開しました。 Download PDF なお第5版のパブリックコメントに対してコメントを1件お寄せいただきました。 コメントの場所 8.3.13 事業継続マネジメントにおける情報セキュリティの側面 システムの継続が困難に

『暗号資産とNFTのトラブル集』

2022/11/7

Cryptoassets Governance Task Forceは、ウェブサイト『暗号資産とNFTのトラブル集』を公開しました。 暗号資産とNFTのトラブル集 暗号資産は利用者同士で直接取引ができることから、交換業者に対して安全対策の必要性を働きかけるだけではなく、利用者（消費者・投資家）に直接届けるドキュメントを作成する必要があるのではないか、との議論をもとに、本サイトを開設することにしました。また、近年目にするようになった言葉でもあるNFTにも触れています。 このサイトの内容は、確定したものではなく、みなさまからのご意見をいただき、よりよいものに改善していきたいと考えております。誤字脱字といったものだけではなく、想定される事例や実際の事例、カテゴリーの追加や変更など、忌憚のないご意見をいただければ幸いです。 ご意見はGithubのIssueにて受け付けます。 本サイトの内容が、少しでもトラブルを未然に防ぐためのお役に立てれば幸いです。 See more

Key takeaways

- **暗号資産は署名鍵取られたらおしまい**
  （private key使って）署名すること＝資産を移動させること
- **自己責任論で終わらせてよいか**
  資産運用管理は鍵管理と同等・消費者保護の観点も必要
  自分で鍵管理できないなら信用できるカストディアンへ
- **CRYPTRECとしてどう対策するか**
  おすみつき制度の導入（EUDIWの例）・技術中立性の確保
  ロビー活動の是非（税制改革ではやってる）

「暗号資産」の定義

「暗号資産（仮想通貨）」とは、インターネット上でやりとりできる財産的価値であり、「資金決済に関する法律」において、次の性質をもつものと定義されています。

（1）不特定の者に対して、代金の支払い等に使用でき、かつ、法定通貨（日本円や米国ドル等）と相互に交換できる

（2）電子的に記録され、移転できる

（3）法定通貨または法定通貨建ての資産（プリペイドカード等）ではない

https://www.boj.or.jp/about/education/oshiete/money/c27.htm

資金決済に関する法律（資金決済法）

7　この法律において「暗号資産交換業」とは、次に掲げる行為のいずれかを業として行うことをいい、「暗号資産の交換等」とは、第一号及び第二号に掲げる行為をいい、「暗号資産の管理」とは、第四号に掲げる行為をいう。

一　暗号資産の売買又は他の暗号資産との交換

二　前号に掲げる行為の媒介、取次ぎ又は代理

三　その行う前二号に掲げる行為に関して、利用者の金銭の管理をすること。

四　他人のために暗号資産の管理をすること（当該管理を業として行うことにつき他の法律に特別の規定のある場合を除く。）。

8　この法律において「暗号資産交換業者」とは、第六十三条の二の登録を受けた者をいう。

（暗号資産交換業者の登録）

第六十三条の二　暗号資産交換業は、内閣総理大臣の登録を受けた者でなければ、行ってはならない。

https://elaws.e-gov.go.jp/document?lawid=421AC0000000059

暗号資産交換業者登録一覧

令和５年４月30日現在

・本一覧に記載された暗号資産交換業者が取り扱う暗号資産は、当該暗号資産交換業者の説明に基づき、資金決済法上の定義に該当することを確認したものにすぎません。
・金融庁・財務局が、これらの暗号資産の価値を保証したり、推奨するものではありません。暗号資産は、必ずしも裏付けとなる資産を持つものではありません。
・暗号資産の取引を行う際には、以下の注意点にご留意ください。

≪暗号資産を利用する際の注意点≫

○ 暗号資産は、日本円やドルなどのように国がその価値を保証している「法定通貨」ではありません。インターネット上でやりとりされる電子データです。

○ 暗号資産は、価格が変動することがあります。暗号資産の価格が急落し、損をする可能性があります。

○ 暗号資産交換業者は金融庁・財務局への登録が必要です。利用する際は登録を受けた事業者か金融庁・財務局のホームページで確認してください。

○ 暗号資産の取引を行う場合、事業者が金融庁・財務局から行政処分を受けているかを含め、取引内容やリスク（価格変動リスク、サイバーセキュリティリスク等）について、利用しようとする事業者から説明を受け、十分に理解するようにしてください。

○ 暗号資産や詐欺的なコインに関する相談が増えています。暗号資産の持つ話題性を利用したり、暗号資産交換業の導入に便乗したりする詐欺や悪質商法にご注意ください。

【全業者数：30】

所管	登録番号	登録年月日	暗号資産交換業者名	法人番号	郵便番号	本店等所在地	代表電話番号	取り扱う暗号資産
関東財務局【計28業者】	関東財務局長第00001号	平成29年9月29日	株式会社マネーパートナーズ	6010401075907	106-6233	東京都港区六本木３－２－１	03-4540-3800	BTC(ビットコイン)
	関東財務局長第00002号	平成29年9月29日	FTX Japan株式会社	7010401115356	101-0054	東京都千代田区神田錦町３－１７	03-6630-7554	BTC(ビットコイン)、ETH(イーサリアム)、BCH(ビットコインキャッシュ)、XRP(リップル)、BAT(ベーシックアテンショントークン)、LTC（ライトコイン）、FTT（エフティエックストークン）、SOL（ソラナ）、DOT（ポルカドット）、ENJ（エンジンコイン）、OMG（オーエムジーネットワーク）、DOGE（ドージコイン）、AVAX（アバランチ）、MKR（メイカー）
	関東財務局長第00003号	平成29年9月29日	株式会社bitFlyer	2011101068824	107-6233	東京都港区赤坂９－７－１	03-6447-5569	BTC(ビットコイン)、ETH(イーサリアム)、ETC(イーサリアムクラシック)、LTC(ライトコイン)、BCH(ビットコインキャッシュ)、MONA(モナコイン)、LSK(リスク)、XRP(リップル)、BAT(ベーシックアテンショントークン)、XEM(ネム)、XLM(ステラルーメン)、XTZ（テゾス）、DOT(ポルカドット)、LINK（チェーンリンク）、XYM（シンボル）、MATIC（ポリゴン）、MKR(メイカー)、ZPG（ジパングコイン）、FLR（フレア）、SHIB（シバイヌ）、PLT（パレットトークン）
	関東財務局長第00004号	平成29年9月29日	ビットバンク株式会社	1010801024625	141-0031	東京都品川区西五反田７－２０－９	03-6427-1520	BTC(ビットコイン)、ETH(イーサリアム)、XRP(リップル)、LTC(ライトコイン)、MONA(モナコイン)、BCC(ビットコインキャッシュ)、XLM(ステラルーメン)、QTUM（クアンタム）、BAT（ベーシック・アテンション・トークン）、OMG（オーエムジー）、XYM(シンボル)、LINK（チェーンリンク）、MKR（メイカー）、BOBA（ボバネットワーク）、ENJ（エンジンコイン）、MATIC（ポリゴン）、DOT（ポルカドット）、DOGE（ドージコイン）、ADA（カルダノ）、ASTR（アスター）、AVAX（アバランチ）、AXS（アクシーインフィニティ）、SAND（ザ・サンドボックス）、FLR（フレア）、GALA（ガラ）、CHZ（チリーズ）、APE（エイプコイン）、OAS（オアシス）
	関東財務局長第00006号	平成29年9月29日	GMOコイン株式会社	7011001113188	150-0043	東京都渋谷区道玄坂１－２－３	03-6221-0219	BTC(ビットコイン)、ETH(イーサリアム)、BCH(ビットコインキャッシュ)、LTC(ライトコイン)、XRP(リップル)、XEM(ネム)、XLM(ステラルーメン)、BAT(ベーシックアテンショントークン)、OMG（オーエムジー）、XTZ（テゾス）QTUM（クアンタム）、ENJ(エンジンコイン)、DOT(ポルカドット)、ATOM（コスモス）、XYM（シンボル）、MONA（モナコイン）、ADA（カルダノ）、MKR（メイカー）、DAI（ダイ）、LINK（チェーンリンク）、FCR（エフシーリュウキュウコイン）、DOGE（ドージコイン）、SOL（ソラナ）、FLR（フレア）、ASTR（アスター）
								BTC(ビットコイン)、ETH(イーサリアム)、XRP(リップル)、LTC(ライトコイン)、MONA(モナコイン)、BCH(ビットコインキャッシュ)、HT(フォビトークン)、XEM(ネム)、XLM(ステラルーメ

https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf

バーチャルな価値とはなにか？

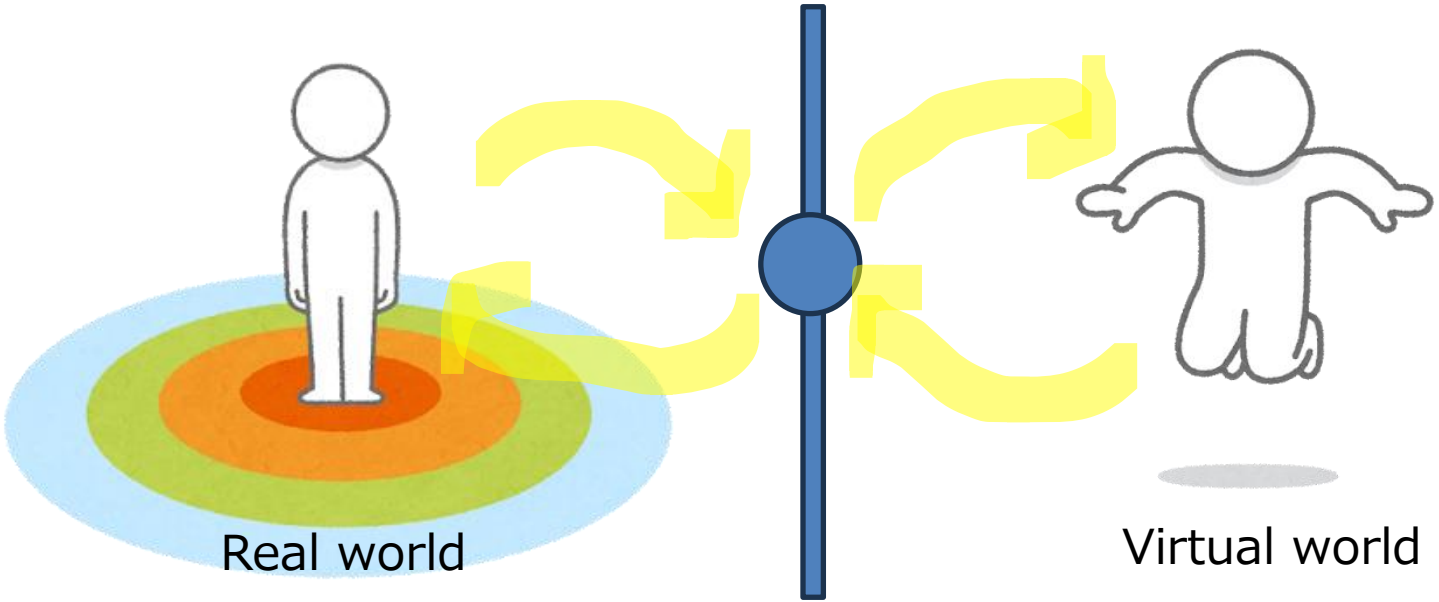
- 向こうで幸せか？優位に立てるか？
- 現実世界のFiat（法定通貨）に簡単に戻せるか？

- 関連：クラウドファンディング，DAO
- 貢献した感があればよいのか？（地域通貨）

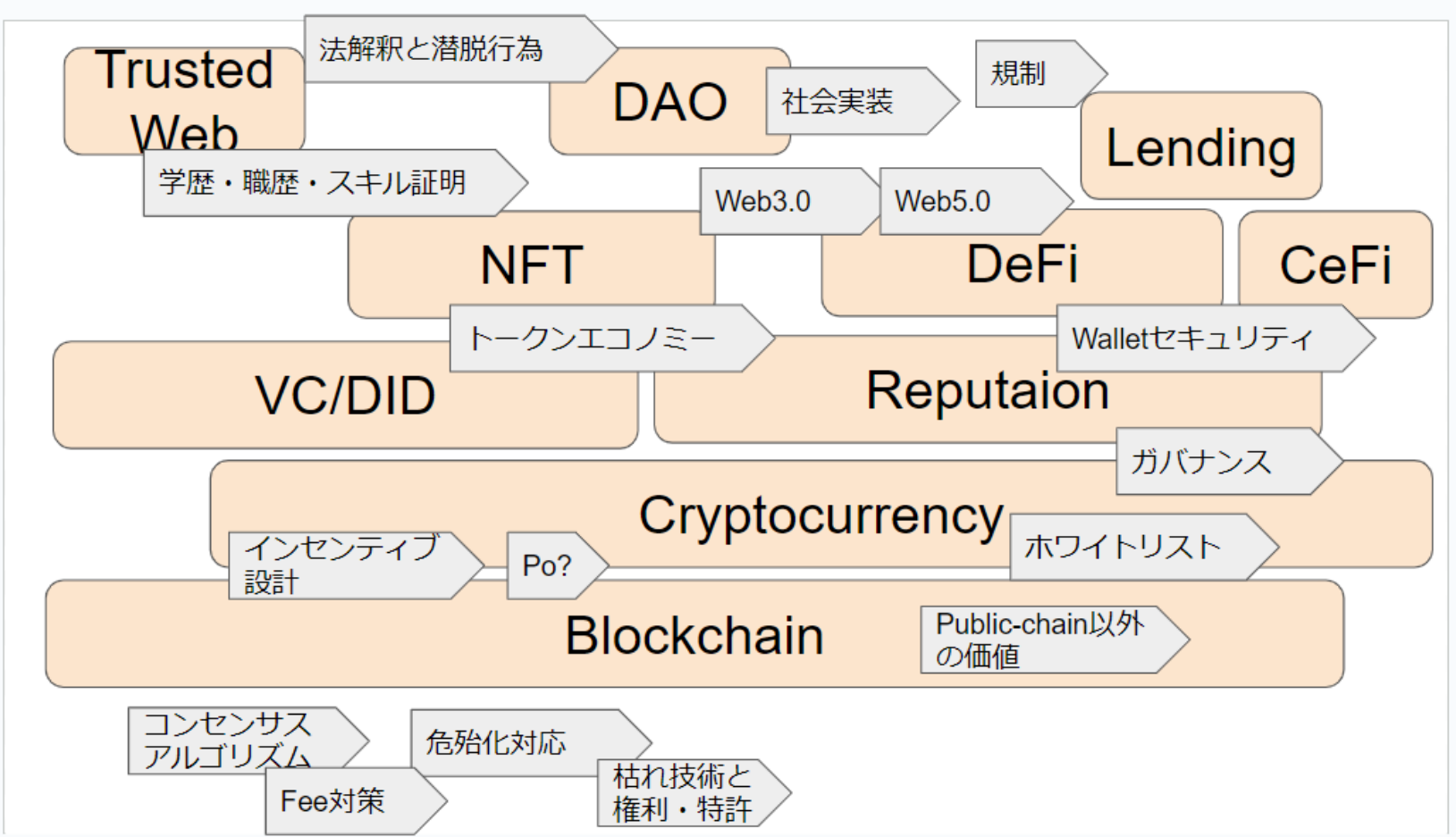
RMTなど接地点としての考え方

- 欲しいと思う人々のこころ
- 投機としての見方（NFT,各種トークン，アーリーアダプタ：ブロックチェーンゲーム）

RMT: Real Money Trading



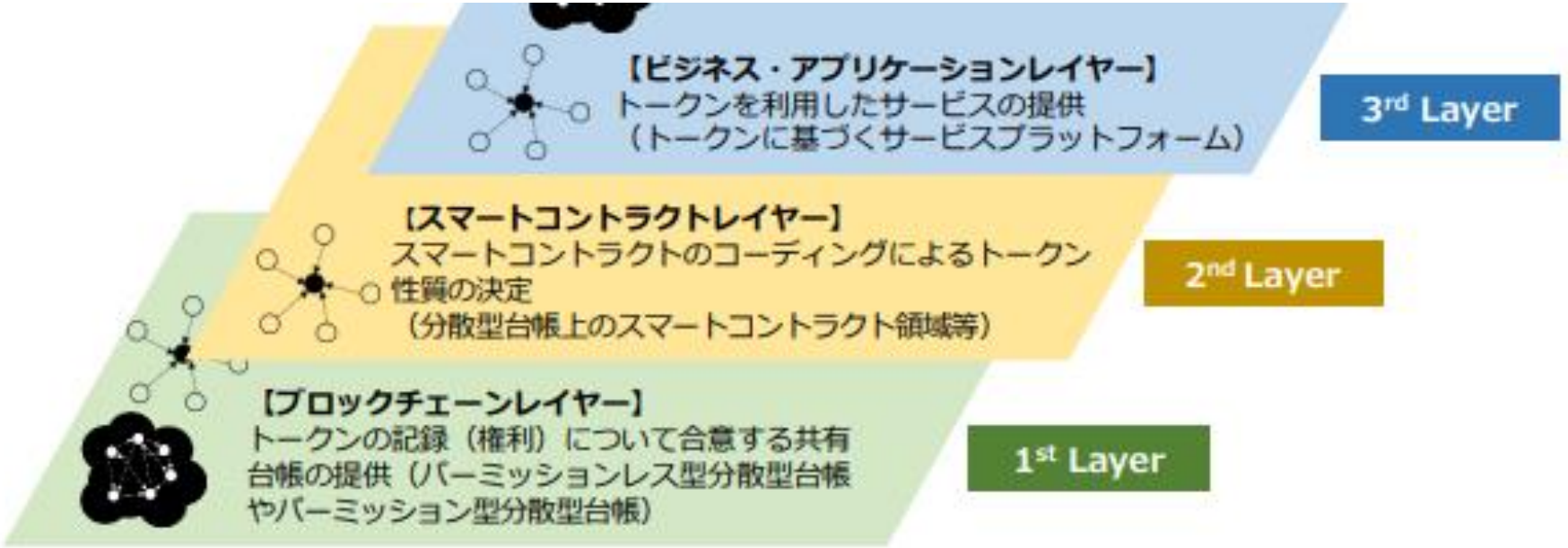
ブロックチェーンをベースとした各種技術



サービスのレイヤー構造

https://www.fsa.go.jp/singi/digital/siryou/20211006/jimukyoku1.pdf

- 暗号資産に関わる人達も概ねこの解釈で議論

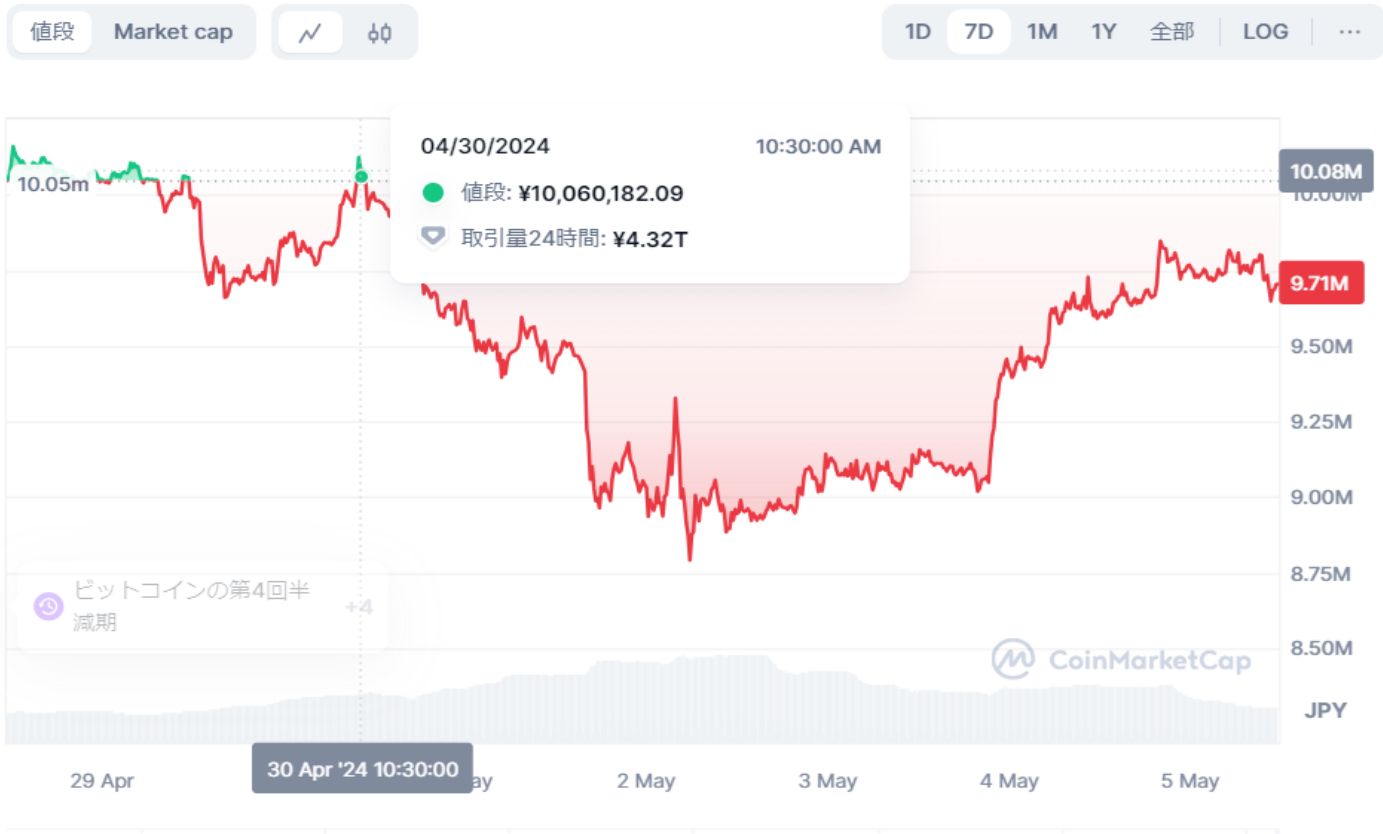


ひとつ前の4半期はいろいろ起こりすぎ

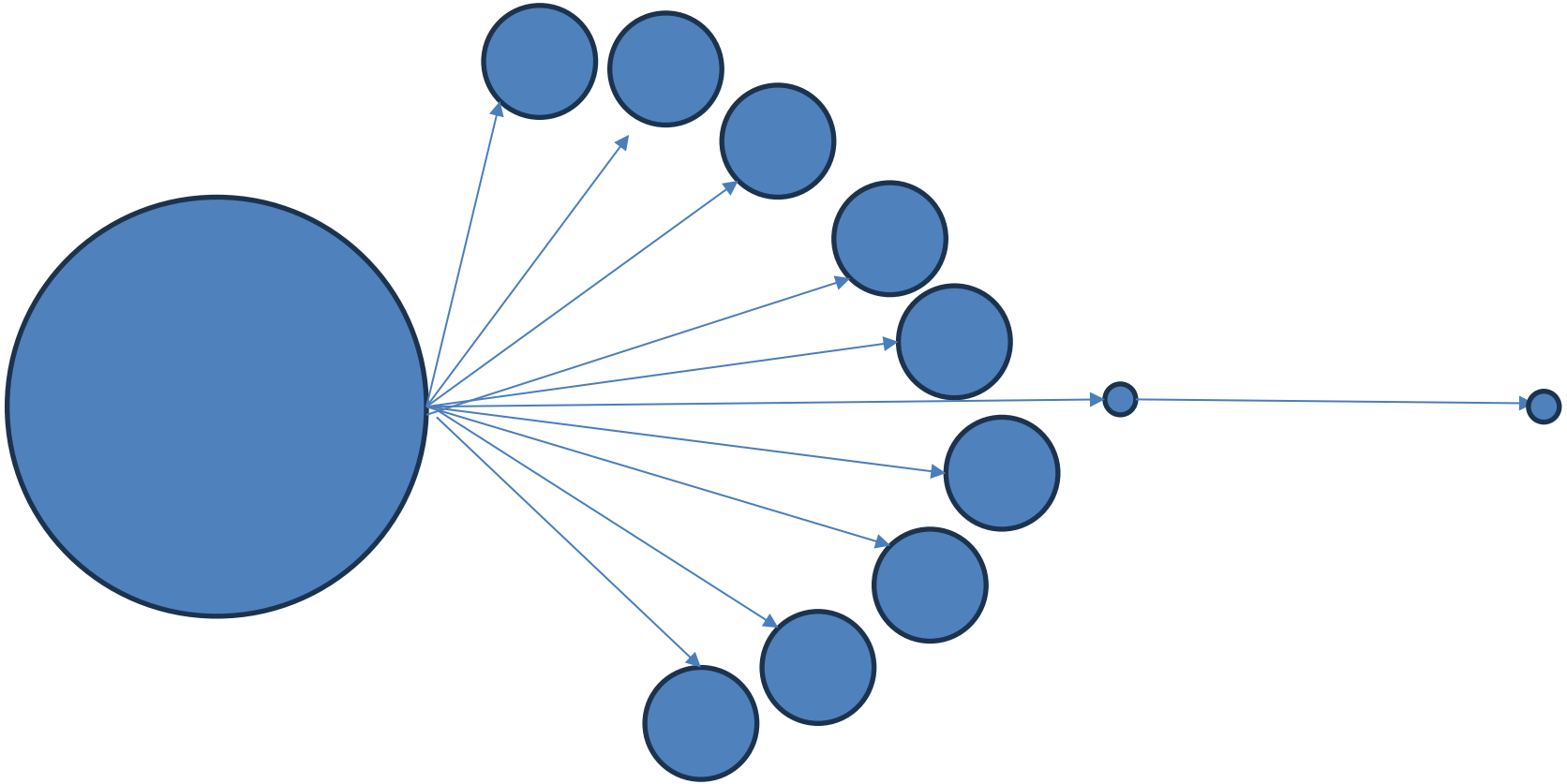
- ビットコイン半減期
- ビットコイン1000万円超える
- A社 483億円流出
- B社 行政処分
- C社がD社を買収

BTC-JPY

https://coinmarketcap.com/ja/currencies/bitcoin/

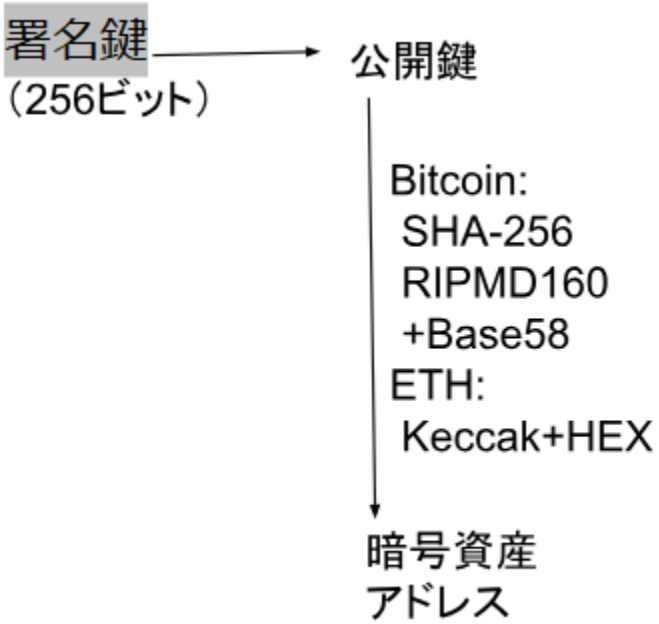


流出アドレス（4502.9BTC）



ざっくりとした暗号資産アドレスの説明

- ECDSA鍵生成→ハッシュ→エンコーディング

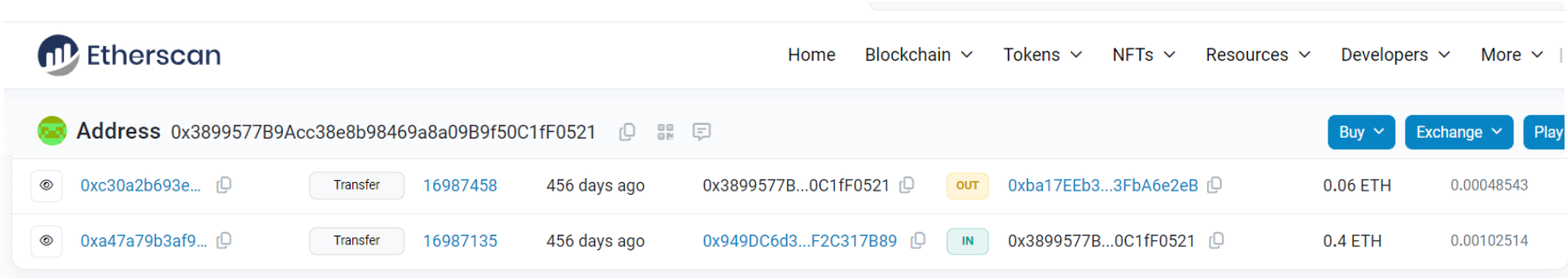


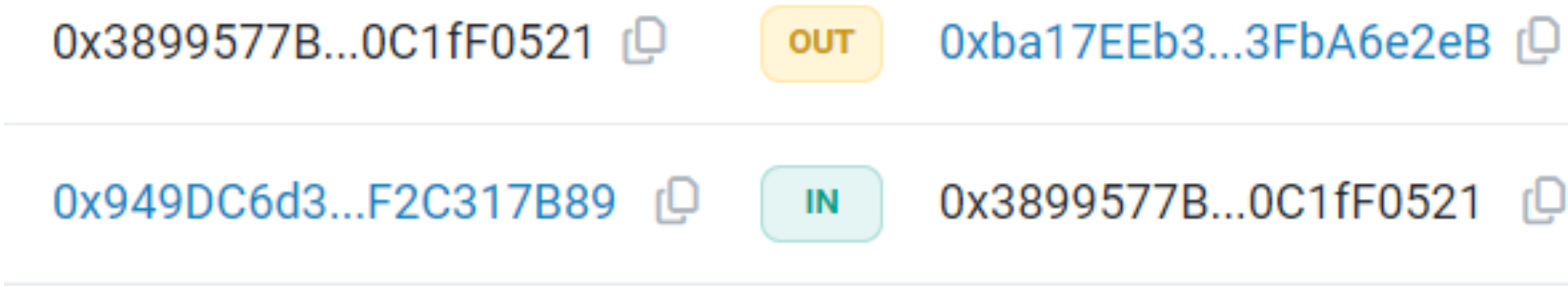
実際の流出アドレスと言われている実例

https://www.blockchain.com/explorer/addresses/btc/1B6rJRfjTXwEy36SCs5zofGMmdv2kdZw7P

https://www.blockchain.com/explorer/addresses/btc/1B6rJ6ZKfZmkqMyBGe5KR27oWkEbQdNM7P

アドレスポイズニングの可能性





今回の件，ポイズンなアドレス生成には2^37*SHA-256くらいの計算量でいけますよって誰も言ってないな・・・
(2^35から修正)

Vanity address

- ユーザの好きな文字が入るように
  計算機ぶん回してアドレスを大量発生させる

今回の事例

- Base58でエンコーディングされているので
  1文字が58通り．頭の1はシングルシグネチャ
  を表現しているので外して
- 今回合致している6文字を考えると
  log2(58^6)=35.15

- 鍵生成はコストゼロとみなして，アドレス生成にはハッシュ4回分かかるから
- 単純計算で2^37 *SHA-256くらいになる

暗号資産アドレスの要件

- 誰でも作成可能（分散型）
  ＝だれかが振り出してくれるわけではない
  （逆の中央集権型：番号はAuthorityが割り当てる）
- 振り込んだ人は言い逃れできないようにしないといけない
- そのアドレスに振り込まれたらその人が使えるようにならないといけない

暗号資産アドレスの要件

- 誰でも作成可能（分散型） ← アドレスは公開鍵にすればよい

でも実際にはアドレス＝公開鍵ではない

bitcoinでの生成方法

(手順1) 公開鍵を2回別のアルゴリズムでハッシュする

(手順2) チェックサムを付加するサブルーチンを呼ぶ

最終的には Base58エンコーディングされたデータを得る（これがbitcoinアドレス）

- 誰でも作成可能（分散型） ← アドレスは公開鍵にすればよい
- 振り込んだ人は言い逃れできないようにしないといけない← 署名作成することそのものの役割
- そのアドレスに振り込まれたらその人が使えるようにならないといけない
  ←「その人が使える」ということは「その人」がさらに署名を行うことを意味する

暗号資産交換業が狙われる理由

- 攻撃が容易．マルウエア仕込んで盗む方が現金強盗よりもはるかにラク

- 外貨を稼ぐ事例
- 手口としては個人にも拡がっている（はず）
  よくある事例はDMにURL貼ってコミュニケーションツールダウンロードさせて仕込む

ウォレットに関する一般的な解釈

- ブロックチェーン上の暗号資産の管理を行うためのインターフェイス
- 暗号資産の管理（操作）には署名鍵が必須
- 署名鍵の管理方法でいくつかに分類可能
- カストディアン（取引所）もある意味ウォレットであるという解釈もある

「一般ピープルに鍵管理などできひん」
という業者さんもいます（関連：Nostr）

ウォレットの種類（いち分類方法）

- [ホットウォレット]
  -[カストディアルウォレット] 業者管理
  -[アンホステッドウォレット] 個人管理
- [コールドウォレット]
  ネットに接続されていない

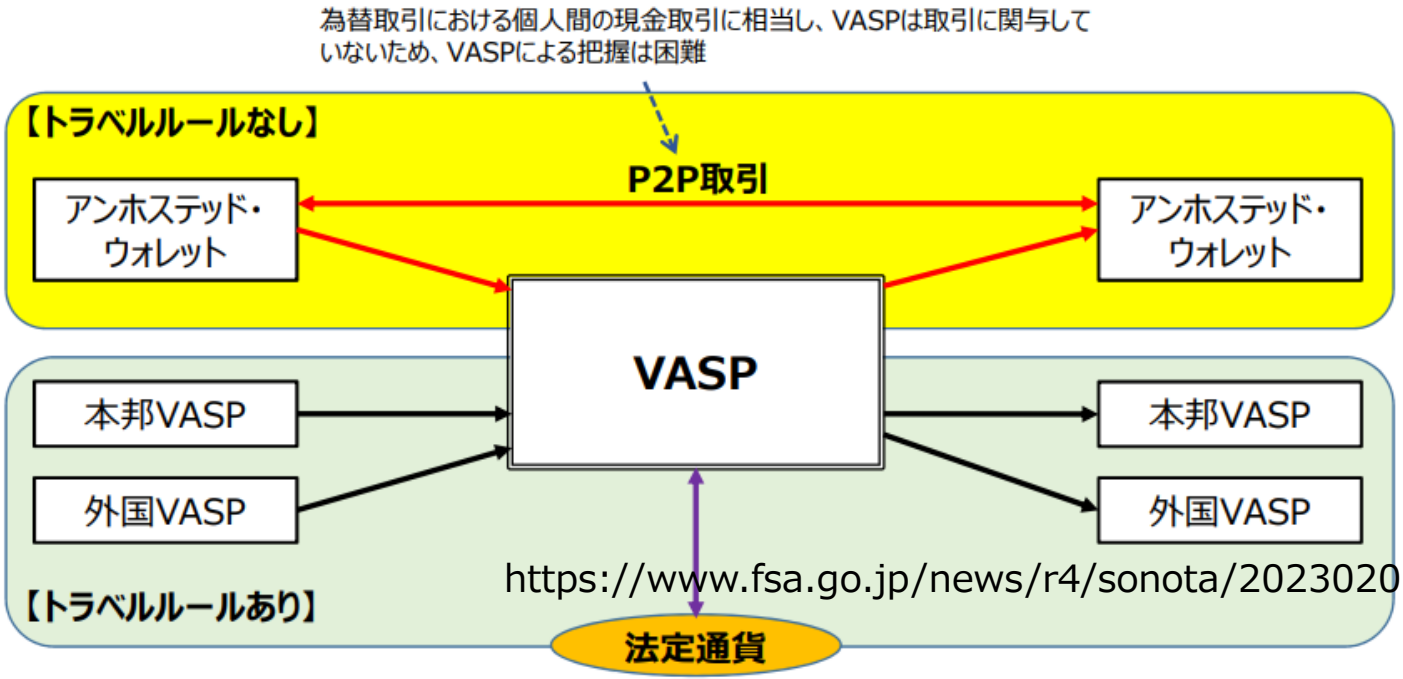
※ ハードウェアウォレット，ペーパーウォレットをどこに分類するかはひとに依る

https://blog.blockchain.bitflyer.com/n/n2cf743fb4d40

アンホステッド・ウォレットについて

- 暗号資産・電子決済手段は、利用者が自ら管理するウォレットである「**アンホステッド・ウォレット**※」に対して移転することが可能であり、当該ウォレットを用いた**P2P取引**が可能。
- アンホステッド・ウォレットとの取引は、その匿名性や管理者による移転制限の欠如によるリスクが存在するところ、**FATF等においても対応の必要性が指摘されており、我が国においても対応を検討**。

※ アンホステッド・ウォレットとは、事業者がホスト（管理）していないウォレット（口座）を意味する。



https://www.fsa.go.jp/news/r4/sonota/20230203-2/00.pdf

FTXの崩壊がアンホステッウォレットにシフトした理由として用いられることも

- 2022年11月に破産を申請
- 投資家や顧客を欺いたとして詐欺罪で有罪判決を受ける
- 流動性の不足と資金の管理不行き届き

【論点】自己責任論でよいのか

- Twitterでウォレット名をつぶやくと
  フィッシングサイトに誘導するレスポンスが
  つくようになってる
  特にサポートの中の人を装って近づいてくるケース.
  日本人での被害報告もある.
- Twitterアカウントが実在業者を謳って存在する
  ケースでは誘導サイトに難読化された
  JavaScriptコードが降ってくる事例も

2023年4月の攻撃

- Walletの脆弱性を突いた（乱数生成のバイアスを狙ったもの？）知られていない攻撃多発
- 当初はパスワード管理サイトのハッキングと連動しているのでは？という憶測も
- いま個人的に気にしてるのは自動バックアップ機能でニーモニックコードが抜かれているのではないか説

「署名鍵」を誰も知らないアドレスが掲載されている一般向け解説記事から

ビットコインアドレスから公開鍵（秘密鍵）を知るすべはないので、極端な例としては秘密鍵なしでもビットコインアドレスを作成できます。例えば次のようなビットコインアドレスも有効です。

1BitCoinDescriptionAddressadTvGDH

このビットコインアドレスにビットコインを送付することはできますが、誰もこのビットコインアドレスの秘密鍵を持っていないので二度と取り出せません。

ID: 068c-7f4d 4/17/2023, 11:21:45	From 7 Inputs To 198 Outputs	0.00190000 BTC • $116.04 Fee 35.8K Sats • $21.86
ID: 242c-5dcc 12/20/2022, 15:56:29	From bc1q-vzej To 2 Outputs	0.01000000 BTC • $610.74 Fee 40.0K Sats • $24.43
ID: 5b2f-ce34 1/25/2022, 07:27:25	From bc1q-vzej To 3 Outputs	0.00100000 BTC • $61.07 Fee 40.0K Sats • $24.43
ID: dcb4-a72f 6/07/2021, 00:07:20	From 3Gqi-j4Cf To 2 Outputs	0.00053800 BTC • $32.86 Fee 521 Sats • $0.32
ID: 2cad-51e5 3/22/2021, 08:37:27	From 36WS-xUfu To 2 Outputs	0.00443200 BTC • $270.68 Fee 9.6K Sats • $5.88
ID: e7dd-77d3 2/09/2021, 17:54:55	From bc1q-vzej To 7 Outputs	0.02756100 BTC • $1,683.27 Fee 42.5K Sats • $25.94
ID: 96c0-5c43 12/14/2020, 14:59:11	From bc1q-hrvs To 3 Outputs	0.00002285 BTC • $1.40 Fee 53.1K Sats • $32.44

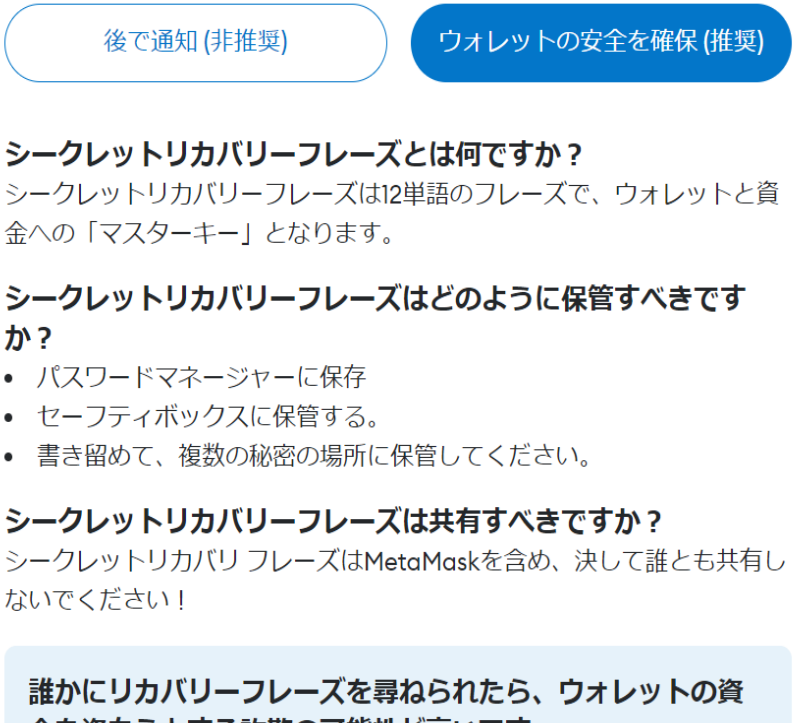
誰でも検索すれば分かる

「デジタル埋蔵金」の存在

- Bitcoin 署名鍵 256ビットをぶち当てたら0.15BTCが懐に入るってこと
- 150万円ゲットできるという意味

これ難しいんじゃないの？

- 256ビットをぶち当てるのは正攻法では無理
- ただし気になることがある→
  （あるソフトウエアウォレットの実装）



BIP-0039

https://github.com/bitcoin/bips/tree/master/bip-0039

- 2048個の辞書から12個のフレーズ
- 鍵生成時にフレーズを書き留めておく運用

1	abandon	9	absurd		2041	yellow
2	ability	10	abuse		2042	you
3	able	11	access		2043	young
4	about	12	accident		2044	youth
5	above	13	account		2045	zebra
6	absent	14	accuse	...	2046	zero
7	absorb	15	achieve		2047	zone
8	abstract	16	acid		2048	zoo

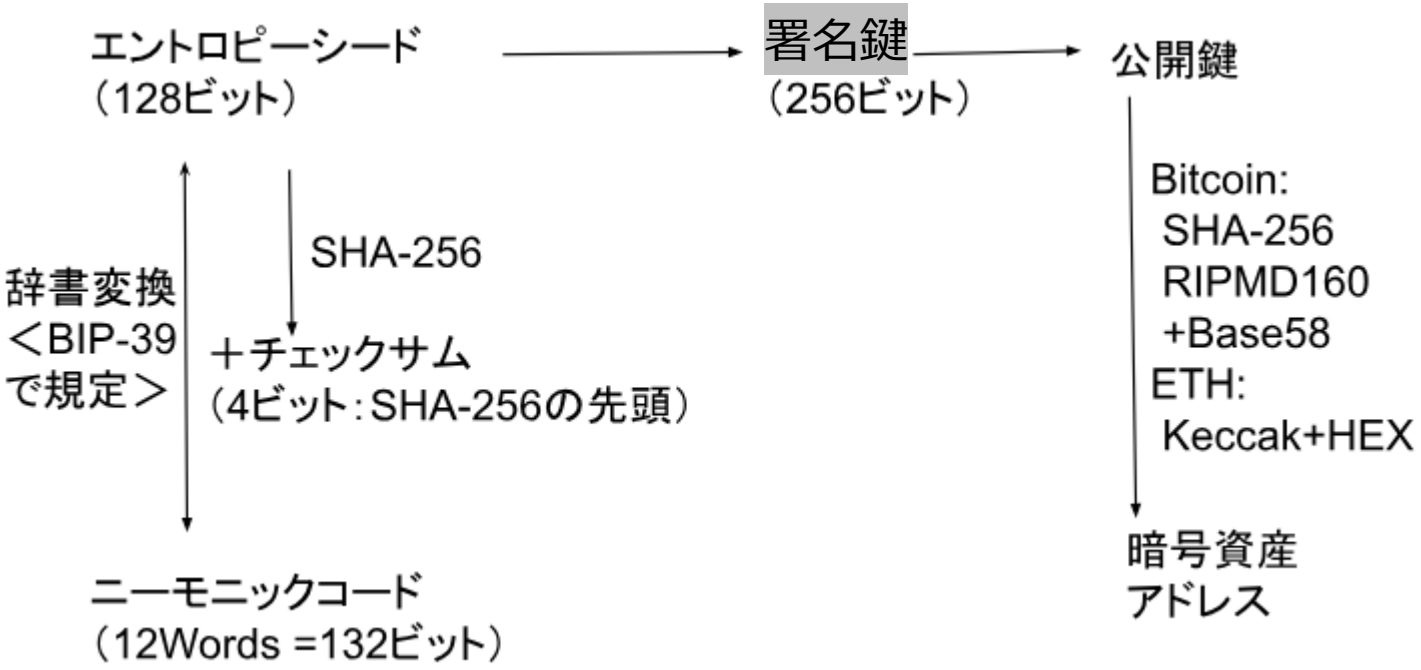
- これがあれば署名鍵のリカバリ可能

ニーモニックコードの鍵空間

- 2048=2^11
- それが12個なので 2^132

実は132ビットのうち4ビットは

https://en.bitcoin.it/wiki/BIP_0039



256ビット鍵のシードが128ビット

- これは完全に“CRYPTO FAIL“
- 利便性を優先させたがために起こった悲劇

- Wallet選択は素人では難しいねという事例
- では，ハードウエアウォレットを活用すればよいのかい？

自己防衛策の一例

- **ハードウエアウォレットの活用**

  鍵生成が確かで（鍵空間，十分なエントロピーを持つ乱数生成器を持つ），かつ署名鍵が取り出せなくて，事業継続性が確かで，ファームのアップデートはなく，他のウォレットと接続可能で，インターフェイスが素晴らしく，トランザクション以外の署名が行えないようになっている製品があれば・・・

- **bitcoinのマルチシグネチャアドレス（秘密分散）**

  ETHでもスマートコントラクトを活用してマルチシグネチャと同様のソリューションあり

自己防衛策の一例

- ハードウエアウォレットの活用
- bitcoinのマルチシグネチャアドレス（秘密分散）
  ETHでもスマートコントラクトを活用してマルチシグネチャと同様のソリューションあり
- MPC wallet, Smart contract wallet, Web3 wallet等のバズワードも登場.
  一般ユーザには よりわかりにくい状況に.

【私見】
CRYPTRECとして何ができるか

- 鍵管理ガイドラインの浸透（考え方だけでも）

【私見】

CRYPTRECとして何ができるか

- 鍵管理ガイドラインの浸透（考え方だけでも）
- とくにライフサイクルの考え方は参考になる
- 面白いのは鍵を捨てるという概念が微妙
  （閉鎖した暗号資産アドレスに入れてくる
  輩は必ず出る）

【私見】

CRYPTRECとして何ができるか

- 鍵管理ガイドラインの浸透（考え方だけでも）
- FIPS140, (J)CMVP等のこれまでの制度をウォレットにも推奨するか（コスト問題）
- 製品の○×表の作成は難しいだろう
- CRYPTREC暗号リストに掲載されていないアルゴリズムを使った暗号資産の存在に対してどうするか？

【私見】

CRYPTRECとして何ができるか

- 鍵管理ガイドラインの浸透（考え方だけでも）
- FIPS140, (J)CMVP等のこれまでの制度を
  ウォレットにも推奨するか（コスト問題）
- 製品の○×表の作成は難しいだろう
- EUDI Walletの議論も参考になりそう
  ＝Walletのお墨付き制度の導入
  ※難しいのは技術中立性の確保

ガバナンスの観点からの指摘

- 交換業はNFTやDeFiを使わせるようにシフトしている傾向が見られる
  ＝アンホステッドウォレットを使わせる方向性
- Layer1で儲からないから利用を勧めている？
- 自己責任論の再考が必要
- 例えば認定自主規制団体が対応するなど
  （一応過度な広告に関する対策はやっている）

トータルなサポートの必要性

- **7つの視点**

アクセス制御
アドレスポリシー

インシデント対応

社員教育
内部不正対策

鍵管理

リスク管理
SBOM・外部監査

横連携強化
ISAC

法令遵守

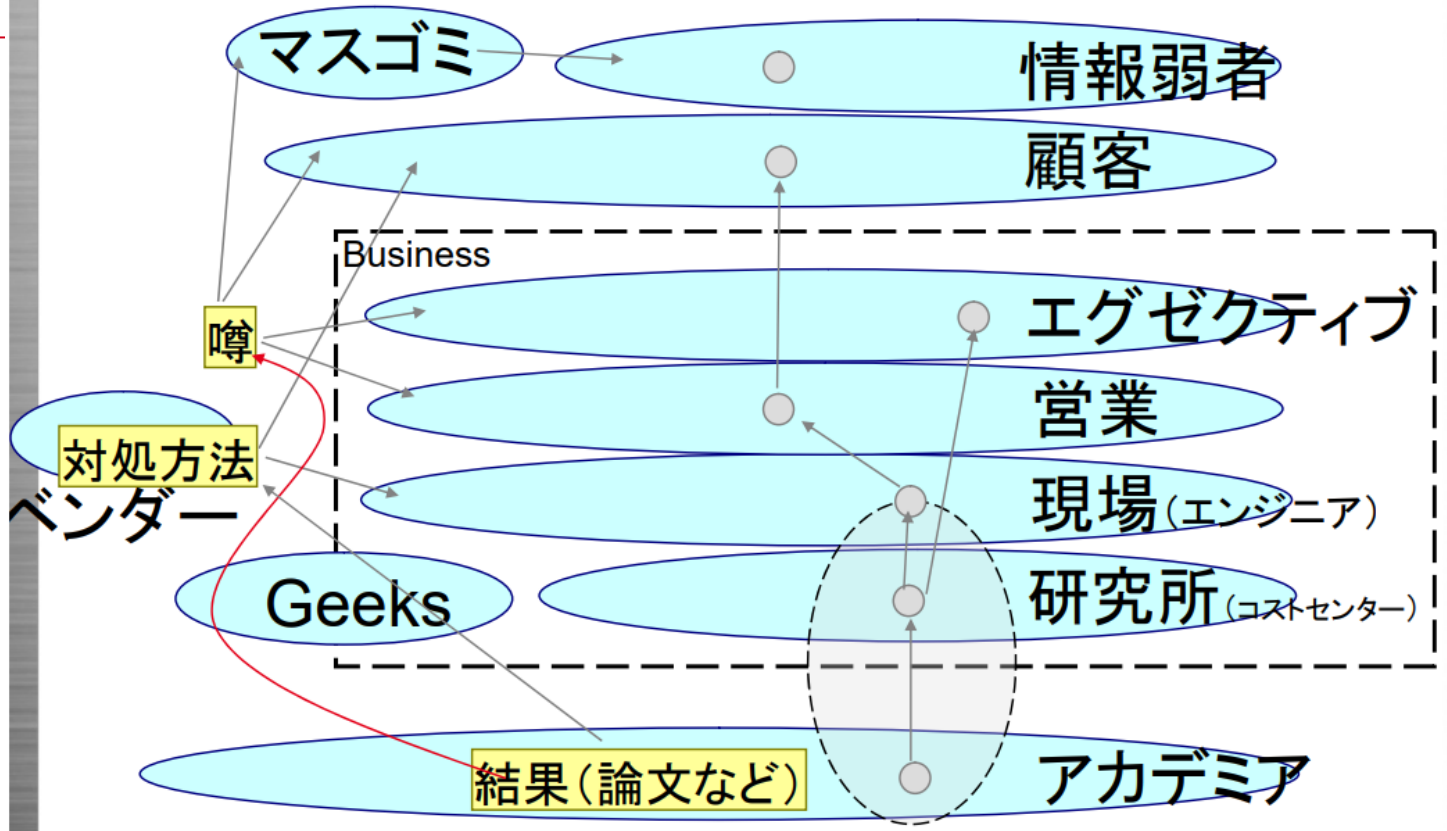
今回皆様に考えて頂きたいこと

- 自分得意レイヤじゃないから考えない・放っておく・自分ごとと思わない

じゃなくて

- カバレッジ大切：レイヤごとにそれぞれやってもいるだけでは対策としてヌケモレは必ず起こってしまう
- トータル・総合的に考えるくせをつけることが大切

「技術翻訳者」連携の必要性



2012年3月総合大会「セキュリティプロトコル仕様の脆弱性事例と世代交代困難性」

【Prediction】

- ウォレット中心の世界が刻々と来てる（DID/VCの話やmdocの話もそう）
- マイナンバーカードがECDSAにシフトしたタイミングで，デジ庁アプリ（スーパーアプリ）と接続して暗号資産ウォレットとして使う事例は出そう（実際今もあったりする）

Ongoing Innovation

IIJ Internet Initiative Japan

Stay safe and healthy