Verificación de smart contracts en Marlowe para la blockchain Cardano

Julián Ferres

Facultad de Ingeniería
Universidad de Buenos Aires.

25 de julio de 2022

.UBAfiuba
FACULTAD DE INGENIERÍA

Índice de Contenidos

.UBAfiuba
FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Cadenas de bloques o *Blockchains*

Las cadenas de bloques, conocidas en inglés como blockchains, son estructuras de datos en las cuales la información se divide en conjuntos (bloques) que cuentan con información adicional relativa a bloques previos de la cadena.

Cadenas de bloques o *Blockchains*

Las cadenas de bloques, conocidas en inglés como blockchains, son estructuras de datos en las cuales la información se divide en conjuntos (bloques) que cuentan con información adicional relativa a bloques previos de la cadena.

Con esta organización relativa, y con ayuda de técnicas criptográficas, la información de un bloque solo puede ser alterada modificando todos los bloques anteriores.

Cadenas de bloques o *Blockchains*

Las cadenas de bloques, conocidas en inglés como blockchains, son estructuras de datos en las cuales la información se divide en conjuntos (bloques) que cuentan con información adicional relativa a bloques previos de la cadena.

Con esta organización relativa, y con ayuda de técnicas criptográficas, la información de un bloque solo puede ser alterada modificando todos los bloques anteriores.

Esta propiedad facilita su aplicación en un entorno distribuido, de manera tal que la cadena de bloques puede modelar una base de datos pública no relacional, que contenga un registro histórico irrefutable de información.

Cadenas de bloques o *Blockchains*

Las cadenas de bloques, conocidas en inglés como blockchains, son estructuras de datos en las cuales la información se divide en conjuntos (bloques) que cuentan con información adicional relativa a bloques previos de la cadena.

Con esta organización relativa, y con ayuda de técnicas criptográficas, la información de un bloque solo puede ser alterada modificando todos los bloques anteriores.

Esta propiedad facilita su aplicación en un entorno distribuido, de manera tal que la cadena de bloques puede modelar una base de datos pública no relacional, que contenga un registro histórico irrefutable de información.

En la práctica esta técnica ha permitido la implementación de un registro contable o ledger distribuido que soporta y garantiza la seguridad de transacciones y dinero digital.

.UBAfiuba FACULTAD DE INGENIERÍA

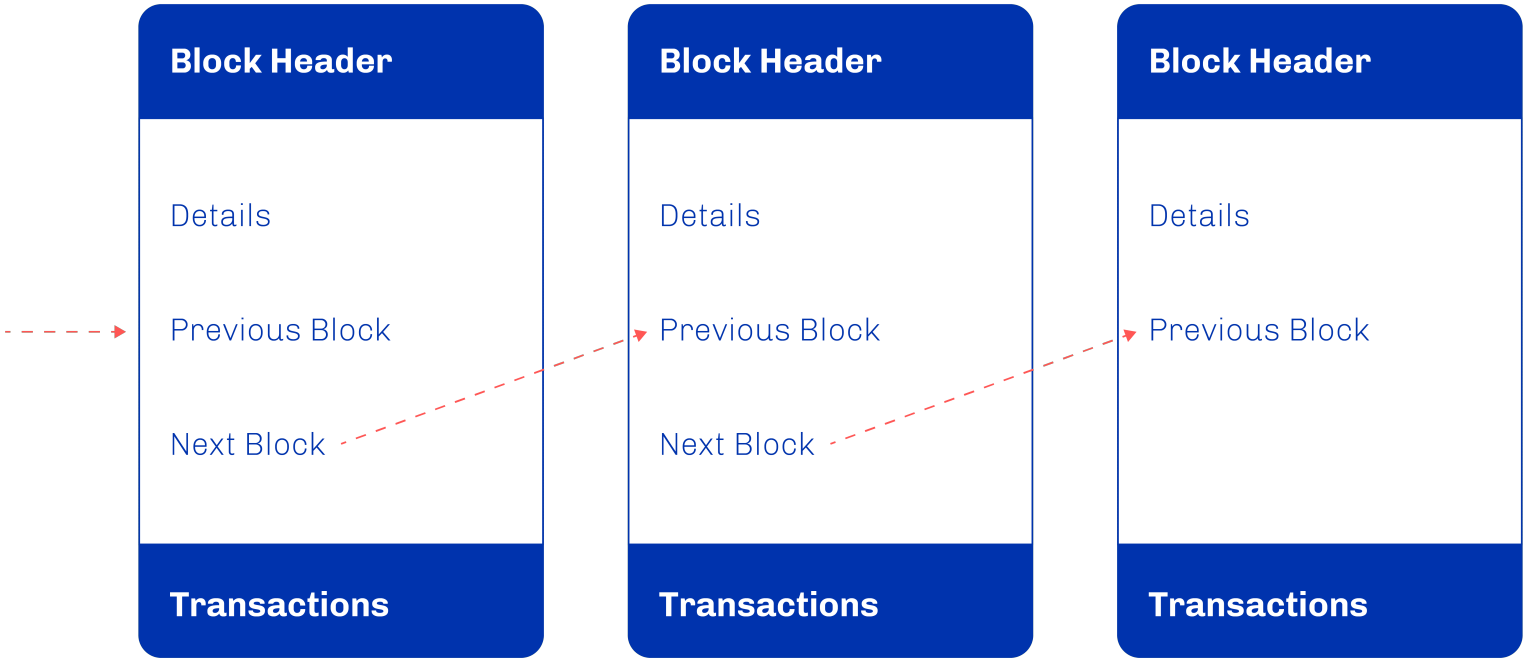

Figura: Representación simplificada de los datos en un bloque de la cadena. Extraída de [Brünjes and Vinogradova, 2019].

Criptomonedas

Las criptomonedas son activos digitales que se almacenan en el ledger y están diseñadas para servir como medio de intercambio de bienes o servicios.

Criptomonedas

Las criptomonedas son activos digitales que se almacenan en el ledger y están diseñadas para servir como medio de intercambio de bienes o servicios.

Los ledgers de blockchain son utilizados como tecnología subyacente para la creación de criptomonedas en un entorno descentralizado.

Criptomonedas

Las criptomonedas son activos digitales que se almacenan en el ledger y están diseñadas para servir como medio de intercambio de bienes o servicios.

Los ledgers de blockchain son utilizados como tecnología subyacente para la creación de criptomonedas en un entorno descentralizado.

Los protocolos de blockchain utilizan técnicas criptográficas rigurosas para permitir la creación de criptomonedas, asegurar y verificar la propiedad de las mismas y los registros de movimiento de fondos.

Criptomonedas

Las criptomonedas son activos digitales que se almacenan en el ledger y están diseñadas para servir como medio de intercambio de bienes o servicios.

Los ledgers de blockchain son utilizados como tecnología subyacente para la creación de criptomonedas en un entorno descentralizado.

Los protocolos de blockchain utilizan técnicas criptográficas rigurosas para permitir la creación de criptomonedas, asegurar y verificar la propiedad de las mismas y los registros de movimiento de fondos.

El precio de la criptomoneda no está controlado por un gobierno o una institución financiera centralizada. Se define por su valor, la correlación con las cifras del mundo real y está impulsado por la oferta y la demanda del mercado.

Smart contracts

Un contrato inteligente o *smart contract* es un acuerdo digital automatizado.

Smart contracts

Un contrato inteligente o *smart contract* es un acuerdo digital automatizado.

Los mismos están escritos en código, rastrean, verifican y ejecutan las transacciones de un contrato entre varias partes.

Smart contracts

Un contrato inteligente o *smart contract* es un acuerdo digital automatizado.

Los mismos están escritos en código, rastrean, verifican y ejecutan las transacciones de un contrato entre varias partes.

Las transacciones del contrato se ejecutan automáticamente mediante el código del smart contract cuando se cumplen las condiciones predeterminadas. Esencialmente, un contrato inteligente es un programa cuyas entradas y salidas son acciones en una cadena de bloques.

Smart contracts

Un contrato inteligente o *smart contract* es un acuerdo digital automatizado.

Los mismos están escritos en código, rastrean, verifican y ejecutan las transacciones de un contrato entre varias partes.

Las transacciones del contrato se ejecutan automáticamente mediante el código del smart contract cuando se cumplen las condiciones predeterminadas. Esencialmente, un contrato inteligente es un programa cuyas entradas y salidas son acciones en una cadena de bloques.

Los smart contracts son auto-ejecutables y no requieren las acciones o la presencia de terceros. El código del contrato inteligente se almacena y distribuye en la *blockchain*, lo que lo hace transparente e irreversible.

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Cardano es una plataforma blockchain descentralizada de tercera generación, cuya criptomoneda es llamada *ada*.

Cardano es una plataforma blockchain descentralizada de tercera generación, cuya criptomoneda es llamada *ada*.

- **La primera generación** de blockchains (con Bitcoin como gran representante) ofrece ledgers descentralizados para la transferencia segura de criptomonedas.

Cardano es una plataforma blockchain descentralizada de tercera generación, cuya criptomoneda es llamada *ada*.

- **La primera generación** de blockchains (con Bitcoin como gran representante) ofrece ledgers descentralizados para la transferencia segura de criptomonedas. Sin embargo, tales *blockchains* no proporcionaron un entorno funcional para la liquidación de acuerdos complejos y el desarrollo de aplicaciones descentralizadas (dApps).

Cardano es una plataforma blockchain descentralizada de tercera generación, cuya criptomoneda es llamada *ada*.

- **La primera generación** de blockchains (con Bitcoin como gran representante) ofrece ledgers descentralizados para la transferencia segura de criptomonedas. Sin embargo, tales *blockchains* no proporcionaron un entorno funcional para la liquidación de acuerdos complejos y el desarrollo de aplicaciones descentralizadas (dApps).
- **La segunda generación** (cuyo ejemplo más conocido es Ethereum) proporcionó soluciones mejoradas para redactar y ejecutar contratos inteligentes, desarrollar aplicaciones y crear diferentes tipos de tokens.

Cardano es una plataforma blockchain descentralizada de tercera generación, cuya criptomoneda es llamada *ada*.

- **La primera generación** de blockchains (con Bitcoin como gran representante) ofrece ledgers descentralizados para la transferencia segura de criptomonedas. Sin embargo, tales *blockchains* no proporcionaron un entorno funcional para la liquidación de acuerdos complejos y el desarrollo de aplicaciones descentralizadas (dApps).
- **La segunda generación** (cuyo ejemplo más conocido es Ethereum) proporcionó soluciones mejoradas para redactar y ejecutar contratos inteligentes, desarrollar aplicaciones y crear diferentes tipos de tokens. Sin embargo, la segunda generación de cadenas de bloques a menudo enfrenta problemas en términos de escalabilidad.

.UBAfiuba FACULTAD DE INGENIERÍA

Cardano como *blockchain* de 3ra generación

Cardano se concibe como la cadena de bloques de tercera generación.
La misma combina las propiedades de las generaciones anteriores y ofrece las siguientes propiedades:

Cardano como *blockchain* de 3ra generación

Cardano se concibe como la cadena de bloques de tercera generación.
La misma combina las propiedades de las generaciones anteriores y ofrece las siguientes propiedades:

- **Seguridad**

Cardano como *blockchain* de 3ra generación

Cardano se concibe como la cadena de bloques de tercera generación.
La misma combina las propiedades de las generaciones anteriores y ofrece las siguientes propiedades:

- **Seguridad**
- **Escalabilidad**: Rendimiento de transacciones, escala de datos, ancho de banda de la red.

Cardano como *blockchain* de 3ra generación

Cardano se concibe como la cadena de bloques de tercera generación.
La misma combina las propiedades de las generaciones anteriores y ofrece las siguientes propiedades:

- **Seguridad**
- **Escalabilidad**: Rendimiento de transacciones, escala de datos, ancho de banda de la red.
- **Funcionalidad**: Además del procesamiento de transacciones, la cadena de bloques debe proporcionar todos los medios para la liquidación de acuerdos comerciales.

Cardano como *blockchain* de 3ra generación

Cardano se concibe como la cadena de bloques de tercera generación.
La misma combina las propiedades de las generaciones anteriores y ofrece las siguientes propiedades:

- **Seguridad**
- **Escalabilidad**: Rendimiento de transacciones, escala de datos, ancho de banda de la red.
- **Funcionalidad**: Además del procesamiento de transacciones, la cadena de bloques debe proporcionar todos los medios para la liquidación de acuerdos comerciales.
- **Desarrollo e Intregración**: Es importante asegurarse que la blockchain esté en constante desarrollo en términos de sostenibilidad y sea interoperable con otras blockchains e instituciones financieras.

.UBAfiuba FACULTAD DE INGENIERÍA

Ada como criptomoneda de Cardano

Cada ledger de blockchain tiene su criptomoneda subyacente o moneda nativa. Ada es la moneda nativa o principal en Cardano. Esto significa que ada es la principal unidad de pago en Cardano.

Ada como criptomoneda de Cardano

Cada ledger de blockchain tiene su criptomoneda subyacente o moneda nativa. Ada es la moneda nativa o principal en Cardano. Esto significa que ada es la principal unidad de pago en Cardano.

Cardano también admite la creación de **tokens nativos**: activos digitales que se crean para fines específicos.

Ada como criptomoneda de Cardano

Cada ledger de blockchain tiene su criptomoneda subyacente o moneda nativa. Ada es la moneda nativa o principal en Cardano. Esto significa que ada es la principal unidad de pago en Cardano.

Cardano también admite la creación de **tokens nativos**: activos digitales que se crean para fines específicos.

Por lo tanto los usuarios, desarrolladores y empresas pueden usar la cadena de bloques de Cardano para crear tokens que representen una huella de valor.

Ada como criptomoneda de Cardano

Cada ledger de blockchain tiene su criptomoneda subyacente o moneda nativa. Ada es la moneda nativa o principal en Cardano. Esto significa que ada es la principal unidad de pago en Cardano.

Cardano también admite la creación de **tokens nativos**: activos digitales que se crean para fines específicos.

Por lo tanto los usuarios, desarrolladores y empresas pueden usar la cadena de bloques de Cardano para crear tokens que representen una huella de valor.

Un token puede ser **fungible** (intercambiable) o **no fungible** (único) y actuar como unidad de pago, recompensa, activo comercial o contenedor de información.

Índice de contenidos

.UBAfiuba
FACULTAD DE INGENIERÍA

Contratos Financieros

Los contratos financieros son acuerdos legales entre dos (o más) partes sobre el futuro intercambio de dinero. Dichos acuerdos legales se definen sin ambigüedades por medio de un conjunto de términos y lógica contractual.

Contratos Financieros

Los contratos financieros son acuerdos legales entre dos (o más) partes sobre el futuro intercambio de dinero. Dichos acuerdos legales se definen sin ambigüedades por medio de un conjunto de términos y lógica contractual.

Como resultado, los mismos pueden describirse matemáticamente y representarse mediante algoritmos.

Los beneficios de representar contratos financieros de esta forma son múltiples:

Los beneficios de representar contratos financieros de esta forma son múltiples:

- Tradicionalmente, el procesamiento de transacciones ha sido un campo en el que se pueden lograr mejoras de eficiencia mediante la automatización de contratos.

Los beneficios de representar contratos financieros de esta forma son múltiples:

- Tradicionalmente, el procesamiento de transacciones ha sido un campo en el que se pueden lograr mejoras de eficiencia mediante la automatización de contratos.
- El análisis financiero se basa en la disponibilidad de representaciones computables de estos acuerdos, donde a menudo se utilizan aproximaciones analíticas.

Los beneficios de representar contratos financieros de esta forma son múltiples:

- Tradicionalmente, el procesamiento de transacciones ha sido un campo en el que se pueden lograr mejoras de eficiencia mediante la automatización de contratos.
- El análisis financiero se basa en la disponibilidad de representaciones computables de estos acuerdos, donde a menudo se utilizan aproximaciones analíticas. Recientemente, el auge de las blockchain, de contabilidad distribuida y los diversos casos de uso de los contratos inteligentes han abierto nuevas posibilidades para los contratos financieros digitales.

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

> *"Se entrega un monto de dinero inicial, a cambio de pagos de intereses cíclicos y la devolución del dinero inicial en el vencimiento del contrato."*

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

> *"Se entrega un monto de dinero inicial, a cambio de pagos de intereses cíclicos y la devolución del dinero inicial en el vencimiento del contrato."*

Si bien los pagos son fijos, existen muchas variantes que determinan cómo se programan y/o pagan los pagos de intereses cíclicos:

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

> *"Se entrega un monto de dinero inicial, a cambio de pagos de intereses cíclicos y la devolución del dinero inicial en el vencimiento del contrato."*

Si bien los pagos son fijos, existen muchas variantes que determinan cómo se programan y/o pagan los pagos de intereses cíclicos:

- Los pagos de intereses pueden ser mensuales, anuales, mediante períodos arbitrarios.

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

> *"Se entrega un monto de dinero inicial, a cambio de pagos de intereses cíclicos y la devolución del dinero inicial en el vencimiento del contrato."*

Si bien los pagos son fijos, existen muchas variantes que determinan cómo se programan y/o pagan los pagos de intereses cíclicos:

- Los pagos de intereses pueden ser mensuales, anuales, mediante períodos arbitrarios.
- Las tasas pueden ser de fijas o variables.

En general, el intercambio de flujos de efectivo entre partes sigue ciertos patrones.
Un patrón típico es un contrato de préstamo de tipo *bullet*:

> *"Se entrega un monto de dinero inicial, a cambio de pagos de intereses cíclicos y la devolución del dinero inicial en el vencimiento del contrato."*

Si bien los pagos son fijos, existen muchas variantes que determinan cómo se programan y/o pagan los pagos de intereses cíclicos:

- Los pagos de intereses pueden ser mensuales, anuales, mediante períodos arbitrarios.
- Las tasas pueden ser de fijas o variables.
- Pueden usarse diferentes métodos de cálculo de fracciones anuales o que no haya ningún interés.

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba
FACULTAD DE INGENIERÍA

Concepto general, herramientas y metodologías

Los asistentes de pruebas formales son herramientas de software diseñadas para ayudar a sus usuarios a realizar pruebas, especialmente en cálculo lógico.

Por lo general, los llamamos asistentes de demostración o demostradores interactivos de teoremas.

Concepto general, herramientas y metodologías

Los asistentes de pruebas formales son herramientas de software diseñadas para ayudar a sus usuarios a realizar pruebas, especialmente en cálculo lógico.

Por lo general, los llamamos asistentes de demostración o demostradores interactivos de teoremas.

La principal fortaleza de los asistentes de prueba es que ayudan a desarrollar pruebas altamente confiables e inequívocas de enunciados matemáticos, usando lógica precisa. Se pueden usar para probar resultados arbitrariamente avanzados, y no solo ejemplos simples.

Algunos asistentes de pruebas

Hay una gran cantidad de asistentes de prueba en desarrollo o uso alrededor del mundo. A continuación presentamos una lista de los principales, clasificados por sus fundamentos lógicos:

Algunos asistentes de pruebas

Hay una gran cantidad de asistentes de prueba en desarrollo o uso alrededor del mundo. A continuación presentamos una lista de los principales, clasificados por sus fundamentos lógicos:

- **Teoría de conjuntos**: Isabelle/ZF, Metamath, Mizar
- **Teoría simple de tipos**: HOL4, HOL Light, Isabelle/HOL
- **Teoría dependiente de tipos**: Agda, Coq, Lean, Matita, PVS
- **Lógica de primer orden, de tipo Lisp**: ACL2

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Índice de contenidos

.UBAfiuba FACULTAD DE INGENIERÍA

Bibliografía I


Brünjes, L. and Vinogradova, P. (2019).
Plutus: Writing reliable smart contracts.
IOHK.