分散台帳技術における
インテグリティとプライバシー保護に関する考察

2018年2月7日

日本アイ・ビー・エム株式会社　東京基礎研究所
吉濱佐知子

Sachiko Yoshihama
IBM Research – Tokyo

※本資料の内容は個人の見解であり、所属企業の見解を代表するものではありません。

分散台帳技術にまつわる疑問

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術は色々あるが、どうやって比較すればいいのか？
  - パフォーマンス？ 安全性？

- 例えばパフォーマンスを比較する場合
  - 「秒間～～件の処理が可能」といっても、ノード数や処理の複雑さ、各種構成パラメーター、によって大きく異なってしまう
  - 条件を揃えるため、様々なユースケースにおける「ベンチマーク」を作成し、様々な基盤を同じ条件で比較するのが一般的。

- 分散台帳技術の安全性の意味は？
  - 「安全」ってどういう意味？
  - 「プライバシーが守れる」ってどういう意味？

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類と役割を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

分散台帳技術の種類を、基本機能の観点から整理する

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 参加者タイプ
- データ構造
- トランザクション処理方式
- コンセンサス

参加形態：Public vs. Permissioned

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

Public Network

誰でもネットワークに参加可能

bitcoin

- 政府により規制されない、転々流通可能な仮想通貨を、中央集権的管理主体なしに実現

Permissioned Network

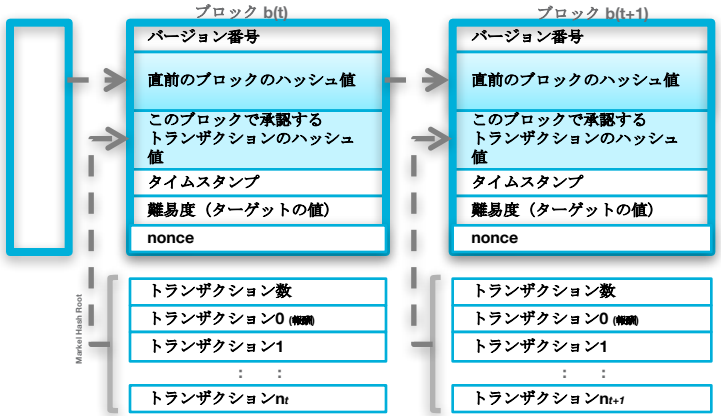
参加許可制

- 業界コンソーシアムなどのビジネスネットワークの中で、組織をまたがる業務に適用
- 高いセキュリティや信頼性への要件
- 分散DB・コンピューティングの技術を取り入れ、業務システムとして受け入れやすい形に変化。

データ構造

ブロック

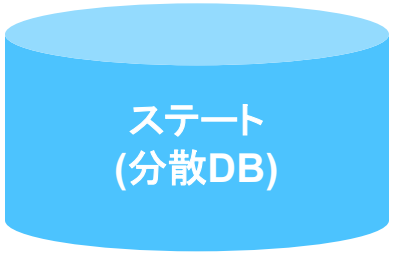
トランザクションの履歴を記録。
暗号的ハッシュ関数により、過去のトランザクション履歴の改竄を困難とする構造。



データ例：取引記録

ステート

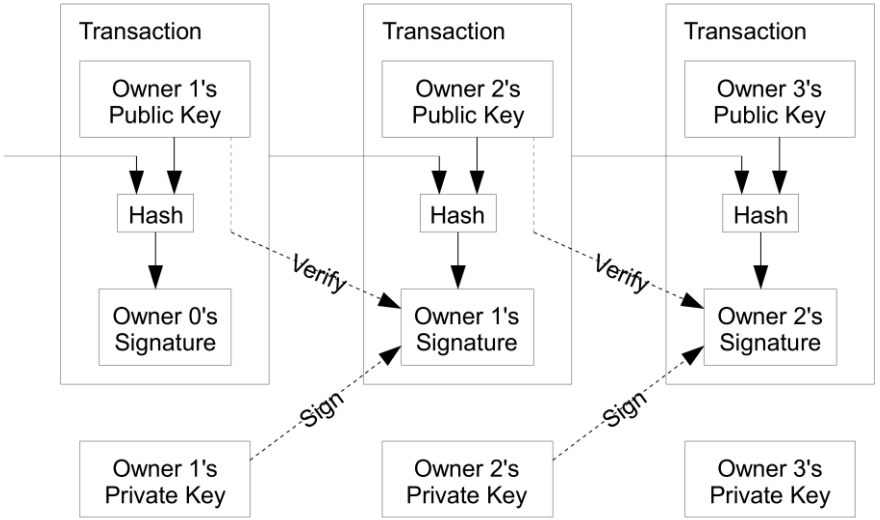
トランザクションを実行した結果の最新状態を記録する。



データ例：口座残高
＋任意の複雑な構造のデータ

トランザクション処理方式

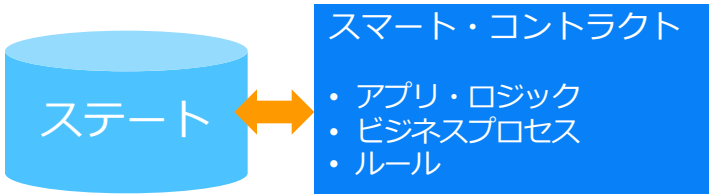
UTXO
(Unspent Transaction Output)



* source: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

スマート・コントラクト

- 任意のアプリケーションロジックを実行
- ビジネス・プロセスやルールを、参加者間で共有
- 複雑な処理を実装可能



コンセンサス方式

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

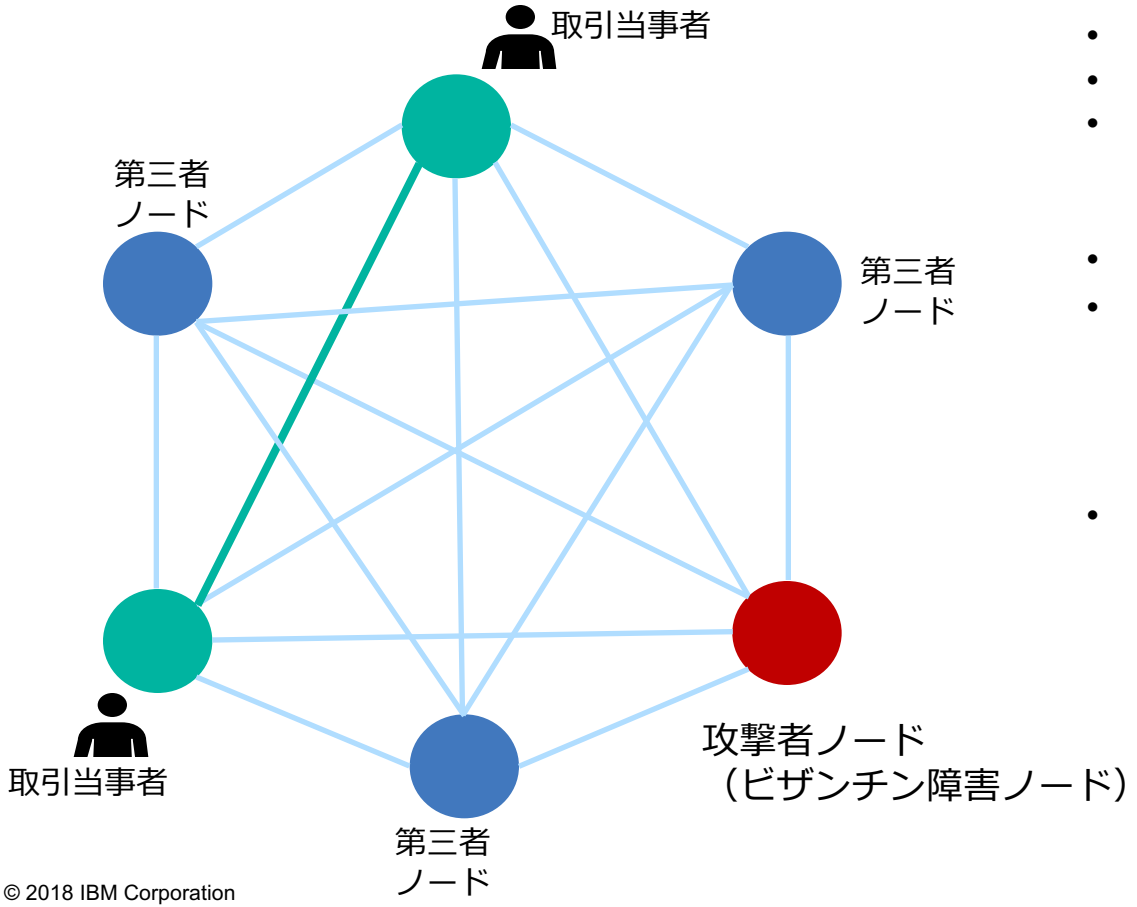
	Proof-of-Work (PoW)	分散コンセンサス形成アルゴリズム
方式	• 計算競争の勝者がブロックを追加するとともに報酬を受ける → 計算資源量等に応じて確率的に勝者が決まる。 亜種: PoI, PoS…	• メッセージ交換により合意形成を行う、分散コンセンサス形アルゴリズム (e.g., Paxos, VSR, Raft, PBFT, etc.)
長所	• スケーラビリティ	• 軽量・低消費電力 • フォークしない • ファイナリティを保証 • 高いパフォーマンスを実現しやすい
短所	• 安全性 (PoWにおける51%攻撃) • フォーク（分岐） • ファイナリティ欠如 • 電力使用量→コスト高	• ノード数が増えるとパフォーマンスが落ちやすい
対応ネットワーク	• Public Network で匿名の不特定多数の参加者間で使用可能	• Permissioned Network が前提

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類と役割を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

分散台帳技術ネットワークのモデル



- *N*個のノードが参加 $\{n_1, n_2, .. n_N\}$
- 最大 *f* 個のノードがビザンチン障害
- 各取引において、取引当事者（カウンターパーティ）がいる。

- i番目のノードの持つ台帳
- $dlt_i = \{ h(tx_1), h(tx_2), \ldots h(tx_m)\}, \{ tx_1, tx_2, \ldots tx_m \}$
  - tx_j：j番目のトランザクション
  - $h(tx_j)$：トランザクションのハッシュ値

- 各ノードは:
  - ✓ トランザクション内容の正当性をチェックするには tx_j を持つ必要がある
  - ✓ トランザクションの改竄を検知するだけなら $h(tx_j)$ を持っていればよい

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類と役割を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

安全性: 分散コンセンサス形成に求められる性質

BCIC Blockchain Innovation Center by IBM Research - Tokyo

- 分散コンセンサス形成アルゴリズムは、分散システムの同期をとるための技術で、数十年来研究されている
- 非同期型のメッセージ通信を前提とする（eventual-synchrony network model ）
- メッセージがネットワーク内に発信 (broadcast) された後，コンセンサスを経て一定時間内に健全なノードに配信 (deliver) され、ノード間でメッセージの順序が保証される

安全＝アトミック・ブロードキャスト の性質を満たす *1

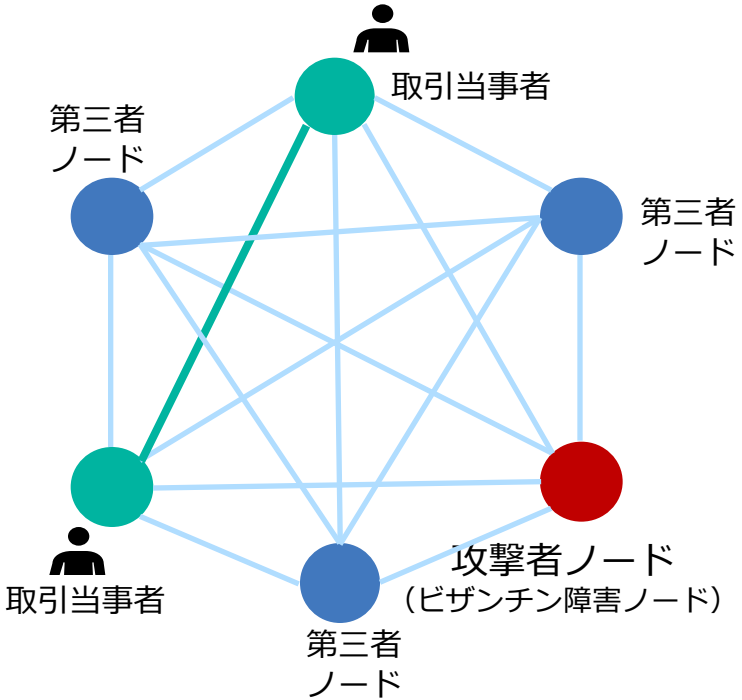
- 有効性 (Validity):
  - 健全なノード *p* がメッセージ m を発信した場合，そのメッセージ m はいずれそのノード *p* 上に配信される.
- 合意 (Agreement) :
  - ある健全なノードにメッセージmが配信される場合，そのメッセージは全ての健全なノードに配信される.
- 完全性 (Integrity) :
  - 健全なノードは各メッセージを最大１回しか配信しない.
- 全順序 (Total Order) :
  - 任意の2 つの健全なノードの間で，常に配信されたメッセージの順序が同一となる.

*1: C. Cachin and M. Vukolić, Blockchain Consensus Protocols in the Wild, 2017.

安全性: セキュリティ

分散台帳技術では、従来の分散システムよりも、セキュリティに対する要件が重要

- 攻撃者の存在する環境で、利益相反する複数の主体が取引を行う



インテグリティ要件

[I1]トランザクション内容の正当性
[I2] 改竄が検知できる
[I3] ファイナリティ

プライバシー/秘匿性要件

[C1]第三者に対する匿名性
[C2] 取引当事者同士の匿名
[C3] 第三者に対するトランザクション内容の秘匿
[C4] 第三者に対するトランザクション存在の秘匿
[C5] 第三者に対するステートの秘匿

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類と役割を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

仮想通貨

- 事例: Bitcoin, その他のコイン
- 一般的な実装: UTXO + PoW（または亜種）によるパブリックネットワーク

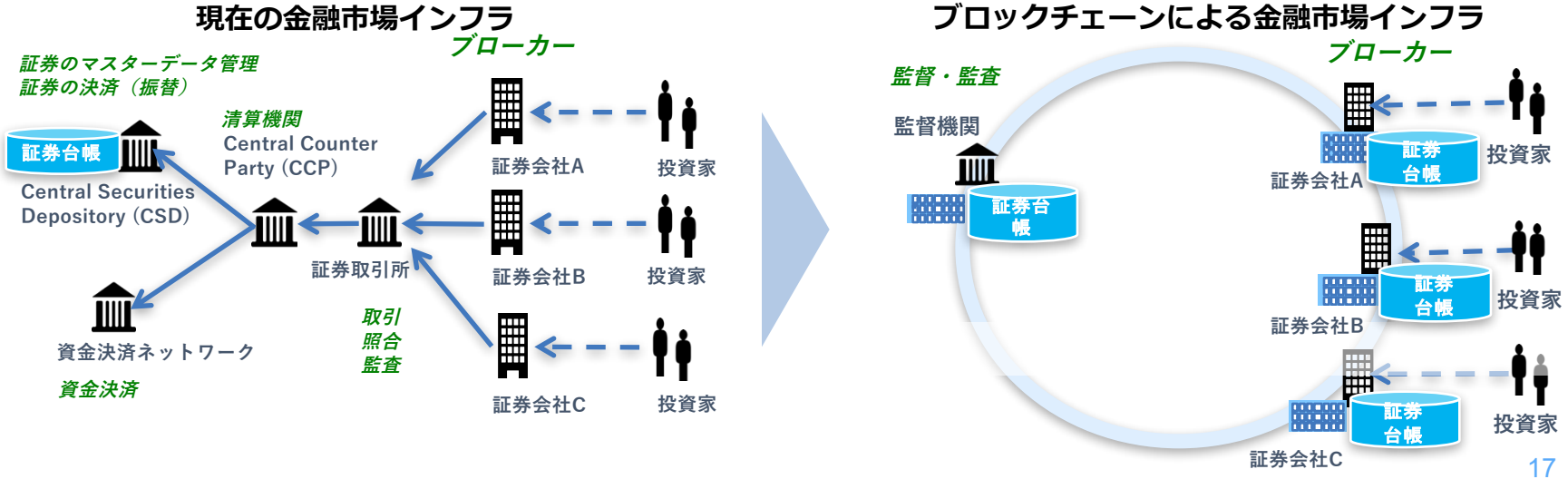
- 実装アプローチ
  - タイプ: **Public** or Permissioned
  - データ構造: ブロック and/or ステート
  - トランザクション処理: UTXO or スマートコントラクト

項目	要件
[I1]トランザクション内容の正当性	必要
[I2] 改竄が検知できる	必要
[I3] ファイナリティ	ゆるい *
[C1]第三者に対する匿名性	要
[C2] 取引当事者同士の匿名性	要
[C3]トランザクション内容の秘匿	ゆるい *
[C4]トランザクションの存在の秘匿	ゆるい *
[C5] ステートの秘匿	ー

* 本来は要件であると思われるが、UTXO実装が多いため、慣習的に満たさなくても許されている

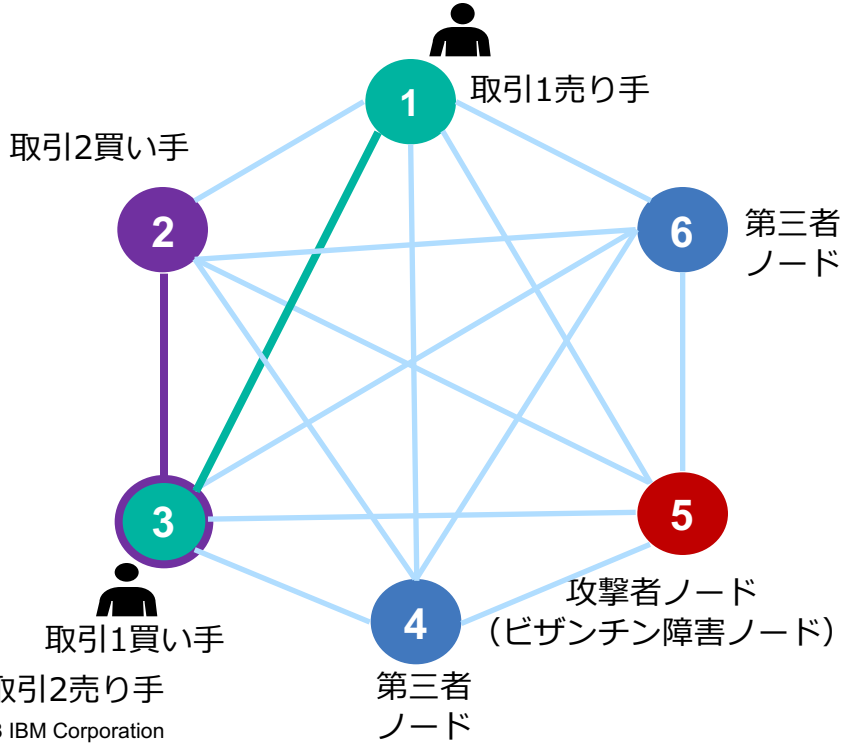
証券ポストトレード処理

- 証券の取引が成立した後の、（売買注文の条件がマッチ）、証券と資金の決済
- 複雑なネッティング処理や、DVP (Delivery-versus-Payment) 決済が必要となる
- 実装アプローチ
  - タイプ: **Permissioned** （認可された金融機関に限定）
  - データ構造: ステート (and ブロック)
  - トランザクション処理: スマートコントラクト



証券ポストトレード処理

- ある取引の決済が完了するためには、売り手の証券残高、買い手の資金残高が共に十分ある必要あり
- 取引の内容は第三者ノードから秘匿する必要がある
- 次に別のノードが取引をするときは、そのノードも証券残高・資金残高を参照できる必要がある

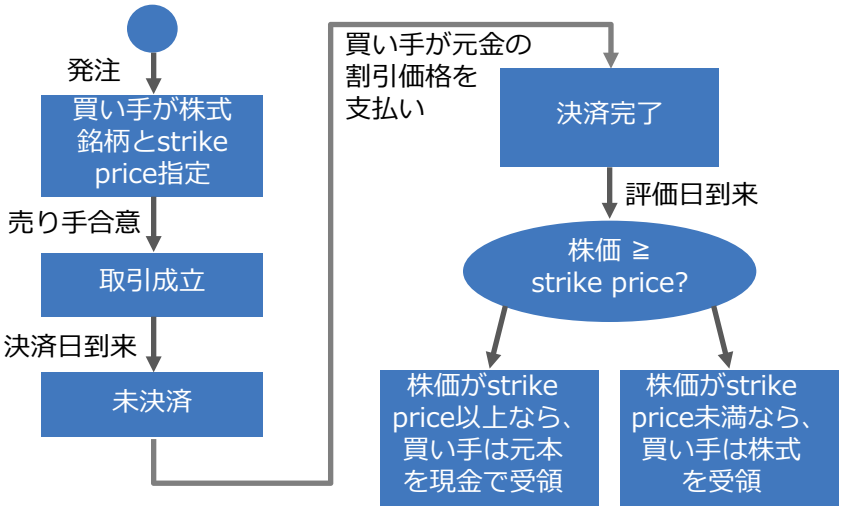


項目	要件
[I1]トランザクション内容の正当性	必要（重要）
[I2] 改竄が検知できる	必要（重要）
[I3] ファイナリティ	必要（重要）
[C1]第三者に対する匿名性	必要（重要）
[C2] 取引当事者同士の匿名性	不要
[C3]トランザクション内容の秘匿	必要（重要）
[C4]トランザクションの存在の秘匿	K-匿名性
[C5] ステートの秘匿	必要（重要）

金融契約

- 事例: デリバティブ契約や、デリバティブを証券化した金融商品
- 例）株価連動社債 (ELN: Equity Linked Note)は，株式とオプション取引を組み合わせた金融商品

- 実装アプローチ
  - タイプ: **Permissioned** （認可された金融機関に限定）
  - データ構造: ステート (and ブロック)
  - トランザクション処理: スマートコントラクト



例: 株価連動社債のロジック

項目	要件
[I1]トランザクション内容の正当性	必要 *1
[I2] 改竄が検知できる	必要 *1
[I3] ファイナリティ	必要 *1
[C1]第三者に対する匿名性	必要（重要）
[C2] 取引当事者同士の匿名性	不要
[C3]トランザクション内容の秘匿	必要（重要）
[C4]トランザクションの存在の秘匿	k-匿名性
[C5] ステートの秘匿	必要（重要）

*1 ただし当事者同士が合意できれば問題ない

分散台帳技術の安全性の意味を定義するには

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術の種類を、基本機能の観点から整理する
- 分散台帳技術を使う参加者の種類と役割を定義する
- 安全性に求められる性質を整理し、その意味を定義する
- 具体的なユースケースにおける安全性の要件を考えてみる
- 代表的な分散台帳技術の実装における、それぞれの要件への対応状況を考察してみる

代表的な分散台帳技術の比較

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

	Public	Permissioned
Smart Contract	ethereum	Quorum HYPERLEDGER Fabric
UTXO	bitcoin	R3 Corda

まとめ

BCIC
Blockchain Innovation Center
by IBM Research - Tokyo

- 分散台帳技術におけるインテグリティやプライバシーといったセキュリティ要件を定義し，既存の実装における要件の充足状況を考察

- 仮想通貨など、分散台帳として従来型のユースケース
  - PoW実装を前提とした歴史上の理由から、ファイナリティに関する要件がゆるい
  - 匿名性以外の秘匿性要件も弱い
- 証券ポストトレード処理や金融契約
  - 金融システムとして高額な決済が行われるため、法規制上強いプライバシー保護要件がある
  - 認可された金融機関だけ → Permissioned ブロックチェーンが必須
  - 複雑な状態遷移が発生するので、実装にはスマートコントラクトやステートが必要
  - プライバシーとインテグリティのトレードオフ
    - 「取引のプライバシーを守りつつ、残高は共有したい」というような相反する要求の難しさ

- 分散台帳技術の比較
  - PoWやその亜種ではファイナリティが保証できない。
  - パブリック型では匿名性は保証できるが、トランザクションの存在や中身は隠せない
  - Permissioned型はデータ暗号化や配布範囲を制限するなどプライバシー保護の工夫をしている一方、特別な役割のノードを持ち、これらのビザンチン障害を許容できない場合が多い