

# スマートクエスチョニング (Smart Questioning) プライバシーを侵害することなく、 サプライチェーンの可視化 を実現

新しい規制、高まる社会的需要、および技術の進歩により、サプライチェーンにおけるトレーサビリティが不可欠な要件となっているため、企業は現在、持続可能性の主張を証明するために必要な透明性を維持しながら、データのプライバシーを保護するという課題に直面しています。これは、循環的で持続可能なサプライチェーンにより高い信頼性を提供する、分散型ブロックチェーン・サプライチェーン・トレーサビリティ・ソリューションに特に顕著です。

Circulariseは、特許取得済みの「Smart Questioning」ソリューションを開発しました。これは、安全で機密性が高く、スケーラブルな方法で、ブロックチェーン上で検証可能な主張を行う安全な方法を提供します。基本的に、最高レベルのプライバシーと機密性でデータを選択的に共有できます。この記事では、Smart Questioningがどのように機能するか、その利点、およびビジネスへの応用の可能性について説明します。



# 目次

01	Smart Questioningとその利点	04
02	ブロックチェーンを使用する理由	05
03	ゼロ知識証明とは？	07
04	Smart Questioningの仕組み	09
05	まとめ	14

# 01

## Smart Questioning とその利点

サプライチェーンを通じて材料を追跡するための適切な管理モデル([Chain of Custody/CoC](#))を整備することが最初のステップですが、機密情報を危険にさらすことなく関連情報を利用できるようにするにはどうすればよいでしょうか。ほとんどの企業にとって、完全な透明性を持つことは、競争上の優位性を失うことを意味する可能性があるため、推奨されるソリューションではありません。

Smart Questioningを使用すると、パブリックブロックチェーン上のデータのプライバシーと機密性を保護しながら証拠を提供できます。最先端のゼロ知識証明([Zero-Knowledge Proof/ZKP](#))

暗号化技術を使用して、生データではなく証明可能な主張を外部の相手と共有し、サプライチェーンの機密情報の機密性を保持できます。

簡単に言えば、企業は何を誰と共有したいかを簡単に決めることができます。主要なOEMやブランドのサプライヤーである場合、Smart Questioningは次のことを可能にします。

- データのプライバシーと機密性を保護しながら透明性を高める
- さまざまな利害関係者にデータへの柔軟かつ選択的なアクセスを提供する
- 高い信頼性
- 競争上の優位性を維持する

Smart Questioningがどのように機能するかをよりよく理解するには、専門用語とその背後にあるテクノロジーについてももう少し理解することが重要です。用語がわかりにくい場合は、この[ブロックチェーン用語集](#)を参照してください。

# 02

## ブロックチェーン を使用する理由

ブロックチェーンは、循環型経済を実現する主な要因の1つとして注目されてきましたが、誇大広告でも万能薬でもありません。Amazon、IBM、SAP、Microsoftなどの大企業が独自の競争力のあるブロックチェーンサービスを開発していることから、この技術が信頼でき、大きな可能性を秘めていることがわかります。Circulariseでは、このトピックに関する広範な調査と専門家パネルを実施しました。

ブロックチェーンは、公開記録または台帳上の不変の「ブロック」として情報を検証および保存する分散型デジタルデータベースです。パブリックブロックチェーンは、分散化され、システムのネットワーク全体に分散された単一の信頼で

きる情報源として機能するブロックチェーンです。ブロックチェーンに記録されたデータは永続的であり、データを変更または操作することは非常に困難であるため、非常に安全で透過的なシステムになっています。

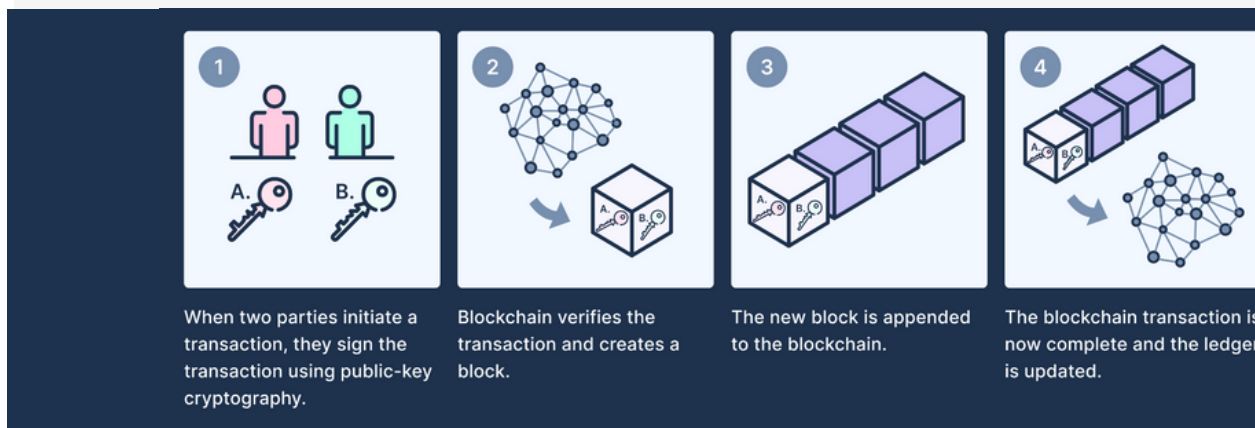


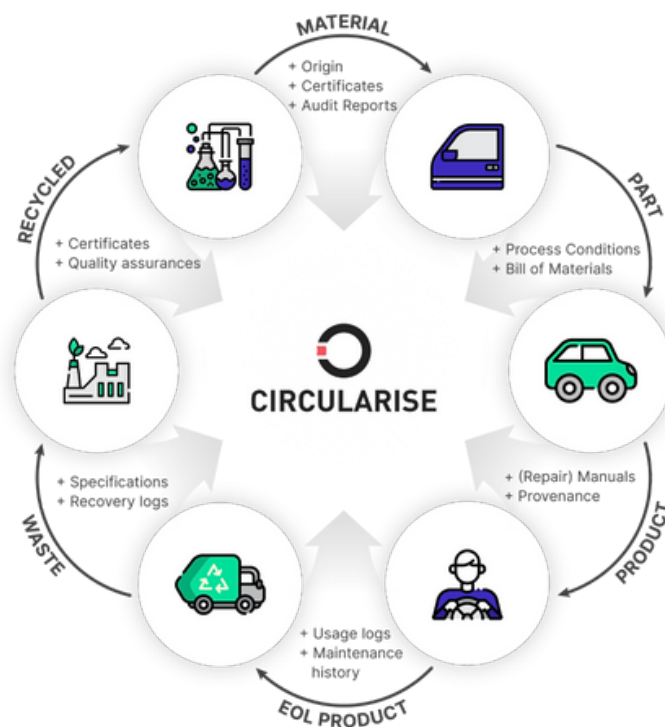
図 1:  
ブロックチェーン トランザクションの作成方法

ブロックチェーンの中心にあるのは、データを安全に送信および保存する方法である暗号化です。

チェーン・オブ・カストディ(生産・流通・加工工程の管理：Chain of Custody /CoC)のトランザクションがブロックチェーンに記録されると、改ざんできなくなり、バリューチェーンパートナーの広大なエコシステムに信頼が構築されます。プロトコルの標準化により、より多くのコラボレーションと透明性を持続可能な製造業にもたらすことができます。

Circulariseのシステムはイーサリアム上に構築されており、最近、**エネルギー使用量を99%削減**しました。証拠の生成と検証には複雑な計算が必要であり、イーサリアムに関連する手数料のコストが増加します。ただし、ブロックで処理されるトランザクションの数をスケーリングすることにより、トランザクションあたりのコストを削減するための追加の取り組みが行われています。

イーサリアムのようなパブリックブロックチェーンは最高レベルの分散化を提供しますが、パブリックブロックチェーンで情報を非公開で機密に保つことは困難です。データを侵害から完全に保護する新しい方法が必要です。私たちは、意図された受信者のみがデータを処理および解読できるようにするゼロ知識証明を実装するSmart Questioningソリューションを開発しました。



# 03

## ゼロ知識証明とは？

ゼロ知識証明(ZKP)は、特定のステートメントが真であるという事実以外の情報を共有することなく、特定のステートメントが真であることを証明者が検証者に証明できる方法です。

私たちのソリューションは、機能がハッシュに非常に似ている暗号化アルゴリズムである Pedersenコミットメントを使用します。これにより、証明者はコミットされた値またはその特定のプロパティを証明できますが、それを明らかにしたり変更したりすることはできません。

これは、ブロックチェーンに保存されているデータのフィンガープリントと考えてください。製品に関する関連データが収集されると、そのデータの一意のフィンガープリントが生成されますが、詳細は明らかにされません。このフィンガープリントにより、製品に関する検証可能なステートメントを作成したり、他のサプライチェーンの利害関係者が特定の質問に対する回答を受け取ったりすることができます。

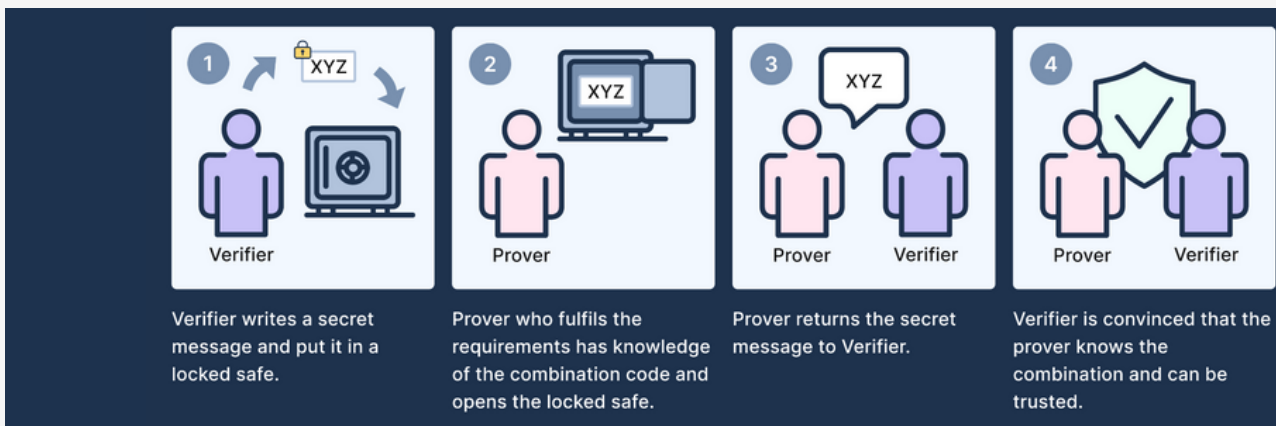
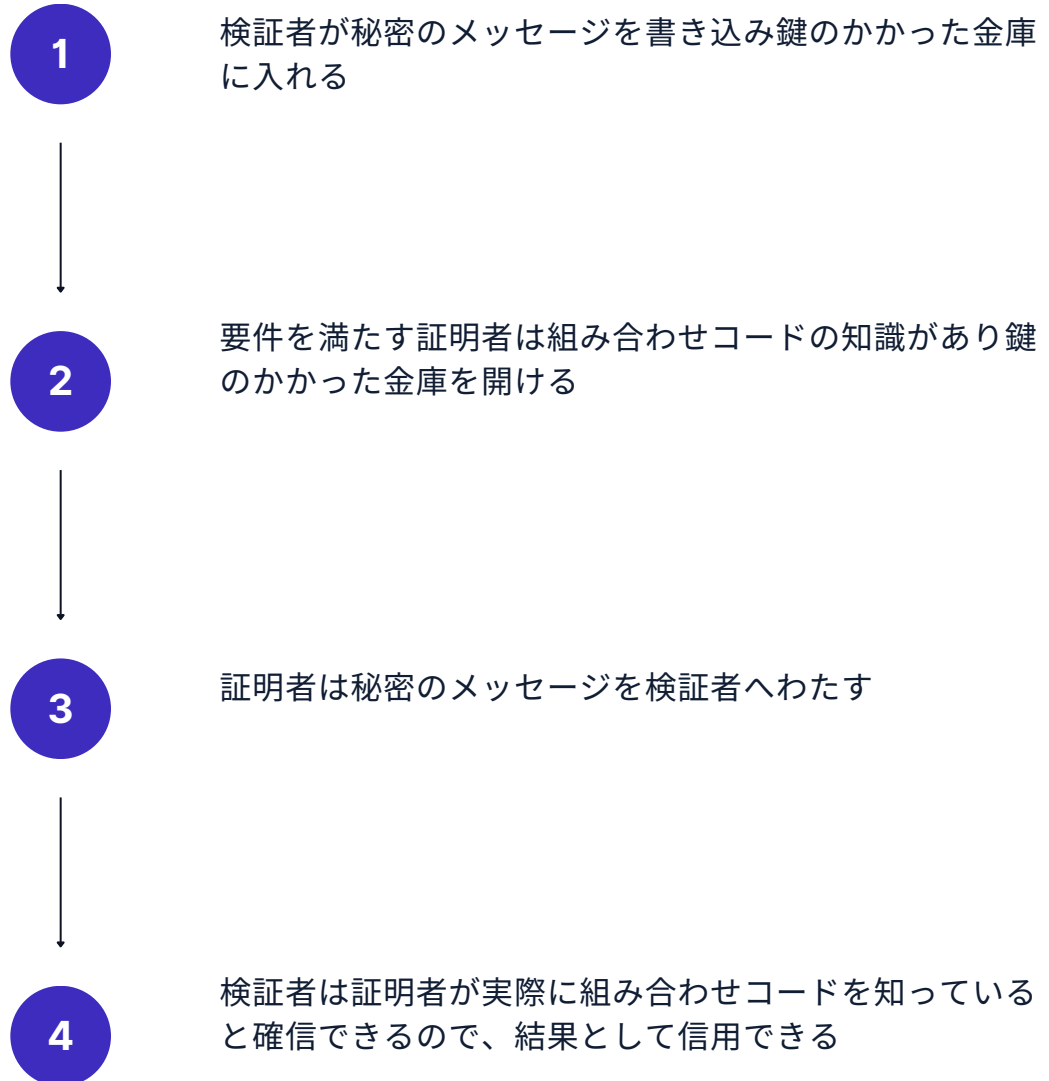


図 2: ゼロ知識証明がどのように機能するかのアナロジー: コードを明らかにせず金庫の組み合わせコードを知っていることを証明する方法

## ゼロ知識証明の仕組み

---

コードを明かさずに金庫の組み合わせコードを知っていることを証明する



# 04

## Smart Questioning の仕組み

バッチを作成するとき、持続可能性の主張に関するデータを一意のフィンガープリントに入れます。つまり、誰でも見ることはできますが、実際のデータは機密に保たれ、改ざんすることはできません。コミットメントは、持続可能性の主張データを使用して計算されたランダムな値です。

誰かが持続可能性の主張の証明を求めると、データを使用してゼロ知識証明が作成されます。質問者は、この証明が持続可能性の主張に関する公開フィンガープリントというだけで、持続可

能性の主張に関するものであるかどうかを確認できます。証明が有効であれば、ゼロ知識証明スキームの数学的保証に基づいて、彼らはあなたの主張を納得することができます。

### 質問リスト

データをバッチに添付する場合:

- サイトデータ
- 製品データ
- バッチデータ

の3つのレベルに分割されます。これらすべてのレベルのデータポイントを質問リストに含めることができます。

**質問リスト**は、認証、規制、業界の需要、およびサプライヤーの要件に関する質問のカテゴリーです。

## スマートな質問とは？

---

Smart Questioningは、機密データを開示することなく製品に関する関連情報を取得するために、検証者(ブランド所有者など)が証明者(サプライヤーなど)から慎重に精選された一連の質問を行えるように設計されたCircularise独自の技術です。

質問リストへのアクセスを許可することで、どの質問を開示するかを制御できます。テンプレートまたはバッチを作成するときは、質問リストを選択する必要があります。質問リストの選択に基づいて、特定のデータポイントが開示されます。

コミットメントがバッチに関するデータで満たされている場合、質問リストをサポートできます。このリストでは、質問にはさまざまな開示レベルがあります。



### 完全な開示

承認された組織へのデータの完全な開示  
(例) メーカー名



### パブリック

データはブロックチェーンに保存されます  
(例) 重量と資産タイプ



### Range Proof

基礎となるデータを開示することなく、特定の中身のみを開示します  
(例) 水銀の濃度は0.001%を超えていません



### 開示なし

データの開示なし  
(例) 外部と共有されないコミットメントのデータ部分



### セットメンバーシップ

データが事前定義されたリストの一部である(ない)ことを開示します  
(例) 住所は紛争地域の一部ではありません

Smart Questioningを使用すると、共有するデータと回答の開示レベルを正確に選択できます。一連の管理、認証、プロセス、バッチ、LCAデータ、化学組成、および調達に関する詳細を含めることができます。チェーン全体と特定のバッチに関する関連情報、およびデータの視覚的表現を便利に表示できます。

以下は、Circulariseにすでにセットアップされているサプライヤー A と OEM B の 2 つの当事者の間の非常に単純な対話を表しています。

## Smart Questioningのプロセス

---

- 01** サプライヤー A は、質問リストに質問を設定し、選択した開示レベルで回答します

---

- 02** サプライヤー A は、GHG プロトコル、TfS CRS、ISO、またはその他の基準への準拠を示す文書をバッチに添付します

---

- 03** これにより、ブロックチェーンに保存されるコミットメントが生成されます

---

- 04** サプライヤー A は OEM B に関連する質問リストへのアクセスを許可します

---

- 05** OEM B は、質問リストでサポートされている質問のリストを確認できます

---

- 06** OEM B は、質問リストから質問を選択します

---

- 07** サプライヤー A は、合意された開示レベルで回答を提供し、それを証拠でサポートします

---

- 08** Smart Questioning はコミットメントを取得し、証拠を検証します

このようにして、OEM B は、サプライヤー A の主張が真実であり、証拠によって裏付けられていることを信頼できますが、サプライヤー A は機密データを放棄する必要はありません。

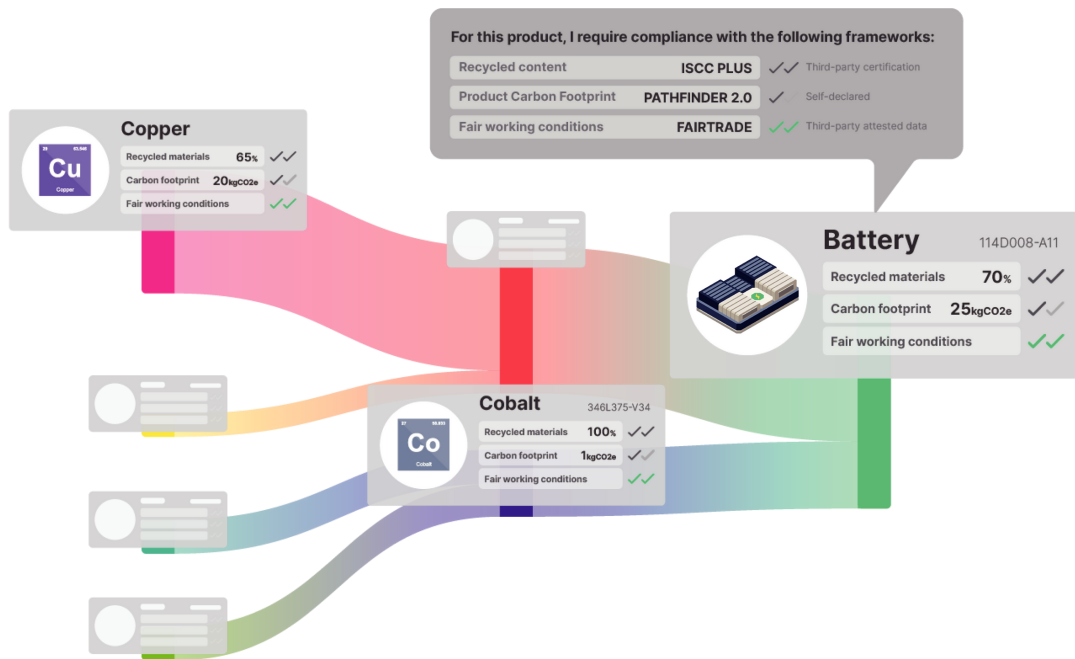


Figure 3:  
スマートな質問と回答

## Smart Questioningは実生活でどのように機能しますか？

ここでは、さまざまな業界におけるスマートな質問、開示タイプ、および回答の例をいくつか紹介します。

### バッテリー産業

**スマートな質問 [Range Proof]:**  
水銀濃度は0.001%に達していますか？

**回答:** いいえ、水銀濃度は0.001%未満です

### エレクトロニクス産業

**スマートな質問 [Range Proof]:**  
製品には鉛(Pb)が含まれていますか？

**回答:** いいえ、製品に鉛(Pb)は含まれていません

### エレクトロニクス産業

**スマートな質問 [セットメンバーシップ]:**  
タングステンはDRC(コンゴ)地域から調達されていますか？

**回答:** いいえ

### プラスチック産業

**スマートな質問 [[範囲証明]:**  
主要な化石物質の含有量は25%未満ですか？

**回答:** はい、一次化石の含有量は25%未満です

### プラスチック産業

**スマートな質問 [セットメンバーシップ]:**  
製品には臭素が含まれていますか？

**回答:** いいえ

### あらゆる業界

**スマートな質問 [範囲証明]:**  
製品の1kgあたりの二酸化炭素排出量は3kg CO2換算を超えていますか？

**回答:** はい

## Smart Questioningはどのようなメリットをもたらしますか？

これは、ライフサイクルアセスメント(LCA)を共有したり、サプライヤーとメーカーの間で製品のスコア3 排出量に関する内容を共有したりするなど、企業間で最も役立ちますが、ブランドはSmart Questioningを使用して消費者と関わることもできます。

顧客はQRコードをスキャンして、製品の持続可能性の主張を確認し、個人の価値観に基づいて詳細を確認できます。たとえば、製品の環境への影響について質問したり、児童労働のない場所で製造されたものかどうかを質問したりできます。

Circularise が**ポルシェ**のサプライチェーンでの認知度向上にどのように役立ったかについては、こちらの記事をご覧ください。

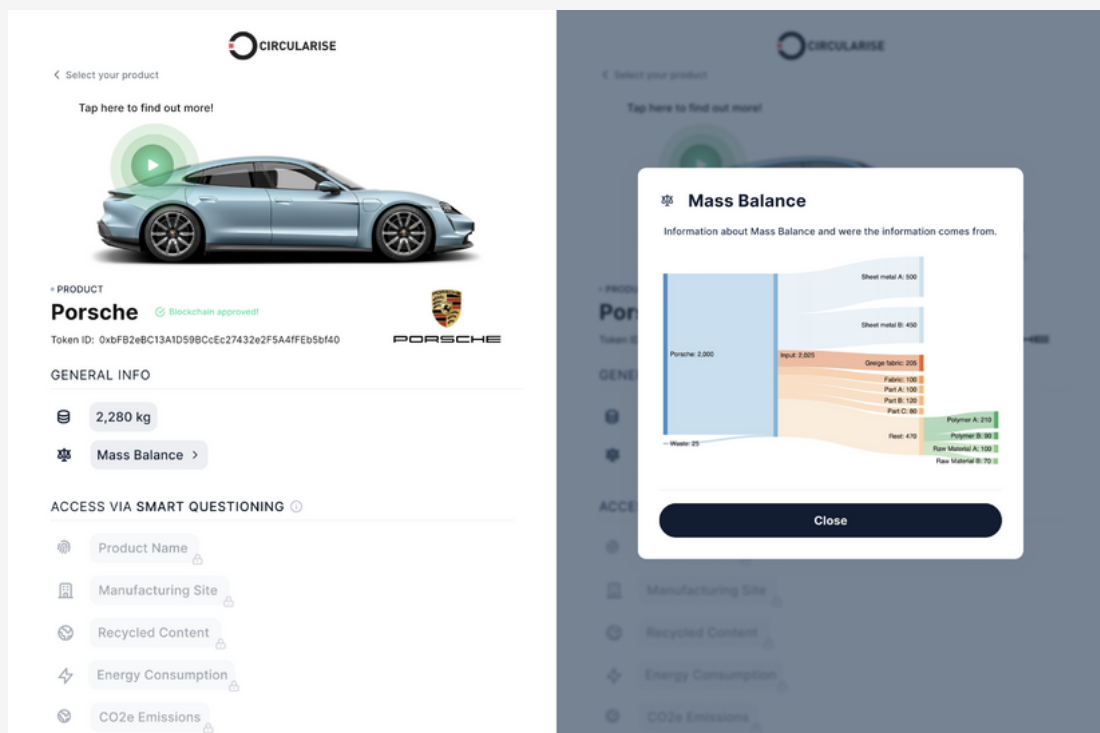


図 4: サプライチェーンで利用可能な情報のダッシュボード

**要約すると、Smart Questioning :**

- ユーザーのデータを安全な方法で保存および管理
- ブロックチェーンに保存されるフィンガープリントを生成
- 機密データとトランザクションを管理
- 質問し、回答を保存し、検証
- 証拠を提示して質問に回答

Smart Questioningの背後にある最先端のテクノロジーは、サプライチェーン全体で機密性を損なうことなく、柔軟な透明性をもたらします。パートナーと消費者の間に信頼を築き、持続可能な調達と生産を奨励し、取引の検証にかかる時間とコストを削減できます。



[ドイツのサプライチェーン法、バッテリーパスポート規則、企業持続可能性報告指令 \(CSRD\)、デジタルプロダクトパスポート](#)など、サプライチェーンのデューデリジェンスを対象とした新しい法律により、より多くの業界や企業が、サプライチェーンでのアプリケーションのためにブロックチェーンテクノロジーに目を向けています。

Circulariseが提供するソリューションは柔軟で、企業のニーズに合わせて完全にカスタマイズできます。機密情報を危険にさらすことなく、Circulariseが企業の持続可能性の主張を証明する方法について詳しく知りたいですか？

## お客様の声をご紹介します

“

Circularise とそのパートナーの協力を得て、原材料の生産から最終的な自動車に至るまで、プラスチックの特定のケースを数多くトレースすることができました。



Antoon Versteeg  
イノベーションリサーチ  
プロジェクトリード  
Porsche

“

Circularise などのメンバーによる貢献で Catena-X は今日の自動車業界の最も困難な課題を解決する最高のネットワークとなっています。



Oliver Ganser  
オートモーティブネットワーク  
取締役会長  
Catena-X

“

私たちは Circularise をグローバルバッテリーアライアンスに迎え入れ、バッテリーパスポートを重要な手段として循環性、環境保護、持続可能な開発という共通のビジョンを推進できることを嬉しく思います。



Inga Petersen  
エグゼクティブディレクター  
Global Battery Alliance

## ご感想をお寄せください

サプライチェーンにおけるトレーサビリティの向上については、  
今すぐお問い合わせください

# 免責事項

本書は、明示または黙示を問わず、いかなる種類の表明、保証または条件（本書の特定の目的または使用に対する適合性、商品性、または第三者の知的財産権の非侵害に関する黙示の保証または条件を含むが、これらに限定されない）もなしに提供されています。Circulariseは、本書に掲載されている情報の正確性、完全性、最新性を保証するものではありません。Circulariseは、本書が適用される法令、規則、規制を遵守していることに関して、いかなる表明も保証も行いません。

Circularise、その社員、子会社、関連会社、またはその従業員、取締役、役員は、いかなる場合においても、特別損害、結果的損害、収入損失、業務中断、データ損失、その他の直接的、間接的、付随的損害、負傷、損失、費用、経費について、その原因の如何を問わず、責任を負うことはありません。データの損失または破損、その他の商業的または経済的損失など、契約、不法行為（過失を含む）、またはその他の責任理論に基づくかどうかにかかわらず、本書へのアクセスまたは所有または使用から生じる、そのような損害、負傷、損失、コスト、費用の可能性についてCirculariseが通知されていたとしても、一切の責任を負わないものとします。

本書の発行および利用可能な状態において、Circulariseはいかなる個人または団体のために、またはその代理として専門的またはその他のサービスを提供すること、あるいはいかなる個人または団体が他の個人または団体に対して負う義務を履行することを引き受けるものではありません。本書の情報は、その内容を使用し適用するのに適切な経験を有する方を対象としており、Circulariseは本書に含まれる情報の使用または信頼から生じるいかなる責任も負いません。



# 循環型経済のための トレーサブルサプライチェーン

Circulariseのソフトウェアシステムは、化学・プラスチック、バッテリー原料、金属、その他の業界のサプライヤーが、機密情報を危険にさらすことなく、部品表や環境データなどの原料データを追跡・共有できるように支援します。

さらに、ブランドやOEMがサプライチェーンを監視し、自社のスコープ3排出量を可視化し、来るべきデューデリジェンス規制を遵守し、事業活動において循環型経済を実現できるように支援します。

[WWW.CIRCULARISE.COM](http://WWW.CIRCULARISE.COM)