Datos en los que puede confiar

Tecnología de cadena de bloques

Coronel Vincent Alcazar, USAF, Retirado

Dicen que los futuros acontecimientos arrojan sombras antes de que ocurran. ¿No pueden a veces arrojar sus luces antes?

—Augusta Ada King–Noel, Condesa de Lovelace

El caso para cambiar

Las fuerzas armadas de EE.UU. siguen esperando que las novedades innovadoras de la guerra centrada en las redes (NCW) suministren el liderazgo tecnológico y los avances de combate que revolucionan la forma de combatir de EE.UU. En vez de eso, en la última década, las FF.AA. de EE.UUU. consiguieron artefactos: acceso a Internet, computadoras portátiles, la introducción de teléfonos inteligentes y así sucesivamente. Los artefactos de avance tecnológico a menudo se identifican de forma errónea como las novedades innovadoras anticipadas de NCW. Básicamente, esos artefactos son mejoras de productividad iterativas de dispositivos y máquinas. Si la NCW tiene una debilidad insidiosa, es la orientación de sus equipos. El enfoque en los artefactos obliga a hacer la pregunta: ¿qué ocurre con los datos que se transportan en equipos, dispositivos, redes e infraestructura relacionada? A pesar de los avances en tecnologías y procesos, los intérpretes de comandos de software y hardware de hoy, es decir, las cosas que rodean y distribuyen datos, siguen siendo crónicamente vulnerables. Entre los detalles recurrentes de la historia es que las vulnerabilidades de los militares, ocultas o reconocidas, pueden convertirse en ejes en la campaña de sorpresa de un oponente. Sin embargo, la sorpresa no necesita ser estratégica para impedir la forma de combate estadounidense. ¿Qué debe hacerse?

Dentro del contexto de vulnerabilidades de datos de EE.UU. y la susceptibilidad potencial de la sorpresa ciberespacial, los guerreros y los líderes de los guerreros necesitan un método diferente, una gran idea, una tecnología viable que puede mitigar la debilidad en el paradigma de protección de datos centralizada del Departamento de Defensa. La mejor (gran) idea no debe ser un enfoque continuado casi exclusivo en mejoras de máquinas de cálculo militares iterativas. En vez de eso, esta mejor idea debe describir un diseño para una mayor seguridad de lo que los equipos de tecnología de información (IT) militar procesan, almacenan y distribuyen: datos. La mejor idea existe; es una tecnología de cadena de bloques. En términos concisos, la cadena de bloques es una tecnología que almacena datos de una forma que hace que sean incorruptibles, haciéndolo por medio de sus libros de datos integrados. Las razones para adoptar la tecnología de salto adelante de la cadena de bloques son dobles: evitar el riesgo negativo de alteración y aumentar al máximo la oportunidad positiva de combate. En lo que se refiere al riesgo negativo, los combatientes necesitan mitigar la alteración y degradación de las operaciones resultantes de una ausencia de datos auténticos, porque muchos de nuestros sistemas de armas requieren datos para funcionar de forma efectiva, si es que lo necesitan. La parte positiva de la cadena de bloques es que las fuerzas armadas de EE.UU. pueden descartar la corrupción y el robo de datos como

cosas que puede hacer un enemigo con sus datos. La primera razón es importante; la segunda razón es un cambio en el combate.

El desarrollo de una gran idea de cadena de bloques, junto con la mejora de la máquina, sugiere un crecimiento significativo en costos de IT del Departamento de Defensa en una época de limitaciones de recursos. No obstante, la cadena de bloques ya existe, y eso ahorra millones de dólares en investigación y reduce los años de un programa de desarrollo. Básicamente, la cadena de bloques es una tecnología de administración y distribución de datos compatible con redes existentes del Departamento de Defensa. Su diseño crítico asegura y marca los datos, protegiéndolos contra las manipulaciones indebidas y la corrupción. La cadena de bloques libera a nuestras fuerzas armadas de la competición continuada contra actores estatales y no estatales, que como atacantes tienen vastos incentivos y bucles de desarrollo de explotación ágiles que producen unas condiciones desiguales. La desigualdad de estas condiciones es consecuencia de una geometría tremendamente desventajosa y muy ineficiente que enfrenta la mitigación de amenazas de equipos/software de empresas que debe ser correcta todo el tiempo a un entorno de seguridad de amenazas en el que un atacante determinado solamente necesita tener éxito brevemente. Para hacer que las condiciones sean favorables para las fuerzas armadas de EE.UU., la solución ideal apunta hacia una unión de la tecnología de cadena de bloques con la inventiva de máquinas/sistemas de cálculo estadounidense.

Problema, tesis, hipótesis

Los datos se han convertido en la dependencia crítica de la organización militar moderna. En la práctica, la falta de datos oportunos y exactos condena a una fuerza y sus líderes a operaciones por medio de un método de conjetura. Por lo general, el método de conjetura de detectar y tomar decisiones plantea problemas. Fue un problema cuando la fuerza era liderada por un solo hombre montado a caballo oteando un campo de batalla. En este siglo, la falta de datos seguros abre cualquier fuerza a una derrota traumática en múltiples dominios. La paradoja es que el modelo de guerra distribuida de EE.UU. alcanza su máximo potencial cuando su vasto y creciente apetito de datos es alimentado regularmente por datos aprobados que se sabe que son seguros. Los usuarios de datos en los márgenes del Departamento de Defensa saben que el problema no es el apetito de datos de nuestras máquinas o la escala de ese apetito.[1] En vez de eso, cualquier afirmación del problema sobre el statu quo no sería un comentario de una línea sino un círculo trazado alrededor de un grupo de preguntas interrelacionadas: ¿cuál es la fiabilidad de los datos que flotan alrededor de nuestros sistemas de IT, los datos que esos combatientes necesitan para seguir en la lucha? ¿Se han alterado indebidamente los datos de combate, de forma parcial o total? ¿Son esos datos realmente auténticos o solamente parecen auténticos y aun así son realmente falsos, plantados por un atacante inteligente? ¿Es el remitente una entidad creíble, o es la presunta fuente realmente un sistema que trata de causar confusión? ¿Cuáles de esas preguntas deben resolverse como problemas, y en qué orden? Realmente, a los combatientes no les importa, pero las respuestas que oyen de los expertos de IT es atender a todos esos asuntos, simultáneamente. Y así, cada uno de estos asuntos se tratan usando métodos separados en silos separados.

Ganar la lucha para proteger y controlar nuestros sistemas de IT requiere un empleo tremendo de recursos. Pero, ¿qué ocurriría si descartáramos todas esas preguntas y los problemas que sugieren desplazando el punto de enfoque de la respuesta? En vez de preguntar que podría hacerse de nuevo en estos sistemas de IT, ¿qué pasaría si se pudiera hacer algo nuevo con los datos mismos? Pasemos a la cadena de bloques, que enfoca la pregunta y la respuesta en los datos. Dado lo anterior, la tesis de este artículo es que, si el Departamento de Defensa despliega una cadena de bloques, una tecnología de administración de datos nueva y radicalmente dife-

rente, entonces los ataques de datos de hoy se hacen mucho menos perjudiciales, con la ventaja clave de los datos en manos de combatientes que se hacen exponencialmente más fiables al ser prácticamente incorruptibles.

A continuación, la hipótesis de este artículo es proteger mejor los datos de combate en redes militares de EE.UU.; la tecnología de datos mejor conocida es la cadena de bloques. Explicado de otra manera, la cadena de bloques puede ayudar a los combatientes a escaparse de la rueda del hámster de mitigar los ciberataques que experimentamos mientras incurrimos en daños de depredación de vulnerabilidades de hardware/software de IT sin anticipar, sin documentar, sin mapear y sin conocer.

Cadena de bloques: vista general

En 2008, un individuo que usaba el seudónimo Satoshi Nakamoto publicó un informe blanco de mucha circulación que describía el concepto de Bitcoin y su sistema de activación fundamental, la tecnología de cadena de bloques.[2] La cadena de bloques podría ser la primera tecnología verdaderamente merecedora de la etiqueta de tecnología de datos alteradora. La cadena de bloques no es simplemente una mejora generacional con respecto al registro de datos y a las tecnologías de documentación actuales. Su importancia es su capacidad de eliminar una vulnerabilidad crucial en nuestros diseños de redes presentes: comprometer las políticas de gestión de confianza de redes. Las funciones de gestión de confianza son un blanco de ataques frecuente debido a la función vital que desempeñan en todas las redes cibernéticas, incluidas las usadas por las fuerzas armadas. El gerente de confianza controla dos funciones vitales: asignación de credenciales al usuario y control de acceso. La gestión de confianza se basa en un dispositivo y su software para desempeñar la función de intermediario a fin de asegurar a los usuarios y sus transacciones de datos siguen siendo fiable.[3] Al fijar como blanco las credenciales del usuario, un atacante puede obtener la entrada en una red para llegar al objetivo de datos final a fin de lograr los objetivos de su ataque.

Los diseñadores fundadores de la cadena de bloques entendieron las limitaciones inherentes en el paradigma de diseño de redes que requiere la existencia de un gerente de confianza. Al crear la forma y lógica básicas de la cadena de bloques, fueron los primeros en usar una tecnología dentro de una nueva estructura de operación que deja a un lado los numerosos puntos débiles del cálculo basados en el sistema del Departamento de Defensa como lo saben los combatientes hoy. Los puntos siguientes son una vista general de cómo y por qué la cadena de bloques se considera una tecnología alteradora.

La cadena de bloques es una nueva fuente de fortaleza

El diseño tradicional de redes seguras otorga funciones de gestión de relación de confianza y guardián a un actor central con autoridad completa dentro de la jerarquía de la red. La cadena de bloques elimina los requisitos de una autoridad centralizada eliminando la necesidad de la función de un intermediario de gestión de confianza. La ausencia de control central confiere una escalabilidad que hace que una red de cadenas de bloques sea capaz de funcionar con la misma efectividad y eficiencia en cualquier umbral de tamaños; es decir, un destacamento de asalto, una fuerza de tarea conjunta grande, y así sucesivamente. Otra ventaja de la cadena de bloques es que su estructura descentralizada (organizaciones más planas) y menos lógica centralizada (menos jerárquico) disminuyen el período de latencia. Más horizontal y menos vertical supera muchos de los retos en redes militares llenas de riesgos de pérdida de gerentes de confianza centralizados. En otras palabras, fortalecer la cadena de bloques no es algo que se hace para hacer una cadena de bloques, es una cadena bloques.

La cadena de bloques invierte el paradigma de centralización de datos

Las amenazas persistentes avanzadas (APT) y los actores estatales y no estatales ejercen una influencia sustancial en el diseño de redes militares estadounidenses. Esas amenazas fuerzan una respuesta defensiva amplia que recopila datos detrás de muros protectores cada vez más complicados protegidos dentro de más capas de seguridad. Lo que resulta de esta mentalidad de amenazas, defensas y respuestas es una multiplicidad de silos de datos en crecimiento constante. La seguridad de datos se convierte en su primer fin, y desde ese fin se produce un resultado inintencionado: la balcanización de los datos. Para los gerentes de datos, esta estructura es adecuada y apropiada. No obstante, para los combatientes que luchan en espacios de batalla en múltiples dominios y desde posiciones de espacio de combate cada vez más distribuidas, los silos, una herramienta de combate, ponen los datos más lejos y no donde deben estar en combate, a mano.

La cadena de bloques cambia la forma de la defensa de datos

La cadena de bloques no hace que todos los actores y amenazas concebibles sean irrelevantes; ningún diseño de redes militares asequible puede hacerlo. No obstante, la estructura de prueba de trabajo de máquinas mineras de rede de la cadena de bloques y su libro distribuido de transacciones de datos reducen considerablemente la posibilidad de robo de datos, corrupción de datos y de que se ponga en riesgo la identidad de los remitentes.[4] Además, el estándar de cifrado de datos de la cadena de bloques, SHA–256, hace que el aprovechamiento inverso del contenido de mensajes de remitentes sea costoso y lleve tiempo. Incluso si un oponente pudiera romper económicamente la norma de cifrado SHA–256, es muy poco probable que pueda hacerlo a la velocidad de combate; es decir, de forma suficientemente rápida para que tenga importancia en un combate.[5]

Datos de cadena de bloques como tejido

En la visión actual de gestión de datos militares de EE.UU., los datos se acumulan en sumideros. La mera existencia de almacenes de datos invita a un ataque. Si se crea una estructura donde los datos son importantes, se ponen esos datos en riesgo constante. La cadena de bloques agita el paradigma de recopilación de datos. Es seguro que los datos siguen siendo lo más importante, pero la cadena de bloques contiene datos dentro de esta configuración de bloques de datos, a medida que cada uno se añade a los libros de la red de cadena de bloques. La alteración de los datos contenidos en cada bloque es imposible después de que se añada un bloque completado a todos los libros de las redes.

La estructura descentralizada de la cadena de bloques complementa la guerra distribuida

Al desconectarse temporalmente de su red de cadenas de bloques nativa, las máquinas mineras no se desactivan, solamente siguen inactivas a la espera de la siguiente transacción de datos.[6] Cuando una red de cadenas de bloques se reconecta a las redes dominantes, se produce una sincronización de prueba de trabajo de bloques. Todos los bloques de datos completados se exportan a cada libro. Esta rutina está diseñada para asegurarse de que cuando las máquinas mineras de una red y las máquinas relacionadas vuelvan a arrancar, lo hagan al unísono, en la misma transacción de datos nuevos. Este diseño de cadena de bloques es importante para los combatientes que saben que no es una cuestión de si falla la conectividad sino cuando falla la conectividad.

Cadena de bloques, una opción para administrar una red de combate de objetos

La estructura de la cadena de bloques se presta a sí misma a la administración de una red de combate de objetos (BNO) conceptual, es decir, una versión militarizada de la Internet civil de las cosas. En vez de una ruta de mando discreta para cada objeto en la red de BNO, centralizada, los objetos de paradigma jerárquico se conectan con miles de otros dispositivos de BNO en una red de cadena de bloques para enviar y recibir datos, que al descifrarlos, se añaden a cada libro de cada objeto o quizás a máquinas que acogen un libro para grupos de dispositivos de BNO relacionados. La cadena de bloques se convierte en el mecanismo de sincronización para dispositivos BNO en una red, sea cual sea su población. La cadena de bloques facilita la carga del combatiente de mantener una alta conciencia en un campo de batalla lleno de objetos conectados por red; en vez de eso, con la cadena de bloques, cada dispositivo BNO sabe.

Cadena de bloques, una opción para controlar enjambres de dispositivos de control

La forma distribuida de la cadena de bloques acoplada con los algoritmos que será diseñados en dispositivos de enjambres desbloquea un comportamiento de enjambres auténtico, logrando así un potencial completamente más militarizado. La cadena de bloques podría lograr eso de dos formas: primero, proporcionando una memoria de enjambre para formar una base de acciones de enjambre, y segundo, proporcionando los medios para la conectividad y comunicación de enjambres. Tal vez lo más interesante es que la tecnología de cadena de bloques podría activar diversos niveles de interacción entre los seres humanos y los robots. La cadena de bloques podría lograr esto mediante memoria de enjambre según se describe arriba y la dinámica de emergencia (autoorganización de enjambres; ambos podrían reforzar la conciencia de enjambre). Con una conciencia elevada, los enjambres podrían lograr altos niveles de autonomía, un atributo útil en escenarios tácticos donde el control directo del operador resulta impráctico o cuando se interrumpe la conectividad entre operadores y enjambres.[7]

Cadena de bloques, ¿cómo funciona?

La primera versión pública de Internet de cadena de bloques debutó en diferentes lugares en diferentes épocas, empezando a finales de 2008 y principios de 2009.[8] Una red de cadena de bloques puede ser de cualquier tamaño y dispone de máquinas interconectadas denominadas máquinas mineras, máquinas centrales de libros y puntos de conexión con otras redes. Las máquinas mineras son máquinas de cálculo cuya tarea es calcular una solución refinada.[9] El algoritmo de identificación digital de curva elíptica (ECDSA) es la aritmética de cadenas de bloques, y la criptografía de clave asimétrica es el medio por el cual las transacciones de datos son cifradas por un remitente y descifradas por un destinatario usando el método de clave pública/privada emparejada.[10] Una vez que una máquina minera haya determinado de forma satisfactoria una solución de ECDSA, se convierte por medio de un algoritmo en una serie de datos de 256 bitioss de largo.[11] La serie de datos es la carga útil de cualquier transacción de datos dada ordenada por la tecnología de bloques de la cadena de bloques. A medida que la transacción pasa del punto A al punto B en la red, las máquinas mineras en su función como destinatarios usan su potencia de cálculo individual para resolver una ecuación de ECDSA de una transacción calculando repetidamente la ecuación hasta que su serie de datos de salida de solución coincida con la serie de datos en la transacción de datos del remitente. Una vez establecida la correspondencia, el bloque de datos está casi completo y podrá agregarse rápidamente a los libros, donde se registran todas las transacciones completadas, de cada máquina minera de redes y máquina central de libros.[12] La tecnología clave pública/privada emparejada protege la solución de modo que un atacante no pueda robar o corromper datos dentro de la red. No hace falta ser un ingeniero in-

formático, un administrador de redes, ni un criptólogo de la Agencia de Seguridad Nacional para entender lo que está haciendo una cadena de bloques: el uso de ideas complejas de formas sencillas para producir algo más importante que meros datos.

La seguridad es la piedra angular de una cadena de bloques. La criptografía digital en la cadena de bloques es tan robusta que llevaría a una sola estación de trabajo de despacho un largo período para calcular todas las posibilidades de piratear la serie de datos de un remitente.[13] La complejidad del cifrado de una cadena de bloques puede modularse, es decir, aumentar o disminuir.[14] Para aplicaciones de cadenas de bloques militares, esta característica de reóstato puede ser instrumental para dar flexibilidad en operaciones expedicionarias; a veces se necesita más complejidad de cifrado, otras veces es apropiada una menor complejidad. En las prácticas de rutina, la generación actual de máquinas mineras de redes de cadenas de bloques tarda un promedio de 10 minutos en resolver la ecuación de cifrado estándar SHA-256.[15] No obstante, la tecnología de bloques más reciente puede reducir este tiempo de cálculo a tres minutos. Con las velocidades de los chips de la siguiente generación y la comercialización de los chips cuánticos, es concebible que la velocidad de cálculo más rápida de hoy pueda reducirse en otra orden de magnitud (seis a ocho segundos). Al final del período de cálculo actual de 10 minutos, la red efectúa lo que se considera un proceso de sincronización de la comunidad por el que todos los libros de redes se actualizan al unísono. Un bloque de datos de cadena de bloques completado de la máquina minera primero para resolver la ecuación y hacer corresponder las series de datos, denominado prueba de trabajo, se exporta a máquinas de la red como una copia y para añadir a cada libro, es decir, el registro de todas las transacciones de datos de la red desde su incepción. Imagine la red de cadena de bloques en acción; una tecnología que mejora nuestro estilo de guerra, no haciendo ese estilo menos flexible y más frágil a medida que continuamos nuestra búsqueda de digitalización.

Lo que ocurre cuando completar un bloque de datos es lo que hace que la cadena de bloques sea única y superior a los métodos de gestión de datos en las redes actuales. Recuerde esa corrupción de la función de gestión de confianza de una red puede poner en cuestión a los usuarios de redes y datos. No obstante, una vez que se complete un bloque de una cadena de bloques, se sella el contenido del bloque, y su carga útil de datos se hace incorruptible. La mecánica de este proceso es sencilla: un bloque completado se publica al unísono en cada libro de la máquina de la red. En lo que se refiere al ataque, el resultado final es que no hay un método cómodo para que un atacante corrompa los datos de transacción, por lo que su recurso sería atacar toda una red. Sin embargo, excepto la destrucción absoluta, esa red es, en el peor de los casos, obstaculizada a corto plazo, no anulada a largo plazo.

En aplicaciones militares, es probable que las máquinas mineras de la cadena de bloques funcionen para diferentes transacciones a diferentes velocidades, se desconecten y reconecten a su red en diferentes momentos y a diferentes ritmos. Las razones de esto podrían ser diferencias de rendimiento de cálculo de la máquina, inestabilidades de las comunicaciones, medidas de control de emisiones o efectos de ataques en la red. En cualquiera de estas condiciones, es posible que se desarrollen múltiples cadenas de bloques, cadenas que podrían competir con una sola cadena de bloques. Por sí mismas, no puede permitirse que persistan múltiples cadenas debido al potencial de transacciones de datos contradictorias que puedan formarse en los libros de datos de la red. El método para mitigar este problema es sencillo: las máquinas mineras y las máquinas participantes de las redes identifican la cadena más larga de bloques y tratan de añadir futuros bloques solamente a esa cadena. Dada la cantidad de procesamiento de datos que se produce en una red de cadena de bloques, las máquinas mineras pueden utilizar una herramienta lógica para mantener la cadena de bloques a una longitud predeterminada. Esta herramienta facilita la demanda de memoria de la máquina a medida que se alarga la cadena de bloques. El uso de esta herramienta ayuda a asegurarse de que, en las operaciones militares, los caudales de transacción de datos de la cadena de bloques siguen siendo a la máxima velocidad

posible.[16] La conclusión es que, la cadena de bloques no solo fortifica los datos, sino que es sensible al rendimiento de la red.

Cadenas de bloques. ¿Cómo podría ser su uso?

A continuación, se indican ejemplos seleccionados de cómo el diseño orgánico de la cadena de bloques puede aplicarse a conjuntos de misiones militares amplias:

- **Órdenes de operaciones y documentos de planificación.** La descentralización de la cadena de bloques da idea de una especie de democratización de la red en lo que se refiere a datos. Para los combatientes en una lucha, no hay nada más democrático y urgente que la necesidad de conocer el plan de combate y mantener los cambios al día. Poner los aspectos relevantes de un plan de combate en manos de los combatientes es una meta de preparación y ejecución. El salto adelante de la cadena de bloques es su tecnología, que asegura que sus datos, en este caso puntos de operación, sea descartada horizontalmente; los datos se preservan en la piedra que son los bloques de datos. Si alguna parte de la red sufre una interrupción de conectividad con una red de la comandancia, esa red superior necesita pasar solamente bloques de datos a una sola máquina minera de una red subordinada. En esa situación, esa máquina minera receptora empujará ese bloque y otros según sea necesario para todos los libros de datos en esa red de cadena de bloques. El entonces qué pasa es que se refuerza la conciencia situacional de la lucha, y la misión continúa.
- **Control de enjambres de dispositivos.** Los diseñadores trabajan en sistemas portadores para dispositivos de enjambres, un método de combate que ha atraído la atención de las FF.AA. de EE.UU., y los ingenieros identifican aplicaciones de dispositivos de enjambres. El máximo reto de empleo de enjambres no es el diseño o empacado de dispositivos; es control.[17] Una de las limitaciones clave del control de cientos, en realidad, miles de dispositivos dentro de un enjambre, es lo que los expertos llaman conocimientos globales. En otras palabras, es una conciencia de no solo dispositivos adyacentes sino también de conciencia compartida entre todos los dispositivos de la población.[18] En combinación con rutinas de operación sencillas programadas en cada dispositivo pero administradas y organizadas por el diseño abierto y distribuido de una red de cadena de bloques, todo lo que detecta un enjambre sería conocido y conocible para todos los dispositivos en ese momento. El resultado es la capacidad de un enjambre de comportarse como una sola entidad. La tecnología de cadena de bloques desbloquea las posibilidades militares de enjambres.
- **Logística**. Con tantos datos logísticos de oferta y demanda intercambiados entre proveedores militares y homólogos civiles, la garantía de que los datos son auténticos, no manipulados, es de importancia suprema. La lógica del libro de la cadena de bloques asegura que se puede confiar inherentemente en lo que es transmitido por remitentes creíbles y recibido por destinatarios autorizados. La cadena de bloques funciona especialmente bien en el mundo de la logística dados sus contratos, acuerdos, formularios de órdenes, documentos de requisición, etc. Tanto si esos documentos logísticos son generados por computadora o no, la lógica orgánica de la cadena de bloques asegura que cada documento sigue siendo fiable, accesible e incorruptible.

Cadena de bloques—Algunas limitaciones

Las vulnerabilidades descubiertas en los primeros experimentos de laboratorio fueron reconocidas y tratadas; una de ellas fue la máquina minera egoísta. El problema de la máquina minera egoísta se basa en una situación donde un grupo de máquinas mineras se confabula para impedir o desviar transacciones para su ganancia; un reto en algunos entornos de cadenas de bloque civiles. En el ejemplo del peor de los casos de una máquina minera egoísta, una minoría de máquinas mineras bandido trata de reclutar otras máquinas mineras para ponerse gradualmente por delante y con el tiempo controlar una red. Los investigadores descubrieron dos aspectos de este fenómeno: primero, el problema de la máquina minera egoísta tiene un límite superior por el que las máquinas bandido con el tiempo asumen el control de la red para convertirse en la red reinventada. El segundo descubrimiento fue que una simple modificación de la codificación de la lógica de la cadena de bloques eliminó brotes de la máquina minera egoísta al principio.[19]

Los ingenieros identificaron otra vulnerabilidad, un ataque Sybil. Este ataque se produce cuando un actor añade máquinas mineras bandido a una población menor de una red, no para resolver rápidamente la ecuación sino para apartar a las máquinas mineras honradas de esa población de la red y evitar que resuelvan ciertas transacciones. El impacto del ataque Sybil es doble: disminuye la potencia de cálculo agrupada de la red y hace más lenta la actualización de los libros de la red. La vulnerabilidad del ataque Sybil puede eliminarse de forma proactiva alterando el comportamiento preferencial de la máquina minera de la cadena de bloques individual más larga; la lógica que obliga a las máquinas mineras a añadir bloques de libros solamente a la cadena existente más larga. En parte, de modo contradictorio a una lógica de operación normal, el antídoto de un ataque Sybil es dividir la población de máquinas mineras de modo que todos los bloques de salida de máquinas mineras se segreguen en dos cadenas discretas hasta que emerja una como la cadena más larga, normalmente compuesta por un solo bloque. Cuando emerge esa cadena individual, el ataque Sybil se detiene, se desecha la cadena más corta y la población de máquinas mineras reanuda la operación normal.

Cadena de bloques—Respuesta a las limitaciones

Para adaptar mejor una cadena de bloques a una aplicación militar, los programadores harán un mapa de los detalles aprendidos de los principios de la cadena de bloques. Los avances en inteligencia artificial (AI) podrían aprovecharse para disuadir y suprimir la minería de datos egoísta como alternativa para modificar la lógica de la cadena de bloques. Otro uso de los algoritmos de AI radicará en la localización de un comportamiento anómalo de máquinas mineras, como la formación temprana de grupos de máquinas mineras egoístas.

La cadena de bloques como tecnología sigue en evolución, produciendo nuevos tipos y usos potenciales. Un ejemplo de dicha innovación es que las cadenas de bloques alternativos son una variante que crea redes de cadenas de bloques que solo buscan y procesan tipos de transacciones de datos específicos. Otra variante de la cadena de bloques son las cadenas laterales, grupos especiales de máquinas mineras para resolver clases específicas de transacciones en redes construidas con un fin. En uso militar, las cadenas de bloques alternativas probablemente tendrán utilidades en redes que efectúan transacciones de datos de inteligencia. La AI, las máquinas mineras y las máquinas podrían trabajar en equipo para filtrar transacciones en diferentes niveles de clasificación en redes de cadenas de bloques alternativas. Para ampliar esta idea, las redes de cadenas de bloques de inteligencia proporcionarían datos a usuarios que usen permisos de acceso guardados en la misma red en vez de en redes separadas lado a lado para usuarios autorizados a niveles y programas diferentes. Una característica de seguridad adicional sería un navegador anonimizador que oculte la información del usuario y otros datos pertinentes.[20]

En operaciones de campo, las cadenas laterales de bloques probablemente tienen una función significativa. Entre otros ejemplos se incluyen redes de misiones que realizan funciones de transferencia e intercambio de datos en apoyo de misiones específicas, como incursiones, ocupaciones, ataque a objetivos de alto valor y así sucesivamente. No obstante, se debe hacer un contraste importante: las redes actuales del Departamento de Defensa descienden al nivel táctico (jerarquizadas, centralizadas). La cadena de bloques es diferente; está descentralizada (horizontal). Los atacantes saben cómo derrotar las redes centralizadas y paralizar la misión militar, que es el problema de hoy. La cadena de bloques descarta ese problema y asegura que las misiones no se vean amenazadas por motivos de seguridad de datos.

Hace uno años llegó una evolución futura, la cadena de bloques 2.0, y generó la aparición de más de una docena de nuevos proveedores de cadenas de bloques comerciales, cada uno de ellos especializado en tecnología de cadena de bloques para adaptarse a aplicaciones comerciales específicas que se basan en varios tipos de cadenas de bloques. Una de dichas entidades, ADEPT, un desarrollo conjunto de IBM y de la fundación Ethereum, está desarrollando una cadena de bloques para aplicaciones de la Internet civil de las cosas.[21] La variante de cadena de bloques de Ethereum reacondicionaría la Internet desde su estado actual a un estado alternativo donde los registros, documentos de títulos, contratos y similares ya no son almacenados ni poseídos por terceras entidades gubernamentales o comerciales. En esta perspectiva, las aplicaciones de almacenamiento y accesibilidad de cadenas de bloques se convierten en el lugar preferido de almacenamiento de dados del siglo XXI.[22] Para los combatientes, todo esto significa que la cadena de bloques ya está adquiriendo nuevas formas y está suficientemente desarrollada para aplicaciones militares adaptadas que apoyan diversas misiones.

Las máquinas mineras de cadenas de bloques requieren una potencia de cálculo amplia. Las instalaciones adecuadas para alojar máquinas mineras es probable que existen en bases, puertos y centros de estado constante. Para colocar máquinas mineras más en vanguardia, las fuerzas de combate cercanas, los diseños de máquinas mineras militarizadas deben consumir menos potencia, ocupar menos espacio y robustecerse debidamente. Hay que hacer algo de trabajo para preparar componentes de la cadena de bloques para el despliegue.

Adopción, ¿qué ha mejorado?

La cadena de bloques es una tecnología de criptografía existente expresada en un nuevo concepto de aplicación con la ventaja principal de asegurarse de que los combatientes mantengan una elevada confianza en la autenticidad y seguridad de los datos que obtienen de las redes del Departamento de Defensa. La conclusión es que la cadena de bloques da a los combatientes lo que necesitan, datos en los que confiar. Como ventaja, los datos fiables tratan de una preocupación del combatiente que son los datos que otros no pueden corromper. En la lucha, en términos prácticos, ¿puedo confiar en datos para ayudar a mitigar la vulnerabilidad cibernética y preservar el momento operacional?

¿Están las FF.AA. de EE.UU. buscando agresivamente el desarrollo de una cadena de bloques? No. Las razones se basan en líneas generales, en escepticismo de nuevas ideas y en una vía de desarrollo que no está clara. A pesar de la fascinación del Departamento de Defensa por la innovación, que demasiado a menudo es una actitud "no inventada aquí" cierra las mentes y las puertas a pensar y a cosas que retan las normas de statu quo. Piense por ejemplo en *La estructura de las revoluciones científicas* por Thomas Kuhn. Aun así, otros críticos del Departamento de Defensa encuentran una razón para rehuir nuevas ideas porque a primera vista no son maduras, pero tampoco lo eran las tecnologías de radar o propulsión a chorro cuando aparecieron por primera vez en escena. La percepción, por supuesto, es que a veces se debe mirar más allá de las limitaciones presentes para ver en que se podría convertir una tecnología. En otro lugar, la idea de

proteger mejor, o al menos más, los datos del Departamento de Defensa, no se ve tan creíble como gastar miles de millones de dólares adicionales en el lado de equipos de la empresa de datos militar masiva de EE.UU.

Por último, hay una cosa que podemos afirmar categóricamente: adquirir datos para una aplicación militar es importante; proteger esos datos es esencial. Desarrollar una cadena de bloques y luego desplegarla para reforzar la seguridad de los datos y mejorar el rendimiento de operación de cada sistema de armas que toca el Departamento de Defensa. ❑

Notas

1. Los *usuarios de los márgenes* incluyen a todos los usuarios fuera de los nodos de comando y control estáticos con énfasis en usuarios tácticos, *combatientes*, en ajustes expedicionarios.

2. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin, un sistema de dinero en efectivo electrónico de red de pares), visitada el 1 de septiembre de 2016, http://www.bitcoin.org/bitcoin.pdf.

3. Michael Crosby, y otros, *Tecnología* de cadena de bloques, Sutardja Center for Entrepreneurship and Technology, 16 de octubre de 2015, 3. Fuera de los operadores de los sistemas de redes, muchos usuarios no reconocen prácticamente las actividades de *confianza* en redes. Crosby y otros citan actividades familiares como productos de actividad de confianza de intermediario de redes: verificación de que el correo electrónico de una persona se entrega en un buzón, verificación de Facebook en que los anuncios son compartidos solamente con contactos amigos, etc.

4. En este ensayo la *autenticidad* se refiere al control de la identidad de un usuario dado.

5. La norma del *Algoritmo de Hash Seguro* (SHA)–256 contiene una orden de alta confianza de dígitos de hasta 256 bitios de largo. La metodología de SHA tiene sus raíces en trabajo de la NSA para mejorar la integridad de las series de datos transmitidas por medio de protocolos de mensajes. Al usar una serie de dígitos de 256 bitios de largo, equivalentes a 2.256 posibles variaciones digitales, una recepción de mensaje puede ejecutar una rutina sencilla que se parece a la serie de datos de SHA–256 de un archivo específico antes /después de la transmisión. La fuerza detrás de la norma SHA–256 es la fuerza aritmética de 2.256. Para reducir el tiempo de procesamiento de transacciones a minutos, las máquinas mineras de la red compiten y al final cooperan para agrupar su fuerza de cálculo a fin de encontrar la correspondencia correcta, la solución. Las futuras aplicaciones de cadenas de bloques militares podrían aprovecharse de series de datos de SHA aún más robustas, 512, 1.064, etc.

6. Las máquinas mineras de cadenas de bloques son máquinas diseñadas de forma especial con una potencia de procesamiento robusta para calcular la solución exclusiva de cada serie de datos de transacción SHA–256.

7. La cadena de bloques no hará que los dispositivos operen como un enjambre, sino que es el medio por el que el enjambre puede lograr los conocimientos globales dentro de máquinas innatos a los enjambres de la naturaleza.

8. Crosby, 5.

9. Erik Rykwalder, "The Math behind Bitcoin" (Las matemáticas detrás de Bitcoin), Próximo mundo con Michio Kaku, 19 de octubre de 2014, http://www.coindesk.com/math-behind-bitcoin/.

10. Ibid., 1. Nota: ECDSA según se usa en la cadena de bloques está relacionado con otros algoritmos criptográficos curvados elípticos. El principio detrás de ECDSA es simple: la buena criptografía activa el principio de trabajo de matemáticas resistente al pirateo informático. ECDSA tiene ventajas porque la cadena de bloques necesita claves públicas /privadas para completar un mensaje de datos (transacción). En la cadena de bloques, la solución es una identificación de la solución exclusiva pero la transacción del mensaje se completa cuando esa solución se hace corresponder con la serie de soluciones cifradas por el remitente. Una vez completado esto, se pone un sello de tiempo en el bloque y se completa. Se puede añadir un bloque completo a ese propio libro de la máquina minera; una vez completado, la prueba de trabajo de la máquina minera se convalida cuando se añade a todos los libros específicos de la red.

11. En la cadena de bloques, el principio es: objeto digital (cálculo de ECDSA) que se procesa en el algoritmo SHA–256 para el que la salida de datos resultante casi exclusiva se denomina *hash*: la huella digital del objeto original.

12. Ibid., 6.

13. Ibid., 8–11. En un chip de estación de trabajo rápida de reloj de 20 MHz de 32 bitios (~ 224 hashes/seg), se estima que la máquina individual necesitaría 139.461 años para igualar la serie de datos de entrada/salida de 256 bitios. Los intervalos de E/S más cortos se pueden producir con más potencia de cálculo de chips. La tarea de la militarización será conseguir un equilibrio entre la robustez criptográfica de SHA y el rendimiento del chip de economía de escala en dispositivos ligeros de enjambres. Ya son comercialmente viables las tecnologías de cadenas de bloques "más ligeras" con intervalos de cálculo reducidos de 10 a 3 minutos.

14. El cifrado estándar de la cadena de bloques básica que apoya a Bitcoin es el algoritmo hash seguro (SHA) que mide 32 bytes (256 bitios) de largo.

15. En sistemas de cadenas de bloques en la industria de pagos, el tiempo asociado con este ciclo de sincronización es sintético. En aplicaciones militares, podría aumentarse o reducirse. *Litecoin* usa un ciclo de sincronización de 2,5 minutos.

16. Esta herramienta lógica es conocida como árbol de M*erkle*. Para recuperar espacio usado de disco de computadora, es decir, utilizado por la memoria en cálculos anteriores, cuando la cadena alcanza una longitud dada, el limitador

de longitud integrado de la máquina minera se pone a funcionar recortando la cadena de bloques más antiguos. Aquí existe una relación más profunda en curso que está relacionada con el cifrado de hash inherente en los bloques en el fondo, donde se inicia el recorte. A medida que aumenta la potencia de cálculo en cada nodo de máquina minera, el número de cadenas que puede retenerse en su respectivo Árbol de M*erkle* difiere de la memoria de otra máquina minera; no obstante, la cantidad de bloques eliminados de la memoria no excede nunca el mínimo requerido para asegurar una operación de la red inalterada.

17. Peter Coy y Olga Karif, "This Is Your Company on Blockchain" (Esta es su compañía en cadena de bloques), Bloomberg Businessweek, 25 de abril de 2016, 8, visitada el 2 de septiembre de 2016, http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain.

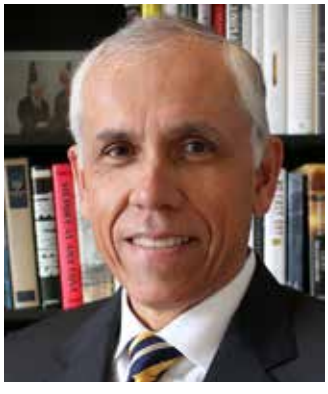
18. Eduardo Castelló Ferrer, "The Blockchain: A New Framework for Robotic Swarm Systems" (La cadena de bloques: una nueva estructura para sistemas de enjambres robóticos), (Cambridge, MA.: MIT Lab, 3 de agosto de 2016), 3, https://www.researchgate.net/publication/305807446_The_blockchain_a_new_framework_for_robotic_swarm_systems.

19. Esta configuración se logra disminuyendo el número de máquinas mineras requerido para lograr el consenso de la red. En esta situación, se disminuye el umbral total; esto actúa como una herramienta para impedir la colusión de máquinas mineras egoístas.

20. El navegador anonimizador TOR es uno de estos ejemplos.

21. *Ethereum* es una organización suiza sin ánimo de lucro, www.ethereum.org.

22. Cellabz, "Blockchain and Beyond" (Cadena de bloques y más allá), Cellabz, Inc., París, Francia, Noviembre de 2015, versión 1.0, 16.



Coronel Vincent Alcazar, **USAF,** retirado del servicio activo en diciembre de 2014. Piloto de avión caza con 3.800 horas de vuelo en diversos aviones caza, instructor de JSUPT, piloto instructor de F-15 FTU y comando. Veterano de misiones de combate de Tormenta el Desierto y despliegues como Libertad Iraquí, es también un ex-agregado aéreo en Irak. Es el antiguo líder de la Fuerza Aérea de Air-Sea Battle, anterior planificador y estratega con experiencia en estado mayor de la comandancia de la Fuerza Área. El Coronel Alcazar reside en el norte de Virginia.