CordaTechMeetup(夏の陣)

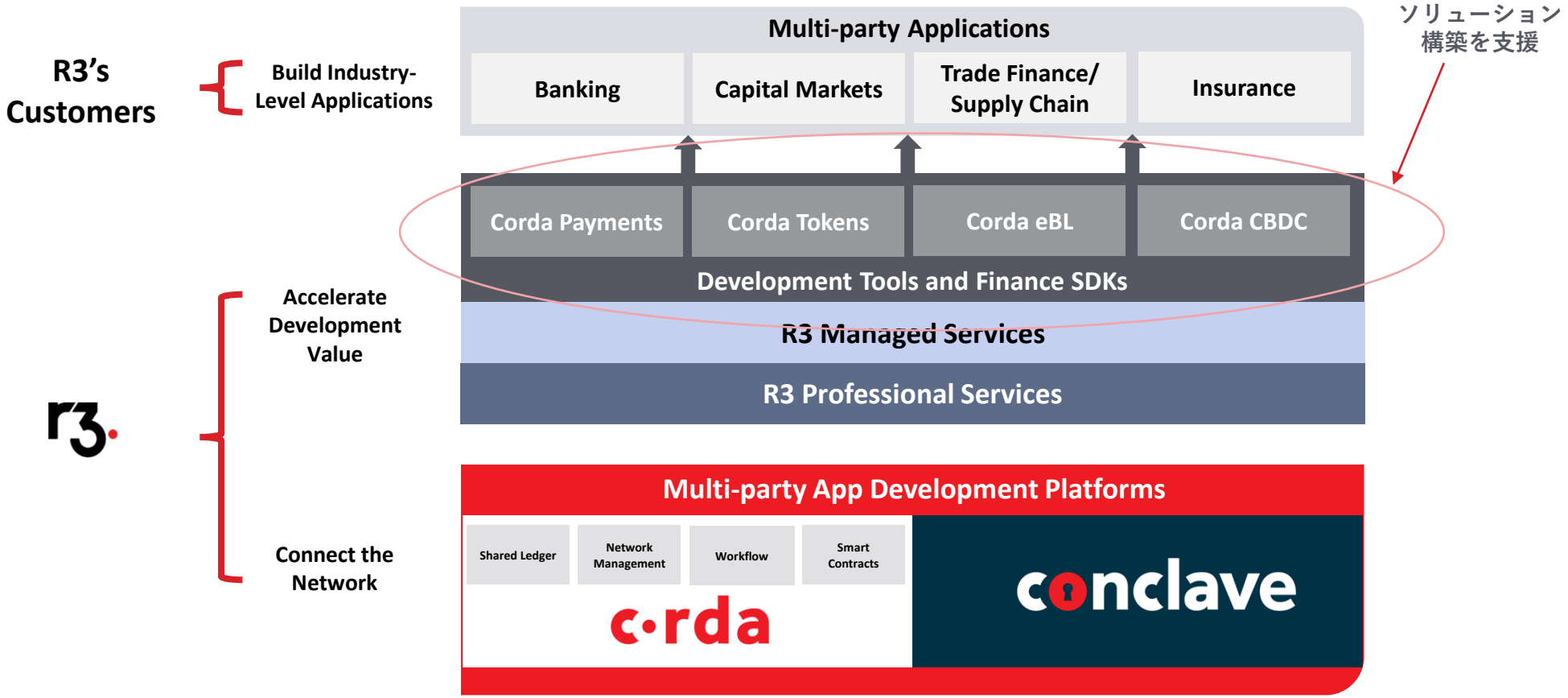
SBI R3 Japan

最後に。。
～R3のソリューションと次回予告～

2021/08/25

SBI R3 Japan株式会社
ビジネス開発部

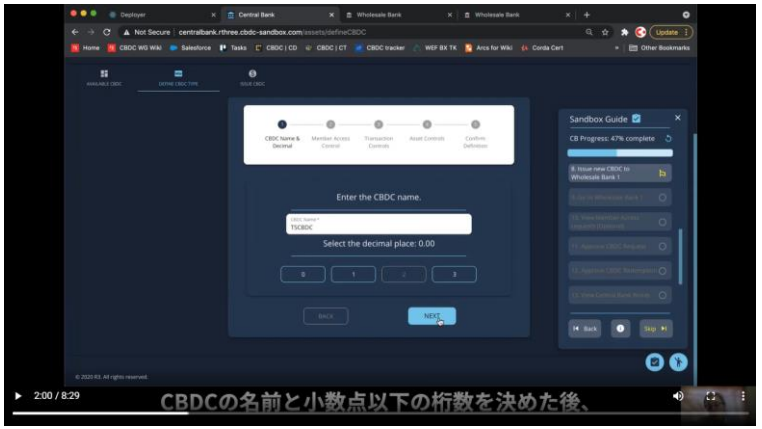
Cordaを基盤とした、ソリューション展開概要



SBI R3 Japan

CBDCサンドボックス

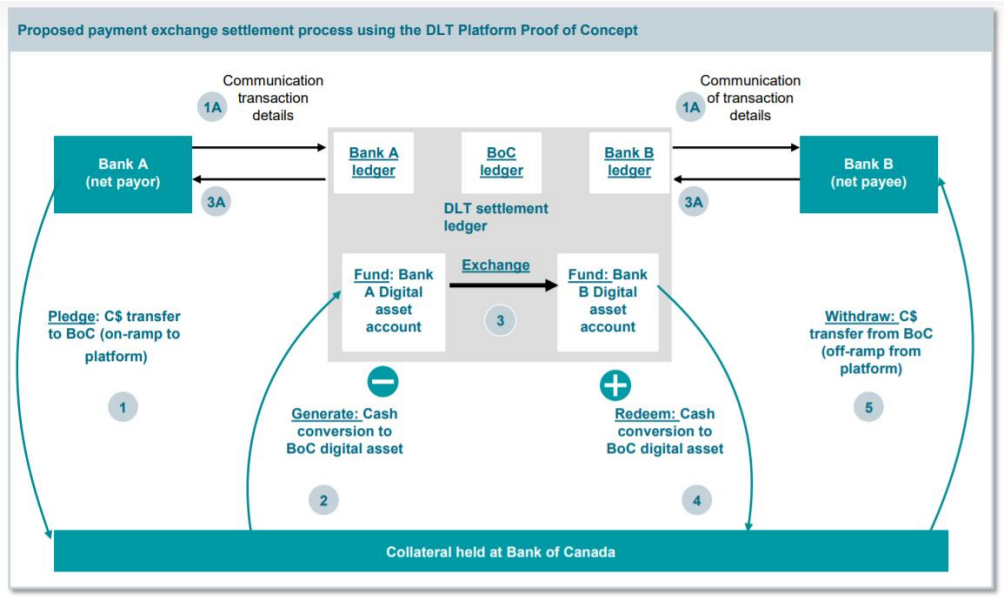
- 現金からデジタル通貨への移行を検証
- プログラムマネーを検証
- デジタル通貨同士の相互運用性を検証
- 決済業務の効率化ができるか
- ステーブルコインの発行



機能概要

- POC as-a-service
- ホールセール銀行間取引
- リテール取引ネットワーク
- 実際の環境をエミュレートするテストスィート
- ステーブルコイン拡張機能
- 開発者の拡張性を高める商用SDK

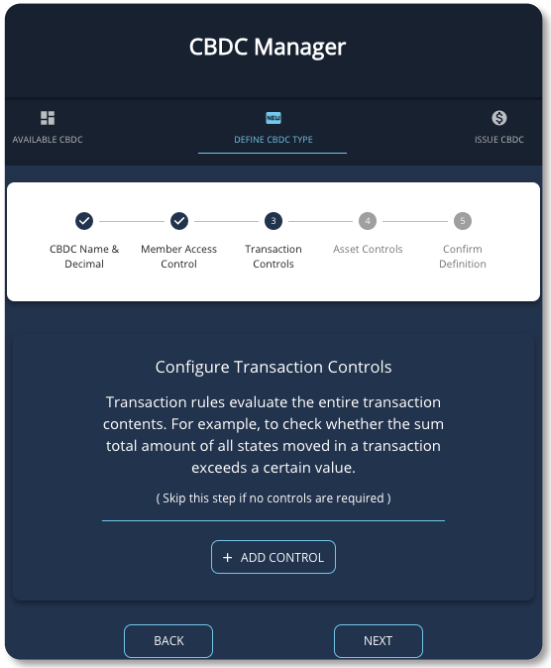
- 発行、償還、プッシュ・プル取引
- アクセスコントロール、アセットコントロール、トランザクションコントロール
- カウンターパーティプライバシー、オペレータープライバシー
- 財務管理、レポーティング
- アトミック DvP と PvP



SBI Japan

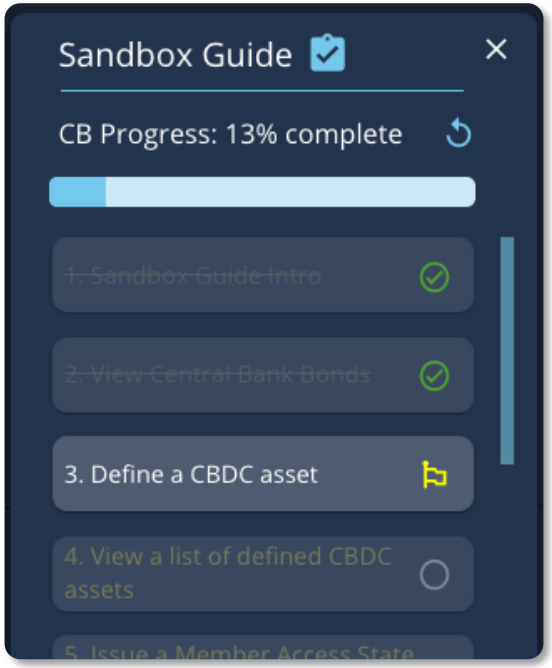
学べるセルフスタディ方式！

Intuitive Controls



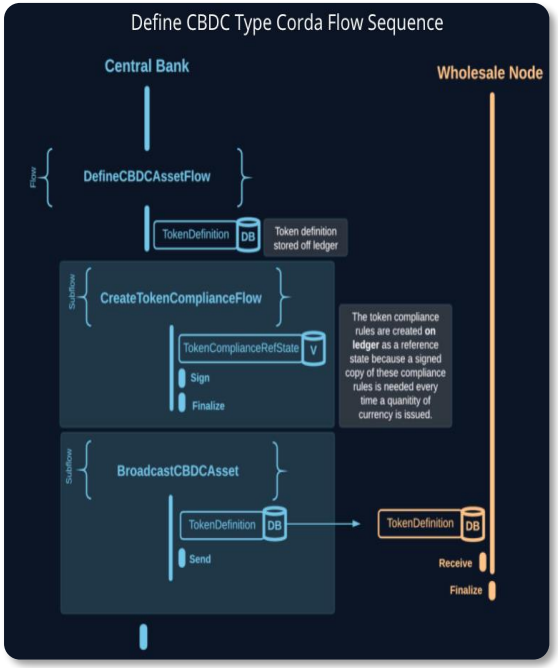
Easy to use controls allow those unfamiliar with the technology to understand its impact

Pop-up Instruction



"Double click" into any decision you make in the sandbox and reveal what it means beneath the surface

Detailed Documentation



Dedicated DocSite that fully explains the code behind the sandbox and how to build upon the Demo CorDapps

Conclave

サービスプロバイダーやクラウドベンダーからデータを保護したまま処理を実行

- ✓ Conclaveは、秘密計算を行うためのハードウェアであるIntel SGXに、アプリケーションの安全な実行環境(TEE)の実装を容易にするSDK(Software Development Kit)
- ✓ ホストアプリケーションの内部にEnclaveという隔離領域を作り、処理を実行
- ✓ 秘匿データにアクセスできるのはこの内部プログラムだけなので、サービスプロバイダーやクラウドベンダーなどからは見えない。またプログラム自体の改ざん不可

秘密計算を実現！

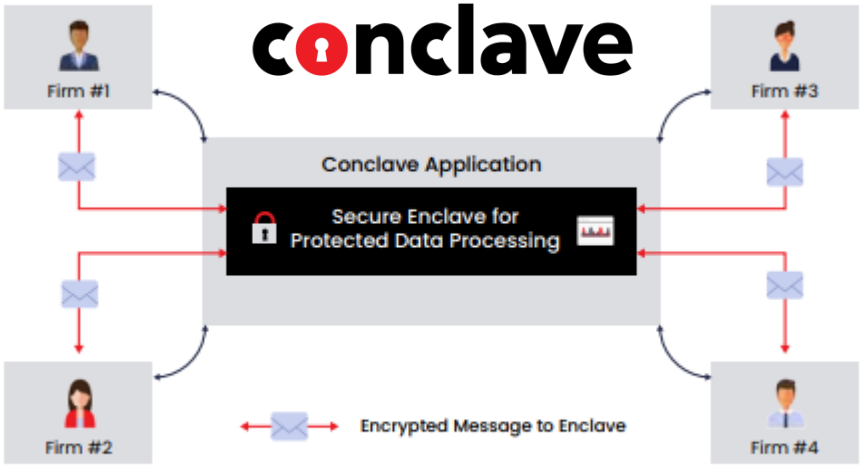


Figure 1: Multi-party data pooling

Conclave公式サイト：リンク

Conclaveの長所

種類		概要	課題
ソフトウェアによる秘密計算	ゼロ知識証明 (ZKP)	✓ データを公開することなく、データへのアクセス権を持つ事を証明する	• 計算能力への高い要求 • スケーラビリティ • 実装が難しい（任意のアルゴリズムを実装できるわけではない）
	準同型暗号化 (HE/FHE)	✓ 部分準同型暗号(HE) ✓ 完全準同型暗号(FHE)	• 計算コストが高い（クラウド移行すら厳しい） • 完全準同型暗号は、平文操作の除外が難しく、ユースケースに制限
	ｾｷｭｱ･ﾏﾙﾁ･ﾊﾟｰﾃｨ･ｺﾝﾋﾟｭｰﾃｰｼｮﾝ (sMPC)	✓ 各当事者がデータの断片だけを保持する「秘密の共有」に依存 ✓ バラバラのデータの一部が知られても元のデータは秘匿可	• ユースケースごとのカスタムアルゴリズム構築 • 高い通信コスト／高い計算コスト
ハードウェアによる秘密計算		✓ ハードウェア依拠 ✓ **様々なアルゴリズムに対応** ✓ コード実行とメモリを他から分離する ✓ TEE(Trusted Execution Environment)を構築	• 低レベル言語や暗号技術に対する専門知識が必要 **conclave** で実装を容易に

次回予告

- 11月中旬（？）予定
- ご紹介したR3社のソリューションデモ（？）
- Corda5 新着情報！（仮）

Corda開発パートナー募集中！！！

～Win-Winな関係を築きましょう～

次回も何卒よろしくお願い申し上げます！

SBI R3 Japan