Confidential Transactions
Theory Justification

Iftach Haitner[*]

July 23, 2025

Abstract

[**Iftach's Note: TODO**]

Contents

1 Introduction **2**

2 Preliminaries **2**

2.1 Notation 2

3 The Confidential Transaction Protocols **3**

3.1 The Ideal Functionality 2

3.2 The Protocol 3

[*] Stellar Development Foundation. E-mail: `iftach.haitner@stellar.org`..

1 Introduction

[**Iftach's Note:** **TODO**]

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables, and lowercase for integers and functions. Let $\mathbb{N}$ denote the set of natural numbers. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$. For a relation $\mathcal{R}$, let $\mathcal{L}(\mathcal{R})$ denote its underlying language, i.e., $\mathcal{L}(\mathcal{R}) := \{x \colon \exists w \colon (x, w) \in \mathcal{R}\}$.

3 The Confidential Transaction Protocols

3.1 The Ideal Functionality

Functionality 3.1 ($\mathcal{F}_{\mathsf{ConfTrans}}$: Confidential transactions)**.**

Parties: Issuer I, Chain C and users $\mathsf{U}_1, \ldots, \mathsf{U}_n$.

Init. Upon receiving init from all parties:

1. For each $i \in [n]$: set $\mathsf{balance}_i, \mathsf{balance}_i^{\mathsf{tmp}} \leftarrow 0$.
2. Set $\mathsf{log} \leftarrow \emptyset$.

Issue. Upon receiving $(\mathsf{sid}, \mathsf{issue}, x, d)$ from V and I:

1. Assert($x \in \mathbb{N}$ and $d \in [n]$).
2. $\mathsf{balance}_d^{\mathsf{tmp}} \mathrel{+}= x$.
3. Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{issue}, x, d)$.

Transfer. On call $(\mathsf{sid}, \mathsf{transfer}, d)$, by C and U_s, with U_s holding private input x.

1. Assert($x \in \mathbb{N}$, $\mathsf{balance}_s \geq x$ and $s, d \in [n]$).
2. $\mathsf{balance}_s \mathrel{-}= x$.
3. $\mathsf{balance}_d^{\mathsf{tmp}} \mathrel{+}= x$.
4. Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{transfer}, s, d)$

Update. Upon receiving $(\mathsf{sid}, \mathsf{update})$ from party P_i and C: C

1. Set $\mathsf{balance}_i \mathrel{+}= \mathsf{balance}_i^{\mathsf{tmp}}$.
2. Set $\mathsf{balance}_i^{\mathsf{tmp}} \leftarrow 0$.

3. Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{update}, i)$

History. Upon receiving $(\mathsf{sid}, \mathsf{history})$ from party P_i and C: Send log to P_i.

[**Iftach's Note: TODO**

1. **Should the receiver be part of the call in which it gets money.**
2. **Auditor?**

]

3.2 The Protocol

Protocol 3.2 ($\Pi_{\mathsf{ConfTrans}}$: Confidential transactions)**.**

Parties: Issuer I, Chain C and users $\mathsf{U}_1, \ldots, \mathsf{U}_n$.

Paramters: 1^{κ_c}.

Subprotocols: See below.

Protocol 3.3 ($\Pi_{\mathsf{ConfTrans}}$.Init)**.**

Participating parties. All parties.

Operation:

1. P_i, for all $i \in [n]$,
   (a) Set $(pk_i, sk_i) \overset{\text{R}}{\leftarrow} \mathsf{KeyGen}(1^{\kappa_\mathsf{c}})$.
   (b) Store sk_i.
   (c) Send pk_i to all parties.
2. All parties store $\{pk_i\}_{i \in [n]}$.
3. C:
   (a) For all $i \in [n]$: Set $B_i, B_i^{\mathsf{tmp}} \overset{\text{R}}{\leftarrow} \mathrm{Enc}_{pk_i}(0)$.
   (b) Set $\mathsf{log} \leftarrow \emptyset$.

Protocol 3.4 ($\Pi_{\mathsf{ConfTrans}}$.Issue)**.**

Participating parties. I and C.

C's input. $x \in \mathbb{N}$ and $i \in [n]$.

Operation:

1. I: Send (x, i) to C.
2. C: Set $B_i^{\mathsf{tmp}} \mathrel{+}= \mathrm{Enc}_{pk_i}(x)$.

3. C: Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{issue}, x, i)$.

Protocol 3.5 ($\Pi_{\mathsf{ConfTrans}}$.Transfer)**.**

Participating parties. P_s and C.

Proof's systems: $\Pi^{\mathsf{pos}}.\Pi^{\mathsf{lrg}}$

Common input. $d \in [n]$.

P_s's private input. $x \in \mathbb{N}$.

Operation:

1. P_s:
   - (a) $X \overset{\mathrm{R}}{\leftarrow} \mathrm{Enc}_{pk_d}(x; r)$ for $r \overset{\mathrm{R}}{\leftarrow} \{0,1\}^{\kappa_{\mathsf{c}}}$.
   - (b) $\pi^{\mathsf{pos}} \overset{\mathrm{R}}{\leftarrow} \mathsf{P}^{\mathsf{lrg}}((pk_d, X), (x, r))$.
   - (c) $\pi^{\mathsf{lrg}} \overset{\mathrm{R}}{\leftarrow} \mathsf{P}^{\mathsf{lrg}}((pk_s, pk_d, B_i, X), (sk_s, x, r))$.
   - (d) Send $(X, \pi^{\mathsf{pos}}, \pi^{\mathsf{lrg}})$ to C.
2. C:
   - (a) $\mathsf{V}^{\mathsf{pos}}(pk_d, X)$.
   - (b) $\mathsf{V}^{\mathsf{lrg}}(pk_s, pk_d, B_i, X)$.
   - (c) Set $B_d^{\mathsf{tmp}} \mathrel{+}= X$.
   - (d) Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{transfer}, s, d)$.

Protocol 3.6 ($\Pi_{\mathsf{ConfTrans}}$.Update)**.**

Participating parties. P_i and C.

Operation: C

1. Set $B_i \mathrel{+}= B_i^{\mathsf{tmp}}$.
2. Set $B_i^{\mathsf{tmp}} \overset{\mathrm{R}}{\leftarrow} \mathrm{Enc}_{pk_i}(0)$.
3. Set $\mathsf{log} \mathrel{+}= (\mathsf{sid}, \mathsf{update}, i)$

Protocol 3.7 ($\Pi_{\mathsf{ConfTrans}}$.History)**.**

Participating parties. P_i and C.

Operation: C sends log to P_i.