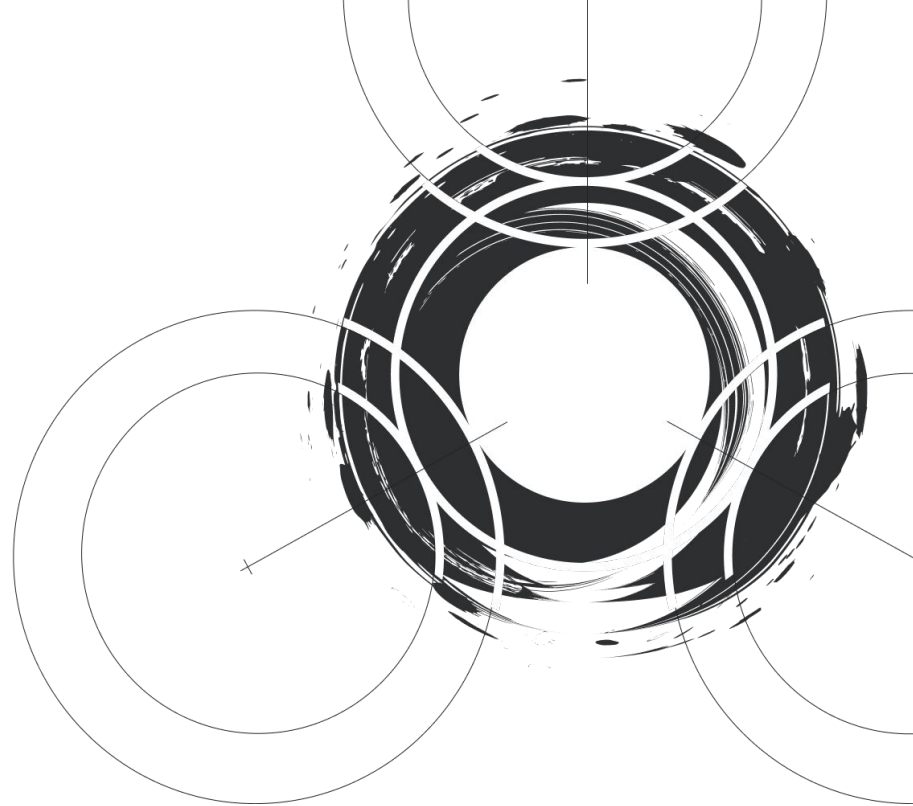




オンチェーン金融におけるプライバシー

2026年9月29日 / CBDCフォーラム

株式会社Datachain 吉田基紀





- 本日は、ステーブルコイン等のデジタル通貨のエンタープライズユースケース創出において不可欠な「ブロックチェーンにおけるプライバシー」に関して、考えるための土台となる枠組みを共有します

1 なぜ今プライバシーか

ステーブルコインの商用利用におけるプライバシーの課題、必要性

2 プライバシーの定義

プライバシーの定義と、満たすべき3つの条件

3 プライバシーソリューションの分類

秘匿方式・信頼前提の2つの軸で方式を評価

4 KuraPrivacyの紹介

KuraPrivacyの設計思想

5 まとめ・質疑応答

本日のお話のまとめ



Datachain

なぜ今プライバシーか

プライバシーの定義

プライバシーソリューションの分類

KuraPrivacyの紹介

まとめ・質疑応答



- パブリックチェーンでは、**金額・送受信者・取引履歴を誰でも閲覧**できる。取引内容を知るのは当事者と銀行だけ、という既存の商取引の前提が成り立たない
- このままでは企業間決済や給与支払い等に使いづらく、**ステーブルコインを本番運用するうえで大きな障壁**となる

BtoB決済

取引先・取引量が競合に見える。発注サイクルまで推測できてしまう

給与支払い

全従業員の給与額が相互に見える。人事情報がチェーン上に常時公開された状態になる

店舗決済

店舗ごとの単価・売上金額・決済時間・リピーター率を、第三者が誰でも集計できる

Block Explorer — すべて公開

From	To	Amount	Time
0x7a...c1	0x3f...9d	1,250,000	10:14
0x7a...c1	0xb2...04	480,000	11:02
0x9e...22	0x7a...c1	2,100,000	13:47
0x7a...c1	0x3f...9d	1,250,000	16:30

同じアドレスの往復・金額・頻度が、そのまま取引関係として読み取れる

※ 利用頻度の高いアドレスは、ブロックチェーン分析ツール（Chainalysis、Elliptic等）によって企業名や個人名が特定され、ラベル付けされていることが多い。『アドレスだけなので匿名』とは言えない



- ステ이블コイン普及に向けて、特に **法人利用を想定したプライバシー保護の仕組み** の実装が進行
- B2Bユースケースを想定した新興チェーンではプライバシー機能が標準化。Ethereum等の既存チェーン上においても、法人利用を想定したプライバシーソリューションが台頭

チェーン毎のプライバシー対応の加速

B2Bユースケースを想定した新興チェーンでは、ローンチ時の重要機能の1つとしてプライバシーが位置づけられている。
既存チェーンでのプライバシー実装の動きも見られる。

Arc (Circle) Tempo (Stripe)	Circle社のArc、Stripe社のTempoは、初期のドキュメント公開時から「プライバシー送金機能」を標榜。
Aleo Midnight Canton	プライバシーに特化/対応したチェーンの開発も加速
EthSystems	Ethereum Foundationのプライバシー部隊IPTFが独立し、EthSystemsを設立 (2026年7月)

マルチチェーンで対応可能なソリューション

多くのユーザーを抱える複数の既存チェーン上で展開するプライバシーソリューションへの注目も集まっている。
2025年から徐々にB2Bユースケースに最適化した製品が台頭。

Railgun	Ethereum上の秘匿ソリューションとして最大規模のTVL (\$82M, 2026年7月時点)。主にweb3ユーザー向け。不正な出所でないことを証明できる機能(Private Proofs of Innocence)を実装。
Zama	FHE(完全準同型暗号)により、既存L1・L2上で機密トークンを実現。2025年12月にEthereumメインネットで稼働し、法人の給与支払いでの利用も始まっている。
KuraPrivacy	規制準拠とプライバシー保護を両立。EVM主要チェーンに対応し、SC発行体に求められる選択的開示・スクリーニング・強制償還を前提に設計。



- 一方で、統制できない秘匿機能は、発行体・電取が秘匿環境内の取引に対して確認・制限・執行ができず、各種の義務を果たすことができなくなるため、そのままでは導入できない
- ただし秘匿の需要に応えなければ、統制の及ばない第三者のツールが広がるか、SCの用途が限られたままになる

統制の効かないプライバシー実装がもたらす3つのリスク

1 取引実態を確認できない

秘匿環境内の取引をモニタリングできず、法令上の義務を履行できない。当然、当局照会にも対応できない。

2 移転制限が十分に機能しない

制裁対象・不正資金の移転を検知も遮断もできないまま利用される。レピュテーションリスクに繋がる。

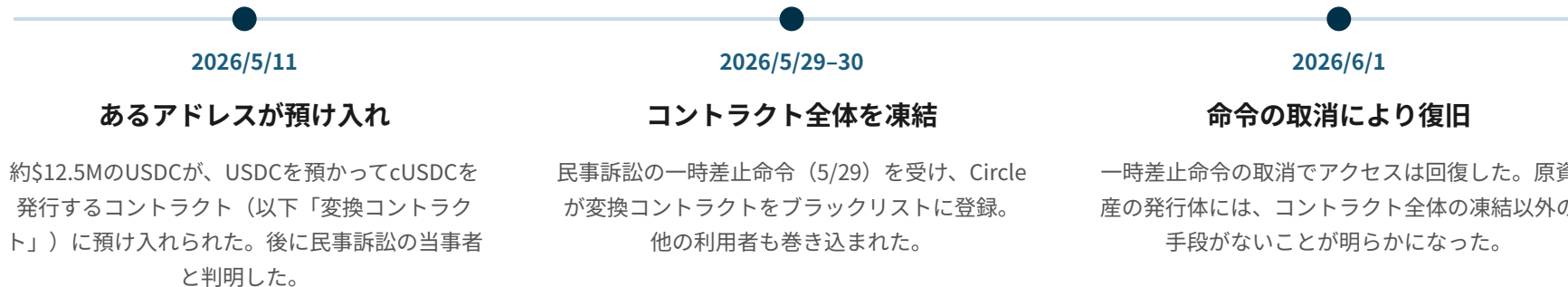
3 対象の利用者だけを凍結できない

対象を絞った執行手段がなく、当局要請時に無関係の利用者を巻き込む



- 米国cUSDC凍結事件では、原資産（USDC）の発行体 Circle 社の統制が個々の利用者の残高に及ばなかったため、cUSDCのサービス提供者Zamaの利用者全員の資産が凍結されることになった
- **発行体対象を絞って執行できる必要**があることが明るみになった

cUSDC凍結事件（2026年5～6月）の経緯



出典：The Block, [Court-ordered Circle freeze traps \\$12.6 million in Zama cUSDC contract amid Overnight Finance suit](#)



Datachain

なぜ今プライバシーか

プライバシーの定義

プライバシーソリューションの分類

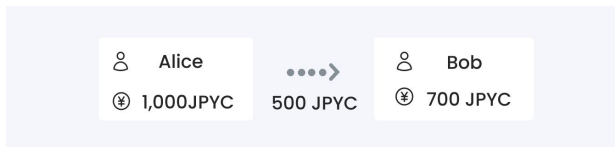
KuraPrivacyの紹介

まとめ・質疑応答

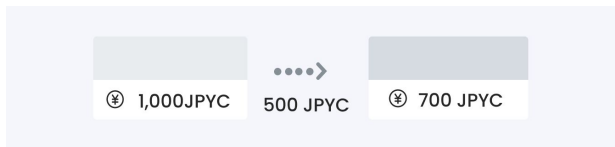


- プライバシーは1つの性質ではなく、**匿名性・機密性・非リンク性**という3つの要素で構成される
- エンタープライズ領域への適用を考えると、3つの要素を網羅することが望ましい

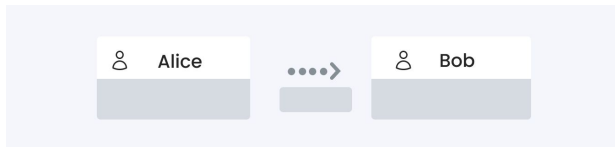
何もない状態



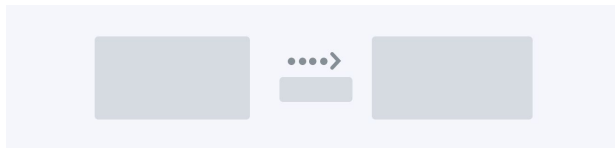
匿名性
(誰が秘匿)



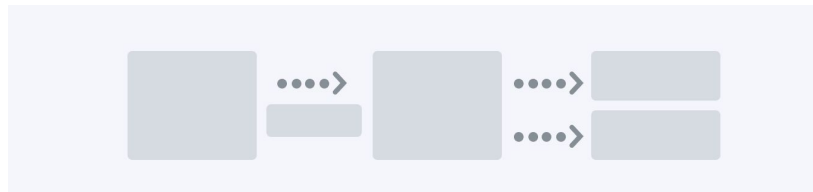
機密性
(残高・取引額)



匿名性＋
機密性



非リンク性（取引グラフの秘匿）が担保できていない

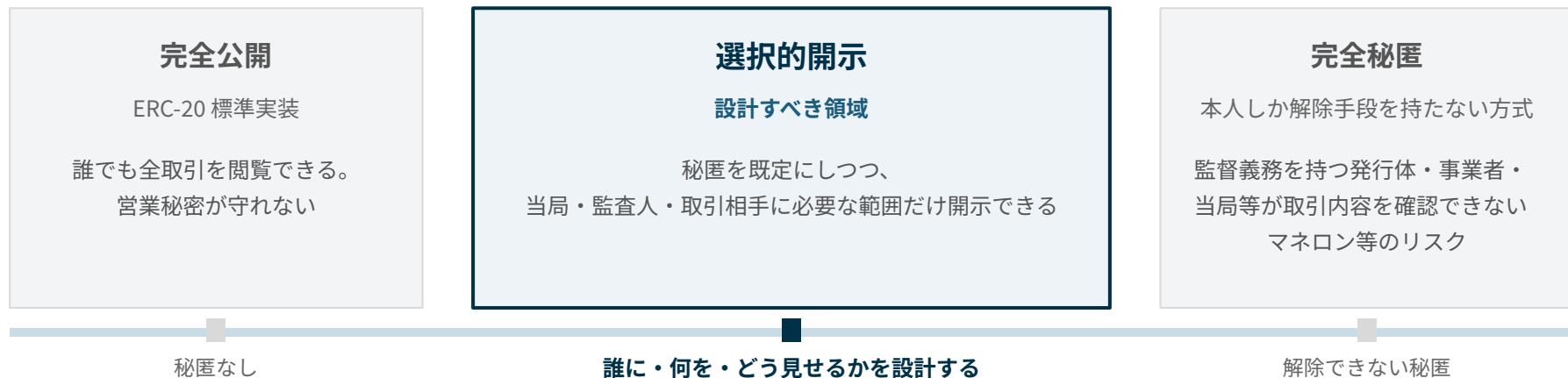


非リンク性まで担保





- 「プライバシー＝完全秘匿化」ではなく、必要なのは「誰に、何を、どう見せるか」という開示ルール設計である
- 特にエンタープライズ文脈におけるオンチェーンプライバシーには、取引情報を適切な範囲で適切な対象に対して開示する「選択的開示」が求められる





- エンタープライズでの利用には、プライバシー・信頼前提・統制の3つの条件がそろう必要がある
- 条件①②は方式でおおむね決まり、条件③はプロダクトごとに確認する必要がある

あるべき姿の3条件

1 プライバシーの3要素を満たす

第三者に対し、匿名性・機密性・非リンク性をすべて守れる

方式で決まる | 秘匿方式

課題① 透明性への対応

2 信頼前提が明確で最小限

取引の正しさと秘匿性のために暗号以外に信頼するものが明確で、事業上許容できる

方式で決まる | 信頼前提

隠すことで生じる追加の信頼

3 統制機能を持つ

発行体・導入事業者が、秘匿したままでも統制できる（主には下記3つの統制）

プロダクトごとに確認

課題② 統制されない秘匿への対応

秘匿したままで主に以下の3つの統制を持つ 課題②の3つのリスクに対応

見る（モニタリング）

監督者が、必要な範囲の取引を確認できる

選択的開示：誰に・何を・どう見せるかを設計する

リスク① 取引実態を確認できない

制限する（移転制限）

制裁対象・不正資金への移転を検知・遮断できる

リスク② 移転制限が十分に機能しない

執行する（凍結・強制償還）

当局要請時に、対象の利用者だけを凍結・強制償還できる

リスク③ 対象の利用者だけを凍結できない



Datachain

なぜ今プライバシーか

プライバシーの定義

プライバシーソリューションの分類

KuraPrivacyの紹介

まとめ・質疑応答



- 条件①「プライバシーの3要素を満たすか」は、秘匿方式でおおむね決まる
- 秘匿環境型／暗号化残高型／選択的データ配布型の3つに整理でき、第三者から隠れる要素が異なる

秘匿方式	どのように秘匿するか	第三者から見えて隠れるか		
		送受信者 (匿名性)	金額 (機密性)	取引グラフ (非リンク性)
I 秘匿環境型 例：KuraPrivacy、Arc、Tempo、Railgun	資産と取引を、外から読めない状態領域の中で処理する。 台帳そのものを外に出さない	● 隠れる	● 隠れる	● 隠れる
II 暗号化残高型 例：Zama、Solana Token-2022	アドレスと取引の流れは公開のまま、残高と金額だけを暗号化する	✕ 隠れない	● 隠れる	✕ 隠れない
III 選択的データ配布型 例：Canton Network	取引明細を当事者のノードにしか配布せず、各ノードは自らに 関係する取引だけを保持する	● 隠れる	● 隠れる	● 隠れる



- 条件②「信頼前提が明確で最小限か」は、方式でおおむね決まる
- 取引を隠すと第三者が中身を確認められなくなるため、「取引の正しさ」と「秘匿性」を担保する追加の信頼が方式ごとに異なる
 - 取引の正しさ: 正しく処理されていることを担保するために信頼するもの
 - 秘匿性: 中身が秘匿されていることを担保するために信頼するもの

方式	例	信頼前提		
		暗号	取引の正しさ 正しさの担保に追加で信頼するもの	秘匿性 秘匿の担保に追加で信頼するもの
1 暗号信頼型 Cryptographic Trust	KuraPrivacy	● 共通の前提	追加なし ZKP利用=暗号への信頼	追加なし／証明生成事業者
2 組織信頼型 Organizational Honesty	Zama、Tempo	● 共通の前提	複数社による委員会	複数社による委員会
3 TEE信頼型 Hardware-anchored Trust	Arc	● 共通の前提	バリデーター群+TEE	TEE
4 当事者信頼型	Canton Network	● 共通の前提	取引の当事者+複数社による委員会	相手方のノード運営者

※ Enterprise Ethereum Alliance [“State of Privacy on Ethereum for Enterprise”](#) を参考に整理。各方式の英語名称は同整理から引用。



- 3要素を満たし、追加の信頼前提が最も少ないのは「秘匿環境型×暗号信頼型」である
- ただし統制機能は方式では決まらないため、同じ枠の中でもプロダクトごとに確認する必要がある

秘匿方式（条件①） ＼ 信頼前提（条件②）	信頼前提（条件②）：暗号以外に追加で信頼するもの			
	暗号信頼型 追加の信頼なし *1	TEE信頼型 TEE・クラウド事業者	組織信頼型 委員会・運営者	当事者信頼型 取引相手のノード運営者
I 秘匿環境型 3要素とも秘匿	KuraPrivacy Railgun Paladin (Zeto)	Arc	Tempo	—
II 暗号化残高型 機密性のみ	Solana Token-2022 eERC (Avalanche)	—	Zama	—
III 選択的データ配布型 3要素とも秘匿	—	—	—	Canton Network Paladin (Noto)

そのうえで、条件③（統制：見る・制限する・執行する）を満たすかは、プロダクトごとに確認する

*1 証明を自ら生成する場合

※ 2026年9月時点の公開情報に基づくDatachainの整理。各プロダクトは代表的な構成で配置しており、仕様により位置づけは異なりうる



Datachain

なぜ今プライバシーか

プライバシーの定義

プライバシーソリューションの分類

KuraPrivacyの紹介

まとめ・質疑応答



妥協のない高いプライバシー保護と、
企業利用に耐える高い運用性の両立を
可能にするオンチェーンプライバシー基盤



- KuraPrivacyは「**秘匿環境型×暗号信頼型**」の方式で条件①②を満たし、そのうえで条件③の統制機能を備える
- さらに、既存のウォレット・認証方式をそのまま使えるため導入のハードルも低い。また、マルチチェーン対応やプログラマビリティにより、「**秘匿×DvP決済**」等の多様なユースケースへの対応も可能。

1 取引情報の完全な秘匿

匿名性・機密性・非リンク性の3つを網羅。ゼロ知識証明で検証するため、取引の正しさに暗号以外の信頼を追加しない

条件①② 方式で満たす

2 取引内容の選択的開示

必要な相手・範囲にだけ、支払権限を渡さずに取引内容を開示。規制当局への報告や監査にも対応

条件③ 統制機能

3 移転制限

許可リストに登録したアカウントのみ取引可能。KYC済みユーザーに限定するなど、コンプライアンス要件に対応

条件③ 統制機能

4 資産の強制償還・凍結に対応

事前定義したポリシーに基づき資産を強制償還。担当者離脱・規制対応・緊急時の資産回収など、運用上の例外処理に対応

条件③ 統制機能

5 既存ウォレット・認証方式に対応

EOA・コントラクトウォレット・Passkeyなど主要な署名方式に対応。既存ウォレットに追加の支払い鍵不要で組み込めるため、セキュリティ・運用性面で優位。

6 低 Gas コストでの運用

プライバシーソリューションの中でも高いGas効率を実現。主要サービスの1/2～1/3のGasコストで取引を実行可能。

7 マルチチェーン対応

初期フェーズではEVM互換チェーンに対応。今後はSolana等の非EVMチェーンへの拡大も検討。

8 プログラマビリティ

秘匿環境下において、DvP決済、クロスチェーン取引、ウォレットにおける送金ポリシー等の多様なユースケースを実現可能

詳細: <https://kura.datachain.jp/ja>



Datachain

なぜ今プライバシーか

プライバシーの定義

プライバシーソリューションの分類

KuraPrivacyの紹介

まとめ・質疑応答



プライバシーとコンプライアンスの両立が、オンチェーン金融の実ユースケースを広げる

持ち帰っていただきたい3つのポイント

01

プライバシーは「隠す」 ではなく「見せ方の設計」

取引情報を一律に隠すのではなく、開示のルールを設計する

- **誰に** 当局・監査人・取引相手
- **何を** 当事者・金額・取引履歴
- **どう見せるか** 必要な範囲だけ開示

02

コンプライアンスと両立しない 秘匿は、本格導入が難しい

発行体・導入事業者が、秘匿したままでも統制できることが前提になる

- **見る** モニタリング
- **制限する** 移転制限
- **執行する** 凍結・強制償還

03

方式で絞り込み、 統制はプロダクトで確認

3つの条件に照らし、方式とプロダクトの両面で見極める

- **どう秘匿するか** 秘匿方式（条件①）
- **何を信頼するか** 信頼前提（条件②）
- **統制できるか** プロダクト（条件③）



オンチェーン金融のユースケース拡大に、**プライバシーは不可欠な技術領域**です。
設計から実装まで伴走いたしますので、お気軽にお問い合わせください。

株式会社Datachain
オンチェーンプライバシー事業統括 吉田 基紀

お問い合わせ: <https://kura.datachain.jp/ja/contact>

免責事項

- 本資料は2026年9月時点の公開情報に基づく株式会社Datachain（以下「当社」）の見解であり、当社はその正確性・完全性を保証するものではありません。
- 他社製品・サービスの分類は、公開情報に基づき当社が独自に整理したものです。
- KuraPrivacyに関する記載には、開発中の内容や当社試算が含まれます。将来の機能・性能を保証するものではありません。
- 本資料は、投資・法律上の助言や、特定の暗号資産・金融商品の勧誘を目的とするものではありません。