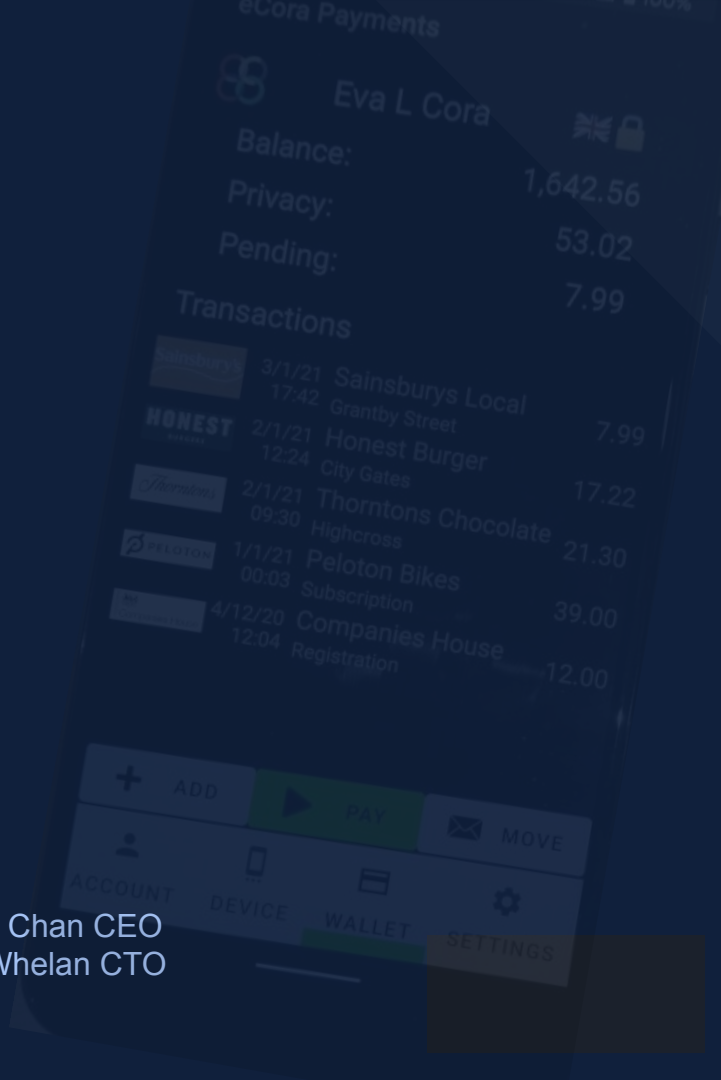
eCora

eCora Design

Programmable Money Platform for CBDCs and Stablecoins

Secure, Scalable, Resilient



eCoraDLT Limited
Leicester, UK

David Chan CEO
Tom Whelan CTO

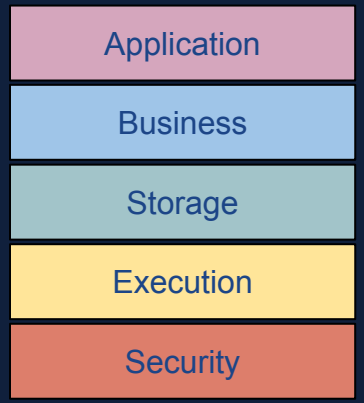
Design Deck
Mar 2022

Introduction

- Programmable money platform
  - Programmable via Smart Contracts
  - Platform is a full stack containing UI, wallet, custody, smart contracts, blockchain and secure hardware
- Full software stack that is
  - Secure - uses Confidential Computing to authorise everything
  - Scalable - uses highly scalable Edge Computing paradigm
  - Resilient - flat, decentralized Blockchain architecture
- Uses a single unified stack
  - Runs the same stack on IoT, Smartcard, Phone, Laptop or Server
  - Every stack instance has the same role and function

eva@eCoraDLT.com

eCora Stack Layers



Application Layer - Contains user application and navigation

Business Layer - Contains transaction processing and management

Storage Layer - Contains Edge Computing storage and controls

Execution Layer - Contains Smart Contracts and permissions

Security Layer - Contains Confidential Computing and secrets

- Stacks usually have the Execution Layer as the bottom layer
- eCora has the Security Layer as the bottom layer

eCora

eva@eCoraDLT.com

First Core Principle: Security

- eCora's Security Layer is built using Confidential Computing
- Confidential Computing is provided by security hardware in the CPU
- Provides secure functionality that is the hardest to hack

- eCora Secure Layer is the base layer of the stack so that
  - Everything in the stack must go through it
  - It controls everything happening in the stack
  - It cannot be bypassed

eva@eCoraDLT.com

Second Core Principle: Scalability

- Edge Computing is the next paradigm after Cloud Computing
- Leverages CDNs which have been around for decades
- Edge Computing is the most scalable infrastructure in existence

- eCora is written as Edge native code (using Rust/WebAssembly)
  - Data is stored encrypted on CDNs
  - CDNs act as a fast global cache
  - API calls out to Edge are always served by nearest location

eCora

eva@eCoraDLT.com

Third Core Principle: Resilience

- A flat, decentralized node architecture is the most resilient
- No specialist servers exist e.g. validators, coordinators, etc
- No centralised locations to attack so minimal attack surface

- eCora's stack is designed as one unified stack
  - Every node instance behaves the same
  - Nodes with elevated privileges aren't required
  - Efficient enough to run on lower powered edge devices

eva@eCoraDLT.com

Application Features

- Key Management and Recovery
  - No 3rd party wallet solution required
- Custody and Delegation
  - No 3rd party custody solution required
- Supports multi-ledgers and tiered-ledgers
  - Different currencies/tokens, DvP, PvP
- Inter-ledger processing
  - Cross-border payments

eva@eCoraDLT.com

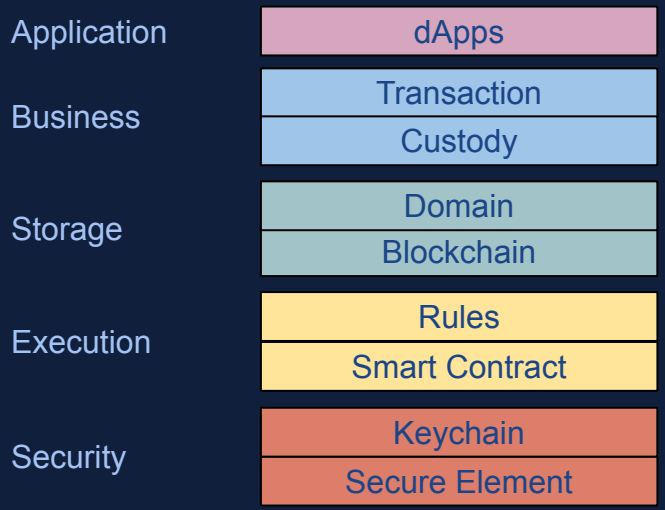
Technical Features

- Efficient blockchain and consensus
  - Different architecture means no mining is required
- Single consistent execution paradigm
  - Everything is a smart contract (e.g. blockchain algorithm)
- Zero Trust applied to the next level
  - Applied to individual request and execution events

eCora

eva@eCoraDLT.com

eCora Stack Overview

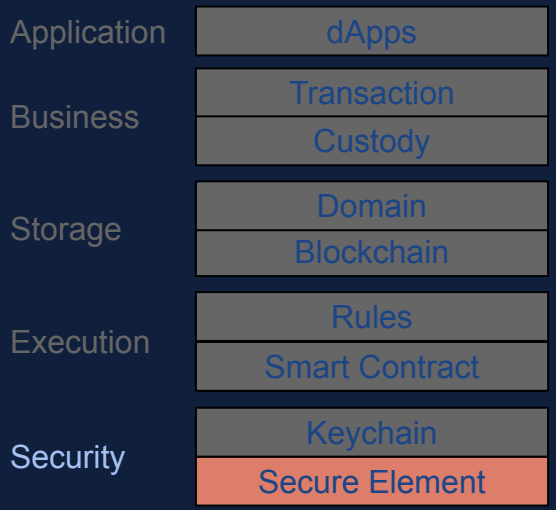


The following pages describe each component starting at the bottom (Secure Element)

eCora

eva@eCoraDLT.com

Security: Secure Element



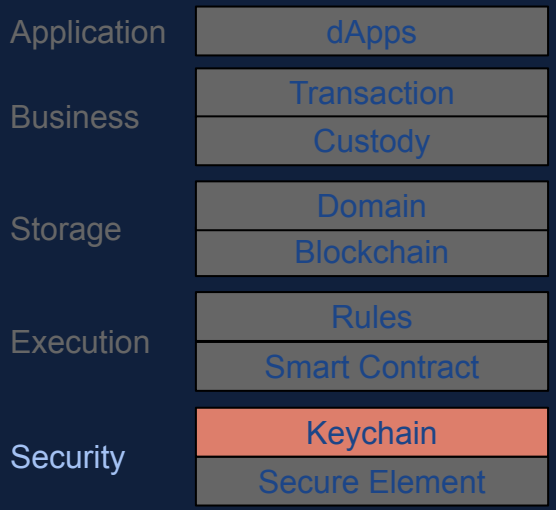
- Secure Element is hardware
  - Located in CPU silicon block
  - Random key fused in during manufacture
  - Manufacturer does not know key
  - Key never leaves Secure Element
  - Keys can be attested to see if they are fake

- eCora uses the Secure Element for every action
  - We use unextractable keys
  - Every action in our stack is always signed
  - Signatures from other instances can be attested

eCora

eva@eCoraDLT.com

Security: Keychain



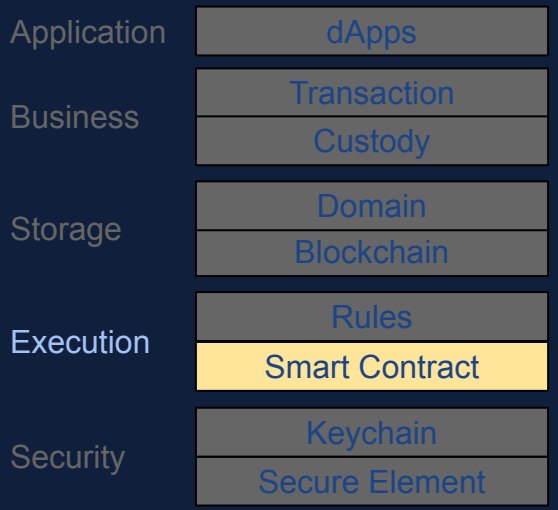
- Keychain manages keys and chains of custody
  - Attested public keys may come from other nodes
  - Every key's origin must be checked
  - Provides the key for signatures and encryptions

- eCora Keychain provides all key management functions
  - Because we use unextractable private keys, eCora can't be used with 3rd party wallets
  - Manages keys for user across all their devices
  - Provides account recovery functions

eCora

eva@eCoraDLT.com

Execution: Smart Contract



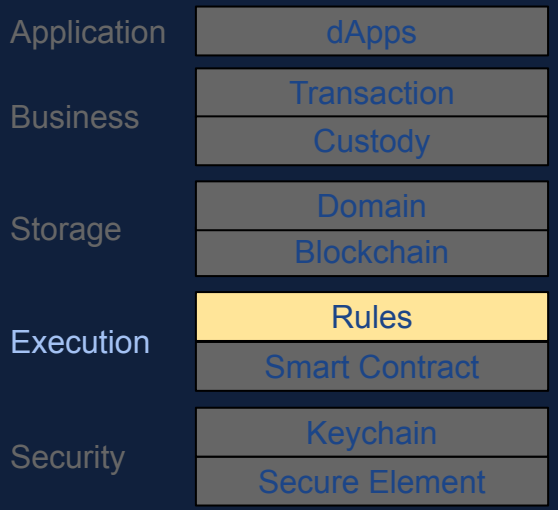
- Smart Contract executes all functionality
  - Stack has a single consistent execution system
  - Everything is written as Smart Contracts
  - The stack itself is written as Smart Contacts

- eCora Smart Contracts have additional security
  - Stores all counterparties with the contract
  - Transaction counterparties must be assigned when a new contract is created
  - Only assigned counterparties can execute functions
  - Counterparty can be defined as an organisation which is a group of users

eCora

eva@eCoraDLT.com

Execution: Rules



- Rules are special smart contracts applied at execution
  - Rules are assigned to customers and merchants
  - They execute alongside the smart contracts
  - Different customers will have different rules

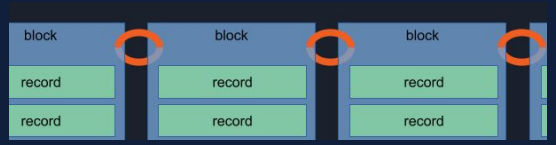
- Rules are a way to add account specific processing
  - Can be used to apply extra validation depending on the customer/merchant
  - Can be used to apply different fees or discounts depending on the customer/merchant
  - For example, a merchant may have signed up for fraud payment protection insurance that requires a small fee added to each payment

eCora

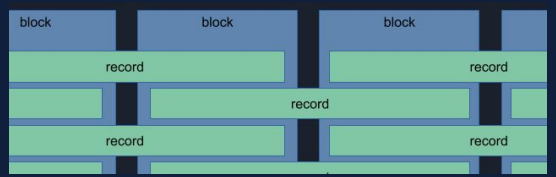
eva@eCoraDLT.com

Storage: Blockchain

Application	dApps
Business	Transaction
	Custody
Storage	Domain
	Blockchain
Execution	Rules
	Smart Contract
Security	Keychain
	Secure Element



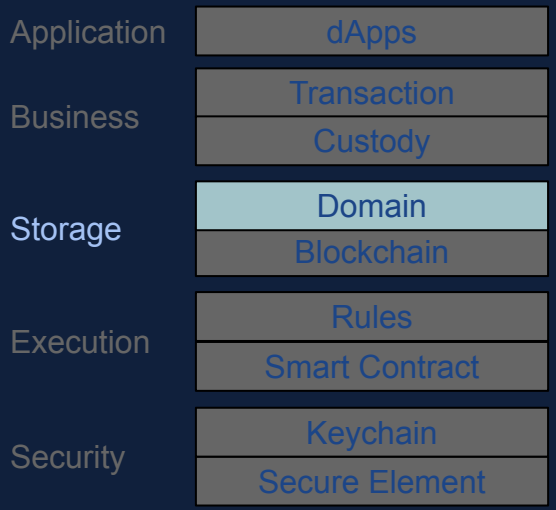
- Blockchain is a secure way to store a history of events
  - The storage is immutable and hard to tamper
  - Blocks are chained together (see above)
  - This chaining can be expensive or complex
- eCora uses our Patent Pending chaining method
  - We use the transactions themselves to chain the blocks together (see below)
  - No mining required but still very secure
  - Very fast, low energy and lightweight



eCora

eva@eCoraDLT.com

Storage: Domain



- A Domain is an independent ledger
  - A domain will have its own governance
  - It can have its own currency, rules, and smart contracts
  - It can also be used for DvP, PvP

- eCora is a multi-ledger system
  - A ledger is managed and owned by a domain
  - Different domains are totally independent of each other but cross domain transaction can be done
  - Each CBDC would be a different domain with each Central Bank specifying the rules for their domain
  - Sub-domains are available for multi-tiered systems

eCora

eva@eCoraDLT.com

Business: Custody

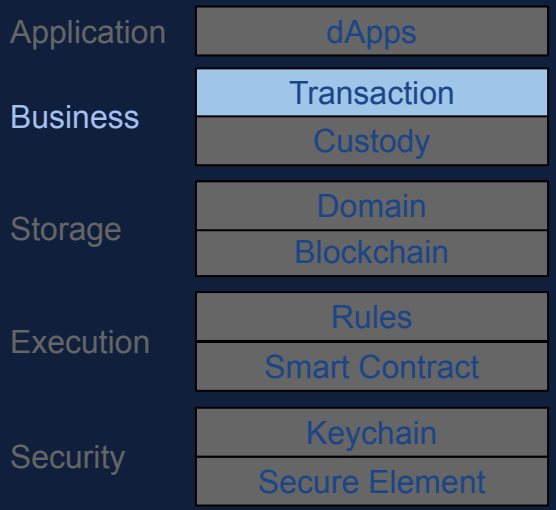
- Custodian manage accounts on behalf of customers
  - Customer can assign a custodian to do transactions for them
  - However, in today's world, a custodian may not actually provide the full service themselves

- eCora extends custody to include outsourcing
  - A custodian may outsource part of their service to another custodian
  - The outsourcing could be many levels deep
  - We track all these levels and can check whether a person many levels away is allowed to execute a function on behalf of a customer
  - Because of the way we check counterparties, eCora cannot be used with 3rd party custody solutions

eCora

eva@eCoraDLT.com

Business: Transaction



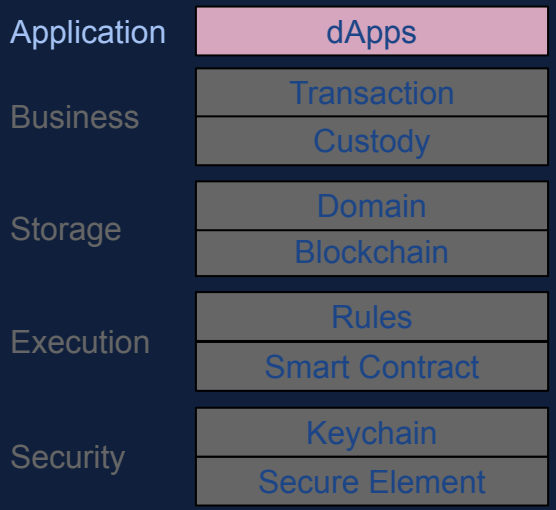
- Transaction can be online, offline, or off-ledger
  - The use of a Secure Element opens up the possibility of doing offline and “ledgerless” transactions
  - Some domains may want this facility for low value transactions

- eCora manages the recording of transactions
  - Provides offline transaction capability backed by the Secure Element that can be synced later
  - Provides different forms of ledgerless transactions
  - Automatically manages the account balance

eCora

eva@eCoraDLT.com

Application: dApps



- dApps are decentralised applications
  - Web or mobile applications
  - All data is processed through smart contracts
  - All security handled by the stack

- eCora allows programmers to develop apps in two ways
  - Via SDK where the UI is outside eCora. The eCora Stack can be called to process transactions
  - Via WebApp where the UI is inside eCora. Simple web applications can be stored directly in eCora (stored on the CDN)

eCora

eva@eCoraDLT.com