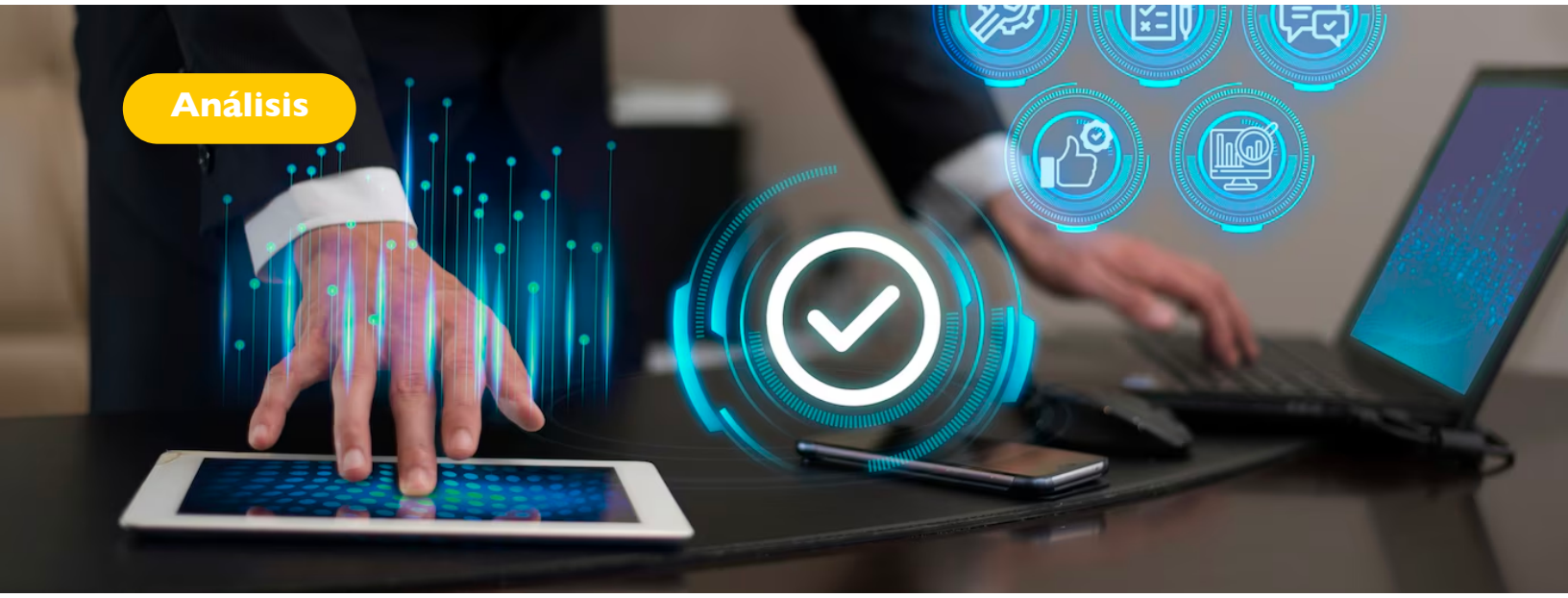
Realidad Empresarial
Administración • Mercadeo • Finanzas • Operaciones

Realidad Empresarial N° 19, Especial 2024, pp.7-18
URL: https://revistas.uca.edu.sv/index.php/reuca/index
ISSN 2789-2689 (en línea) - ISSN 2415-5721 (impreso)



Una aproximación al uso de patrones de eventos para el modelado de contratos inteligentes

An approach to using event patterns for smart contract modeling

DOI: https://doi.org/10.51378/reuca.vi19.8710

Fecha de recibido: 18 de junio de 2024
Fecha de aceptado: 13 de septiembre de 2024

Oscar Carlos Medina
Docente investigador
Universidad Tecnológica Nacional
omedina@frc.utn.edu.ar
ORCID: 0000-0003-3300-633X
Argentina

Rubén Aníbal Romero
Docente investigador
Universidad Tecnológica Nacional
rromero@frc.utn.edu.ar
ORCID: 0009-0009-4738-6194
Argentina

Marcelo Martín Marciszack
Docente investigador
Universidad Tecnológica Nacional
mmarciszack@frc.utn.edu.ar
ORCID: 0000-0003-1398-6094
Argentina

Brenda Elizabeth Meloni
Docente investigador
Universidad Tecnológica Nacional
bmeloni@frc.utn.edu.ar
ORCID: 0000-0002-9721-4595
Argentina

Ana María Strub
Docente investigador
Universidad Tecnológica Nacional
astrub@frc.utn.edu.ar
ORCID: 0009-0009-2730-7209
Argentina

María Soledad Romero
Docente investigador
Universidad Tecnológica Nacional
msromero@frc.utn.edu.ar
ORCID: 0009-0000-1061-0855
Argentina

Diego Morardo
Becario graduado
Universidad Tecnológica Nacional
diegomorardo@gmail.com
ORCID: 0009-0005-7022-7387
Argentina

José Ignacio Nájera Gibert
Becario estudiante
Universidad Tecnológica Nacional
JoseNajeraGibert@gmail.com
ORCID: 0009-0001-8507-0985
Argentina

Resumen

El uso de patrones de eventos en el modelado de contratos inteligentes es una tendencia emergente según los resultados de varias investigaciones. Este trabajo propone elaborar un modelo de diseño de contratos inteligentes basado en patrones de eventos, basados en una metodología de estudios exploratorios de blockchain Este proceso sistematizado y ágil permite mediante los patrones de eventos reutilizar el conocimiento y la experiencia de soluciones anteriores descriptas con patrones de negocio para los mismos casos de uso. Contrato inteligente es un código de programación que se ejecuta automáticamente cuando se cumplen ciertas condiciones predefinidas; estos contratos se crean y se almacenan en una plataforma Blockchain, lo que permite su ejecución automática y su verificación por parte de múltiples nodos de la red. Realizando un mapeo de la bibliografía científica publicada a la fecha, se encuentran trabajos que proponen la aplicación de patrones al modelado de contratos inteligentes. Los patrones de eventos se utilizan para modelar las interacciones entre los contratos inteligentes y su entorno, lo que ayuda a mejorar la eficiencia, seguridad y flexibilidad de los contratos inteligentes. Entre los patrones de eventos más utilizados se encuentran los de tiempo, los de control de flujo y los de comunicación. Además, se han desarrollado herramientas y lenguajes específicos para el modelado de contratos inteligentes basados en patrones de eventos. Lo que lleva a sugerir que el uso de patrones de eventos en el modelado de contratos inteligentes es una tendencia prometedora que puede mejorar significativamente la eficiencia, seguridad y flexibilidad de los contratos inteligentes en diversas aplicaciones.

Palabras Claves: blockchain, contrato inteligente, patrón de eventos, modelado.

Abstract

In this work, it is proposed to develop a smart contract design model event patterns-based. The use of event patterns in smart contract modeling is an emerging trend. This systematized and agile process allows, through event patterns, to reuse the knowledge and experience of previous solutions described with business patterns for the same use cases. Smart contract is programming code that is automatically executed when certain predefined conditions are met. These contracts are created and stored on a Blockchain platform, allowing for automatic execution and verification by multiple nodes on the network. Mapping the scientific literature published to date, one finds works that propose the application of patterns to the modeling of smart contracts. The results show that the use of event patterns in smart contract modeling is an emerging trend. Event patterns are used to model interactions between smart contracts and their environment, helping to improve the efficiency, security, and flexibility of smart contracts. Among the most commonly used event patterns are time patterns, flow control patterns, and communication patterns. In addition, specific tools and languages have been developed for modeling smart contracts based on event patterns. In conclusion, it is suggested that the use of event patterns in smart contract modeling is a promising trend that can significantly improve the efficiency, security and flexibility of smart contracts in various applications.

Keywords: blockchain, smart contract, event pattern, modeling.

Introducción

Blockchain es una tecnología de registro distribuido que permite la creación de registros inmutables y a prueba de manipulaciones. En esencia, es una base de datos descentralizada y distribuida en la que múltiples partes pueden realizar transacciones y compartir información sin necesidad de confiar en un intermediario centralizado. Nace como una tecnología de libros de registro digitalizado y descentralizado, introducida por Satoshi Nakamoto en un documento publicado en 2008 llamado *Bitcoin: un sistema de efectivo electrónico de igual a igual* El artículo detalla un sistema de criptomoneda conocido como Bitcoin. Cada Bitcoin se genera electrónicamente, y cada transacción que utiliza un Bitcoin queda asentado en un libro de registro digital, y está abierto a la actualización de cualquier involucrado en la transacción. Bitcoin se conoce como un sistema de moneda digital entre pares que funciona sin ningún intermediario confiable, es descentralizado y no tiene supervisión de un organismo de gobierno estatal (Nakamoto, 2008).

La tecnología Blockchain funciona mediante la creación de bloques de datos que se conectan entre sí en una cadena, de ahí el nombre de "Blockchain" o cadena de bloques en español. Cada bloque contiene una lista de transacciones verificadas y validadas por la red de nodos que participan en el sistema. Una vez que un bloque se agrega a la cadena, se vuelve inmutable y no se puede modificar sin afectar toda la cadena.

Esta tecnología ha encontrado numerosas aplicaciones en diferentes sectores, incluyendo finanzas, salud, logística, energía y más. Por ejemplo, en el sector financiero, se utiliza para la creación de criptomonedas como Bitcoin y para realizar transacciones financieras más seguras y eficientes.

A fines de 2013, Vitalik Buterin comenzó el desarrollo de una nueva red Blockchain denominada Ethereum (Ethereum, 2024), con la primera prueba de concepto publicada en febrero de 2014. Esta plataforma se fijó como horizonte construir un sistema que permitiese crear contratos inteligentes sobre una red Blockchain, ya sea pública o privada.

Contrato inteligente es un conjunto de algoritmos u operaciones informáticas que tienen como principal atractivo la eliminación de intermediarios para simplificar procesos, pero también para verificar su verdadero cumplimiento (Endeavor, 2018). Sólo si una tarea se cumple, se procede a la siguiente etapa. Al estar

montado sobre Blockchain, se convierte en un acuerdo transparente, auditable e inalterable, que además conlleva un ahorro de tiempo y dinero.

Los contratos inteligentes son autónomos y autoejecutables, lo que significa que se ejecutan sin la necesidad de un intermediario humano. Por ejemplo, si se establece un contrato inteligente para el pago de una cantidad determinada cuando se cumplan ciertas condiciones, como la entrega de un producto, el contrato se ejecutará automáticamente y realizará el pago una vez que se hayan cumplido dichas condiciones.

La tecnología de contratos inteligentes ha encontrado aplicaciones en muchos sectores, incluyendo finanzas, seguros, bienes raíces, entre otros. Al eliminar la necesidad de intermediarios humanos, los contratos inteligentes pueden reducir costos, aumentar la eficiencia y mejorar la transparencia y la seguridad en las transacciones.

Patrones de eventos

Un patrón es una descripción de una solución común a un problema recurrente que puede ser aplicado a un contexto específico. Los patrones ayudan a aprovechar la experiencia colectiva de software especializado, donde los ingenieros representan la experiencia existente y probada en el desarrollo de sistemas.

Eriksson y Penker (2000) distinguen tres tipos de patrones en relación con los problemas que abordan:

- Patrones de negocio: abordan problemas del dominio organizacional, cómo definir y relacionar procesos y reglas de negocios, visiones y objetivos corporativos
- Patrones de arquitectura: se ocupan de problemas del diseño arquitectónico de los sistemas de información.
- Patrones de diseño: se utilizan para situaciones en las que el análisis ya está descrito, y se enfocan en producir soluciones técnicas flexibles y adaptables.

Entre los patrones de arquitectura, se destacan los de eventos que son un enfoque de Ingeniería de Software para describir, analizar y modelar sistemas basados en eventos. En este enfoque, se considera que los sistemas están compuestos por una serie de situaciones que ocurren en el tiempo y que pueden ser observados y capturados por sensores o dispositivos.

Los patrones de eventos se utilizan para modelar las interacciones entre los contratos inteligentes y su entorno, lo que ayuda a mejorar la eficiencia, la seguridad y la flexibilidad de los contratos inteligentes. Entre los patrones de eventos más utilizados se encuentran los de tiempo, de control de flujo y los de comunicación. Además, se han desarrollado herramientas y lenguajes específicos para el modelado de contratos inteligentes basados en estos mismos. Además, permiten definir cómo se deben interpretar los eventos y cómo se relacionan entre sí; pueden incluir reglas de negocio, condiciones y acciones que se deben tomar cuando ocurren ciertos eventos.

Los patrones de eventos son útiles para modelar sistemas basados en eventos, como aplicaciones de IoT (Internet de las cosas), aplicaciones descentralizadas basadas en contratos inteligentes, sistemas de monitoreo de red, sistemas de detección de intrusiones, sistemas de trading de criptomonedas, entre otros. Además, ayudan a analizar los datos generados por estos sistemas, y permiten una mejor comprensión de los eventos que ocurren y su relación con otros en el sistema.

Modelado de contratos inteligentes utilizando patrones

En esta investigación propone estudiar el caso particular de los sistemas de información de contratos inteligentes y su modelado basado en patrones de eventos.

El modelado conceptual de un sistema tiene como objetivo identificar y explicar los conceptos significativos en un dominio de problema, identificando los atributos y las asociaciones existentes entre ellos. Se plantea incorporar en la actividad de modelado patrones de eventos, por ser esquemas predeterminados de análisis y diseño, para optimizar la definición inicial del comportamiento de un nuevo contrato inteligente, formalizando dicha definición, facilitando la validación de los requerimientos funcionales y reutilizando el conocimiento y experiencia de aplicaciones distribuidas anteriores.

Las razones por las cuales se propone usar patrones de eventos en vez de los de diseño o de negocio se detallan a continuación:

Los patrones de diseño nacieron en el paradigma de la programación orientada a objetos, y se utilizan en la etapa de construcción del sistema. A diferencia de los patrones de negocio, que se formularon a posteriori basándose en los de diseño, pero se orientan al modelado de procesos de negocio. En esta etapa se potencia la utilidad de los patrones de eventos por su especialización en modelar el comportamiento autónomo de los contratos inteligentes.

En la exploración del marco conceptual se encontró la revisión sistemática de la literatura de (Zhao et al., 2021) cuyo objetivo es identificar el estado actual de la investigación sobre el uso de patrones de eventos en el modelado de contratos inteligentes. Los autores identificaron cuarenta y dos artículos relevantes publicados entre 2014 y 2019 y los analizaron en detalle. Los resultados muestran que el uso de patrones de eventos en el modelado de contratos inteligentes es una tendencia emergente. Los patrones de eventos se utilizan para modelar las interacciones entre los contratos inteligentes y su entorno, lo que ayuda a mejorar la eficiencia, la seguridad y la flexibilidad de los contratos inteligentes. Entre los patrones de eventos más utilizados se encuentran los patrones de tiempo, de control de flujo y los de comunicación. Además, se han desarrollado herramientas y lenguajes específicos para el modelado de contratos inteligentes basados en patrones de eventos. Los autores sugieren que el uso de patrones de eventos en el modelado de contratos inteligentes es una tendencia prometedora que puede mejorar significativamente la eficiencia, la seguridad y la flexibilidad de los contratos inteligentes en diversas aplicaciones.

También, existen publicaciones anteriores de los autores de este artículo (Marciszack et al., 2018) y (Medina et al., 2021a-2021b) que desarrollan un modelo de análisis para la definición de patrones en el Modelo Conceptual de sistemas de información. En la presente investigación se continúan los mencionados trabajos elaborando un modelo de diseño que utiliza patrones de eventos al modelar contratos inteligentes incorporando los resultados de investigaciones propias anteriores, sumadas las mejoras identificadas en las revisiones bibliográficas y una nueva evaluación experimental.

Metodología

El diseño metodológico de esta investigación tiene un enfoque cualitativo con estudios exploratorios de Blockchain, contratos inteligentes y patrones de eventos dentro del marco teórico de la ingeniería de software. Se realiza un análisis descriptivo de los patrones de eventos que puedan aplicarse en el modelo conceptual de contratos inteligentes; además, se elabora un modelo de diseño el cual se evaluará de forma empírica. El resultado de este proyecto es el mencionado modelo y su evaluación en casos experimentales.

El término *ingeniería*, tanto en el caso de ingeniería de software como en ingeniería en sistemas de información, hace referencia directa a la dimensión técnica de uno de los niveles ontológicos de un sistema de información, como resultado de bases teóricas y disciplinas prácticas, que son tradicionales en las ramas establecidas de la ingeniería. Pero el software tiene también otros niveles ontológicos asociados a dimensiones que están más próximas a ciencias de la administración y ciencias sociales. Esos niveles son, por ejemplo, el desarrollo de sistemas informáticos como proceso de producción relacionado con la teoría de la organización o la elicitación de requerimientos y experiencia de usuario que tratan temas del comportamiento humano y psicología social.

En informática los estudios empíricos generan información que pueden mejorar el conocimiento de una realidad, así como las prácticas que de ellos derivan. De la misma forma que la ingeniería del software comprende los aspectos de la producción de software desde las etapas iníciales de la especificación de un sistema, hasta el mantenimiento de éste después de su implementación, en particular la ingeniería del software basada en la evidencia, se fundamenta en leyes naturales, resultados experimentales y fórmulas empíricas para proponer y respaldar soluciones a los problemas que se le presentan. Por lo que se propone emplear en este proyecto herramientas empíricas propias de la ingeniería del software basada en evidencia como la revisión sistemática de la literatura y el estudio de casos.

Considerando el marco conceptual, el objetivo de este trabajo es elaborar un método que permita reutilizar patrones de negocio en el modelado de los procesos de sistemas información que utilicen contratos inteligentes implementados sobre redes Blockchain. Esta investigación busca dar respuesta a los siguientes interrogantes:

a) ¿Qué es Blockchain y qué son contratos inteligentes? ¿Cuáles son sus principales características y funcionamiento?

b) ¿Qué son patrones de eventos? ¿Cómo se pueden utilizar en el modelado de contratos inteligentes?

c) ¿Es factible el modelado de contratos inteligentes basado en patrones de eventos? ¿Qué ventajas y desventajas empíricas implica su utilización?

Los objetivos específicos que se pretenden alcanzar son: se inicia con caracterizar los contratos inteligentes, luego describir las características básicas de los patrones de eventos y su funcionalidad, para continuar con la identificación de los patrones de eventos y sus catálogos publicados que se pueden aplicar en el modelado de contratos inteligentes, posteriormente se propone la aplicación de patrones de eventos en el modelo conceptual de contratos inteligentes, y finalmente, se evalúa el modelo de diseño propuesto para el modelado de contratos inteligentes basado en patrones de eventos.

Para la consecución de cada uno de los objetivos específicos se lleva a cabo el siguiente conjunto de actividades:

Actualmente se está llevando a cabo un método de investigación denominado RSL, acrónimo de Revisión Sistemática de la Literatura. Este método es parte de la disciplina ISBE, Ingeniería de Software Basada en Evidencias que busca evaluar e interpretar toda la evidencia empírica disponible en relación con preguntas de investigación particulares o un fenómeno de interés (Wohlin et al., 2012) y (Genero Bocco et al., 2014). Una RSL es un estudio empírico secundario que tiene la finalidad de brindar una aproximación global sobre un tema de interés, las investigaciones y sus resultados publicados en un período de tiempo. Cuando se descubre que existe poca evidencia o que el tema a tratar es muy amplio, se recomienda utilizar RSL, pues servirán como punto de partida, siempre y cuando se realicen con rigor (Kitchenham et al., 2010). La RSL permite graficar la evidencia de un dominio a un alto nivel de granularidad. También posibilita la identificación de grupos y *desiertos* de evidencia para dirigir el foco de futuras revisiones sistemáticas, y detectar áreas donde conducir más estudios primarios. La RSL no está basado solamente en evidencia empírica. La RSL se orienta a documentación científica relacionada con el estudio de los patrones de eventos, desde el punto de vista de la ingeniería de software y a los contratos inteligentes.

Se evalúan las características básicas de los patrones de eventos identificados, a través de su grado de representación, completitud en su definición, facilidad de implementación y métricas de calidad. Con ellos, se formaliza una heurística de asociación a cada problemática de contratos inteligentes.

Con la información analizada de la RSL, se definen conceptos esenciales y aspectos relacionados a la elaboración de patrones de eventos que se emplean en el desarrollo de software, sobre todo en la etapa de licitación de requerimientos, en la actividad de creación del modelo conceptual.

Las características que serán utilizadas para determinar los atributos que involucra la aplicación de patrones de eventos, los cuales se transforman en criterios, que posteriormente se utilizan en el proceso de comparación de diferentes propuestas utilizadas para el modelado de sistemas de información. Se identifican claramente y en forma precisa las funcionalidades, objetivos, variables y atributos de cada uno de los patrones definidos, lo que además sirve para detectar la correcta determinación de los mismos, de acuerdo a la investigación documental realizada.

Se seleccionan catálogos de patrones de eventos para definir con ellos en forma estandarizada implementaciones exitosas de sistemas de contratos inteligentes, de acuerdo con el análisis comparativo de criterios y subcriterios obtenidos en la actividad anterior. Se evalúan las características básicas de los patrones identificados, a través de su grado de representación, completitud en su definición, facilidad de implementación y métricas de reusabilidad.

Se procede a investigar la viabilidad de uso de los patrones de eventos, y a verificar si la gestión de patrones contempla

y resuelve los déficits de reusabilidad identificados en el modelo conceptual del software que no estuvo basado en dichos patrones. Se definirá un modelo de diseño para incorporar estos patrones al modelo conceptual de los contratos inteligentes.

Se desarrollan distintos prototipos de contratos inteligentes aplicando los patrones de eventos en la cantidad que sea necesaria para garantizar el resultado de la evaluación. Por lo cual, se realizará el diseño, planificación y ejecución de un estudio de casos.

Estudio de casos es la investigación empírica que hace uso de múltiples fuentes de evidencia para investigar una instancia (o un pequeño número de instancias) de un fenómeno contemporáneo relacionado con la ingeniería de software dentro de su contexto real, específicamente cuando las fronteras entre el fenómeno y su contexto no pueden definirse claramente. Como el objetivo del estudio de casos no es encontrar relaciones causales sino comprender más en profundidad el fenómeno que se está estudiando en su contexto real, es particularmente útil para trabajar con la realidad observable de una teoría dentro del cinturón protector de un PIC. Kitchenham, uno de los fundadores de esta disciplina, define los pilares básicos de este método (Kitchenham et al., 1995); también describe cómo los estudios de caso ayudan a la industria de software a evaluar los beneficios de sus métodos y herramientas, y proporcionan una forma rentable de garantizar que los cambios en el proceso de desarrollo proporcionen los resultados deseados.

Se adopta como premisa de trabajo que las organizaciones donde se realice el estudio de casos actua racionalmente y sólo implementa patrones de eventos en el modelo conceptual de sus contratos inteligentes bajo el supuesto que éstos optimizann la reusabilidad.

Se analizan y discuten los resultados del estudio de casos y se elaboran trabajos que se exponen a consideración de la comunidad científica mediante publicaciones y asistencia a congresos científicos.

Se plantea realizar la transferencia a Instituciones de Educación Superior (IES) del método de modelado de contratos inteligentes, y a la Industria, de casos de aplicación de ejemplo en trazabilidad de alimentos a las Cámaras del Maní y de la Carne (AFIC) que son miembros de la Red RIBCi (RIBCi, 2024), Red Iberoamericana de Blockchain y Ciberseguridad, a la que pertenecen los autores de este trabajo. La Red RIBCi fue creada en 2023 con fondos del programa CYTED, está conformada por 24 grupos de investigación de 10 países de Iberoamérica, vinculando a 152 investigadores y tiene por finalidad contribuir a la industrialización inclusiva y sostenible fomentando la innovación mediante la aplicación de tecnologías Blockchain y Ciberseguridad, dentro de marcos normativos sólidos y equitativos, para el fortalecimiento del capital humano y la transferencia a los sectores productivos estratégicos y de gobierno en los países de Iberoamérica.

Resultados

Se realizó previamente un mapeo de la bibliografía científica publicada a la fecha y se encontraron trabajos que proponen la aplicación de distintos tipos de patrones al modelado de contratos inteligentes.

Un ejemplo es el de Bartoletti y Pompianu (2017) donde, tras analizar y definir una taxonomía de contratos inteligentes en base a un estudio de 811 proyectos, proponen patrones de diseño para contratos inteligentes, a los cuales luego correlaciona con el dominio de aplicación, dando soporte de esta forma a la elección del diseño más apropiado. Estudian sólo patrones de diseño y no otros tipos como por ejemplo los patrones de negocio que propone este trabajo.

Otro caso es el de Wöhrer y Zdun que publicaron dos trabajos sobre patrones de diseño en el desarrollo Blockchain. El primero ofrece la descripción de patrones de diseño que fijan pautas en el desarrollo de contratos inteligentes sobre la plataforma Ethereum (Wöhrer y Zdun, 2018a). Los autores explican en detalle y proporcionan ejemplos de patrones que responden a necesidades comunes en el diseño de contratos inteligentes durante el abordaje de los requisitos de una aplicación, y permiten resolver problemas comunes. El segundo, expone un enfoque específico sobre los patrones de diseño desde la mirada puesta en la seguridad de los contratos inteligentes (Wöhrer y Zdun, 2018). Detallan soluciones a problemas de seguridad típicos con el fin de que los desarrolladores Solidity puedan aplicarlos para conseguir mitigar los posibles escenarios de ataque; pero al igual que Bartoletti y Pompianu sólo desarrollaron patrones de diseño.

También existen autores que definen un proceso de diseño para aplicaciones basadas en Blockchain (Xu et al., 2019), o realizan una aproximación a una metodología de diseño de contratos inteligentes (Solis-Osorio et al., 2019), pero no utilizan patrones.

En Medina et al. (2021b) se hizo un mapeo sistemático de la literatura de patrones que apliquen al modelado conceptual de sistemas de información. Como resultado se encontró 25 estudios primarios de interés, publicados entre enero de 1995 y diciembre de 2019. Se pudo identificar los tipos de patrones más relevantes que se aplican en el Modelado de sistemas que son los patrones de diseño, negocio, análisis, arquitectura y escenario. Se destacan los patrones de diseño, que son los primeros patrones definidos en Ingeniería de Software; y los patrones de negocio, debido a que se utilizan para la especificación de procesos en la fase de modelado.

Recientemente, en Zhao et al. (2021) se realizó una revisión sistemática de la literatura sobre el uso de patrones de eventos en el modelado de contratos inteligentes. Los autores identificaron 42 artículos relevantes publicados entre 2014 y 2019 y los analizaron en detalle. Los resultados muestran que el uso de patrones de eventos en el modelado de contratos inteligentes es una tendencia emergente. Los patrones de eventos se utilizan para modelar las interacciones entre los contratos inteligentes y su entorno, lo que ayuda a mejorar la eficiencia, la seguridad y la flexibilidad de los contratos inteligentes. Lo que los autores no incluyeron en su trabajo, es una propuesta de modelado para nuevos contratos inteligentes, pero reutilizando patrones de eventos existentes y asociados a casos de uso Blockchain que tratan dicha problemática.

Partiendo de este enfoque, y sumados los resultados de investigaciones anteriores de los integrantes de este proyecto, es que se pone a consideración avanzar un paso más y modelar contratos inteligentes basados en patrones de eventos, según los lineamientos de MDD.

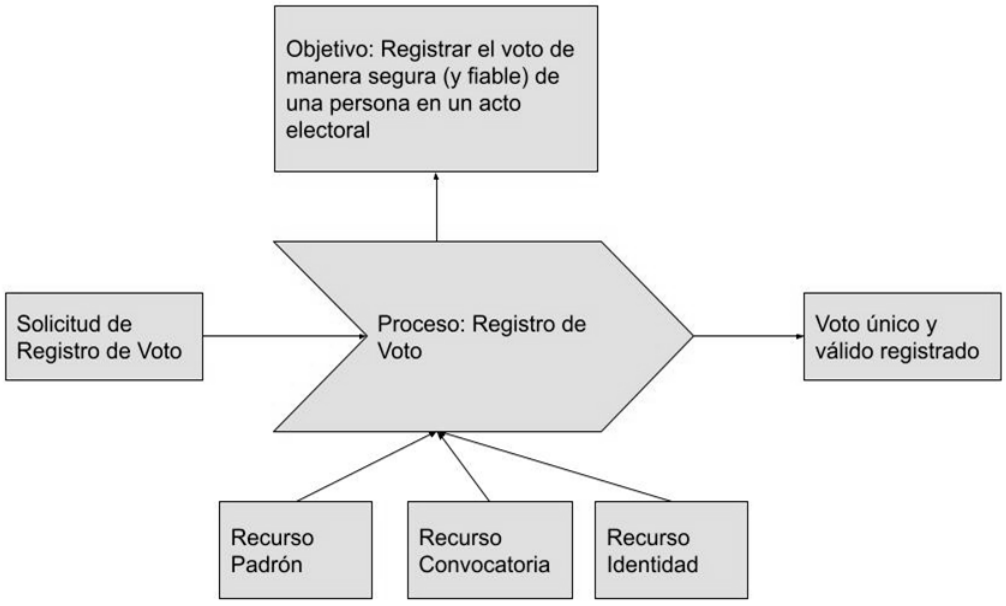
Para ejemplificar el modelado dirigido por casos de uso, que se toma como base para el modelado incorporando patrones de eventos, se expone a continuación el modelo conceptual de una aplicación descentralizada para voto electrónico usando Blockchain.

La metodología mencionada consta de once actividades que se desarrollan a continuación:

1) Proceso. Registrar el voto de un votante para una elección o asamblea, indicando candidato o ley según corresponda. Se aplicaron los patrones de Problema – Objetivo, de eventos y el de estructura básica de proceso como se puede apreciar en la Figura 1:

Figura 1

Patrón de estructura básica del proceso Registro de voto



2) Caso de uso Blockchain al que aplica el proceso. Voto electrónico. No se encontraron patrones en catálogos que se puedan reutilizar para este caso de uso.

3) Cambios de estado del proceso. Se define para el proceso registro de voto los siguientes estados:

- Validado
- Registrado
- Contado
- Auditado
- Creado

En la Figura 2 se muestra el correspondiente diagrama de transición de estado del proceso:

Figura 2

Diagrama de transición de estado del proceso Registro de voto

En la nueva metodología este diagrama va a ser reemplazado por un patrón de eventos.

4) Creación de valor y flujo de ingresos. Se definen como Socio clave: Socio tecnológico: DAML, Afiliación de DAO: Sin afiliación de DAO, Cargos al cliente: Suscripción + Costo por transacción. Se cobra un monto fijo por el servicio de elección más el costo variable por votante registrado en el padrón, Aceptación de monedas: Cargos al cliente, si la Blockchain es externa, y Sistema de token: Sin token.

5) Red Blockchain. Se definen para Posición en la cadena de valor: Usuario Blockchain, Suministro de Blockchain: Externo/Propia porque cada cliente puede optar por crear su propia red o unirse a una infraestructura establecida para votaciones/asambleas similares, y Tipo de Blockchain: Permisionada porque se pueden agregar a listas/partidos o entes reguladores de confianza para que participen en el proceso de consenso según se requiera.

6) Lenguaje de desarrollo y características técnicas. se definen Canal clave: sitio web/Aplicación móvil; Personalización: ambas tanto integración de desarrollo interno y/o externo del cliente; Criptoactivos: otro porque está orientado a redes permisionadas como LacChain, Ripple entre otros son candidatos; Mecanismo de consenso: existente porque la prueba de autoridad en el que las partes autorizadas son las encargadas de agregar bloques a la cadena; Tecnología adicional: nube porque puede aplicar la distribución de una infraestructura "serverless" a través de internet; Costo de suministro: suministro de software y, si la Blockchain es externa, suministro de plataforma también; y Suministro de red: uso de Blockchain externa o red propia de minado.

7) Activos. El Activo principal es el voto (activo lógico).

8) Participantes. Son los votantes y el órgano electoral.

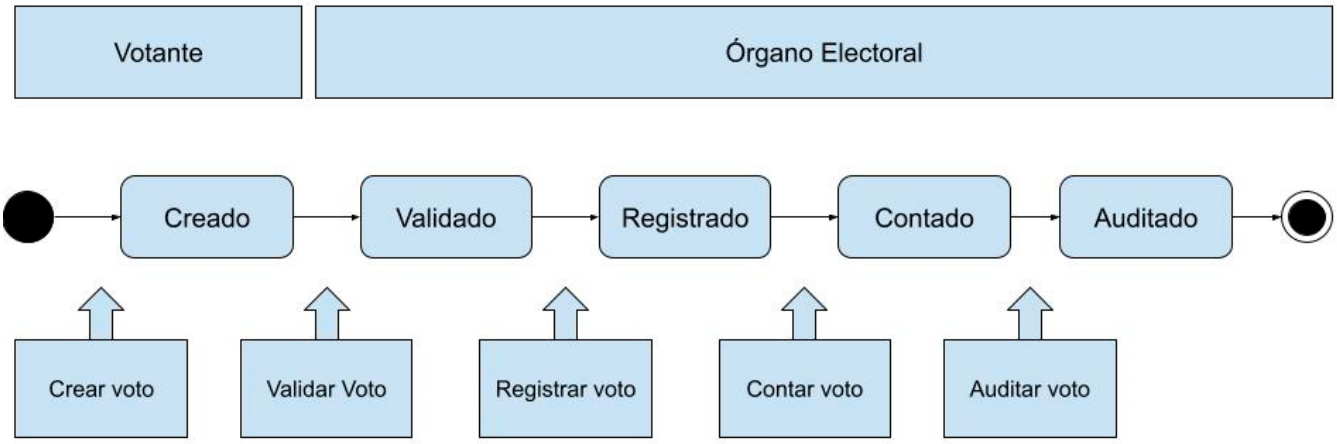
9) Estructura de los contratos inteligentes. Se especifican los siguientes atributos: convocatoria, votante identificado por tipo y número de documento, en caso de ser voto anónimo se reemplaza con un alias al registrar el voto; y Candidato/Ley-Hash que es un código único que valida la integridad del voto.

10) Transacciones. En caso de ser voto nominal se registra el voto en una sola transacción. En caso de ser voto privado se registra el voto y el votante por separado, además de hacerlo con un registro de lotes buscando aleatoriedad en el orden de votos para evitar la trazabilidad del votante y resguardar su anonimato. Los eventos que instancian estas transacciones son: crear voto, validar voto, registrar voto, contar voto y anular voto.

11) Diagrama de modelo integrado. En la Figura 3 se muestra el correspondiente diagrama de modelo integrado que unifica los cambios de estados del proceso, los participantes y los eventos que instancian las transacciones del contrato inteligente.

Figura 3

Diagrama de modelo integrado del proceso registro de voto



De esta manera queda conformado un modelo de análisis dirigido por casos de uso de un contrato inteligente de voto electrónico que es plausible de ser catalogado a partir de los patrones de negocio empleados. En este proyecto se van a incorporar patrones de eventos para modelar el comportamiento del contrato inteligente, para cuando se presente el problema en un mismo escenario de caso de uso, que este modelo conceptual pueda ser reutilizado.

Discusión

La premisa que se indaga en este proyecto es si los contratos inteligentes que resuelven un mismo caso de uso Blockchain, permiten incorporar los mismos patrones de eventos en su modelo conceptual. En caso afirmativo, un modelo de diseño de contratos inteligentes dirigido por patrones de eventos, asociados a casos de uso, por ejemplo, facilitaría la reusabilidad del conocimiento, de contratos inteligentes anteriores, desde etapas tempranas del proceso de desarrollo.

La propuesta sigue los lineamientos del Diseño de software Dirigido por Modelos, que es un enfoque de la ingeniería de software generador de variadas expectativas como alternativa sobresaliente a los métodos convencionales de producción de software, más orientado al Espacio de la Solución que al Espacio del Problema. Después de muchos años intentándolo, parece que por fin la comunidad de la ingeniería del software acepta que un proceso robusto de producción de software debe estar soportado por modelos conceptuales y dirigido por las transformaciones correspondientes entre modelos definidas de forma precisa.

La incorporación de patrones en el Modelo Conceptual sigue la premisa de promover la reusabilidad en las etapas tempranas del desarrollo, pero actualmente existen patrones que pueden aplicarse en todas las etapas y actividades del proceso de desarrollo.

Por otra parte, los resultados expuestos en este trabajo surgen de actividades académicas, pero para validar la propuesta se requiere de una evaluación experimental que obtenga conclusiones objetivas a partir de la eficacia y eficiencia de la aplicación de este nuevo método de modelado respecto de los tradicionales.

El Centro CIDS al que pertenecen los autores de este trabajo, han realizado investigaciones anteriores para la incorporación de patrones en el modelado conceptual de sistemas de información. La particularidad que tienen los sistemas que emplean tecnologías Blockchain y que están basados en contratos inteligentes, es que sus dominios de problemas pueden agruparse en lo que se denomina casos de uso. Se identificó que los casos de uso son candidatos para describir de manera eficaz mediante patrones, de negocio en primera instancia, y luego modelar su comportamiento con patrones de eventos.

Este es el objetivo que busca indagar este proyecto y obtener evidencia experimental del desempeño de su

nueva propuesta, por lo que se pone a consideración a la comunidad científica desde sus primeros resultados.

Conclusión

En este trabajo se presenta una propuesta de modelado de contratos inteligentes incorporando patrones de eventos que permitan su reusabilidad. Los patrones que se aplican al modelado conceptual cumplen la función de reutilizar el conocimiento y experiencia de sistemas anteriores.

En las actividades prácticas llevadas a cabo por estudiantes de trayectos formativos en tecnologías Blockchain, se observó que la aplicación de patrones permitió esclarecer los principales requerimientos del sistema basado en contratos inteligentes, plantear problemáticas, encontrar soluciones y similitudes entre los escenarios para simplificar el modelado. La representación de patrones a través de gráficos permite tener una mejor visión del negocio. Posibilita identificar fácilmente el proceso y sus actividades, y validar la reutilización del patrón.

También se comprobó que el uso del método de modelado elaborado en proyectos de investigación anteriores facilita anticipar algunas de las situaciones problema-solución en el circuito del proceso y gestionarlas en el mismo lenguaje del usuario del sistema. Además, conduce a emplear un vocabulario preciso y común entre el responsable de un proceso y su analista, para eliminar ambigüedades y conducir a una elicitación de requerimientos más asertiva a posteriori.

Se prevé que, al alcanzar los resultados planificados, el presente proyecto provea al mercado informático, no solo de una nueva herramienta de modelado de contratos inteligentes, sino también de un modelo de diseño de soluciones exitosas desde etapas tempranas de su construcción a través de la aplicación de patrones de eventos. A su vez garantizará la reutilización de modelos de comportamiento y cierto grado de performance de contratos inteligentes por la utilización de aplicaciones descentralizadas que ayudarían para tener en cuenta posibles requisitos necesarios para etapas posteriores del ciclo de desarrollo del software.

Además, está concebido realizar transferencia a la nueva asignatura "Desarrollo con tecnologías Blockchain", asignatura del último de la carrera Ingeniería en Sistemas de Información de la Regional Córdoba. Los resultados de la investigación transferidos al aula permitirán reforzar la competencia de los estudiantes sobre el modelado de contratos inteligentes.

De esta forma, las consultoras de software, las IES, los integrantes de la Red Ribci, apoyada por el programa CYTED, tendrán la posibilidad de acceder al fruto de esta investigación, lo que coadyuvará a mejores servicios en las diversas instituciones de la región al contar con patrones y buenas prácticas contribuyendo así al desarrollo productivo del software en el país. De esta forma se desea promover el uso de tecnologías Blockchain mediante la articulación del "triángulo de Sábato": Universidad, Gobierno y Empresas.

Referencias bibliográficas

Bartoletti, M. and Pompianu, L. (2017). An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns, en actas de International Conference on Financial Cryptography and Data Security 2017, págs. 494-509, Ed. Springer. https://doi.org/10.1007/978-3-319-70278-0

Ethereum (18 de junio 2024). *Welcome to Ethereum*. https://ethereum.org/en/.

Endeavor (2024).. *Blockchain, ¿la promesa de una revolución?* [Insight blockchain] Endeavor México. https://mexico.endeavor.org/blockchain2018/

Eriksson, H.-E. & Penker, M. (2000). Business Modeling with UML: Business Patterns at Work, OMG Press.

Genero Bocco, M., Cruz-Lemus J.A. y Piattini Velthuis, M.G. (2014). Métodos de investigación en ingeniería de software, Ed. Ra-ma.

Kitchenham, B., Pickard, L.M., Pfleeger, S.L. (1995). Case studies for method and tool evaluation, Ed. IEEE Software.

Kitchenham, B., Brereton, P., Turner, M., Niazi, M. y Linkman, S. (2010). Literature reviews in software engineering – a tertiary study, Information and Software Technology, 52(8), págs. 79-805. Ed. Elsevier.

Marciszack, M.M., Moreno, J.C., Sánchez, C.E., Medina, O.C., Delgado, A.F., Castro, C.S. (2018). Patrones en la construcción del Modelo Conceptual para sistemas de información, Editorial edUTecNe, Universidad Tecnológica Nacional.

Medina, O.C., Pérez Cota, M., Meloni, B.E., Marciszack, M.M. (2021a). Business Patterns Catalogue and selection proposal for the Conceptual Model of a software product publicado en J.UCS Journal 27(2), págs. 135-151, Editorial J.UCS Consortium.

Medina, O.C., Pérez Cota, M., Damiano, L.E., Della Mea, K., Marciszack, M.M. (2021b). Systematic Mapping of Literature on Applicable Patterns in Conceptual Modelling of Information Sys-tems publicado en "New perspectives in Software Engineering (CIMPS 2021)", págs. 41-54, Editorial Springer.

Nakamoto, S. Bitcoin (2008). A Peer-To-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf.

RIBCi (18 de junio de 2024). RIBCI - *Red iberoamericana de blockchain y ciberseguridad*. https://www.cyted.org/ribci.

Solis-Osorio, C.A., Pérez-Cortés, E., Cervantes-Maceda, H. (2019). Hacia una metodología para el diseño de contratos inteligentes", ReCIBE, Año 8 No. 1, México, Ed. UAM.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B. (2012). Experimentation in software engineering, Ed. Springer.

Wöhrer, M. and Zdun, U. (2018). Design Patterns for Smart Contracts in the Ethereum Ecosystem, 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Compu-ting and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, Ed. IEEE.

Xu, X., Weber, I. and Staples, M. (2019). Architecture for blockchain applications, págs. 1-307, Berlin, Germany, Ed. Springer.

Zhao, W.; Huang,T.; Chen, Y.; Deng, Y. & Tan, W. (2021). A systematic literature review on event pattern-based modeling of smart contracts. Concurrency and Computation: Practice and Experience.