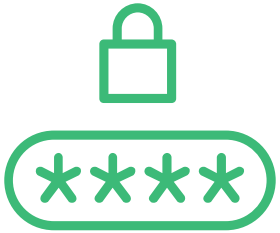


ブロックチェーンの安全性とセキュリティ

Consensus Base

コンセンサス・ベイス株式会社

代表取締役社長　志茂博

自己紹介

Consensus Base

志茂　博　Shimo Hiroshi

コンセンサス・ベイス株式会社　代表取締役社長

アメリカの大学にてコンピュータ・サイエンスを専攻。CTC、インターネットイニシアティブ、フリーランスのエンジニアを経て、Webサービス会社を起業。
現在、ブロックチェーン技術専門企業である「コンセンサス・ベイス」を起業し、代表を務める。

個人のブロックチェーンにおける活動

- 経済産業省「ブロックチェーン検討会」委員
- 暗号通貨技術ユーザ会：Cryptocurrency Tech Japan 代表

メディア掲載

- 週刊ダイヤモンド「FinTechの正体」に掲載
- 日経CNBCのテレビ番組「ザ・金融闘論～仮想通貨 最前線～システム進化の光と影～」に出演

実績（15案件以上）

Consensus Base

会　社

コンサルティング・開発

大手通信会社様（ビットコイン関連サービス）
ソフトバンク様（国際募金プラットフォーム）
大和証券グループ様（ミャンマー資本市場）
大手メーカー様（コンサルティング）
某システム会社様（金融系サービス）
スタートアップ数社（販売所、取引所など）　その他、多数

教育

セブン銀行様（社内勉強会）
IIJ様（技術ワークショップ）

個人の実績

NRI様：証券分野の実証実験
某メーカー：スタンプ関連の実証実験
みずほFG様+ISID様+日本マイクロソフト様：シンジケートローンの実証実験
NRI様+JPX（日本取引所グループ）様：証券の実証実験　その他、多数

Consensus Base

本日のプレゼンテーション

ブロックチェーン全般の
セキュリティ（主にパブリック）の概要

パブリックとプライベートは、ほぼ別物

- プライベート　→　ほぼ従来通りのセキュリティ対策
- パブリック　　→　従来とは違うセキュリティ対策

ブロックチェーンの新しいセキュリティの形

- 新しい実装と新しい攻撃手法（分散型合意やフォーク）
- ガバナンスや経済合理性というセキュリティ
  → 従来のセキュリティの考え方や人材では難しいのでは？

結論：今までの経験からの私見

Consensus Base

セキュアでない？使える場所で使うという発想

既存の要件を満たさない、ではなく利用できるところで使う

セキュリティの話しは、かなり先

それ以前にやるべきことが沢山ある

教育のための情報と人材の育成

まだブロックチェーンを正しく理解するという段階ガバナンスや経済合理性に関する知見を持つ人も必要

Consensus Base

セキュリティって？

セキュリティとは？

Consensus Base

情報セキュリティの三大要件（ＣＩＡ）

正当な権利を持った人のみ利用できる
（情報漏えい、アクセス権）

正当な権利を持たない人に
変更されてない（改ざん防止、検出）

必要な時に利用できる
（二重化など）

ブロックチェーンは、２と3が強く、１が弱い？

セキュリティとは？

Consensus Base

情報セキュリティのその他四要件

4. 真正性
Authenticity

ある主体又は資源が、
主張通りであることを確実に
する特性利用者、プロセス、
システム、情報などのエンティ
ティに対して適用する

5. 責任追跡性
Accountability

あるエンティティの動作が、
その動作から動作主の
エンティティまで一意に追跡
できることを確実にする特性

6. 否認防止
Non-repudiation

ある活動又は事象が
起きたことを、
後になって否認されない
ように証明する能力

7. 信頼性
Reliability

意図した動作および
結果に一致する特性

設計、実装による？

Consensus Base

ブロックチェーン特有のセキュリティ

セキュリティのレイヤー例

Consensus Base

セキュリティ・レベル	
ガバナンス	ブロックサイズ、ハードフォーク
ネットワーク	51%攻撃など
分散組織	分散組織運営
プログラミング	スクリプト、コントラクト
アカウント	秘密鍵の管理
トランザクション	検証されているか？

http://startupmanagement.org/2016/08/08/blockchain-security-is-multi-layered-here-are-the-6-most-important-levels/

ガバナンスと経済性

Consensus Base

- **ガバナンスと経済合理性が、安全性を決める**
- **ネットワークやソフトウェアのガバナンス**
  - ・安全なソフトウェアか？
  - ・方針を誰がどう決める？（ハードフォークと自分のコインの価値）
- **インセンティブ設計**
  - ・報酬設計：マイナー集中やハッシュパワーに影響（PoW）
  - ・経済合理性：自分のコインの価値を下げたくないから攻撃しない？
  - ・シェアの設計　：密かにシェアが多いと攻撃される（PoS）

1．パブリック、コンソーシアム、プライベートの違い

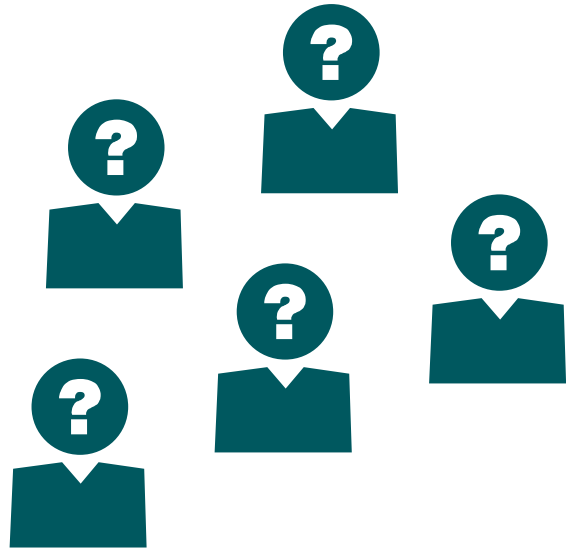
2．コンセンサス・アルゴリズムによる違い

3．ノードの管理方法

設計の仕方が、非常に重要

パブリック

- 誰かわからない人からの攻撃（シビル攻撃）
- 不安定なネットワーク
- 確率的なことが多い
  ⇒ ファイナリティ、秘密鍵の衝突
- 鍵の管理など、自己管理・自己責任



プライベート／コンソーシアム

- お互いに知っている主体間のネットワーク
  ⇒ 攻撃者が少ない、特定可能
- ネットワークの安定性をコントロール可能
- フォークせず、ファイナリティのある形を作れる
- 鍵の管理も、管理者でコントロール可能 （より良いUX）

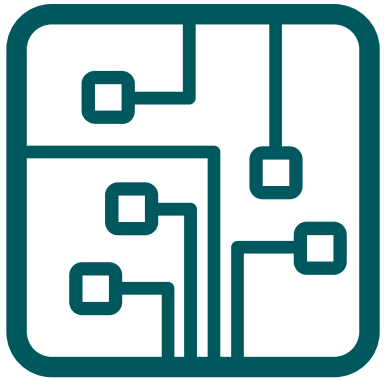
2．コンセンサス・アルゴリズムの安全性

Consensus Base

Proof of Work

51%攻撃

ASICによる中央集権化



Proof of Stake

Nothing at Stake： 復数のフォークで同時にブロック承認できる

Stake Grinding： 過去に遡って過半数を取得できるブロックがあれば、それ以降のブロックを全て改ざんできる

低コスト51%攻撃： コインの51%を買える資金の証明をし、買うと公表しコインの価格を下げて、コインを購入する

どのアルゴリズムが安全と言える？

Consensus Base

アルゴリズム名	
Proof of Importance	アカウントの重要性にもとづく
DPOS	代理投票
Ripple Consensus	信頼できるノードリストを利用
Stellar Consensus Protocol	ノードのグループによる分散合意
Tendermint	デポジット式のPoS
PBFT	従来型コンセンサス・アルゴリズム

ファイナリティ問題

ビットコインでは、ブロックが承認されるまでに10分～60分などかかる
時間の長短はそのときのブロックマイニングの状況、フォーク（同時に2つ以上のブロックチェーンが生じること）の有無に左右される

対　策

- コンセンサスアルゴリズムの改変・高性能化
- スーパーノードの導入

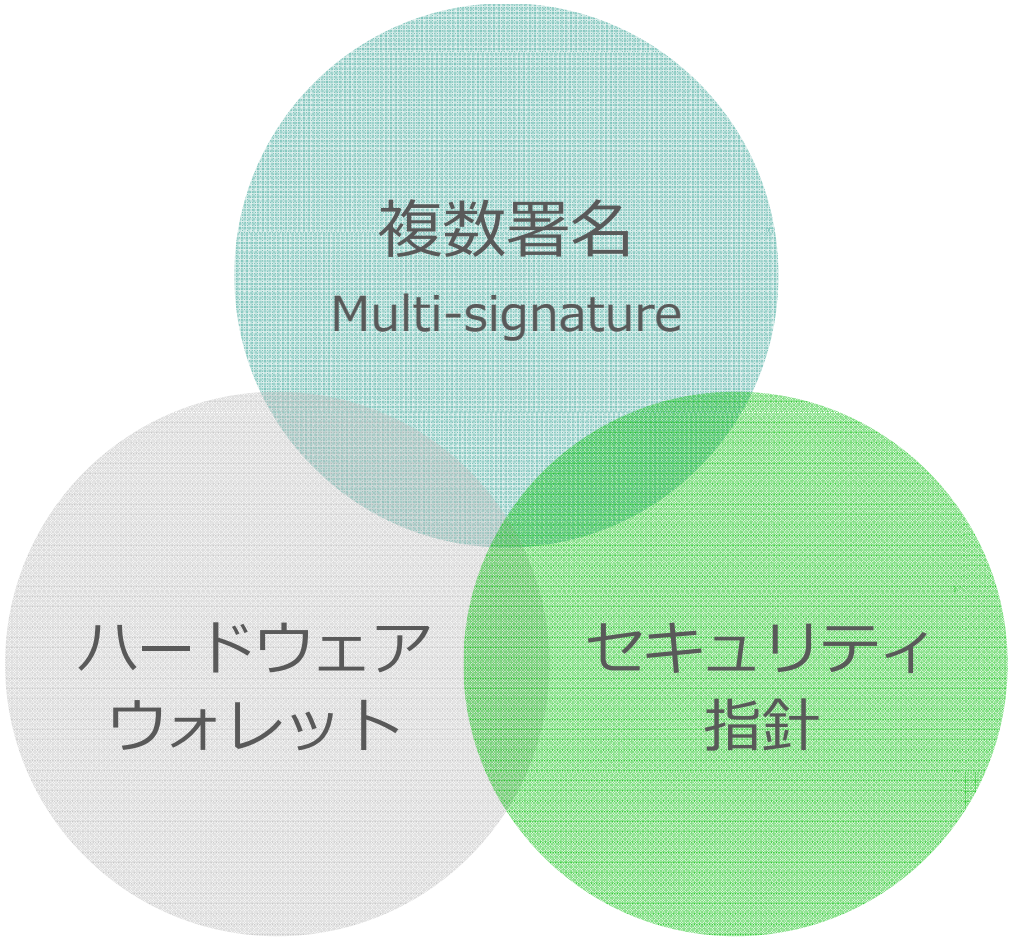
ノードの数　⇒ 可用性と、機密保持の範囲

ノード管理者 ⇒ 信頼の範囲、機密保持の範囲

秘密鍵の保管場所と管理方法

秘密鍵の管理に関する安全性

Consensus Base



vs. **利便性**

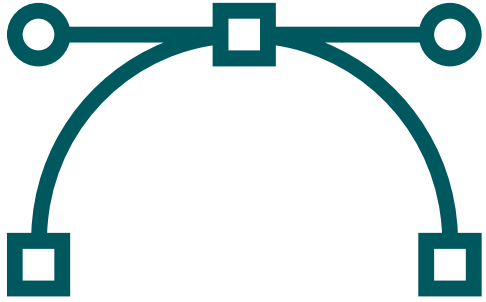
Consensus Base

ネットワークのセキュリティ

ノード発見に関する安全性

初期ノードの発見方法

- クライアントソフトウェアに直書き
- DNSに問い合わせ
  ⇒ DNSSECを利用していない?
- 前回アクセスしたリストを利用



エクリプス攻撃

- P2Pネットワークの分断攻撃
- ネットワークAとネットワークBがあったとき、双方のネットワークを繋ぐ悪意のあるノードが、A側から来た通信データを書き換えてB側に送り、B側から来たデータを書き換えてA側に送る、またはデータを送らないという攻撃。
- ビットコインのネットワークの場合、ブロックチェーンが分岐し、別々のブロックチェーンになる。

対　策

双方のネットワークのノードに届くようにデータを送信する。

経路の安全性

Consensus Base

今までとさほど変わらず

ＳＳＨ

ＶＰＮ

専用線

その他：フルメッシュにするのか？

フォークが起こす問題

Consensus Base

ファイナリティ

データが確定しない

２重支払い

商品を盗まれる

Consensus Base

ソフトウェアの安全性

コントラクト（チェーンコード）の安全性

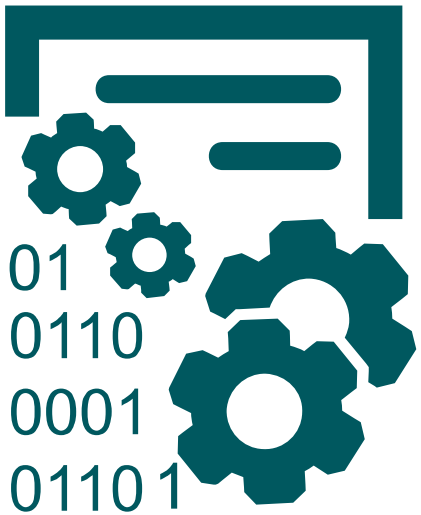
レビュー、段階的リリースなど

ブロックチェーン・ソフトウェアの安全性

- クライアント・ソフトウェアの安全性（検証）
- Gitian（複数人でバイナリを作ってサインする）

- **鍵の再生成**
- **乱数生成（衝突）**
- **ハッシュ関数（ダブルハッシュ）**

の問題



今後の安全性の展望と動き

Consensus Base

アカデミックな動き

BSafe.network

MITのDr.WongとDr.Matsuoが立ち上げた、ブロックチェーン研究期間のネットワーク

Enigma

- MITが立ち上げ分散型クラウドコンピューティングプロジェクト
- 制限付き完全準同型暗号を用いて、プライバシーを保ちつつ、かつスケーラブルなクラウドコンピューティンの実装を目指している

ブロックチェーンのご相談はお気軽に

Consensus Base

コンセンサス・ベイス株式会社

代表取締役社長　志茂博

support@consensus-base.com