UNIVERSIDAD POLITÉCNICA DE PACHUCA

Maestría en Tecnologías de la Información y Comunicaciones

Materia: Proyecto de Tesis
Actividad: Citas

Nombre del Alumno:
Benjamin Oribe Mendieta
Nombre del Profesor:
Dra.Ocotlán Díaz Parra

1. Blockchain

Normalmente se considera a Blockchain como una sola tecnología, pero en [Halaburda, 2018] se advierte como características propias de la tecnología como la encriptación, el manejo de transacciones distribuido y los contratos inteligentes son tecnologías importantes por si mismas que pueden cambiar varias industrias.

Actualmente se desarrollan varias implementaciones alternativas al método utilizado por Bitcoin para el manejo de inconsistencia por tolerancia Bizantina como en [Bessani et al., 2017] donde crearon un servicio con el sistema Hyperledger Fabric[Bessani et al., 2014].

En [Puthal et al., 2018] presentan un análisis de las posibilidades de blockchain para solventar problemas de seguridad y validación de transacciones.

1.1. Seguridad

Blockchain no es inmune a ataques, en [Hasanova et al., 2019] y [Apostolaki et al., 2017]se muestran las vulnerabilidades de esta tecnología como el ataque de DDOS a Ethereum en 2016[Atzei et al., 2016]. En el trabajo de [Destefanis et al., 2018] se describe como el programar de manera insegura los *smart contracts* de Etherewum([Buterin, 2016]) llevo a un congelamiento de 500 Ethers por medio de la wallet *Parity*[Par, 2020] en 2017.

Los sistemas criptográficos de firma digital se consideran vulnerables ante ataques por métodos cuánticos, en [Li et al., 2018] se presentan una opción por medio del algoritmo de Arboles Bonsai[Cash et al., 2010] y el algoritmo de *RandBasis* para[Sciabarra, 2013] crear wallets no deterministas para aplicaciones de blockchain. [Xu, 2016] hace un listado de al menos 4 tipos de amenazas a los sistema blockchain.

En [Gervais et al., 2016] desarrollan un framework capaz de analizar la vulnerabilidad de varias plataformas blockchain a diferentes grupos de ataques, con interés en el ataque de Eclipse([Wüst and Gervais, 2016]).

En [Wüst and Gervais, 2016] se hace un análisis a los ataques por medio de Eclipse a la plataforma Ethereum y en [Nayak et al., 2016] se maneja el crecimiento de estos ataques en general y sobre el crecimiento de la minería no egoísta de cripto monedas.

Las cripto monedas es uno de los mas populares sectores de implementación de blockchain, muchas nuevas se unen a bitcoin[Nakamoto et al., 2008], en [Chan et al., 2017], se hace un análisis las estadísticas principales de las principales monedas en el mercado. En [Kyriazis, 2019] se busca ver si el precio de las cripto monedas principales así como esta se relaciona con la eficiencia de cada una. Por su parte [Ivanov et al., 2018] genera una plataforma de comparación para analizar los aspectos técnicos de las plataformas principales de cripto monedas para determinar la mejor para resolver cada problema específico.

1.2. Mejoras

Existen muchas cripto monedas en el mercado y atrae a muchas organizaciones, en [Members, 2019] Facebook presenta Libra, una cripto moneda para el pago de servicios que busca ser soportada por organizaciones gubernamentales y bancarias, en [Taskinsoy, 2019] se intenta advertir si Libra puede cumplir la idea de una cripto moneda para las transacciones de todos los días.

Aunque uno de los pilares de las plataformas Blockchain es la transparencia de las operaciones, también existen investigaciones como la de [Feng et al., 2019] donde analiza protección de la privacidad en sistemas Blockchain. En [Esposito et al., 2018] se analiza si Blockchain puede ser una opción para la privacidad en registros médicos compartidos. [Jiang et al., 2019] analizan la

privacidad de un sistema de llave publica para clientes livianos. En [Lemieux, 2016]se advierte si la tecnología blockchain actual es capas de mantener un sistema de registro conmfiable usando la plataforma como ejemplo Bitcoin y Factom([Snow et al., 2015]).

La obtención del proof-of-work es uno de los pasos de Blockchain donde existe espacio para mejorar en [Hazari and Mahmoud, 2019] presentan un método para hacer el proceso de minado de manera paralela. En [Kang et al., 2018] se genera un sistema para la rápida propagación del consenso de nodos en sistemas basados en Proof-Stake([Kiayias et al., 2017]) utilizando un juego de Stackelberg([Zhang and Zhang, 2009]) para maximizar la ganancia de los mineros.

En [Saleh, 2020] se presenta un modelo económico basado en proof-of-stake donde se puede obtener el consenso de manera general al evitar que los .ªccionistasretrasen el consenso. En [Liu et al., 2019] se busca crear un modelo consenso hibrido basado en el Proof-of-activity de [Bentov et al., 2014] y la implementación de [Pass and Shi, 2017] que permite un modelo libre de *forks*.

También [Yoo et al., 2018] advierten que la estrategia no cooperativa de Ethereum ayuda a que la generación de bloques vacíos (sin transacciones) sean mas comunes, lo cual reduce la velocidad de proceso de transacciones y proponen un sistema con una estrategia cooperativa para solucionar este problema.

Existe un lado ecológico que se debe tomar en cuenta para los sistemas Blockchain,[Li et al., 2019] hace el análisis de la energía requerida en un año para minar la cripto moneda *Monero* [Mon, 2020]. Por su parte [Krause and Tolaymat, 2018] analiza los factores que influyen en marca de carbono de la minería de cripto monedas.

1.3. Aplicaciones

Blockchain ha atraído a varios mercados, de esta manera, [Cai et al., 2018] han hecho un survey de las posibles aplicaciones que se verían beneficiadas del uso de esta arquitectura/plataforma. Así mismo [Singh et al., 2020] analizan las posibilidades y retos inherentes en formalizar los contratos inteligentes por medio de blockchain.

Blockchain y su implementación es de mucha importancia para las aplicaciones de la industria, en [Mohamed and Al-Jaroodi, 2019] se muestra un listado de los puntos en los cuales la tecnología blockchain tendría un impacto para la implementación de la industria 4.0 ([Lasi et al., 2014]).

En [Yi, 2019] se busca implementar un sistema seguro para sistemas de voto electrónico.

La implementación de Internet of Things requiere de unión de varias tecnologías para poder implementarse cabalmente, en [Dai et al., 2019] y [Wang et al., 2019a] se hace un listado de como blockchain puede ayudar en este proceso. En el proyecto de [Alphand et al., 2018] se propone un concepto IoTChain, una combinación de la arquitectura OSCAR([Vučinić et al., 2015]) y el framework de autorización ACE ([Seitz et al., 2017] para manejo de clientes de IOT entre nodos finales.

Para reducir la letencia ente dispositivos parta IOT en [Sharma and Park, 2018] proponen una arquitectura híbrida por software que maneje secciones centralizadas y descentralizadas para su implementación sen ciudades inteligentes.

En el trabajo de [Khan and Salah, 2018] se analizan los aspectos a tomar en cuenta a nivel de seguridad de implementar sistemas basados en Blockchain para IOT.

En [Motohashi et al., 2019] analiza y diseña un sistema para manejar sistema de Salud Móvil (mHealth) basado en blockchain. En el mismo ámbito [Cao et al., 2019] diseñan un sistema basado en la nube para manejo electrónico de registros médicos electrónicos.

Dentro del survey de [Rabah, 2018] se analiza los puntos en que tecnologías como blockchain convergen cono IoT, el análisis de Big Data y la Inteligencia Artificial.

En campo de la robótica [Ferrer, 2018] presenta como blockchain puede solventar problemas en los campos de seguridad, toma de desiciones, diferenciación de comportamientos y modelos de negocios para el campo de la robótica de enjambres.

2. Hashchain

Las funciones hash para el manejo de firmas digitales, y es necesario tener implementaciones de las mas conocidas para varios dispositivos. [Osvik, 2012] presentan un listado de eficiencia de las implementaciones de funciones hash en para sistemas embebidos, mientras [kyu Kang et al., 2002] desarrollan una función hash implementación para procesadores IPSEC, [Cheng et al., 2018] desarrollan una implementación de SHA-512 para procesadores ARV, comunes en las tarjetas arduino. En [Kim and Shin, 2018] se desarrolla una implementación de SHA-3 para sistemas en un chip (SOC) para procesadores ARM.

En [Wang et al., 2019b] se desarrolla un protocolo de identificación de mensajes por medio de una función hash cuántica, basada en quantum walks ([Li et al., 2013]).

El IOT también busca en la firma por medio de hash chains([Lamport, 1981] una manera segura de firmar información, en [Alshahrani and Traore, 2019] crean un a identidad temporal basado en hash chain para identificación mutua y control automatizado para hogares inteligentes.

En [Jeong, 2020] se desarrolla un sistema para recuperación de información multimedia para sistema distribuidos para IoT basado en hash chains.

En [Tariq et al., 2018] se utilizan hash chains para analizar la entrada de datos falsos en redes de sensores inalámbricos tomando en cuanta sus limitadas capacidades de procesamiento. A si mismo —citelu2018research utiliza hash chains para resolver el problema de falta de autentificación en el modo de trasnmisión de las redes DNP3([Clarke et al., 2004]).

Una de las aplicaciones mas comunes de hash chains es la generación de passwords temporales como se muestras en la implementación de [Park, 2018].

Referencias

[Par, 2020] ((acceso Junio 2, 2020)). *Blockchain Infrastructure for the Decentralised Web.* https://www.parity.io/.

[Mon, 2020] ((acceso Junio 2, 2020)). *MONERO, A Reasonably Private Digital Currency.* https://getmonero.org.

[Alphand et al., 2018] Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L., and Zanichelli, F. (2018). Iotchain: A blockchain security architecture for the internet of things. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE.

[Alshahrani and Traore, 2019] Alshahrani, M. and Traore, I. (2019). Secure mutual authentication and automated access control for iot smart home using cumulative keyed-hash chain. *Journal of information security and applications*, 45:156–175.

[Apostolaki et al., 2017] Apostolaki, M., Zohar, A., and Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 375–392. IEEE.

[Atzei et al., 2016] Atzei, N., Bartoletti, M., and Cimoli, T. (2016). A survey of attacks on ethereum smart contracts. *IACR Cryptology ePrint archive*, 2016:1007.

[Bentov et al., 2014] Bentov, I., Lee, C., Mizrahi, A., and Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Performance Evaluation Review*, 42(3):34–37.

[Bessani et al., 2014] Bessani, A., Sousa, J., and Alchieri, E. E. (2014). State machine replication for the masses with bft-smart. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 355–362. IEEE.

[Bessani et al., 2017] Bessani, A., Sousa, J. a., and Vukolić, M. (2017). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, SERIAL '17, New York, NY, USA. Association for Computing Machinery.

[Buterin, 2016] Buterin, V. (2016). What is ethereum? *Ethereum Official webpage. Available: http://www. ethdocs. org/en/latest/introduction/what-is-ethereum. html*.

[Cai et al., 2018] Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., and Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE Access*, 6:53019–53033.

[Cao et al., 2019] Cao, S., Zhang, G., Liu, P., Zhang, X., and Neri, F. (2019). Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain. *Information Sciences*, 485:427–440.

[Cash et al., 2010] Cash, D., Hofheinz, D., Kiltz, E., and Peikert, C. (2010). Bonsai trees, or how to delegate a lattice basis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 523–552. Springer.

[Chan et al., 2017] Chan, S., Chu, J., Nadarajah, S., and Osterrieder, J. (2017). A statistical analysis of cryptocurrencies. *Journal of Risk and Financial Management*, 10(2):12.

[Cheng et al., 2018] Cheng, H., Dinu, D., and Großschädl, J. (2018). Efficient implementation of the sha-512 hash function for 8-bit avr microcontrollers. In *International Conference on Security for Information Technology and Communications*, pages 273–287. Springer.

[Clarke et al., 2004] Clarke, G., Reynders, D., and Wright, E. (2004). *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes.

[Dai et al., 2019] Dai, H.-N., Zheng, Z., and Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal*, 6(5):8076–8094.

[Destefanis et al., 2018] Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., and Hierons, R. (2018). Smart contracts vulnerabilities: a call for blockchain software engineering? In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pages 19–25. IEEE.

[Esposito et al., 2018] Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K.-K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37.

[Feng et al., 2019] Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58.

[Ferrer, 2018] Ferrer, E. C. (2018). The blockchain: a new framework for robotic swarm systems. In *Proceedings of the future technologies conference*, pages 1037–1058. Springer.

[Gervais et al., 2016] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16.

[Halaburda, 2018] Halaburda, H. (2018). Blockchain revolution without the blockchain? *Communications of the ACM*, 61(7):27–29.

[Hasanova et al., 2019] Hasanova, H., Baek, U.-j., Shin, M.-g., Cho, K., and Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management*, 29(2):e2060.

[Hazari and Mahmoud, 2019] Hazari, S. S. and Mahmoud, Q. H. (2019). A parallel proof of work to improve transaction speed and scalability in blockchain systems. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0916–0921. IEEE.

[Ivanov et al., 2018] Ivanov, A., Babichenko, Y., Kanunnikov, H., Karpus, P., Foiu-Khatskevych, L., Kravchenko, R., Gorokhovskyi, K., and Nevmerzhitskyi, I. (2018). Technical comparison aspects of leading blockchain-based platforms on key characteristics.

[Jeong, 2020] Jeong, Y.-S. (2020). Multi-hash chain based multimedia search technology optimized for distributed environments using iot devices. *Multimedia Tools and Applications*, pages 1–18.

[Jiang et al., 2019] Jiang, W., Li, H., Xu, G., Wen, M., Dong, G., and Lin, X. (2019). Ptas: Privacy-preserving thin-client authentication scheme in blockchain-based pki. *Future Generation Computer Systems*, 96:185–195.

[Kang et al., 2018] Kang, J., Xiong, Z., Niyato, D., Wang, P., Ye, D., and Kim, D. I. (2018). Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks. *IEEE Wireless Communications Letters*, 8(1):157–160.

[Khan and Salah, 2018] Khan, M. A. and Salah, K. (2018). Iot security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411.

[Kiayias et al., 2017] Kiayias, A., Russell, A., David, B., and Oliynykov, R. (2017). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer.

[Kim and Shin, 2018] Kim, D.-S. and Shin, K.-W. (2018). An optimized hardware implementation of sha-3 hash functions. *Journal of IKEEE*, 22(4):886–895.

[Krause and Tolaymat, 2018] Krause, M. J. and Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, 1(11):711–718.

[Kyriazis, 2019] Kyriazis, N. A. (2019). A survey on efficiency and profitable trading opportunities in cryptocurrency markets. *Journal of Risk and Financial Management*, 12(2):67.

[kyu Kang et al., 2002] kyu Kang, Y., Kim, D. W., Kwon, T. W., and Choi, J. R. (2002). An efficient implementation of hash function processor for ipsec. In *Proceedings of Third IEEE Asia-Pacific Conference on ASICs, Taipei, Taiwan*. Citeseer.

[Lamport, 1981] Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772.

[Lasi et al., 2014] Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., and Hoffmann, M. (2014). Industry 4.0. *Business & information systems engineering*, 6(4):239–242.

[Lemieux, 2016] Lemieux, V. L. (2016). Trusting records: is blockchain technology the answer? *Records Management Journal*.

[Li et al., 2018] Li, C.-Y., Chen, X.-B., Chen, Y.-L., Hou, Y.-Y., and Li, J. (2018). A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, 7:2026–2033.

[Li et al., 2013] Li, D., Zhang, J., Guo, F.-Z., Huang, W., Wen, Q.-Y., and Chen, H. (2013). Discrete-time interacting quantum walks and quantum hash schemes. *Quantum information processing*, 12(3):1501–1513.

[Li et al., 2019] Li, J., Li, N., Peng, J., Cui, H., and Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*, 168:160–168.

[Liu et al., 2019] Liu, Z., Tang, S., Chow, S. S., Liu, Z., and Long, Y. (2019). Fork-free hybrid consensus with flexible proof-of-activity. *Future Generation Computer Systems*, 96:515–524.

[Members, 2019] Members, L. A. (2019). Libra White Paper. Technical report.

[Mohamed and Al-Jaroodi, 2019] Mohamed, N. and Al-Jaroodi, J. (2019). Applying blockchain in industry 4.0 applications. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0852–0858. IEEE.

[Motohashi et al., 2019] Motohashi, T., Hirano, T., Okumura, K., Kashiyama, M., Ichikawa, D., and Ueno, T. (2019). Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation. *Journal of medical Internet research*, 21(5):e13385.

[Nakamoto et al., 2008] Nakamoto, S. et al. (2008). Bitcoin: A peer-to-peer electronic cash system.

[Nayak et al., 2016] Nayak, K., Kumar, S., Miller, A., and Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 305–320. IEEE.

[Osvik, 2012] Osvik, D. A. (2012). Fast embedded software hashing. *IACR Cryptology ePrint Archive*, 2012:156.

[Park, 2018] Park, C.-S. (2018). One-time password based on hash chain without shared secret and re-registration. *Computers & Security*, 75:138–146.

[Pass and Shi, 2017] Pass, R. and Shi, E. (2017). Hybrid consensus: Efficient consensus in the permissionless model. In *31st International Symposium on Distributed Computing (DISC 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[Puthal et al., 2018] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., and Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21.

[Rabah, 2018] Rabah, K. (2018). Convergence of ai, iot, big data and blockchain: a review. *The Lake Institute Journal*, 1(1):1–18.

[Saleh, 2020] Saleh, F. (2020). Blockchain without waste: Proof-of-stake. *Available at SSRN 3183935*.

[Sciabarra, 2013] Sciabarra, C. M. (2013). *Ayn Rand: The Russian Radical*. Penn State Press.

[Seitz et al., 2017] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and Tschofenig, H. (2017). Authentication and authorization for constrained environments (ace). *Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07*.

[Sharma and Park, 2018] Sharma, P. K. and Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, 86:650–655.

[Singh et al., 2020] Singh, A., Parizi, R. M., Zhang, Q., Choo, K.-K. R., and Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, 88:101654.

[Snow et al., 2015] Snow, P., Deery, B., Kirby, P., and Johnston, D. (2015). Factom ledger by consensus.

[Tariq et al., 2018] Tariq, M., Khan, M., and Fatima, S. (2018). Detection of false data in wireless sensor network using hash chain. In *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, pages 126–129. IEEE.

[Taskinsoy, 2019] Taskinsoy, J. (2019). Facebook's project libra: Will libra sputter out or spur central banks to introduce their own unique cryptocurrency projects? *Available at SSRN 3423453*.

[Vučinić et al., 2015] Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., and Guizzetti, R. (2015). Oscar: Object security architecture for the internet of things. *Ad Hoc Networks*, 32:3–16.

[Wang et al., 2019a] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., and Zheng, K. (2019a). Survey on blockchain for internet of things. *Computer Communications*, 136:10–29.

[Wang et al., 2019b] Wang, Y., Chen, Y., Ahmad, H., and Wei, Z. (2019b). Message authentication with a new quantum hash function. *CMC-COMPUTERS MATERIALS & CONTINUA*, 59(2):635–648.

[Wüst and Gervais, 2016] Wüst, K. and Gervais, A. (2016). Ethereum eclipse attacks. Technical report, ETH Zurich.

[Xu, 2016] Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation*, 2(1):1–9.

[Yi, 2019] Yi, H. (2019). Securing e-voting based on blockchain in p2p network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1):1–9.

[Yoo et al., 2018] Yoo, S., Kim, S., Joy, J., and Gerla, M. (2018). Promoting cooperative strategies on proof-of-work blockchain. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE.

[Zhang and Zhang, 2009] Zhang, J. and Zhang, Q. (2009). Stackelberg game for utility-based cooperative cognitiveradio networks. In *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, pages 23–32.