PROYECTOS DE INVESTIGACIÓN 2020

MEMORIA DEL PROYECTO Nº 24

1. Datos del proyecto

Título: Análisis de las principales redes de Blockchain para la mejora en la toma de decisiones

Investigador/a/es responsable/es: Rafael Rosillo Camblor

Teléfono: 985 18 2657 **E-mail:** rosillo@uniovi.es

Otros investigadores: Francisco Javier Puente García; Alberto Gómez Gómez; José Parreño Fernández

Empresas o instituciones colaboradoras: Zapiens Technologies

2. Memoria descriptiva del proyecto

2.1 Resumen ejecutivo

La principal motivación de este proyecto de investigación ha sido la realización de un estudio para conocer las principales características de las redes blockchain que sirva para la toma de decisiones empresariales. Optimizando los recursos de las empresas se puede elegir entre diversas redes dependiendo de las necesidades de los usuarios finales.

La tecnología blockchain ofrece múltiples ventajas, como una reducción de tiempo y costes, y una reconciliación más rápida entre las partes que realizan la transacción. Esto se logra mediante la ausencia de intermediarios. Blockchain utiliza diferentes mecanismos de consenso dependiendo de la red blockchain utilizada para validar información a través de sus nodos. Estos mecanismos son el concepto central del sistema, asegurando un entorno libre de manipulaciones donde todas las transacciones son acordadas por consenso por los nodos de esta red descentralizada.

Blockchain tiene una serie de características que fomenta la creación de aplicaciones alrededor de sus redes. Algunas de las características más importantes son:

- **Reconciliación**: la reducción de tiempo y costes, y la conciliación entre las partes que realizan la transacción se logra mediante la ausencia de una autoridad central. Aunque algunas redes tienen tiempos de reconciliación más rápidos que otras (es decir, alrededor de 10 minutos en Bitcoin frente a 14 segundos en Ethereum), el objetivo de cada red es reducir este tiempo para evitar problemas de escalabilidad. En Bitcoin, por ejemplo, en 2017 y 2018, muchas transacciones pequeñas se retrasaron ya que proporcionaron tarifas de transacción más bajas que las transacciones más grandes para los mineros.
- **Fiabilidad y trazabilidad**: la información se envía a todos los participantes de la red a través del ledger (libro mayor distribuido) y la nueva información se actualiza en tiempo real.

- **Inmutabilidad**: cada bloque se identifica por su hash criptográfico y por el hash del bloque anterior. Esta característica garantiza la seguridad de la cadena ya que no se puede alterar ningún bloque.
- **Consenso en la red**: la cadena de bloques es tan sólida y robusta como su algoritmo de consenso. La red está de acuerdo con el contenido del DLT y solo se asegura de la creación de un nuevo bloque una vez que se llega a un acuerdo. Con este mecanismo, no se necesita una autoridad central.

Desafíos de blockchain

Algunos de los principales desafíos con respecto a las redes blockchain están relacionados con lo siguiente

- **Seguridad**: existen numerosos problemas de seguridad que deben abordarse en blockchain. Por ejemplo, amenazas como el *ataque del 51%* ocurren cuando los atacantes tienen una capacidad de minería superior al 50%, tomando el control total de la cadena de bloques. Esto puede crear bifurcaciones que pueden llevar a que se registren transacciones falsas en la cadena de bloques. Otro problema de seguridad se relaciona con la seguridad del monedero electrónico. Mediante el uso de scripts configurados incorrectamente, se pueden desencadenar fallos de seguridad que pueden resultar en la pérdida total o parcial del monedero electrónico de criptomonedas de un usuario.
- **Escalabilidad**: uno de los principales desafíos de blockchain es la escalabilidad. Hoy en día, se considera que mejorar la escala de la red es un objetivo primordial. El objetivo principal de las criptomonedas es lograr una tasa de transacciones por segundo comparable a la de un sistema centralizado, sin alterar el núcleo de su tecnología.
- **Legal y regulatorio**: El cumplimiento legal y de la regulación por parte de las autoridades en cada jurisdicción es un aspecto muy importante si esta tecnología quiere abrirse camino en el mundo financiero. Por un lado, con respecto a la aplicación de la ley, los reguladores se enfrentan a varios dilemas al abordar este tema. Por otro lado, los responsables de la formulación de políticas podrían caer en la trampa de no incentivar lo suficiente la innovación mediante la expansión adecuada de una regulación adaptada. No poder lograrlo podría significar la pérdida de la ventaja competitiva de un país.
- **Latencia**: Hoy en día, la cantidad de transacciones realizadas por segundo (tps) parecen muy lejanas a las de las tarjetas de crédito (de 2.500 tps en promedio, alcanzando 45.000 tps en su máximo).

A continuación, se resumen los hallazgos más relevantes que se han hallado en esta investigación:

1. Bitcoin: Bitcoin es la primera y más utilizada criptomoneda del mundo. Podría decirse que se considera la criptografía más exitosa jamás creada. Ésta es precisamente su mayor ventaja. Estados Unidos, Japón, Corea del Sur, Italia, Holanda, Reino Unido o Suiza son algunos de los países en los que los usuarios pueden pagar con Bitcoin, ya que es ampliamente aceptado.
2. Ethereum: Ethereum es bien conocido por su robusta funcionalidad y flexibilidad de los contratos inteligentes. Se utiliza ampliamente en numerosas industrias. Esta red ha desarrollado una gran comunidad de soporte en línea que lanza actualizaciones y desarrollos frecuentes de productos, conocida como Ethereum Enterprise Alliance (EEA).
3. Ripple: Ripple's obtiene su ventaja competitiva al proporcionar un mecanismo de pago a bancos, bolsas de activos digitales y corporaciones. Esta red es más adecuada para pagos transfronterizos, lo que permite a las entidades realizar transacciones a través de las fronteras nacionales con tarifas de transacción bajas, mejor escalabilidad y velocidad de procesamiento rápida.

4. EOS: esta plataforma está diseñada para el desarrollo de dApps. Uno de los principales objetivos de la red es ofrecer alojamiento, almacenamiento de soluciones comerciales descentralizadas y experiencia en contratos inteligentes, lo que ayudaría a resolver los problemas de escalabilidad que enfrentan Bitcoin y Ethereum. Esta red tiene su propio foro comunitario, EOS Talk, en el que desarrolladores e inversores discuten lanzamientos y mejoras de la plataforma.
5. Cardano: Cardano nació como un modelo alternativo para la tecnología de contrato inteligente. Está muy centrado en la autenticación formal y el lenguaje funcional. Su consumo de energía es menor en comparación con las redes PoW, debido a que en Ouroboros, solo los líderes electos pueden crear bloques. Una sólida base teórica y definiciones formales del protocolo Ouroboros también son algunas de las ventajas de esta red.

A partir del análisis exhaustivo de las redes y sus protocolos de consenso (Tabla 1), se han sentado las bases para nuevos estudios sobre las aplicaciones emergentes de blockchain en diferentes sectores. Nuestro foco se ha puesto en el análisis de las características más relevantes de cada red. Se espera que este análisis comparativo sirva como guía para una mayor comprensión de las diferentes redes blockchain y la exploración de direcciones de investigación prometedoras que pueden conducir a resultados inspiradores en áreas relacionadas.

	bitcoin	ethereum	ripple	EOS	CARDANO
Moneda	Bitcoin (BTC)	Ether (ETH)	XRP	EOS	ADA
Creación	2009	2014	2013	2017	2017
Algoritmo de Consenso	PoW	PoW	RPCA	DPoS	PoS (Ouroboros)
Contratos inteligentes	No	Si	Si	Si	Si
Suministro de monedas	21,000,000 BTC	No cap	100 billion XRP	No cap	45 billones ADA
Tiempo de generación de bloques	10 minutos	~ 14 segundos	5 to 10 segundos	500 segundos	20 segundos
Transacciones por segundo procesadas	7	15-20	1500	4000	50-250
Tamaño de bloque	1 MB limite	Sobre 2KB	Sin limite	Sin limite	4 KB
Consumo de energía	Muy alta	Alta	Poco	Poco	Poco
Volumen diario ($)	41,185,185,761	19,585,998,814	2,313,819,448	3,836,639,709	190,486,307
Capitalización de mercado ($)	180,963,233,540	30,065,188,433	12,368,433,149	4,181,807,799	1,594,775,788
Lenguaje programación	C++	Solidity	C++	C++	Plutus
Panorama	Alto consumo de energía sin plan de mejora	Alto consumo de energía con un plan para pasar a PoS	El bajo consumo energético garantiza la sostenibilidad futura	El bajo consumo energético garantiza la sostenibilidad futura	El bajo consumo energético garantiza la sostenibilidad futura

Tabla 1. Análisis comparativo de las principales redes blockchain.

2.2 Objetivos iniciales del proyecto y grado de consecución

Los resultados de este proyecto han superado las expectativas iniciales. Los objetivos y grado de consecución se detallan a continuación:

1. Dada la investigación tan novedosa (aunque Bitcoin comenzó en el año 2009, no fue hasta el 2015 en el que se le incluye su cotización en el NYSE), es necesario realizar un análisis profundo del estado del arte de las principales redes blockchain – Completado para las principales redes blockchain (100%).
2. Se realizará un análisis comparativo de las diferentes redes blockchain más importantes. Para significar su importancia, nos centraremos en la capitalización que tienen sus tokens a nivel mundial – Completado para todas las redes (100%).
3. Se estudiará cada una de las características de la red, y se analizará qué tipo de red se ajusta mejor a cada modelo de negocio – Completado para todas las redes (100%).
4. Trataremos de publicar los resultados en una revista de alto impacto y en un congreso internacional – Actualmente se está en proceso de divulgación mediante el envío de los resultados del proyecto a revistas de alto impacto para su publicación.

2.3 Tareas realizadas

Las tareas realizadas han sido las siguientes:

1. Análisis del Estado del Arte y adquisición de conocimiento

2. Estudio las principales redes blockchain y sus características más relevantes.

3. Realización de un análisis técnico de los algoritmos de consenso para cada red identificada en el punto anterior.

4. Evaluación de los resultados obtenidos. Difusión y explotación de los mismos.

2.4 Resultados obtenidos

Los resultados obtenidos son los siguientes.

Resultados para la investigación

Tras el trabajo realizado se dispone de un análisis comparativo de las principales redes blockchain para su utilización. Este resultado tiene un gran valor en nuestro proyecto por dos motivos: (1) facilita y mejora la contribución al mundo académico y (2) permite avanzar hacia el desarrollo de futuras aplicaciones descentralizadas.

Resultados de las principales redes:

Bitcoin: Bitcoin es la criptomoneda más utilizada del mundo. Podría decirse que se considera la criptomoneda más exitosa jamás creada. Ésta es precisamente su mayor ventaja. Estados Unidos, Japón, Corea del Sur, Italia, Holanda, Reino Unido o Suiza son algunos de los países en los que los usuarios pueden pagar con Bitcoin, ya que es ampliamente aceptada. Una de las principales ventajas a la hora de utilizar esta moneda como medio de pago radica en el hecho de que no se requiere DNI o pasaporte para abrir una cuenta. Las cuentas, o direcciones de Bitcoin, se generan a través de una billetera de Bitcoin (conocidas como wallets). En comparación con los métodos tradicionales de transferencia de dinero, las tarifas cuando

se usa Bitcoin son más baratas (los bancos generalmente cobran entre el 3% y el 5% del monto de la transferencia). El uso principal de la red Bitcoin está relacionado con el sector financiero, donde reside su ventaja competitiva.

Ethereum: Ethereum es conocido por su robusta funcionalidad y flexibilidad de los llamados smart contracts. Se utiliza ampliamente en numerosas industrias. Esta red ha desarrollado una gran comunidad de soporte en línea que lanza actualizaciones y desarrollos frecuentes de productos, conocida como Ethereum Enterprise Alliance (EEA). La EEA es una organización sin fines de lucro con más de 250 miembros que conecta a las empresas Fortune 500, las nuevas empresas, el mundo académico y los especialistas en tecnología con los expertos en Ethereum. Ethereum es una plataforma sin permiso (o pública) diseñada para consumo masivo en comparación con las redes de acceso restringido. Además, su protocolo PoW puede provocar problemas de latencia, aunque esto podría cambiar en un futuro cercano con la adopción del algoritmo de consenso PoS más rápido. Las principales dApps (aplicaciones descentralizadas) para las que se está construyendo esta red incluyen: juegos, apuestas, finanzas, redes sociales, billetera y mercados.

Ripple: Ripple obtiene su ventaja competitiva al proporcionar un mecanismo de pago a bancos, casas de cambio, bolsas de activos digitales y corporaciones. Esta red es más adecuada para pagos transfronterizos, lo que permite a las entidades realizar transacciones a través de las fronteras nacionales con tarifas de transacción bajas, mejor escalabilidad y velocidad de procesamiento rápida. Funciona mejor para empresas de gran tamaño con grandes volúmenes en lugar de pequeñas y medianas empresas o usuarios individuales. Empresas como Banco Santander, American Express, MoneyGram International, SBI Holdings o Deloitte, están planeando integrar Ripple para hacer pagos más rápidos y seguros.

EOS: esta plataforma está diseñada para el desarrollo de dApps. Uno de los principales objetivos de la red es ofrecer alojamiento, almacenamiento de soluciones comerciales descentralizadas y experiencia en contratos inteligentes, lo que ayudaría a resolver los problemas de escalabilidad que enfrentan Bitcoin y Ethereum. Esta red tiene su propio foro comunitario, EOS Talk, en el que desarrolladores e inversores discuten lanzamientos y mejoras de la plataforma. En comparación con otras plataformas, los usuarios no pagan para realizar ciertas tareas o enviar mensajes, los productores participan en un sistema de votación para validar transacciones y realizar ediciones en el código fuente, y las cuentas tienen diversos niveles de permisos para guardar datos de manera segura, mejorando su autenticidad. Las principales dApps para las que se está construyendo esta red incluyen: juegos de azar, juegos, redes sociales, intercambios y wallets.

Cardano: Cardano nació como un modelo alternativo para la tecnología de contrato inteligente. Está muy centrado en el lenguaje funcional. Su consumo de energía es menor en comparación con las redes PoW, debido a que en Ouroboros, solo los líderes electos pueden crear bloques. Una sólida base teórica y definiciones formales del protocolo Ouroboros también son algunas de las ventajas de esta red. Aunque actualmente hay muy pocas dApps desarrolladas para la red, con los próximos lanzamientos de Basho y Voltaire, Cardano verá la introducción de sistemas de votación y tesorería, donde los participantes de la red tendrán el poder de usar su participación y derechos de voto para influir en la futura expansión del sistema.

Resultados para el estudiante beneficiario

El estudiante se inició a la investigación en un proyecto multidisciplinar y aplicado en un campo en auge como es el blockchain. El estudiante es firmante de un artículo que se va a presentar a una revista de alto impacto para su publicación.

Resultados para la empresa de apoyo y el municipio de Gijón

Los resultados de investigación obtenidos son muy útiles para ser aprovechados por empresas que quieran implantar esta nueva tecnología.

2.5 Trabajos o necesidades futuras

Se pretende realizar una investigación hacia la implementación de estas redes a aplicaciones reales aumentando su funcionalidad para un uso sencillo y rápido por parte de los usuarios finales. La temática versará sobre el ámbito de organización de empresas.

2.6 Divulgación de los resultados (publicaciones, artículos, ponencias…)

Actualmente se está en proceso de divulgación mediante el envío de los resultados del proyecto a revistas de alto impacto para su publicación.

Referencias

Atzei N., Bartoletti, M, Cimoli, T. (2017) "A survey of Attacks on Ethereum Smart Contracts (SoK)". Principles of Security and Trust (Post 2017), doi: 10.1007/978-3-662-54455-6_8

Biryukov, A., Khovratovich D., (2017), "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," Ledger Journal, vol. 2, pp. 1–30.

Buterin, V. (2013) "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform". https://github.com/ethereum/wiki/wiki/White-Paper. Accessed 3rd September 2020.

David B., Gaži P., Kiayias A., Russell A. (2018) "Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain:. In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – Eurocrypt 2018. Lecture Notes in Computer Science, vol 10821. Springer, doi: https://doi.org/10.1007/978-3-319-78375-8_3

Dennis, R., Disso, J.P. (2019) "An Analysis into the Scalability of Bitcoin and Ethereum", Third International Congress On Information And Communication Technology, Book Series: Advances in Intelligent Systems and Computing, doi: 10.1007/978-981-13-1165-9_57

Dziembowski, S., Faust, S., Kolmogorov V., Pietrzak, K. (2015), "Proofs of space," Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, Aug. 2015, pp. 585–605.

Ethereum Frontier Guide (2019), https://ethereum.gitbooks.io/frontier-guide/, Accessed 13th November 2020.

Eyal, I. (2017) "Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities" Computer, 50, 38–49.

Ripple Inc. (2015), "Implementing the Interledger Protocol in Ripple", https://www.ripple.com/insights/implementing-the-interledger-protocol/. Accessed 25th October 2020.

Rodrigues, B.; Bocek, T.; Stiller, B. (2018) "The Use of Blockchains: Application-Driven Analysis of Applicability" Blockchain Technology, 111, 163–198.

Szabo N. (1994) "Smart Contracts", http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, Accessed 12th September 2020.

Tikhomirov, S. (2018) "Ethereum: State of Knowledge and Research Perspectives", Foundations And Practice Of Security, doi: 10.1007/978-3-319-75650-9_14

3. Memoria económica

Financiación		Personal	Inventariable	Fungible	Otros gastos
IUTA	SV-20-GIJÓN-24	907,81 €			
Otras fuentes	Referencia proyecto/contrato				
Estudiante con ayuda a la investigación	Nombre	Simón Fernández Vázquez			
	Tareas	Análisis de la investigación y compilación de datos			
	Período	24 Julio 2020 – 28 Septiembre 2020			

4. Otros proyectos y contratos con financiación externa

Título del proyecto/contrato	
Referencia	
Investigador/a/es principal/es	
Equipo investigador	
Periodo de vigencia	
Entidad financiadora	
Cantidad subvencionada	