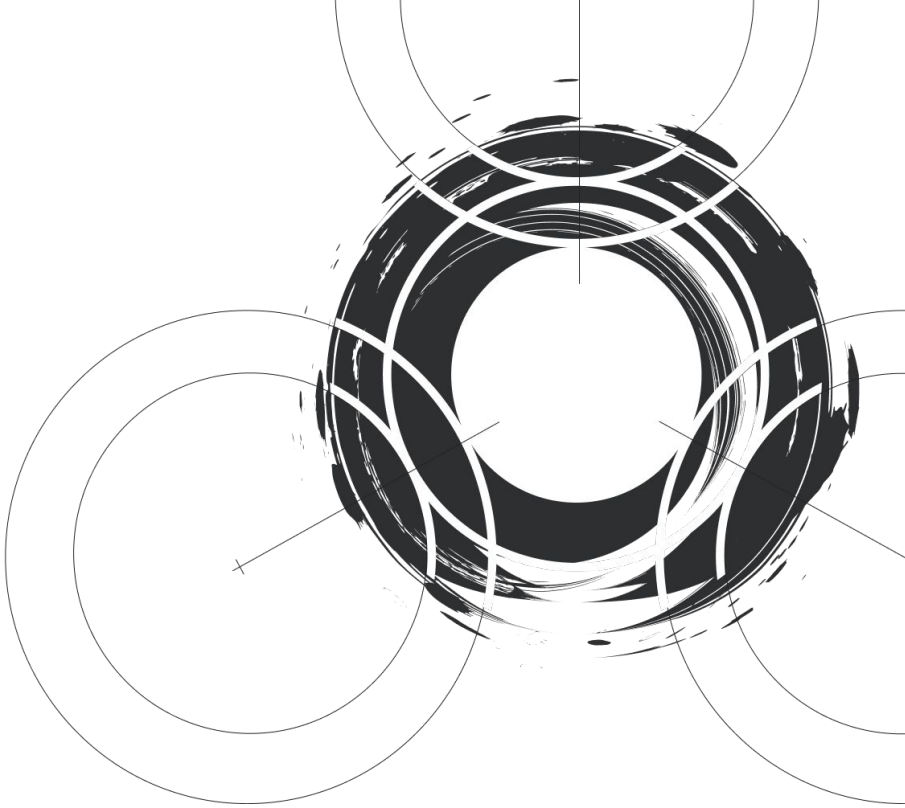
Datachain

オンチェーン金融におけるプライバシー



株式会社Speee

2026年11月13日

Copyright © 2026 Datachain, Inc. All Rights Reserved.

本日の内容

Datachain

- 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、主要な特長のご紹介
5	**まとめ**	本日のお話のまとめ

Copyright © 2026 Datachain, Inc. All Rights Reserved.



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

課題①: 取引の透明性がステーブルコインの法人利用を妨げる

Datachain

- 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

Copyright © 2026 Datachain, Inc. All Rights Reserved.

プライバシーに関する動向：主要チェーン・新興チェーンそれぞれで実装が進む

Datachain

- ステーブル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

新興チェーンにおけるプライバシー実装

B2Bユースケースを想定した新興チェーンでは、初期段階から重要機能の1つとしてプライバシー保護が位置づけられている。

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・利用も加速

既存の主要チェーン上でプライバシーを実現

Ethereum等のすでに多くのユーザーや流動性を持つブロックチェーンにおいて、プライバシー保護が可能なソリューションの利用が加速。

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、ステーブルコイン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。

Copyright © 2026 Datachain, Inc. All Rights Reserved.

課題②: 発行体・電取が統制できないプライバシー実装のリスク

- 一方で、発行体・電子決済手段等取引業者（以下「電取」）が統制できないプライバシー機能は、発行体・電取が秘匿環境内で「確認・制限・執行」ができず、本来求められる一連の義務を果たすことができなくなる

発行体・電取によ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、発行体・電取が義務を履行できない。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

制裁対象アドレスや不正資金と関連のあるアドレスによる取引を制限できない。Allowlist型のステーブルコインの場合には、その適用が秘匿環境内では機能しない

3 対象者を絞った凍結ができない

対象者（アドレス）を絞った執行手段がなく、当局や裁判所からあるアドレスの凍結を要請されても、アドレス単位での凍結ができず、不特定多数の利用者を巻き込んでしまう

規制対応とステーブルコイン利用の拡大を両立するには、**「発行体・電取が統制できる秘匿」**を、自ら提供または採用する必要がある

Copyright © 2026 Datachain, Inc. All Rights Reserved.

事例: 米国 cUSDC凍結事件の経緯と論点

- 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
- **発行体が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

2026/5/11

あるアドレスが預け入れ

約$12.5MのUSDCが、USDCを預かってcUSDCを発行するコントラクト（以下「変換コントラクト」）に預け入れられた。後に民事訴訟の当事者と判明した。

2026/5/29–30

コントラクト全体を凍結

民事訴訟の一時差止命令（5/29）を受け、Circleが変換コントラクトをブラックリストに登録。他の利用者も巻き込まれた。

2026/6/1

命令の取消により復旧

一時差止命令の取消でアクセスは回復した。原資産の発行体には、コントラクト全体の凍結以外の手段がないことが明らかになった。

出典：The Block, Court-ordered Circle freeze traps $12.6 million in Zama cUSDC contract amid Overnight Finance suit

Copyright © 2026 Datachain, Inc. All Rights Reserved.



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

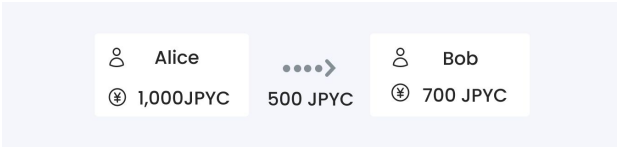
KuraPrivacyの紹介

まとめ

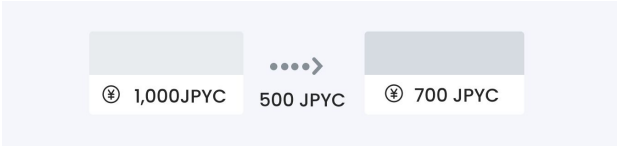
プライバシーの3つの要素

- 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

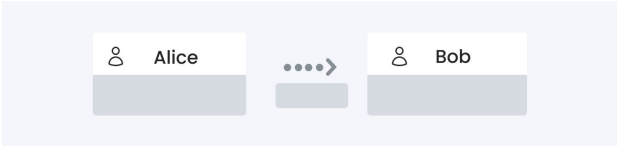
何もない状態



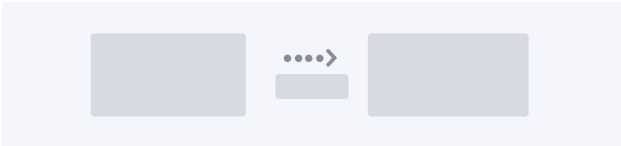
匿名性
(誰が秘匿)



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



取引の関連性を分析すれば、取引グラフからアドレスが解析・推測されてしまう

非リンク性まで担保

つながりが消えて、単独の関連性のない何かが発生していることしかわからない

Copyright © 2026 Datachain, Inc. All Rights Reserved.

秘匿の度合いと選択的開示

- 「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」**という開示ルールの設計である
- 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

完全公開

ERC-20 標準実装

誰でも全取引を閲覧できる。
営業秘密が守れない

選択的開示

設計すべき領域

秘匿を既定にしつつ、
当局・監査人・取引相手に必要な範囲だけ開示できる

完全秘匿

本人しか閲覧権限を持たない方式

監督義務を持つ発行体・事業者・
当局等が取引内容を確認できない
マネロン等のリスク

秘匿なし

誰に・何を・どう見せるかを設計する

解除できない秘匿

Copyright © 2026 Datachain, Inc. All Rights Reserved.

あるべき姿：3つの条件

Datachain

- 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

秘匿する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（確認・開示）

発行体・電取が必要な範囲の取引を確認でき、当局等の要請に応じて対象を絞って開示できる

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）

Allowlist等による事前の判定で遮断できる

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　対象者を絞った凍結ができない

Copyright © 2026 Datachain, Inc. All Rights Reserved.



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

秘匿方式の3分類

Datachain

- 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
- 主要サービスは、秘匿環境型／暗号化残高型／選択的データ配布型の3類型に整理でき、秘匿される要素が異なる

秘匿方式	どのように秘匿するか	第三者から秘匿されるか		
		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、第三者が読めない領域（秘匿環境）の中で処理する。実現手法は多数	● 秘匿可能	● 秘匿可能	● 秘匿可能
II 暗号化残高型 例：Zama、Solana Token-2022	アドレスと取引グラフは公開のまま、残高と金額だけを暗号化する	✕ 秘匿不可	● 秘匿可能	✕ 秘匿不可
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	● 秘匿可能	● 秘匿可能	● 秘匿可能

※ 2026年11月時点の公開情報をもとに当社が整理

Copyright © 2026 Datachain, Inc. All Rights Reserved.

追加の信頼前提（何を信頼する必要があるか）

Datachain

- 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
- 取引を秘匿すると第三者が取引内容を検証できなくなるため、「取引の正しさ」と「秘匿性」を担保する追加の信頼前提が必要になる
  - 取引の正しさ: 正しく取引が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: 取引内容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	追加なし （証明生成を委託する場合は委託先）
2 **組織信頼型** Organizational Honesty	Zama、Tempo	● 共通の前提	複数社の委員会、運営者	複数社の委員会、運営者
3 **TEE信頼型** Hardware-anchored Trust	Arc	● 共通の前提	TEE＋承認済みコード	TEE
4 **当事者信頼型**	Canton Network	● 共通の前提	取引の当事者 ＋発行体（または複数社の委員会）	各ノードの運営者

※ 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。
※ 暗号以外の主体や技術（委員会・TEE等）に頼る部分は、外部委託先管理・システムリスク管理の対象となるため、少ないほど望ましい

Copyright © 2026 Datachain, Inc. All Rights Reserved.

秘匿方式×信頼前提のマトリクス

Datachain

- 分類上、3要素の秘匿と追加の信頼の少なさを両立しうるのは「秘匿環境型×暗号信頼型」である
- ただし秘匿性は証明生成・鍵管理を誰が担うかに左右され、統制機能も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	**組織信頼型** 委員会・運営者	**TEE信頼型** TEE	**当事者信頼型** 各ノード運営者
I 秘匿環境型 3要素とも秘匿	**KuraPrivacy** **Railgun** **Paladin（Zeto）**	**Tempo Zones**	**Arc**	—
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11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

Copyright © 2026 Datachain, Inc. All Rights Reserved.



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

KuraPrivacy

妥協のないプライバシー保護と、
企業利用に耐えう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

Copyright © 2026 Datachain, Inc. All Rights Reserved.

KuraPrivacyの特徴

Datachain

- オンチェーンのプライバシー保護と、発行体・電取による統制機能を併せ持つプライバシー基盤
- 「秘匿環境型×暗号信頼型」の方式で3要素を秘匿し、取引の正しさを暗号で担保したうえで、統制機能を備える
- 既存の署名方式への対応やプログラマビリティにより、導入・運用もしやすく、多様なユースケースにも対応

プライバシー保護 01

プライバシーの３つの要素すべてに対応。法人利用に適した秘匿

- **匿名性**
  送受信者の秘匿
- **機密性**
  残高や取引金額の秘匿
- **非リンク性**
  取引グラフの秘匿

これらを最小限の追加信頼のもとで実現

統制・規制準拠 02

日本国内の規制対応を見据えた統制機能を提供

- **選択的開示**
  秘匿を既定としつつ、当局・監査人・取引相手など開示が必要な相手に、必要な範囲に限って取引内容を開示可能
- **移転制限**
  発行体の指定するAllowlistやDenylistを秘匿取引においても適用
- **凍結・強制償還**
  秘匿環境においても、発行体が対象の利用者に絞って凍結・強制償還を実行可能

運用性 03

ウォレット・決済事業者が導入しやすく、エンドユーザーも使いやすい

- **既存の署名方式に対応**
  ECDSA (EOA)、ERC-1271、WebAuthn (Passkey)等に対応。既存ウォレットの鍵をそのまま使える
- **ガスコスト効率化**
  ガスコストは主要サービスの1/2〜1/3程度（当社試算）
- **プログラマビリティ**
  秘匿環境内で任意のコントラクトを実装可能。DvP決済、ウォレットの送金ポリシーなどにも対応可能

Copyright © 2026 Datachain, Inc. All Rights Reserved.



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

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「秘匿」ではなく「見せ方の設計」

取引情報を一律に秘匿するのではなく、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**　確認・開示
- **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）

Copyright © 2026 Datachain, Inc. All Rights Reserved.