risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 11/02/2019
Aceitação/Acceptance: 22/04/2019

Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada

Ignacio Gallardo[1 2], Patricia Bazan[2], Paula Venosa[2]

igallardo@est.iue.edu.ar, pbaz@info.unlp.edu.ar, pvenosa@info.unlp.edu.ar

[1] Universidad de la Defensa Nacional - Facultad de Ingeniería, Palermo, CABA, Argentina.

[2] Universidad Nacional de la Plata - Facultad de Informática - Laboratorio de Investigación de Nuevas Tecnologías Informáticas, La Plata, Argentina.

DOI: 10.17013/risti.32.49–66

Resumen: Los principales esfuerzos de los últimos años se han concentrado en el problema de asignar de forma segura nombres a claves públicas, de hecho, la comunidad científica adoptó progresivamente el uso de sistemas basados en Public Key Infrastructure (PKI) con el fin de proporcionar servicios de seguridad a los sistemas, los cuales dependen de la existencia de una arquitectura centralizada y jerárquica. Esta misma problemática se traspola a la gestión del comercio electrónico, donde en el modelo inicial se requería de una entidad central que debía emitir divisa electrónica a los diferentes usuarios, no obstante, en 2009, Satoshi Nakamoto crea Bitcoin: una criptomoneda con tecnología peer-to-peer para operar sin una autoridad central o bancos. En esta investigación se aplica en PKI lo mismo que logró Nakamoto en el comercio electrónico, una reingeniería, migrando una arquitectura centralizada y jerárquica a una completamente descentralizada por medio de su innovación tecnológica llamada Blockchain.

Palabras-clave: PKI; certificados digitales; blockchain; bitcoin, ciberseguridad.

Architecture of Certificates: form a hierarchical architecture and centralized to a distributed and decentralized

Abstract: The main efforts of recent years have focused on the problem of set a name securely to public keys, in fact, the scientific community has been gradually adopting the use of systems based in Public Key Infrastructure (PKI) in order to provide security services. However, that systems depend on the existence of a centralized and hierarchical method. This same problem is translated into the management of electronic commerce, which presents a central entity that must issue electronic currency to different users. In 2009, Satoshi Nakamoto creates Bitcoin: a peer-to-peer technology to operate without a central authority or banks. This investigation applies in PKI the same concepts that Nakamoto applied in the electronic commerce, a reengineering and a paradigm shift, a migration from a

centralized and hierarchical architecture to a decentralized and not hierarchical through the innovative technology called Blockchain.

***Keywords**:* PKI; digital certificates; blockchain; bitcoin, cybersecurity.

1. Introducción

Una forma de entender qué es una ***blockchain*** (Bahga, A., & Madisetti, V., 2017) es antes comprender qué es una **criptomoneda** con sus diferencias respecto del dinero electrónico, y para comprender fácilmente estos conceptos, primero hay que definir qué es una moneda fiduciaria (Adams, M., 2016).

Moneda fiduciaria es toda moneda de curso legal designada y emitida por una **autoridad central** que las personas están dispuestas a aceptar a cambio de productos o servicios porque está respaldada por la regulación vigente y por la **confianza** en dicha autoridad central.

El dinero fiduciario es similar al dinero respaldado por los productos básicos en apariencia y uso, pero no puede ser canjeado por uno de esos productos, como por ejemplo la plata y/o el oro.

Por el contrario, una **moneda virtual** es un tipo de **dinero digital** no regulado que emiten y controlan sus creadores, y que se utilizan y aceptan entre miembros de la comunidad virtual (Capoti, D., Colacchi, E., & Maggioni, M., 2015).

La criptodivisa **Bitcoin** (Capoti, D., Colacchi, E., & Maggioni, M. 2015) surgió en el año 2009 como una alternativa a la moneda fiduciaria, con la diferencia que éstos no se emiten como este último, sino que se "extraen" mediante un procedimiento denominado "minería de bitcoins" utilizando la capacidad de una inmensa red de cómputo conectada y distribuida a través de todo el mundo. Esta tecnología surge con el objetivo de **descentralizar** los pagos entre usuarios, eliminando la necesidad de la **presencia de instituciones** financieras en las transacciones. Para llevar a cabo estos requerimientos, bitcoin se despliega en una **red P2P** (Peer to Peer) (Steinmetz, R., Wehrle, K., 2005). por la cual se mantienen, distribuyen y coexisten todas las transacciones asegurando la **no alteración** de las mismas sin tener que realizar operaciones demasiadas exigentes desde el punto de vista computacional para converger todo el sistema (Nakamoto, S., 2009).

Esencialmente, no solo Bitcoin sino las demás criptomonedas como Ethereum, Litecoin, Ripple, etc. son nada más ni menos que un archivo digital donde se enumeran todas las transacciones de la red al mejor estilo "libro de contabilidad", con la peculiaridad que este mismo, se encuentra presente en todos los participantes del juego y no puede ser alterado.

Aparte del formato digital, son mínimas las similitudes entre el dinero electrónico y las criptomonedas. El dinero electrónico, como muchos otros formatos digitales de la moneda fiduciaria —como las tarjetas de crédito y débito, PayPal y las transferencias electrónicas—, es simplemente un mecanismo mediante el cual se interactúa con esa moneda fiduciaria. Para mitigar riesgos sistémicos y de protección del consumidor, el efectivo que respalda el dinero electrónico emitido habitualmente se deposita en

instituciones financieras que siguen todas las regulaciones prudenciales. A diferencia de la moneda criptográfica, el dinero electrónico no es una moneda individual y está supervisado por la misma autoridad central que controla la moneda nacional que lo respalda.

Este sistema inicialmente aplicado a las criptomonedas es el primer ejemplo de una creciente revolución teleinformática, potencialmente aplicable a infinitas áreas de conocimiento, en la que mediante software de código abierto se resuelven **sincronizadamente** cálculos matemáticos para **validar todas las operaciones** realizadas por cada individuo perteneciente a la red sin necesidad de ser comandados y regulados por un **ente central**, y no obstante, **manteniendo la integridad**, **máxima disponibilidad** del historial de las transacciones, y **desconcentrando** no solo la confianza en esta única autoridad central, sino también la información y los procesos, lo cual proporciona una ventaja a la hora de la existencia de una violación a la seguridad.

De todo este procedimiento descripto surge el término **cadena de bloques** o ***blockchain*** —mecanismo utilizado por Bitcoin— ya que todas las operaciones de la red se acumulan en bloques de transacciones y estos mismos se van adjuntando entre sí formando una cadena y aplicando los conceptos de un árbol de **Merkle**, no obstante, existe una réplica irrevocable de este árbol —archivo digital— en todos los integrantes del sistema mantenido a la orden del día (Nakamoto, S., 2009).

Resulta llamativo pensar que una tecnología implementada hace menos de nueve años y desarrollada por una persona desconocida podría pasar a ser más eficiente, confiable y popular que ya varias décadas de la vigencia del dinero electrónico, pero la realidad es que toda su arquitectura y diseño contempla hasta el último detalle a la hora de pensar en confiabilidad, robustez y seguridad.

El objetivo general de este trabajo consiste en analizar y seleccionar los conceptos de descentralización, distribución, validación masiva y comunitaria, sincronismo, integridad, transparencia, escalabilidad, redundancia y confiabilidad presentes en ***blockchain*** o **cadena de bloques,** para poder extraerlos y aplicarlos en una propuesta de rediseño y mejora a otro ámbito que ya lleva bastante tiempo de estudio desde el punto de vista no solo de la seguridad sino también de la ingeniería de software llamado: Arquitectura de **Certificados Digitales** o **Infraestructura de clave pública** (Vimercati, S. D., & Mitchell, C., 2013). Estas ventajas serán aprovechadas volcando de forma teórica en la modificación del diseño y arquitectura existente en los **certificados digitales** (Thomas, S. A., 2000).

Este trabajo integra conocimientos avanzados de Seguridad en Teleinformática, Criptografía, **Criptodivisas**, Arquitectura de **certificados digitales**, Arquitectura de sistemas distribuidos, ***Blockchain*** (Gallardo, I., 2018).

2. Motivación y Estado del Arte

Las redes P2P (Steinmetz, R.; Wehrle, K., 2005).) presentan características que las convierten en un activo para el que es difícil encontrar comparación en el mundo real. En primer lugar, porque las conforman sistemas distribuidos y vivos que no presentan un único punto de fallo y que toleran la desconexión de algunos de ellos de forma flexible

y sin dejar que el funcionamiento de la red en su conjunto se vea comprometida. Se trata de organismos cuya robustez radica precisamente en el número de nodos que las componen y en cómo estos están conectados unos a otros.

Con esto, se puede afirmar que la aparición de los métodos de pago modernos que exploten la potencia de estas tecnologías es el fruto de la evolución natural del marco tecnológico reciente.

La materialización de las criptomonedas como fenómeno contemporáneo tiene un trasfondo ideológico muy ligado a conceptos que forman parte de la cultura *hacker* tradicional: evitar la hasta ahora necesaria presencia de un organismo central de control financiero que es considerado como poco democrático y potencialmente corrompible. Aunque las implicaciones de una economía desregulada y el reparto de divisas son materias controvertidas que se han afrontado desde cada comunidad con puntos de vistas diferentes, la consecución de estos objetivos requiere, desde un punto de vista técnico, la colaboración de distintas entidades que asuman aunadas ese rol de organismo central multifacético. Si a su naturaleza descentralizada (Shane, P. M., & Hunker, J. A., 2013) se le suma que los nodos que forman parte de la red no tienen por qué ser conocidos entre sí y que, aun así, tienen que ser capaces de seguir funcionando de forma consensuada incluso en un escenario en el que hay que dar por supuesta la presencia de agentes no confiables, permite toparse con un escenario real del conocido *problema de los generales bizantinos de tolerancia a fallos* (Byzantine Fault Tolerance o BFT).

El libro mayor de contabilidad distribuido ***blockchain*** (basado en una arquitectura de comunicaciones P2P) (Steinmetz, R.; Wehrle, K., 2005)., fue creado, para registrar, organizar y sostener la más importante criptomoneda, el Bitcoin, pero eso no quiere decir que esta tecnología pueda utilizarse sólo para ello. De hecho, ahora es cuando la ***blockchain*** tiene casi ilimitadas puertas por abrir: si ella es capaz de registrar digitalmente, de forma segura y pública a la vez, todo el ciclo de vida de cada bitcoin; en teoría, también puede registrar todo el ciclo de vida de cualquier otra cosa (desde facturas de hospital, hasta diamantes).

En contraste a esto, y polarizando los mismos conceptos, la idea de descartar la estructura jerárquica en la que se basa hoy en día la infraestructura PKI (Nash, A., 2002), logra no sólo una total transparencia en la emisión de certificados sino también se disipa el riesgo y aumenta la confiabilidad, ya que no existe una entidad central de gestión. Por otro lado, la arquitectura **propuesta** proporcionará a los usuarios eficiencia total en el proceso de gestión de certificados, ya que ahorraría tiempo (eliminando las cuestiones burocráticas de papelerías), tediosas configuraciones y dinero (Gallardo, I., 2018).

2.1. Propuestas Similares

Existen varias propuestas de investigación y desarrollo o implementaciones que abordan problemáticas similares a la de promover una reingeniería y rediseño de la infraestructura de clave pública actual. Entre estas, algunas abordan extendiendo funcionalidades, otra reemplazando la arquitectura actual y desde distintos puntos de vista, por ejemplo:

- Certificate Transparency Using Blockchain: Es una propuesta realizada por estudiantes de la Universidad de Ashoka que pretende implementar una PKI distribuida utilizando una plataforma de IBM para interactuar con una

blockchain de negocios open source (Jhanwar, M. P., Chattopadhyay, A., Madala, D. S. V., 2018).

- BlockPGP, a Blockchain-based Framework for PGP Key Servers: Es un proyecto presentado por la Universidad de Luxemburgo, en donde se pretende reemplazar los servidores de claves PGP por un repositorio de claves PGP distribuidas sobre blockchain, en particular, la cadena de bloques de Ethereum (Yakubov, A., Shbair, W. M., State, R., 2018).
- CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections: Es una solución de auditoría de gestión de certificados digitales de la PKI sobre blockchain presentado en un congreso en Honolulu, HI, USA (Chen, J., Yao, S., Yuan, Q., He, K, Ji, S., Du, R., 2018).
- Decentralized Public Key Infrastructure for Internet-of-Things: Es la solución que estratégicamente se parece más a la presentada en este trabajo de investigación, pero con la diferencia de que se aplica para dispositivos IoT y presenta un proceso diferente de validación de identidades. Este trabajo fué presentado en Washington, USA (Won, J., Singla, A., Bertino, E., Bollella, G., 2018).
- PTAS, Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI: Es una implementación presentada por investigadores Chinos, que aborda un proceso de autenticación innovador vía blockchain para seguridad en dispositivos de IoT (Jiang, W., Li, H., Xu et al, G., 2019).
- BlockPKI, an Automated, Resilient, and Transparent Public-Key Infrastructure: En este trabajo, investigadores singapurenses agregan a la PKI un tercero de confianza, el cual, este último se materializa en una blockchain (Dykcik, L., Chuat, L., Szalachowski, P., Perring, A., 2018).

Como se puede ver en la breve descripción de cada solución propuesta, al igual que la presentada en este trabajo, todas abordan la problemática que existe a la hora de confiar en un ente central y jerárquico, no obstante, presentan implementaciones montadas sobre blockchain con el fin de disipar este potencial riesgo de seguridad, descansando en una arquitectura descentralizada y no jerárquica. Como se pueden apreciar en las diferentes publicaciones, esta problemática es tan amplia que es abordada por investigadores de diferentes partes del mundo.

Lo que sí debe quedar claro es que la diferencia principal y totalmente innovadora que presenta este trabajo presentado por investigadores argentinos, llamado "Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada" es que se realiza una reingeniería y rediseño, migrando totalmente la PKI a una arquitectura de certificados digitales sobre blockchain, presentando nuevos procedimientos e innovadores en cada etapa existente en la infraestructura de clave pública, aplicado específicamente para servicios HTTPs y finalmente soportando la integración con la arquitectura actual PKI.

3. Metodología

Se realizó un estudio en profundidad de la tecnología ***blockchain*** evaluando sus fortalezas y debilidades para luego realizar una propuesta utilizando su esencia y procedimientos de aseguramiento y confiabilidad en las transacciones para aplicar

en el campo de la emisión, validación y manejo de **certificados digitales** de clave pública/privada. ***Blockchain***, entre unas de sus funcionalidades, logra validar de forma distribuida y así determinar del lado del receptor si el emisor de la transacción es quien dice ser. Con la aplicación de esta característica sumada a otros procedimientos implementados en otras tecnologías como ser: Criptografía Contemporánea (Blake, I. F., Seroussi, G., & Smart, N. P., 1999), Arquitecturas Distribuidas (Zhao, W., 2014), **Certificados Digitales** (Leuf, B., 2002) y Conceptos de Seguridad Informática (Vacca, J. R., & Vacca, J. R., 2013), se logró eliminar las jerarquías de autoridades certificadoras, descentralizando la arquitectura. Para que dicha propuesta haya funcionado se debió cumplir tres características importantes. La primera y como se mencionó antes, debió ser descentralizada -al no existir un ente centralizador para emitir **certificados digitales**, esta actividad será realizada de forma repartida entre los participantes de la red-. También debió ser distribuida, ya que cada nodo funcionará como cliente/servidor y teniendo una copia de la base de datos de todo el sistema. Por último, el sistema fué totalmente auditable por cualquier nodo para así poder determinar anomalías en la red.

Para enriquecer el estudio exclusivo de esta tecnología, se abordó un análisis cualitativo de la arquitectura de gestión de certificados digitales vigente a fin de detectar y exponer las debilidades. En base a ello se elaboró una propuesta de rediseño de la arquitectura para así cubrir dicha endeblez. Finalmente se implementó un prototipo que permitió validar dicha propuesta (Gallardo, I., 2018).

4. Desarrollo Experimental

Para validar la propuesta y probar los flujos propuestos en su funcionamiento se desarrolló un componente de software que está compuesto por cuatro módulos e interactúa con otros dos. El componente fue desarrollado en Java (Lafosse, J., 2009) y Typescript (Pardi, P., 2015).

El módulo de software número uno (denominado **PkChain**) se encarga de la columna vertebral de esta propuesta, es decir, realiza una simulación del funcionamiento de ***blockchain*** que permitirá utilizar su "API" (Masse´, M., 2012) para luego incorporar las siguientes funcionalidades.

El segundo módulo emula a la arquitectura de comunicación peer-to-peer (denominado **Gestor de Servicios**) para así poder tener este tipo de conectividad entre los diferentes nodos ***blockchain*** como propone el protocolo de Bitcoin.

El tercer componente de software agrega a la **cadena de bloques** la inteligencia propuesta en este trabajo. Está inteligencia tiene el rol de un plugin/librería para la **PkChain**, y se denominará **LibCerts**.

El cuarto módulo es un **Cliente PkChain**, que básicamente consume la red ***blockchain*** como un nodo de la red.

Finalmente, para lograr la prueba de todo el procedimiento de verificación, validación, emisión y revocación de certificados se crea un **Cliente Web** que realiza consultas a un **Servidor Web** que también se lo implementó (Gallardo, I., 2018).

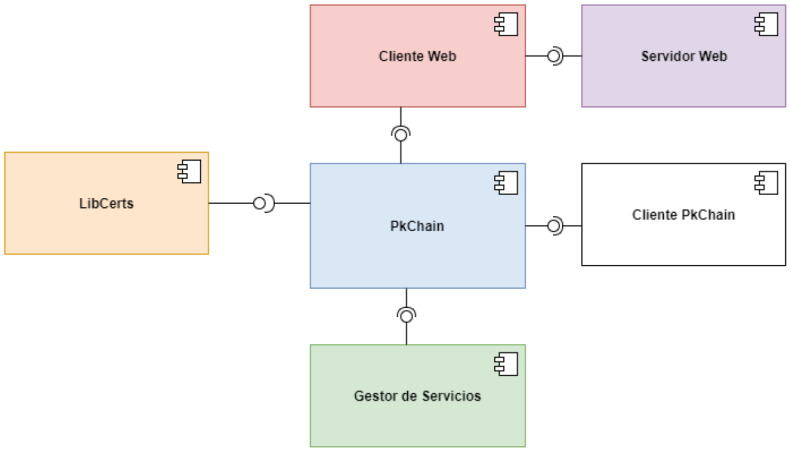

Figura 1 – Diagrama de Componentes de la Propuesta

4.1. Procesos y Operaciones de la Arquitectura Propuesta

Las operaciones y procesos que la arquitectura contempla son: gestión de claves, emisión, distribución, revocación, renovación y validación (Nash, A., 2002).

4.1.1. Proceso de Gestión de Claves

Este proceso queda tal cual funciona en la arquitectura PKI vigente, ya que bajo cuestiones de gestión/generación de claves la solución se encuentra compatible e interoperable a la actual, y desde el punto de vista técnico no se detectaron contramedidas en esta etapa, no obstante, se decidió no modificar el mismo.

4.1.2. Proceso de Emisión de Certificados

Al igual que la arquitectura PKI vigente, este proceso se encarga de aceptar la petición de emisión de certificados digitales de los diferentes usuarios.

En consiguiente, una vez generado el par de claves, el portador de las mismas expone la clave pública en formato Base58 Check en el servidor web, en la dirección "URL-RAÍZ/emit/pk", por ejemplo: "www.prueba-clave-publica.com/emit/pk". Es decir, si un usuario realiza una petición web GET de ese recurso, obtendría la clave pública expuesta anteriormente en formato Base58 Check.

Ya generado esto, se crea una **transacción** de emisión de certificados que lleva dentro:

- Como **dirección:** el hash de la misma.
- La **clave pública** del servidor (clave pública a dar de alta).
- El **dominio** portador de la clave pública (URL-RAÍZ).
- La ruta donde buscarla (/emit/pk).

Luego se disemina esta transacción por la red *peer to peer* y el portador de la clave pública aguarda su confirmación.

Todos los nodos que reciban dich a transacción, verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto en la misma. Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la transacción y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción debe generar un certificado x.509 autofirmado o firmado por una Autoridad Certificante propia, desconocida por los demás o incluso conocida. Este certificado contendrá los diferentes campos correspondientes al estándar y a la configuración que se desee, salvo la particularidad de que en el campo opcional ***issuerUniqueID*** se dejará asentado el identificador de la **transacción** confirmada. Ya a esta altura el usuario se encuentra en condiciones de agregarlo a la configuración HTTPS del servidor con su dominio en cuestión y/o firmar otros certificados digitales.

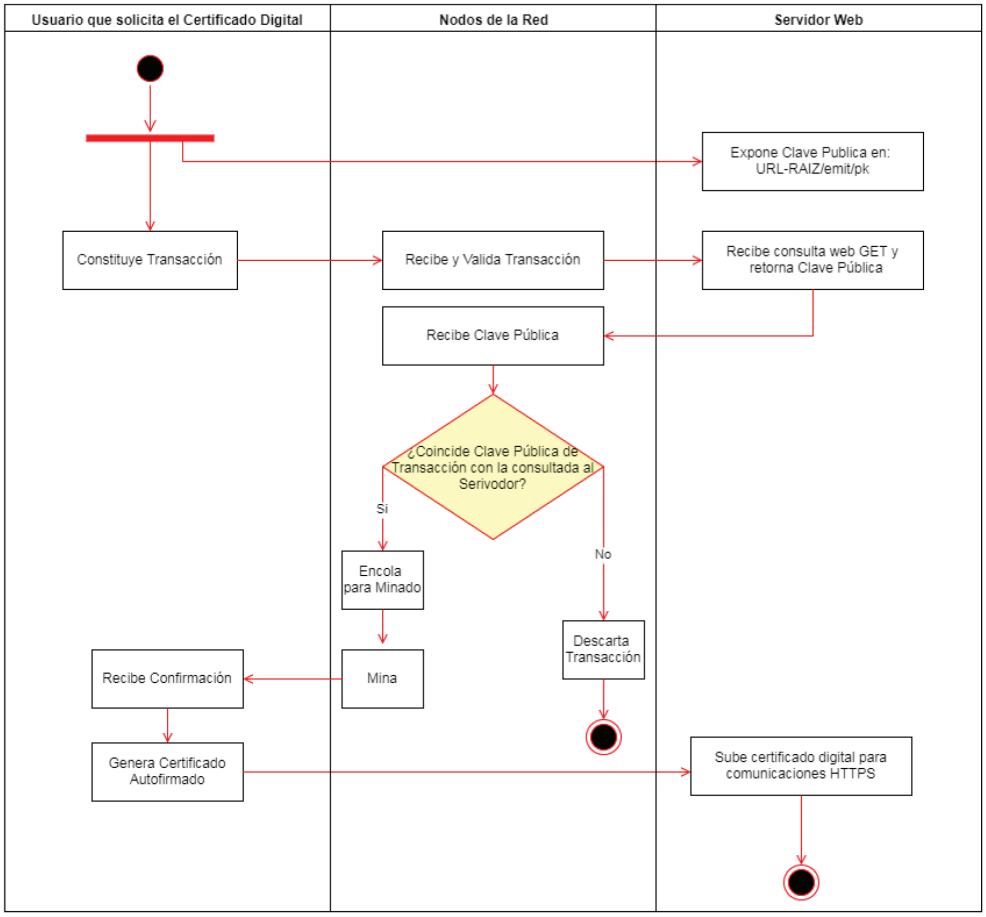

Figura 2 – Diagrama de Actividades del Proceso de Emisión

4.1.2. Proceso de Distribución de Certificados

El método utilizado para la distribución de los certificados es el basado ***blockchain***, es decir, distribuido en la totalidad de los nodos en la red. Tanto para operaciones de verificación de firmas o de cifrado, el acceso a los certificados se lleva a cabo mediante consultas a la **cadena de bloques** donde las claves públicas emitidas, renovadas o revocadas se encuentran disponibles gracias a la convergencia y consenso de la red. Esta base de datos pública además proporciona información extra que resulta útil a la hora de realizar el proceso de validación, como ser, información del dominio en donde validar las mismas. Esto es debido a que (como visto en el proceso anterior) cada usuario que desea emitir, renovar o revocar un certificado digital debe agregar su clave pública a modo de recurso web, donde cada nodo de la red accede a la misma para poder validarla y converger en la emisión, renovación o revocación del mismo.

4.1.2. Proceso de Revocación de Certificados

Este proceso se lleva a cabo con el fin de dar de baja o declararlo como no confiable a un certificado digital, por consiguiente y al igual que el proceso de emisión, al momento de generar una revocación, el usuario deberá exponer la clave a revocar en el servidor web para que sea accesible por los nodos que la validan, luego generar una transacción y diseminarse por la red.

Dicho ésto, el usuario portador de la clave pública del servidor expone la misma en "URL-RAÍZ/revoke/pk" y genera una transacción con las siguientes características:

- Como **dirección:** el hash de la misma.
- La **clave pública** del servidor (clave pública a revocar).
- El **dominio** portador de la clave pública.
- La ruta donde buscarla (/revoke/pk).
- La **dirección** de la transacción de emisión o de renovación (transacción anterior).

Todos los nodos que reciban dicha transacción verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto (por medio de la ruta proporcionada en la transacción de revocación o en la indicada en la transacción de emisión o renovación anterior). Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la **transacción de emisión o renovación** y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción ya da la clave por revocada.

4.1.3. Proceso de Renovación de Certificados

En esta etapa usuario portador de la clave pública del servidor debe exponer la **nueva** clave pública en "URL-RAÍZ/renovate/pk" y genera una transacción con las siguientes características:

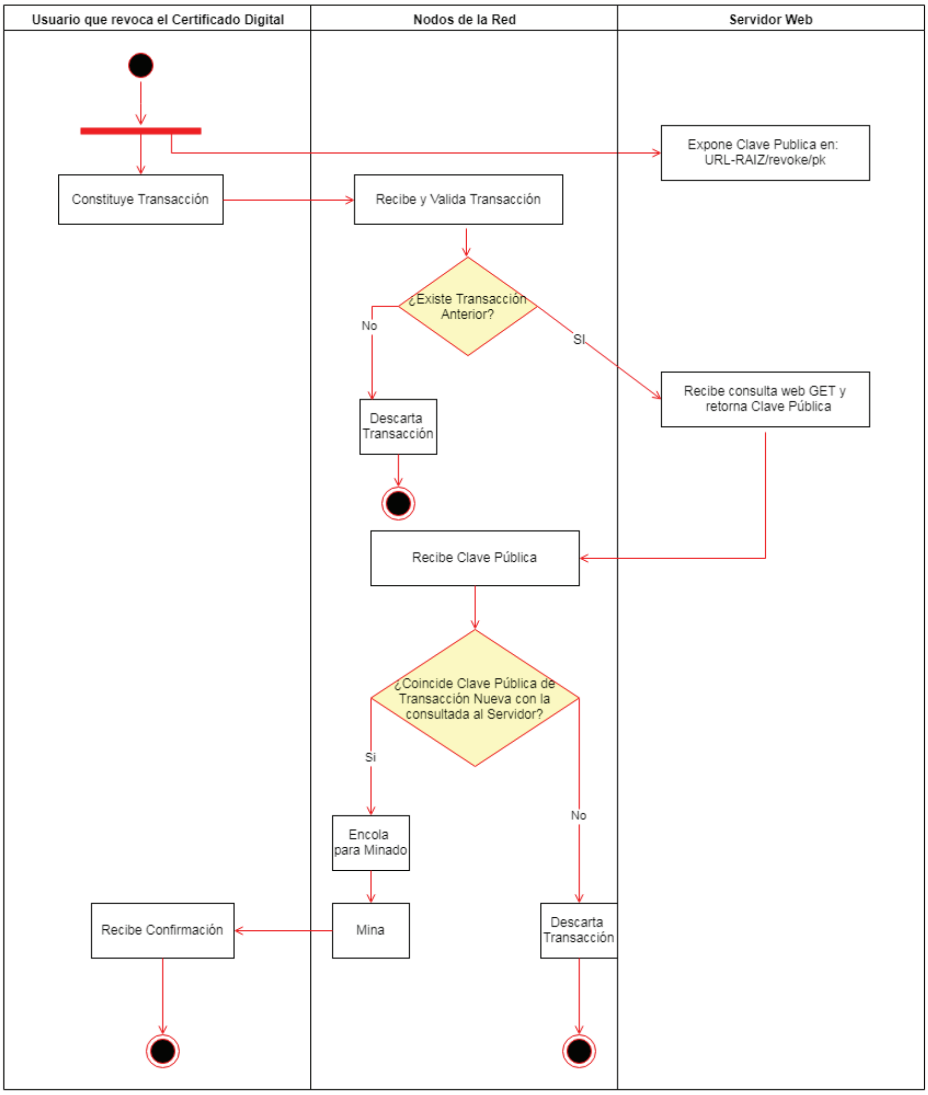

Figura 3 – Diagrama de Actividades del Proceso de Revocación

- Como **dirección:** el hash de la misma.
- Nueva **clave pública** del servidor.
- El **dominio** portador de la clave pública.
- La ruta donde buscarla (/renovate/pk).
- La **dirección** de la transacción de emisión o renovación (transacción anterior).

Todos los nodos que reciban dicha transacción verificarán su integridad y realizarán una petición web GET hacia el recurso expuesto (por medio de la ruta proporcionada en la transacción de revocación o en la indicada en la transacción de emisión o renovación

anterior). Ya recibida la respuesta de la petición, se compara el resultado con la clave pública del servidor contenida dentro de la **transacción** realizada recientemente y en caso afirmativo se retransmite a los demás nodos y se encola para realizar el proceso de minado, en su defecto la misma se descarta.

Una vez minada y confirmada la transacción (al igual que en Bitcoin, para la confirmación se aconsejan 10 bloques por delante del bloque en donde se encuentra la transacción), el creador de la transacción debe generar un certificado x.509. Este certificado al igual que en el proceso de emisión deberá rellenar en el campo opcional ***issuerUniqueID*** (Identificador único del emisor) con el identificador de la **transacción** confirmada. Ya a esta altura el usuario se encuentra en condiciones de agregarlo a la configuración HTTPS del servidor con su dominio en cuestión y/o firmar otros certificados digitales.

4.2. Transacciones.

Las transacciones al igual que en Bitcoin son estructuras de datos firmadas digitalmente, pero que en vez de cambiar el propietario de un bitcoin, realizan una acción de emisión, revocación o renovación de certificados digitales.

La estructura de datos es la siguiente (*Ilustración 13, Ilustración 14 e Ilustración 15*):

- **Transacción anterior**: registro que referencia a una transacción previa. Para transacciones de **emisión** este campo se lo fija en 0, ya que no posee transacciones anteriores, y para transacciones de **renovación** o **revocación** se referencia a la transacción anterior.
- **Dominio del servidor:** portador del certificado a emitir, renovar o revocar.
- **Clave pública del servidor:** que se quiere dar de alta, relacionada a ese dominio.
- **Dirección (path/url):** en donde encontrar la **clave pública del servidor** para cotejar con la contenida en la transacción. Para transacciones de emisión se completa el campo “emit”, para renovación el “renovate” y para revocación el“revoke”.
- **Hash de transacción (identificador)**: resumen de toda la estructura de datos.
- **Firma digital del emisor**: encripción del **hash de la transacción** con la clave privada del nodo emisor.

Por ejemplo, si **A** desea **emitir** un certificado digital para el dominio “www.prueba-pkchain.com”, entonces se genera el par de claves para su servidor, expone la clave pública en “www.prueba-pkchain.com/emit/pk”, y genera la transacción con los siguientes campos:

- **server domain:** “www.prueba-pkchain.com”
- **emit:** “/emit/pk”
- **revoke:** “” (Vacío, ya que es una transacción de emisión)
- **renovate:** “” (Vacío, ya que es una transacción de emisión)
- **server public key**: “clave pública perteneciente al par de clave generado”
- **previous transaction:** “” (Vacío, ya una transacción de emisión no posee transacción anterior).

Si **A** desea **renovar** esta emisión, deberá generar el nuevo par de claves, publicar la nueva clave en la dirección de "renovate" declarada en esta nueva transacción. La transacción contendrá los siguientes campos:

- **server domain:** "www.prueba-pkchain.com"
- **emit:** "" (Vacío, ya que es una transacción de renovación)
- **revoke:** ""(Vacío, ya que es una transacción de renovación)
- **renovate:** "/renovate/pk"
- **server public key:** "clave pública perteneciente al nuevo par de clave generado".
- **previous transaction:** Identificador de transacción anterior.


```
{
"id": "f1b7fed773accafad5088eb4c3957cb050912535a4ce2ed81b0781ea69ba4669",
"libCert": {
        "serverDomain": "http://www.prueba-pkchain.com",
        "emit": "/emit/pk",
        "revoke": "",
        "renovate": "",
        "serverPublicKey": "04d50ce5ff067e2dbb28f197ff05ab3a4d363227f169da5dd821d821...",
        "previousTx": ""
      }
}
```


Figura 2 – Transacción de Emisión en formato JSON


```
{
"id": "abc1345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3dee873",
"libCert": {
        "serverDomain": "http://www.prueba-pkchain.com",
        "emit": "",
        "revoke": "",
        "renovate": "/renovate/pk",
        "serverPublicKey": "04fe71e62fc22b20e3473a90b3d1005d49f9d0c0aab69cfb7dd99122...",
        "previousTx": "f1b7fed773accafad5088eb4c3957cb050912535a4ce2ed81b0781ea69ba4669"
      }
}
```


Figura 3 – Transacción de Renovación en formato JSON.

Por último, si **A** desea **revocar** un certificado, deberá publicar la clave a revocar en la dirección de "revoke" declarada en la transacción nueva. La estructura de datos contendrá los siguientes campos:

- **server domain:** "www.prueba-pkchain.com"
- **emit:** "" (Vacío, ya que es una transacción de revocación)
- **revoke:** "/revoke/pk"
- **renovate:** "" (Vacío, ya que es una transacción de revocación)
- **server public key:** clave pública que se quiere revocar.
- **previous transaction:** Identificador de transacción anterior.

Cada transacción excepto las de “emisión”, poseen referencias o “punteros” a anteriores que se encuentran reconocidas por toda la red y almacenada en la base de datos distribuida, no obstante, se encuentran disponibles para que todos los nodos puedan consultarlas.


```
{
"id": "zf11345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3deeds3",
"libCert": {
        "serverDomain": "http://www.prueba-pkchain.com",
        "emit": "",
        "revoke": "/revoke/pk",
        "renovate": "",
        "serverPublicKey": "04fe71e62fc22b20e3473a90b3d1005d49f9d0c0aab69cfb7dd99122...",
        "previousTx": "abc1345fdf2e75064b1559e5520a51f896c7f28c8576d68205e326a8d3dee873"
      }
}
```


Figura 4 – Transacción de Revocación en formato JSON.

4.3. Construcción del Camino a la Certificación.

Si un **cliente pkchain** se conecta a un servidor web, este último retorna el certificado digital. El cliente, accede al campo “***issuerUniqueID*** ” y con el identificador de transacción contenido dentro busca en toda la blockchain hacia atrás. Si este no se encuentra como entrada de una transacción de revocación, la transacción existe contenida dentro de un bloque de la *blockchain*, y la información contenida dentro de la transacción coincide con la del certificado digital enviado por el servidor (dominio y clave pública), entonces se da luz verde y el mismo se acepta, de lo contrario se lo rechaza.

4.4. Consideraciones Generales.

Desde el punto de vista de la convergencia de la red a nivel blockchain, se intentó emular el proceso idéntico al implementado en Bitcoin, es decir, en cuestiones de minería, pruebas de trabajo, estructura de datos de bloques, tiempos entre bloques, criptografía utilizada y ajustes de dificultad se realizó una copia de la lógica vigente de la *blockchain* de Bitcoin.

5. Trabajos Futuros

Blockchain pone sobre la mesa la posibilidad de realizar transacciones entre entidades (personas u organizaciones) de manera distribuida, segura y sin necesidad de intermediarios, donde las reglas del juego están definidas por medio de algoritmos computacionales.

Llegar a tener una sociedad más distribuida y autónoma en cuanto a su estructura, sus redes y transacciones es algo que podría venir de la mano de esta tecnología y que podría cambiar la forma en que muchas cosas están pensadas hoy.

De la misma manera que **internet** cambió para siempre los modelos de negocio de miles de industrias y empresas, la ***blockchain*** o **cadena de bloques** está dando lugar

a una nueva revolución, proponiendo nuevas formas de optimizar las relaciones entre usuarios, ahorrar costes administrativos, favorecer cooperaciones y comprender todas las posibilidades imaginables que ofrecía el internet de la información en una segunda ola tecnológica de cambio.

Blockchain es la verdadera innovación que hizo posible la existencia de **Bitcoin** (su primer uso de esa tecnología) y eso le permitió ser, hasta el día de hoy, la más popular de todas, al punto de ser más popular en el consciente colectivo que ***Blockchain*** en sí, no obstante, lo más importante que se extrae de esta gran solución es la posibilidad de utilizar la **cadena de bloques** en otros ámbitos, como por ejemplo, su incorporación en la propuesta abordada en esta investigación.

En este trabajo se abordó una propuesta de reingeniería y migración de la arquitectura de certificados digitales vigente a una montada sobre ***blockchain***, sería interesante analizar una propuesta de implementación que se monte sobre su alternativa: ***hashgraph***.

En esta propuesta se ha desarrollado un prototipo a modo de validar el modelo, no obstante, la implementación real junto con la apertura de un proyecto ***open source*** para que la comunidad pueda realizar sus aportes invocando a la inteligencia colectiva, es el principal trabajo que queda pendiente por realizar.

Esta arquitectura de certificados digitales distribuida y descentralizada tiene un enfoque orientado a arquitecturas web, por lo tanto, realizar un análisis de viabilidad de implementación en diferentes ámbitos como ser firma digital de expedientes o en voto electrónico sería de gran interés.

Sería muy interesante poder también lograr la interoperabilidad entre la propuesta de esta investigación y la lógica de negocios de **Bitcoin**, de modo de integrar las dos soluciones para que puedan convivir al mismo tiempo en la misma **cadena de bloques**. Para lograr esto, en vez de quitar la lógica de negocios de **Bitcoin** (como se planteó en este trabajo), se deberá realizar una modificación en la misma para agregar la lógica de negocios de esta propuesta.

Por último, visto y considerando que la solución planteada en esta investigación descansa sobre ***blockchain***, también acarrea sus mismas debilidades, no obstante, es motivo de trabajo a futuro contemplar mejoras en este sentido.

6. Conclusiones

Dada la gran frecuencia en la que surgen proyectos montados sobre ***blockchain***, y no solo eso, sino la cantidad de criptomonedas vigentes y por aparecer que están revolucionando la economía mundial, es necesario conocer los fundamentos que se hacen del núcleo de esta área de conocimiento de forma tal de dominar la tecnología, conocer sus posibles vulnerabilidades, y mejoras.

Ha habido gran cantidad propuestas para lograr una formalización de la ingeniería en seguridad de ***Blockchain***, pero la mayoría tienen un alcance limitado. Resulta totalmente relevante incursionar en el tema ya que hasta el momento no se ha podido

probar de manera exhaustiva si la arquitectura de ***Blockchain*** sea totalmente segura o no, o más aún, si es tan útil como se dice o no.

Dentro de la filosofía ***Blockchain*** existen muy pocas obras que realicen una utilización en serio de sus funcionalidades, y de las pocas que existen, la mayor parte la aborda con un enfoque indiscreto e irreal sobre cómo descentralizar en dos pasos al mundo.

Cabe destacar que en la actualidad casi no existe bibliografía seria y en español que aborde y exponga una detallada descripción de los procesos internos, arquitecturas y operaciones tanto de **Bitcoin** como de ***Blockchain***. La escasa bibliografía existente brinda diferentes análisis y proyecciones genéricas más inclinadas a puntos de vistas de las ciencias económicas que técnicas de la ingeniería.

En este trabajo se puede apreciar una detallada descripción en español de todos los conocimientos que se encuentran detrás de este telón, comenzando por los fundamentos básicos, hasta entrando en las entrañas matemáticas que dirigen la orquesta. No obstante, se hace mención a una necesidad contemporánea muy importante, básica y colectiva, que obliga a enfocarse hacia un cambio de paradigma en la arquitectura de certificados digitales vigente. En consiguiente, se presenta una propuesta que integra conocimientos y funcionalidades provenientes de tecnologías de punta como es la implementación de diferentes sistemas sobre ***Blockchain***.

Para ir finalizando, como conclusión no solo personal, sino de la comunidad informática en general, es que el aporte más grande que ha dado Satoshi Nakamoto (Nakamoto, S., 2009) con su publicación en 2009 no fue **Bitcoin**, sino su columna vertebral, es decir, ***Blockchain***. Una tecnología que tiene características ilimitadas tanto desde el punto de vista técnico como económico, que permite abordar investigaciones, realizar propuestas innovadoras y simples implementaciones como la presentada en esta investigación.

Por último, este rediseño de la arquitectura plasmado en este trabajo de investigación fue llevado a cabo y probado experimentalmente, en donde para mayor detalle de esta propuesta de reingeniería e implementación se dejan referencias de la tesis[1] que extiende en detalle todos estos conceptos junto al repositorio[2] correspondiente.

Referencias

Adams, M. (2016). *Blockchain: The history, mechanics, technical implementation and powerful uses of blockchain technology. CreateSpace Independent Publishing Platform.*

Allison, I. (2010). Organizational factors shaping software process improvement in small-medium sized software teams: A multi-case analysis. In Proceedings - 7th International Conference on the Quality of Information and Communications Technology, QUATIC 2010 (pp. 418–423). Porto, Portugal: IEEE. https://doi.org/10.1109/QUATIC.2010.81

[1] Tesis de maestria: http://sedici.unlp.edu.ar/handle/10915/72076

[2] Repositorio del código de la Tesis de maestría: https://gitlab.com/ignaciomgu/pkchain

Antonopoulos, A. M. (2018). *Mastering bitcoin: Programming the open blockchain*. Sebastopol, CA: O'Reilly media.

Bahga, A., & Madisetti, V. (2017). *Blockchain applications a hands-on approach*. Vpt.

Blake, I. F., Seroussi, G., & Smart, N. P. (1999). *Elliptic curves in cryptography*. Cambridge : Cambridge University Press.

Capoti, D., Colacchi, E., & Maggioni, M. (2015). *Bitcoin revolution: La moneta digitale alla conquista del mondo*. Milano: U. Hoepli.

Chen, J., Yao, S., Yuan, Q., He, K, Ji, S., Du, R. (2018). CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections. In Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, (pp. 2060-2068). Honolulu, HI, USA. Doi: 10.1109/INFOCOM.2018.8486344.

Diffie, W.; & Hellman, M. (1976). "New directions in cryptography". *IEEE Transactions on Information Theory*. 22 (6): 644–654. Doi: 10.1.1.37.9720. doi:10.1109/TIT.1976.1055638.

Doglio, F. (2018). *REST API Development with Node. js: Manage and Understand the Full Capabilities of Successful REST Development*. New York: Apress LP.

Dykcik, L., Chuat, L., Szalachowski, P., & Perring, A. (2018). BlockPKI: An Automated, Resilient, and Transparent Public-Key Infrastructure. In Proceedings of the Workshop on Blockchain and Sharing Economy Applications, (pp. 316-322). Singapore. doi: 10.1109-ICDMW.2018.00022.

Finch, V. (2017). *Bitcoin: The only complete quick & easy guide to mastering Bitcoin and digital currencies*. Auva Press.

Friedman, W. F. (1922). "The index of coincidence and its applications in cryptology". *Department of Ciphers. Publ 22*. Geneva, Illinois, USA: Riverbank Laboratories.

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge: Cambridge University Press.

Gallardo, I. (2018). *Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. (*Master Thesis in Data Networks), University of La Plata, Argentina.

Hoffman, N. (2017). *Blockchain: The insider's guide to Blockchain technology, Bitcoin mining, investing and trading cryptocurrencie. Blockchain, cryptocurrency.*

Hoskinson, C. (2013), "The Mathematician's Defense of Bitcoin: It's Just Another Option". PBS News Hour.

Housley, R., & Polk, T. (2001). *Planning for PKI: Best practices guide for deploying public key infrastructure*. Hoboken: Wiley.

Jenkins, Y., & Jenkins, Y. (2015). *Bitcoin: Millionaire maker or monopoly money?* Publisher not identified.

Jiang, W., Li, H., ...& Xu, G. (2019). PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI. January 2019 Future Generation Computer Systems 96. doi: 10.1016/j.future.2019.01.026

Johnson, E. C. (2017). *Cryptocurrency: The beginner's guide to investing and trading in cryptocurrency*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.

Jhanwar, M. P., Chattopadhyay, A., & Madala, D. S. V. (2018). Certificate Transparency Using Blockchain. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), (pp. 71-80). Singapore. from: https://eprint.iacr.org/2018/1232.pdf

Kohnfelder, L. M. (1978). "On the Signature Reblocking Problem in Public Key Cryptography". *Communications of the ACM*. 21 (2): 179.

Lafosse, J. (2009). *Java EE: Guide de développement d'applications web en Java*. Epsilon

Leuf, B. (2002). *Peer to peer: Collaboration and sharing over the Internet*. Boston: Addison-Wesley.

Massé, M. (2012). *REST API design rulebook*. Sebastopol, CA: O'Reilly media.

Mohanty, H., & Pattnaik, P. K. (2019). *Webservices: Theory and practice*. Berlin: Springer.

Mudunuri, S. (2013). *Spring Framework: A step by step approach for learning Spring framework*. Scotts Valley, CA: CreateSpace.

Nash, A. (2002). *PKI: Infraestructura de claves públicas: La mejor tecnología para implementar y administrar la seguridad electrónica de su negocio*. New York: McGraw-Hill.

Pathak, N., & Bhandari, A. (2018). *IOT, AI, and Blockchain for .NET: Building a next -generation application from the ground up*. New York: Apress.

Pardi, P. (2015). *The TypeScript programming language*. Microsoft.

Prieto, A. & Piattini, M. (2015). Propuesta de marco de mejora continua de gobierno TI en entidades financieras. RISTI - Revista ibérica de Sistemas y Tecnologías de Información RISTI, (15), pp. 51–67. DOI: 10.17013/risti.15.51-67.

Satoshi, Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf.

Shane, P. M., & Hunker, J. A. (2013). *Cybersecurity: Shared risks, shared responsibilities*. Durham: Carolina Academic Press.

Springer, S. (2018). *Node.js das umfassende Handbuch*. Bonn: Rheinwerk Verlag.

Steinmetz, R.; Wehrle, K (2005). *2. What Is This "Peer-to-Peer" About?*. pp. 9-16. Berlin Heidelberg: Springer..

Thomas, S. A. (2000). *SSL & TLS essentials: Securing the Web*. Hoboken: Wiley.

Vacca, J. R. (2002). *Public key infrastructure*. Boca Raton, FL: Auerbach.

Vacca, J. R. (2013). *Computer and information security handbook*. Morgan Kaufmann.

Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*.

Vimercati, S. D., & Mitchell, C. (2013). *Public key infrastructures, services and applications. In 9th European Workshop, EuroPKI 2012, Pisa, Italy, September 13-14, 2012: Revised selected papers*. Berlin: Springer.

Won, J., Singla, A., Bertino, E., & Bollella, G. (2018). Decentralized Public Key Infrastructure for Internet-of-Things. In Milcom 2018 Track 5 - Big Data and Machine Learning, (pp. 907-913). Washington, USA. doi: 10.1109/MILCOM.2018.8599710.

Yakubov, A., Shbair, W. M., & State, R. (2018). BlockPGP: A Blockchain-based Framework for PGP Key Servers. In Proceedings of the 6th International Symposium on Computing and Networking Workshop, (pp. 316-322). Hida Takayama, Japan.

Zhao, W. (2014). *Building dependable distributed systems*. Scrivener Publishing/Wiley.