CBDCフォーラムWG4

ディスカッションペーパー

ブロックチェーン取引における プライバシー保護機能（Encrypted ERC）について

2025.10.14

TIS株式会社

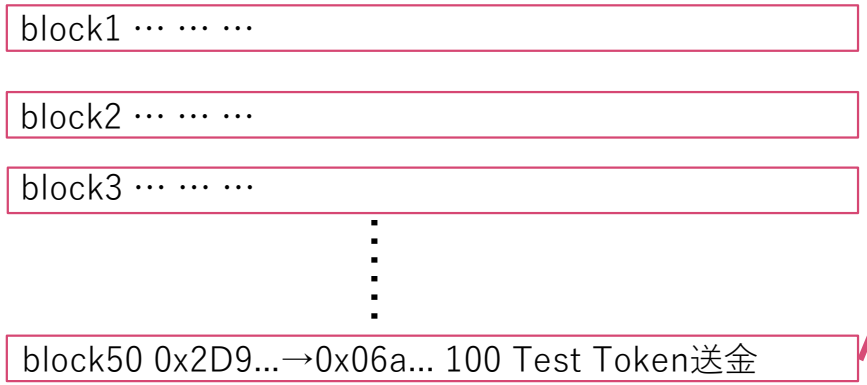
1. ブロックチェーンにおけるプライバシー強化の事例

背景（現状と課題）

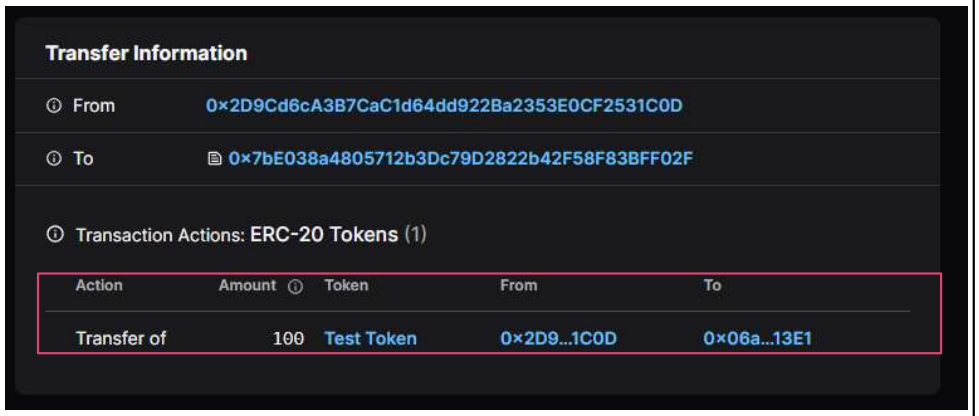
ブロックチェーンは「誰が誰に暗号資産を送ったか」等の取引履歴（トランザクション履歴）が**すべて記録、公開される。**

→透明性は高いが、不特定多数から取引履歴（ステーブルコインの送金情報等）が参照できるため
金融取引を非公開に保つ必要がある企業や個人にとっては問題となる可能性がある。

ブロックチェーンにおける取引履歴の記録イメージ
→各ブロックに取引履歴が記録されている。
ステーブルコイン（例：Test Token）の送金情報も平文で記録される。



UIツール、API等で誰でも送金情報を見ることができる。
以下はBlockchain Explorerでブラウザから参照した例。



1. ブロックチェーンにおけるプライバシー強化の事例

ブロックチェーンにおけるプライバシー強化の事例

Aztec Protocol	ゼロ知識証明を活用してスマートコントラクトやトークン取引のプライバシーを強化する Ethereumのセカンドレイヤー（Layer2）ネットワーク。
Oasis Network	二層構造やTEEなどの技術によりデータや処理内容の秘匿性・プライバシーを確保する 独立したLayer1ブロックチェーン
Encrypted ERC	**取引額や残高などの情報を暗号技術で秘匿できる、AvaLabs社で開発された ERC20と互換性のあるスマートコントラクト。 EVM互換のチェーンであればどのチェーンに対しても実装可能。**

→ 今回の発表ではEncrypted ERCについて紹介する。

2. Encrypted ERCの概要

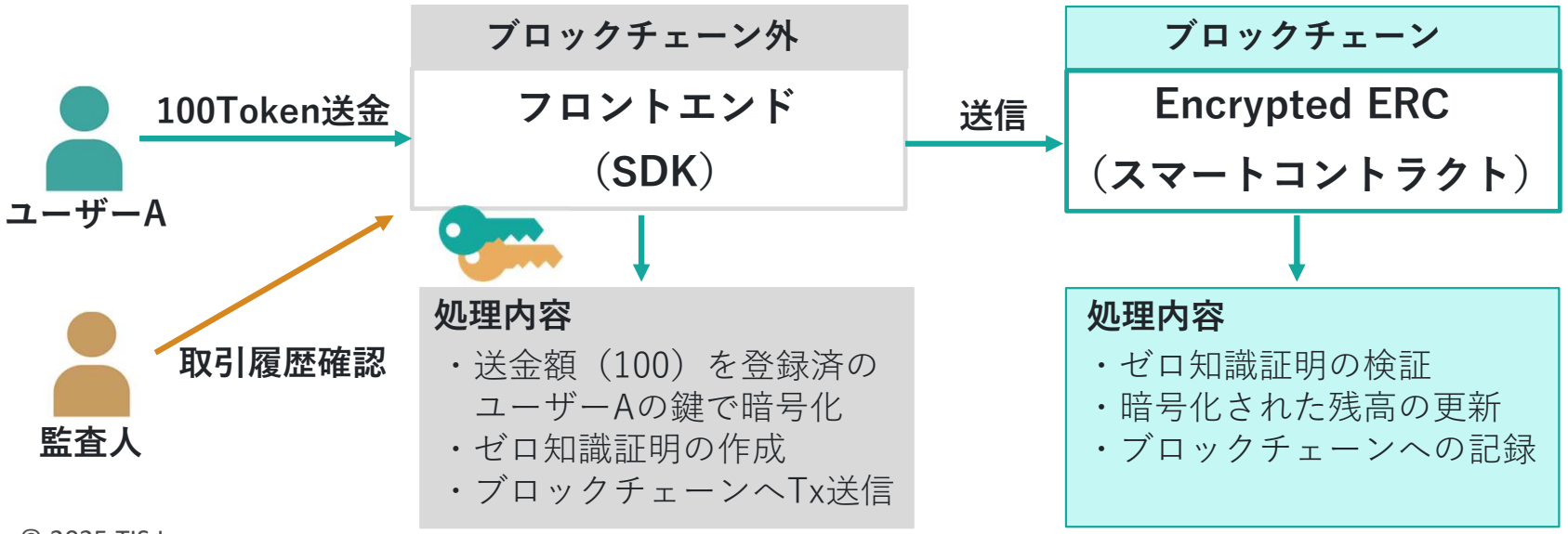
Encrypted ERCの特徴

① 残高・送金額・取引履歴は暗号化されてブロックチェーンに記録

② 取引の正当性証明にゼロ知識証明を活用

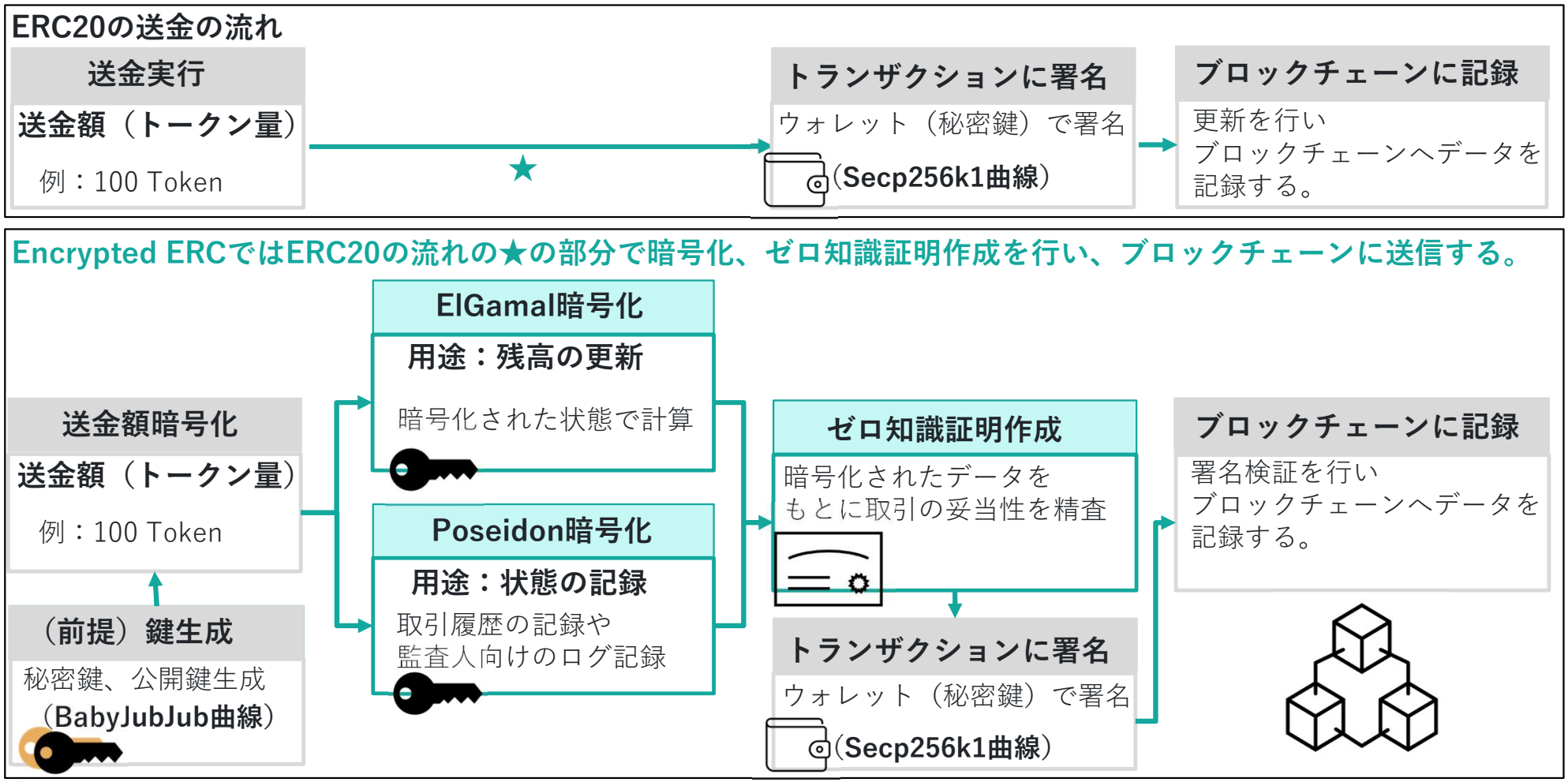
③ 取引に関わるユーザーの他に、監査人と呼ばれる管理者は取引履歴を復号できる

④ 既存のERC20トークンにも対応（すでに発行されたトークンを変換する）



3. Encrypted ERCが採用している技術要素

Encrypted ERCの仕組みを支える暗号技術と用途



3. Encrypted ERCが採用している技術要素

用語説明

BabyJubJub曲線

楕円曲線の一種であり、公開鍵と秘密鍵のペアを算出する。

ElGamal暗号とPoseidon暗号

項目	ElGamal暗号	Poseidon暗号
種類	楕円曲線暗号	Poseidonハッシュ+楕円曲線暗号
用途	残高の更新（計算）	状態の記録（取引履歴、監査ログ等）
復号	BabyJubJub秘密鍵で復号可能	BabyJubJub秘密鍵で復号可能
特徴	暗号化したまま加算・減算が可能	ゼロ知識証明の計算に最適化

ゼロ知識証明

自身の持つ秘密情報を明かすことなく、それが正しいことを相手に証明することができる方法。

4. 処理フロー

処理フロー（ブロックチェーン外処理：暗号化、ゼロ知識証明作成）

（前提）鍵生成
「送信者/受信者/監査人」の「公開鍵、秘密鍵」を生成、登録（**BabyJubJubで計算**）

Encrypted ERC固有

↓

① 送金情報の入力
送金先アドレスと送金額を指定

↓

② データの暗号化
送金額を送信者/受信者の公開鍵で**ElGamal暗号化（残高更新に利用）**
送金額を受信者/監査人の公開鍵で**Poseidon暗号化（取引履歴、監査ログの記録に利用）**
送信者の新残高を送信者の公開鍵で**Poseidon暗号化（取引履歴の記録に利用）**

Encrypted ERC固有

↓

③ ゼロ知識証明の作成
①と②のデータをゼロ知識証明の回路に入力し、以下条件が満たしていることを示すproof作成
送金額が送信者の残高以下であること
送信者の暗号化された残高、送金額、公開鍵が正しいこと
受信者の公開鍵で暗号化された送金額が正しいこと
監査人の公開鍵で暗号化された送金額が正しいこと

Encrypted ERC固有

↓

④ トランザクション署名
スマートコントラクトのtransfer関数呼び出しのためのデータに署名する。

4. 処理フロー

処理フロー（ブロックチェーン処理：証明検証、残高更新、ブロックチェーンに記録）

⑤ スマートコントラクト処理（transfer関数呼び出し）

- **Proof（ゼロ知識証明）を検証し、取引条件が満たされていることを確認**

- 残高の更新
  送信者残高の減算処理（**残高は暗号化されたままで計算を行う**）
  受信者残高に加算処理（**残高は暗号化されたままで計算を行う**）

- イベント発行（**暗号化された監査ログデータ**を出力）

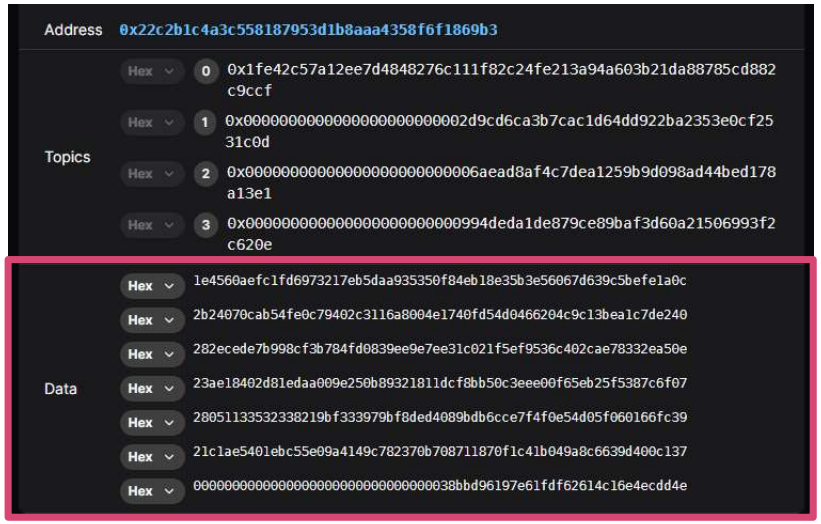
transfer関数の比較（Encrypted ERC vs ERC20 ）

項目	Encrypted ERC	ERC20
関数シグネチャ	transfer(to, **tokenId**, **proof**,**balancePCT**)	transfer(to, **amount**)
引数	to　　送金先アドレス tokenId　　トークンID（既存のトークンの管理番号） proof　　ゼロ知識証明で作成されたproof balancePCT　暗号化された送信者の新残高	to　　送金先アドレス amount　　送金額

5. Encrypted ERCの実行結果

Encrypted ERCの実行結果（ERC20との比較）

Encrypted ERCの送金



ERC20の送金

項目	Encrypted ERC	ERC20
ガス手数料	1,129,061	34,532
データサイズ	1572 bytes	68 bytes
送金額の暗号化	あり	なし

送金額暗号化に伴い
データサイズが約23倍
ガス手数料が約32倍

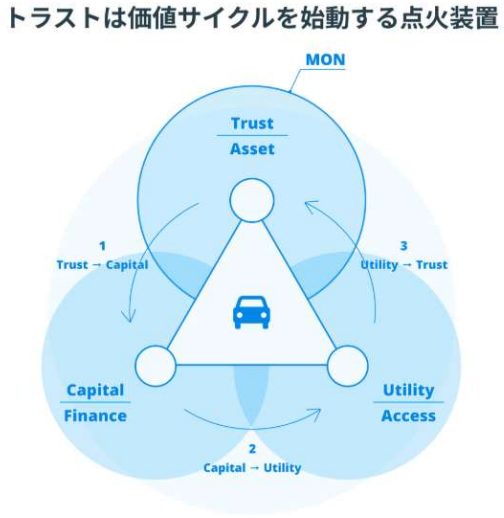
6. Encrypted ERCの取り組み事例のご紹介

取り組み事例のご紹介

以下実証実験においてSC（ステーブルコイン）やST（セキュリティートークン）にEncrypted ERCを活用。
今後、CBDCサンドボックスとの接続実験も予定。

トヨタ・ブロックチェーン・ラボ様

ホワイトペーパー（2025/8/20 発表）より
https://www.toyota-blockchain-lab.org/ja/library/mon-orchestrating-trust-into-mobility-ecosystems



THANK YOU

ITで、社会の願い叶えよう。

TIS INTEC
Group