Blockchain: tendências no mercado e oportunidades de aplicação para a segurança de dados e ativos digitais em unidades de combate ao crime[1]

Gleidson Sobreira Leite[2]

RESUMO

No contexto do combate ao crime, instituições governamentais de vários países instituíram unidades ou setores especializados para atuar em diferentes áreas e expertises como, por exemplo, em atividades de investigação e inteligência. Entretanto, por atuarem em um cenário voltado a atividades restritas, ou que muitas vezes envolvem informações ou ativos sigilosos, surge a necessidade de adoção de soluções alternativas voltadas à gestão, armazenamento e/ou compartilhamento de ativos digitais com a preocupação em segurança da informação. Sendo uma das tecnologias que vem ganhando cada vez mais espaço no mercado mundial, *blockchain* vem se apresentando como uma solução viável para o setor público e o governo. Explorando as principais características da tecnologia *blockchain*, este documento apresenta uma visão geral das diferentes tendências de aplicação da tecnologia, e propõe o uso de *blockchain* como mecanismo de suporte no gerenciamento, armazenamento e/ou compartilhamento de ativos digitais gerados no contexto de unidades especializadas que atuam no combate à criminalidade.

1 Data de Recebimento: 07/02/2020. Data de Aceite: 29/05/2020.
2 Servidor público. Analista Ministerial de tecnologia da informação do Ministério Público do Estado do Ceará lotado no Núcleo de Inteligência e Apoio Técnico (NIAT). Pós-Graduação em segurança da Informação da Universidade Estácio de Sá. Mestre em Informática Aplicada pela Universidade de Fortaleza. Doutorando em Informática Aplicada pela Universidade de Fortaleza. E-mail: gleidson.sleite@gmail.com

Palavras-chave: *Blockchain*. Combate ao Crime. Governo. Segurança da Informação. Setor Público.

1 INTRODUÇÃO

Existem diversas variações nas taxas de criminalidade apresentadas em estudos estatísticos em diferentes épocas e lugares do mundo, onde, sendo um tópico emergente e muito importante, principalmente devido aos impactos econômicos e sociais negativos, a prevenção ao crime é uma preocupação mundial.

Uma pesquisa realizada em março de 2018 por Refinitiv (2018), por exemplo, que contou com a participação de 2.373 gerentes seniores de grandes organizações globais em 19 países, encontrou cerca de 1,45 trilhões de dólares em volume total perdido estimado como resultado de crimes financeiros. Com relação a crimes violentos, FBI (2019) realizou estudos estatísticos, e salientou que, em 2018, havia um número estimado de 1.206.836 crimes violentos apenas nos Estados Unidos.

Esses e vários outros estudos apontam preocupações sobre a evolução e expansão do crime, onde, devido à diversidade e ao volume das práticas criminais existentes, é essencial a ação preventiva, repressiva (impedimento de continuidade), controle ou punição por parte das instituições do governo para minimizar os danos causados à sociedade.

Com esse fim, instituições governamentais de vários países, e que trabalham no combate ao crime, estabeleceram unidades, ou setores especializados em atividades de investigação e inteligência para atuar em diferentes áreas e conhecimentos, como, por exemplo, FBI (2020) ou EUROPOL (2020), que possuem unidades especializadas no combate a crimes como corrupção, organizações criminosas, crimes violentos, crimes de colarinho branco, crimes financeiros, entre outros.

Como exemplo de unidades especializadas, no Brasil uma ação estratégica nacional (Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro - ENCCLA) possibilitou a criação de uma rede de laboratórios de tecnologia e combate a lavagem de dinheiro (LAB--LD), que atuam com foco em crimes financeiros. (ENCCLA, 2003).

Segundo Pina (2014), o LAB-LD é uma unidade de investigação e análise de dados que visa à identificação de atividades ilícitas por meio da aplicação de soluções tecnológicas, metodologias e técnicas diversas, possui especialistas com perfis profissionais ou expertises distintas, e normalmente trabalha com alto volume de dados proveniente de diversas fontes. (FRANÇA JUNIOR, 2001).

No entanto, no caso de unidades especializadas em combate ao crime, existe a questão de também trabalharem com informações sigilosas (ou sensíveis) e atividades restritas, muito específicas e com considerável complexidade. Esses problemas geram uma grande preocupação com a segurança, e a confidencialidade durante todos os processos operacionais internos, incluindo a geração, armazenamento e compartilhamento de informações, ou ativos entre membros da mesma unidade ou mesmo entre diferentes unidades ou instituições. (DREZEWSKI, 2015; UNDP, 2019).

Nessas situações, em caso de exposição, ou vazamento de informações, ou mesmo de ativos como documentos eletrônicos contendo padrões, metodologias, técnicas ou estratégias adotadas, pode prejudicar o desempenho não apenas de um setor especializado, mas também da instituição como um todo e de demais envolvidos. (UNODC, 2011).

Com o intuito de minimizar o uso indiscriminado de informações, nortear o tratamento (coleta, uso, manutenção e armazenamento) das mesmas, assim como prover meios de possibilitar atuações mais efetivas de monitoramento, fiscalização ou punição, regulamentações voltadas à proteção e segurança de dados vem sendo aplicadas em diversos países.

No Brasil, o Decreto nº 9.637 de 26 de dezembro de 2018, que institui a Política nacional de segurança da informação, e dispõe sobre a governança da segurança da informação, é um exemplo de ação para fortalecimento da cultura de segurança da informação na sociedade. O decreto abrange a segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais e ações destinadas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. (BRASIL, 2018, p. 23).

A administração pública, em todos os seus níveis e órgãos, processa informações consideradas "sensíveis", que requerem a proteção contra a intrusão e modificação desautorizadas. Assim, o estabelecimento de uma política de segurança do material informativo que é armazenado e documentado em sistemas de computação e bases de dados, ou até mesmo ativos digitais como documentos eletrônicos, áudios, vídeos, entre outros, é de extrema importância.

Com relação a aspectos da responsabilidade pela guarda da informação, a União Europeia foi pioneira na regulamentação e proteção de dados com a *General Data Protection Regulation* (GDPR), que entrou em vigor em maio de 2018, e serviu de base para inúmeras outras legislações nacionais como, por exemplo, a Lei Geral de Proteção de Dados (LGBD) no Brasil. (GDPR, 2018; BRASIL, 2018, p. 59).

Porém, embora as abordagens atuais relacionadas ao gerenciamento de ativos digitais tenham trazido benefícios para mercado, ainda é um grande desafio oferecer uma maneira eficaz, segura, verificável e rastreável de gerenciar, armazenar, organizar e recuperar dados e ativos digitais. Em alguns casos, devido ao envolvimento de terceiros que são responsáveis por armazenar esses ativos (exemplo: armazenamento na nuvem), muitas abordagens carecem de confiança, transparência e segurança. (ZHU, 2018).

Motivado por esse cenário, e devido à considerável preocupação com segurança da informação, além das características inerentes ao contexto dessas unidades especializadas, surge uma oportunidade

para a adoção de soluções alternativas voltadas ao gerenciamento, armazenamento e compartilhamento de ativos digitais.

Com base nesse contexto, e explorando as principais características da tecnologia *blockchain*, este documento apresenta uma visão geral das diferentes tendências de aplicação da tecnologia, e propõe o uso de *blockchain* como mecanismo de suporte no gerenciamento, armazenamento e/ou compartilhamento de ativos digitais gerados no contexto dessas unidades especializadas.

Este trabalho também pretende ser uma contribuição ao conjunto de conhecimentos relacionados aos estudos sobre o uso da tecnologia da informação no combate ao crime, e pode ser adotado para auxiliar profissionais e pesquisadores na identificação de possíveis tendências de aplicações.

Para a realização do objetivo deste trabalho, realizaram-se três ações específicas, sendo elas: pesquisa e exploração das principais características da tecnologia *blockchain* apresentadas em estudos acadêmicos; pesquisa bibliográfica e seleção de tendências de aplicação em diferentes domínios; e proposta de uso da tecnologia *blockchain* como mecanismo de suporte no gerenciamento, armazenamento e/ou compartilhamento de ativos digitais gerados no contexto de unidades de especializadas no combate ao crime, e discutir suas contribuições com relação à segurança da informação.

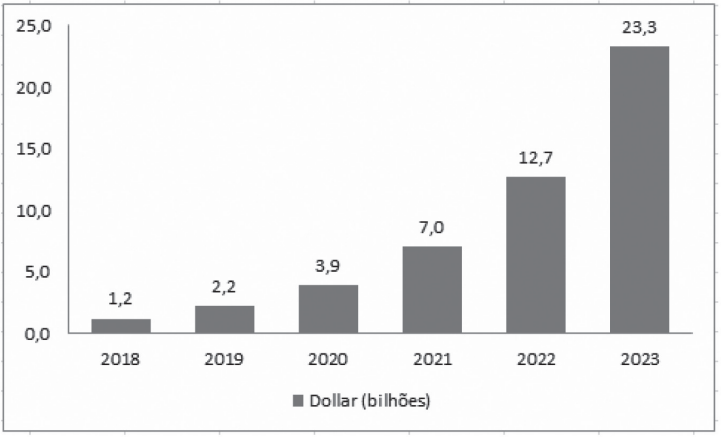
Este artigo, organizado em seções, procura apresentar em linhas gerais: metodologia de pesquisa do trabalho (Seção 2); principais características da tecnologia *blockchain* e tendências de aplicação em diferentes domínios (Seção 3); uma proposta de uso da tecnologia no contexto de unidades de combate ao crime, seguida de discussões (Seção 4); e finalmente, as considerações finais e possibilidades de trabalhos futuros (Seção 5).

2 A TECNOLOGIA *BLOCKCHAIN* E APLICAÇÕES NO SETOR PÚBLICO

Sendo introduzida pela primeira vez como a principal tecnologia por trás da criptomoeda Bitcoin proposta por Satoshi Nakamoto (2018), em um artigo pseudônimo, a *blockchain* vem atraindo cada vez mais atenção da indústria e da academia.

Com o crescente interesse global por tecnologias de informação e comunicação, é possível prever o futuro da *blockchain* como uma das tecnologias em progresso da era atual. Em dezembro de 2018, por exemplo, a Statista conduziu uma pesquisa estatística em que, de 2019 a 2023, foi observado um grande aumento no tamanho do mercado da tecnologia *blockchain* em todo o mundo (Figura 1).

Figura 1 – Tamanho do mercado mundial da tecnologia *blockchain* de 2018 a 2023 (em bilhões de dólares). Período da pesquisa: 2018. Data de publicação: dezembro de 2018.



Fonte: statista.com

De acordo com Swan (2015), *blockchain* é uma tecnologia baseada em um sequenciamento ou cadeia de informações armazenadas em blocos. Ela pode ser definida como uma rede distribuída e descentralizada, na qual as transações realizadas pelos participantes são armazenadas em ordem estrita em um "livro de registros" (ledger), imutável e transparente, composto de blocos conectados entre si por hashes criptográficos, o que dificulta a ocorrência de fraudes.

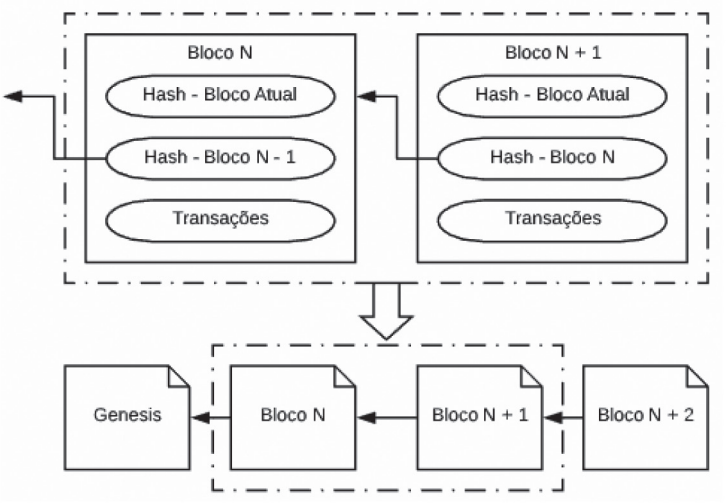
Hashes criptográficos permitem a geração de um identificador único de tamanho fixo (representação em texto) mapeado a partir de entradas de tamanho variável (exemplo: um ativo digital como um documento eletrônico). Com isso, verificações de integridade podem ser realizadas, visto que, com a geração do *hash* de um arquivo, qualquer alteração do mesmo acarretaria também em uma alteração do valor *hash*. (PINHEIRO, 2019).

A ideia básica por trás da tecnologia *blockchain* é que ela permite que os atores de um sistema (chamados nós) transacionem dados ou ativos digitais, usando uma rede que armazena essas transações de maneira distribuída pela rede. Os proprietários dos ativos e as transações, que envolvem mudança de propriedade (ou demais transações), são registrados no livro de registros pelo uso de criptografia de chave pública e assinaturas digitais. Toda transação é validada pelos nós da rede, empregando algum tipo de "mecanismo de consenso" (protocolo de consenso). (BACK, 2014; WARBURG, 2016).

Isso funciona da seguinte maneira: sempre que uma transação é inserida na rede, os nós primeiro validam a transação. Se os nós concordam com sua legitimidade, confirmam a transação e essa decisão é inserida em um bloco, onde este novo bloco é adicionado à cadeia anterior de blocos. Dessa maneira, o último bloco mantém uma visão compartilhada e acordada do estado atual da *blockchain.* (BUTERIN, 2014).

Um exemplo ilustrativo da estrutura de dados da cadeia de blocos do *blockchain* é apresentado na Figura 2.

Figura 2 – Estrutura de dados da cadeia do blockchain



Fonte: Elaborado pelo autor

Em relação ao conteúdo dos blocos, eles são divididos em hash, formando um identificador único de bloco armazenado no bloco atual e subsequente. Cada bloco contém transações de dados com registro de data e hora *(timestamp),* cuja integridade e autenticidade são garantidas graças aos algoritmos de *hash* e criptografia de chave pública. A partir do resultado determinístico e irreversível da função hash, é possível verificar se o conteúdo do bloco foi modificado. Cada bloco faz referência ao *hash* do bloco que veio antes dele, estabelecendo um link entre eles e, assim, criando o *blockchain*. Os hashes a seguir do bloco atual terminam com o primeiro bloco criado em uma *blockchain* específica (chamada de bloco de gênesis). (JAMIL, 2019; ALKURDI, 2018; ZHENG, 2019).

Com o uso de *hash, timestamp* e demais informações inseridas no livro de registros imutável, é possível obter um prova concreta e irrefutável sobre a existência, data de criação, origem, propriedade, conteúdo, segurança e integridade de ativos digitais (exemplo:

documentos eletrônicos, áudios, vídeos, entre outros), e sem necessariamente revelar seu conteúdo, mas com relevante valor jurídico.

Para formalizar e proteger digitalmente os relacionamentos e transações em uma rede *blockchain*, um contrato inteligente pode ser usado para automatizar o processo de acordo entre os participantes.

Conforme mencionado por Szabo (1994), um contrato inteligente é um aplicativo (como um protocolo digital) que verifica, executa e aplica os termos dos contratos que foram acordados entre as partes, ajudando as transações a serem executadas automaticamente de forma transparente, sem conflitos, de forma obrigatória, mais rápida e segura, sem precisar depender de intermediários. (ZHENG, 2017; FENG, 2019).

Com o desenvolvimento contínuo da tecnologia *blockchain*, o escopo de aplicação da *blockchain* é muito amplo e pode ser dividido em três tipos: pública, consórcio e privada. A Tabela 1 apresenta uma comparação geral sobre os tipos de *blockchain*.

Tabela 1 - Tipos *blockchain* (publico, privado e consórcio)

	Público	**Privado**	**Consórcio**
Definição	Todo participante pode ler, escrever, monitorar, negociar e participar do processo de consenso.	Usado em uma única organização. Permite apenas que os participantes escolhidos ingressem na rede com participações restritas.	Opera sob a liderança de um grupo de organizações. Permite apenas que os participantes escolhidos ingressem na rede com participações restritas.
Acesso	Aberto	Permissionado	Permissionado
Segurança	Alta	Média	Média
Privacidade	Média	Alta	Alta
Ambiente	Não-confiável	Confiável	Confiável

Fonte: ZHENG, 2019; YANG, 2019

A seleção e uso do tipo de *blockchain* leva em consideração o domínio de aplicação. Por exemplo, para o cenário de unidades especializadas, onde é importante que os participantes sejam devidamente identificados e autorizados (acesso permissionado), que todas as

suas transações sejam registradas, e que normalmente estão dentro de um ambiente com maior nível de segurança (ex: rede privada ao invés da internet), a seleção do tipo privado ou em consórcio seria mais adequado a depender do número de organizações participantes.

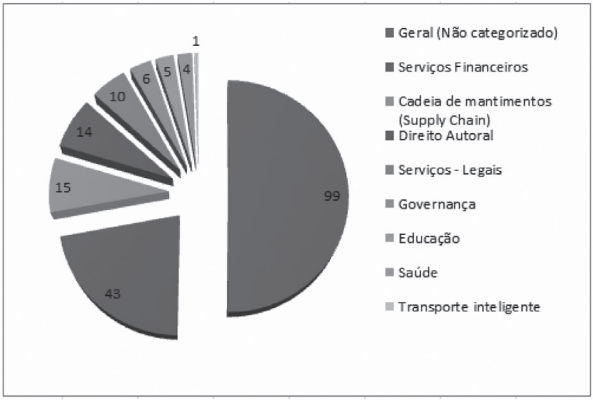
2.1 Tendências de Aplicações de *Blockchain* e uso no Setor Público

No que diz respeito às tendências de aplicação e perspectivas de uso da tecnologia *blockchain*, empresas e instituições de vários setores e indústrias da economia global vêm explorando seu potencial nos últimos anos.

Com base no conjunto de dados do Cambridge Center for Alternative Finance (CCAF) de 67 redes *blockchain* corporativas de 25 países globalmente implantados em produção e atualmente ativos, Rauchs (2019) apontou que 43% da lista de casos de uso são aplicáveis setor financeiro e de seguros. Os serviços de acomodação e alimentação, bem como os setores de assistência médica e assistência social ficaram em um segundo lugar distante, com 6% de todas as redes cada.

No início de 2019 havia, segundo CAC (2019), 197 provedores de serviços de *blockchain* registrados na *Cyberspace Administration of China.* A Figura 3 apresenta um agrupamento por categorias de domínios de aplicação apresentado por Zheng. (2019).

Figura 3 - Estatísticas de provedores de serviços de *blockchain* registradas no início de 2019 na China



Fonte: (ZHENG, 2019)

No Brasil, a *blockchain* vem sendo adotada onde um dos pioneiros foi o Cartório Azevedo Bastos, localizado em João Pessoa (PB), em parceria com uma *start-up* denominada OriginalMy, que utilizou a tecnologia para tornar disponíveis serviços de autenticação de documentos. O cartório oferece o serviço de autenticação digital para pessoas jurídicas por meio de uma rede *blockchain.* (ANDRIGHI, 2018, p. 610).

No campo jurídico, Aleixo (2017) aponta exemplos de aplicações de *blockchain* como registros de propriedades, comprovações de autoria e propriedade intelectual, contratos automatizados, remessas internacionais de valores, emissão de títulos privados, organizações descentralizadas autônomas, armazenamento remoto e distribuído de dados na nuvem, além de produtos financeiros diversos.

Com relação às aplicações da tecnologia no setor público e governo, Batubara (2018) realizou uma revisão sistemática para entender os tópicos atuais de pesquisa, desafios e orientações futuras sobre a adoção da *blockchain* para o governo eletrônico.

Dos 21 artigos científicos encontrados em sua pesquisa, e que propuseram a integração de *blockchain* no governo eletrônico, a maioria das pesquisas (sete artigos) discute a aplicação do *blockchain* para o governo eletrônico em geral, discutindo a ideia, benefícios potenciais, questões atuais, uso potencial, abordagem e avaliação de adoção de *blockchain*.

As aplicações de *blockchain* na saúde pública receberam a maior atenção em quatro artigos. Enquanto isso, três artigos examinaram o uso da *blockchain* em serviços educacionais, e também três artigos no contexto de cidades inteligentes. Dois artigos analisam no contexto do governo as cadeias de suprimentos comerciais, e artigos únicos foram dedicados à identidade digital, votação eletrônica e sistema tributário. Os resultados mostraram que a adoção de soluções baseadas em *blockchain* no governo eletrônico ainda é muito limitada.

Os benefícios potenciais em termos de aspectos estratégicos, organizacionais, econômicos, informacionais e tecnológicos no governo foram identificados por Ølnes (2017) e, de acordo com Jun (2018), em 2018, mais de 100 projetos de *blockchain* criados para transformar sistemas governamentais estavam sendo conduzidos em mais de 40 países ao redor do mundo.

Zhang (2019) também citou que governos como no Reino Unido, Europa, China, Estados Unidos da América (EUA), entre outros, divulgaram documentos oficiais e relatórios técnicos sobre *blockchain*, para mostrar sua atitude positiva em relação ao desenvolvimento da tecnologia.

Robichez (2019) apresentou um relatório temático elaborado por pesquisadores e apoiado pela Fundação Carlos Chagas com o objetivo de fornecer uma visão consolidada sobre o potencial da tecnologia *blockchain* quanto sua aplicação em governos e setor público. Sua pesquisa apontou estudos pelo mundo com foco em identidade digital, votação, registros públicos, compartilhamento de dados, transparência pública, contratações, mercado de ativos e

criptomoedas, dados do cidadão e E-social.

Apesar de que a adoção da tecnologia *blockchain* vem sendo uma tendência crescente, nos último anos, no entanto, apesar das diversas aplicações em distintos contextos, no que diz respeito às aplicações dentro do domínio das unidades de inteligência e investigação, verificou-se uma carência de abordagens nos aspectos industrial e acadêmico.

Motivado a partir dos trabalhos de Warburg (2016), Naz (2019), Xia (2017) e Xuan (2019), na próxima seção, o uso de blockchain é proposto como um mecanismo de suporte no gerenciamento, armazenamento e/ou compartilhamento de ativos digitais gerados no contexto de unidades de investigação e inteligência.

3 APLICAÇÃO DE BLOCKCHAIN NO SENÁRIO DE UNIDADES ESPECIALIZADAS

3.1 Cenário e arquitetura proposta

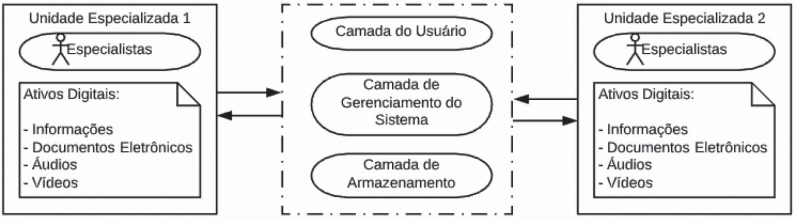
A Figura 4 apresenta o cenário referente ao gerenciamento, armazenamento e/ou compartilhamento de ativos digitais de uma ou mais unidades especializadas no contexto de atividades de inteligência e investigação.

Nesse cenário, durante a execução de várias atividades inerentes a essas unidades especializadas, diferentes ativos (exemplo: documentos eletrônicos, áudios e vídeos) são gerados e pode ser necessário gerenciar seu uso, armazenamento e/ou compartilhamento em uma unidade, ou entre unidades diferentes (unidades podem estar localizadas em uma ou mais organizações).

Nesse caso, os especialistas responsáveis por esses ativos precisam não apenas executar operações CRUD (criar, ler, atualizar e excluir) nos ativos gerados, mas também ter meios disponíveis para executar controle de acesso, realização de auditorias, identificação

de versão, autenticidade, não-repúdio, verificação de integridade, confidencialidade e segurança dos ativos digitais gerados.

Figura 4 – Cenário: iteração de unidades especializadas no gerenciamento, armazenamento e/ou compartilhamento de ativos digitais



Fonte: Elaborado pelo autor

No projeto proposto, foram adotadas 3 camadas. A camada do usuário é composta de um ou mais aplicações (sistemas) para permitir que os usuários acessem a camada de gerenciamento, realizem operações com ativos digitais e outras atividades de gerenciamento. As aplicações podem ser desenvolvidas em diferentes linguagens de programação ou não, dependendo do consenso entre os participantes.

Por meio dessa camada, os usuários enviam propostas de transações para chamar serviços (por exemplo, operações CRUD, verificar entradas de log ou compartilhar ativos digitais) fornecidos pela rede *blockchain* que distribui os dados entre os participantes.

A camada de gerenciamento do sistema é onde a rede *blockchain* é implementada, e é composta por entidades conectadas responsáveis pelo estabelecimento seguro e pela execução eficiente do esquema. As informações sobre todas as operações são registradas em um livro de registros distribuído composto por blocos, onde cada bloco compreende um número de transações, *hashs* gerados e informações criptografadas (quando necessário).

No cenário de unidades especializadas, as *blockchains* permis-

sionadas (privadas ou consorciadas) são mais apropriadas devido à necessidade de limitar o acesso a ambientes mais confiáveis e restritos, além de identificar participantes e suas operações.

Juntamente com o uso de contratos inteligentes, livro de registros imutáveis, criptografia, assinatura digital e políticas de controle de acesso, é possível restringir as operações a participantes autorizados, além de permitir realização de auditorias, identificação de versão, autenticidade, verificação de integridade, confidencialidade e segurança dos ativos digitais gerados.

Na camada de gerenciamento do sistema, os contratos inteligentes são usados para fornecer acesso controlado ao livro de registro e permitir que os participantes executem certos aspectos das transações automaticamente. Invocado pelas aplicações, o contrato inteligente realiza as transações e executa vários tipos de consultas e atualiza o estado do livro de registros, anexando cada transação em blocos, e retornando o resultado atualizado à aplicação como resposta.

Enquanto um livro de registros contém fatos sobre o estado atual e histórico (logs de transações) de um conjunto de objetos (ativos digitais), um contrato inteligente define a lógica executável que gera novos fatos que são adicionados ao livro. Tomados em conjunto, esses contratos estabelecem o modelo de negócios que governa todas as interações entre as partes envolvidas na transação. A Fig. 5 ilustra as operações do livro de registros usando contrato inteligente.

Figura 5 – Operações no livro de registros usando contratos inteligentes

Fonte: Elaborado pelo autor

Por fim, a terceira camada compõe a infraestrutura responsável pelo armazenamento dos ativos digitais (armazenamento fora da *blockchain*). Em relação ao armazenamento, podem ser adotadas abordagens distribuídas ou centralizadas (por exemplo, armazenamento em nuvem ou bancos de dados tradicionais), dependendo das necessidades dos participantes.

Assim, operações realizadas pelos usuários em ativos digitais são gerenciadas e registradas na camada de gerenciamento (2ª camada), ativos são armazenados em servidores de armazenamento (3ª camada), e aplicações são utilizadas como interface de acesso para possibilitar a realização das operações pelos usuários (1ª camada).

3.2 Discussões

As características inerentes à tecnologia *blockchain*, bem como a adoção de *blockchains* permitidas e contratos inteligentes na abordagem proposta, proveem os meios para executar o controle de acesso, realização de auditorias, identificação de versionamento, autenticidade, não repúdio, integridade verificação, confidencialidade e segurança dos ativos digitais gerados.

Através da característica de resistência à violação do *blockchain*, a integridade dos dados do usuário é garantida. Todos os blocos e transações válidos registrados no livro de registros são praticamente imutáveis devido à necessidade de validação por outros nós. Com o log imutável de transações, é possível realizar a rastreabilidade de alterações, a auditoria e a identificação de versão sem receios de que a informação foi adulterada.

Como todas as transações são assinadas e registradas com um valor de hash gerado nos blocos, também adotando criptografia para permitir mais segurança e confidencialidade quando necessário, também é possível fornecer verificação de integridade e autenticidade. O uso de canais privados e/ou criptografia aumenta a proteção contra vazamentos de dados.

Com a adoção de uma *blockchain* permissionada (apenas permite a participação de pessoas identificadas e autorizadas) e contratos inteligentes não apenas todas as transações são identificadas e verificadas, mas também permitem que apenas participantes autorizados possam acessar e realizar transações na rede.

Além disso, todo o livro de registros é sincronizado entre os participantes da rede distribuída *blockchain* de acordo com um mecanismo de consenso, dando aos usuários maior confiança na autenticidade e precisão dos dados na rede.

4 CONSIDERAÇÕES FINAIS

Devido à evolução e expansão do crime, bem como à diversidade e volume das práticas criminais existentes (inclusive relacionadas a ataques cibernéticos que podem comprometer informações armazenadas por organizações diversas), são necessárias pesquisas destinadas a ajudar ou fortalecer o desempenho de instituições que se concentram no combate ao crime.

Motivado por esse cenário, e explorando as principais características da tecnologia *blockchain*, este documento apresentou uma visão geral das diferentes tendências de aplicação da tecnologia blockchain e propôs o uso da tecnologia como mecanismo de suporte no gerenciamento, armazenamento e/ou compartilhamento de dados e ativos digitais gerados no contexto de unidades especializadas no combate ao crime.

Devido às características inerentes à tecnologia *blockchain*, bem como à adoção de *blockchains* permitidas, contratos inteligentes e criptografia, uma oportunidade de adoção de uma solução alternativa para fornecer meios para executar o controle de acesso, realização de auditorias, identificação de versão, autenticidade, verificação de integridade, confidencialidade e segurança dos ativos digitais gerados foi apresentada.

Porém cabe acrescentar que, apesar da existência de uma cres-

cente tendência de aplicação da tecnologia *blockchain* no mercado púbico e privado, em muitos países, incluindo no Brasil, há uma carência de legislação sobre o tema, assim como definições de padrões oficiais quanto ao uso da tecnologia, o que pode acarretar em vulnerabilidades diversas ao ser aplicado sem o devido planejamento.

Trabalhos futuros recomendam expandir o escopo deste trabalho através da realização de um estudo de caso voltado a aplicação da proposta deste trabalho em um cenário real de unidades voltadas no combate à criminalidade.

BLOCKCHAIN: MARKET TRENDS AND APPLICATION OPPORTUNITIES FOR THE SECURITY OF DATA AND DIGITAL ASSETS IN CRIME COMBATING UNITS

ABSTRACT

In the context of crime combat, government entities in several countries have established specialized units or sectors to act in different areas and expertise as, for example, in investigation and intelligence activities. However, because they act in a scenario focused on restricted activities or that often involve sensitive information or assets, there is a need for the adoption of alternative solutions focused in management, storage or sharing of digital assets with a concern for information security. As one of the technologies that is gaining more attention in the world market, blockchain has been presenting itself as a viable solution for the public sector and government. Exploring the main characteristics of blockchain technology, this document presents an overview of the different application trends of the technology and proposes the use of blockchain as a support mechanism for management, storage or sharing of digital assets generated in the context of specialized units that operate in crime combat.

Keywords: Blockchain. Crime Combat. Government. Information Security. Public Sector.

REFERÊNCIAS

ALEIXO, Gabriel. Como o bitcoin e os smart contracts estão transformando os modelos de negócios. **E-gov**, Florianópolis, 5 nov. 2017. Disponível em: <http://www.egov.ufsc.br/ portal/conteudo/como-o-bitcoin-e-os-smart-contracts-est%C3%A3o-transformando-osmodelos-de-neg%C3%B3cios>. Acesso em: 05 jul. 2020.

ALKURDI, F.; Elgendi, I.; MUNASINGHE, K.S.; SHARMA, D.; JAMALIPOUR, A. Blockchain in IoT Security: A Survey. **Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)**, Sydney, NSW, Australia. p. 1–4. 21–23 nov. 2018. doi:10.1109/atnac.2018.8615409

ANDRIGHI, Fátima Nancy. **O surgimento da tecnologia blockchain e dos contratos inteligentes (smart contracts)**: funcionamento e desafios jurídicos. YARSHELL, Flávio Luiz; PEREIRA, Guilherme Setoguti J. (coord.). Processo societário. São Paulo: Quartier Latin, 2018. v. 3.

BACK, A., CORALLO, M., DASHJR, L., FRIEDENBACH, M., MAXWELL, G., MILLER, A.. WUILLE, P.. **Enabling blockchain innovations with pegged sidechains**. 2014. Open science re-view. Disponível em: <https://www.blockstream.ca/sidechains.pdf>. Acesso em: 18 jan. 2020.

BATUBARA, F. R.; UBACHT, J.; JANSSEN, M.. Challenges of blockchain technology adoption for e-government. **Proceedings of the 19th Annual International Conference on Digital Government Research Governance** in the Data Age - Dgo'18. 30 May 2018 – 01 Jun 2018. doi:10.1145/3209281.3209317

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. **Diário Oficial da União**, Brasília, 27 de dezembro de 2018. Edição: 248, Seção: 1, Página: 23. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938>. Acesso em: 10 Jan. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGBD). **Diário Oficial da União**, Brasília, 15 de agosto de 2018, Edição: 157, Seção: 1, Página: 59. Disponível em: < http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>. Acesso em: 10 Jan. 2020.

BUTERIN, V.. **Ethereum White Paper**: A next-generation smart contract and decentralized ap-plication platform. Ethereum white paper. 2014. Disponível em: <https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>. Acesso em: 18 jan 2020.

CAC. **Announcement by the Cyberspace Administration of China on the Issuance of the First Batch of Domestic Blockchain Information Service (chines)**. 2019. Office of the Central Cyberspace Affairs Commission. Chine Netcom. Disponível em: <http://www.cac.gov.cn/2019-03/30/ c_1124305122.htm>. Acesso em: 03 jan. 2019.

DREZEWSKI, Rafal; SEPIELAK, Jan; FILIPKOWSKI, Wojciech. The application of social network analysis algorithms in a system supporting money laundering detection. **Information Sciences**, v. 95. p. 18-32. 2015. doi: 10.1016/j.ins.2014.10.015.

ENCCLA. **Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, 2003**. *Disponível em: <http://enccla.camara.leg.br/>. Acesso em: 07 jan 2020.*

EUROPOL. **Crime Areas – Fighting Crime on a Number of Fronts. European Union Agency for Law Enforcement Cooperation**. Disponível em: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas>. Acesso em: 11 jan. 2020.

FBI. **FBI Releases 2018 Crime Statistics. Federal Bureau of Investigation National Press Office**, Department of Justice, United States, September 30, 2019. Disponível em: <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2018-crime-statistics>. Acesso em: 16 jan. 2020.

FBI. **What We Investigate**. Federal Bureau of Investigation Department of

Justice, United States. Disponível em: <https://www.fbi.gov/investigate>. Acesso em: 11 jan. 2020.

FENG, Q.; HE, D.B.; ZEADALLY, S.K.; MUHAMMAD, K.K.. **A survey on privacy protection in blockchain system.** J. Netw. Comput. Appl.. v. 126, pp. 45–58. 2019.

FRANÇA JÚNIOR, F. F.. Atividade de inteligência no Ministério Público. **Revista do MPRN***, v. 1, p. 52. 2011.*

GDPR. **General Data Protection Regulation***. 2018. Disponível em: <https://gdpr-info.eu/>. Acesso em: 10 Jan. 2020*

JAMIL, F.; HANG, L.; KIM, K.; KIM, D.. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. **Electronics**, 8(5), 505. 2019. doi:10.3390/electronics8050505

JUN, M.. Blockchain government - a next form of infrastructure for the twenty-first century. **Journal of Open Innovation: Technology, Market, and Complexity**, 4(1). 2018. doi:10.1186/s40852-018-0086-3

RAUCHS, Michel; BLANDIN, Apolline; BEAR, Keith; MCKEON, Stephen. **2nd Global Enterprise Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance. University of Cambridge Judge Busines School. 2019**. Disponível em: <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-ccaf-second-global-enterprise-blockchain-report.pdf>. Acesso em: 03 jan. 2020.

NAKAMOTO, S. **Bitcoin**: A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 18 jan. 2020.

NAZ, M.; AL-ZAHRANI, F.A.; KHALID, R.; JAVAID, N.; QAMAR, A.M.; AFZAL, M.K.; SHAFIQ, M.. A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. **Sustaina-bility**, v. 11, 7054. 2019.

ØLNES, S.; UBACHT, J.; JANSSEN, M.. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. **Government Information Quarterly**, 34(3), p. 355–364. 2017. doi:10.1016/j.giq.2017.09.007.

PINHEIRO, Alessandro Maia; TIGRE, Paulo Bastos. **Inovação em Serviços e a Economia do Compartilhamento. Administração - Administração Geral. 1.** ed. São Paulo: Editora Saraiva, 2019.

ISBN 978-85-7144-042-5
REFINITIV. **Revealing the true cost of financial crime - 2018 Survey Report**. 2018. Disponível em: <https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/true-cost-of-financial-crime-global-focus.pdf>. Acesso em: 20 jan. 2020.
ROBICHEZ, Gustavo. *et.al*. **Blockchain para Governos e Serviços**. 2019. 24f. Monografia (Especialização em Ciência da Computação). Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, Brasil, 2019.
SWAN, M. **Blockchain**: Blueprint for a New Economy; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
SZABO, N.. **Smart Contracts**. 1994. Disponível em: <http://szabo.best.vwh.net/smart.contracts.html>. Acesso em: 12 jan. 2020.
UNDP. **Investigation Guidelines. United Nations Development Programme. 2019.** Disponível em: <https://www.undp.org/content/dam/undp/library/corporate/Transparency/Investigation_Guidelines_ENG_August_2019.pdf>. Acesso em: 2 jan. 2020.
UNODC. **Criminal Intelligence – Manual for Analysts. United Nations Office on Drugs and Crime**. Vienna, United Nations, 2011. Disponível em: <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf>. Acesso em: 09 jan. 2020.
WARBURG, B.. **How the blockchain will radically transform the economy**. TEDSummit TED Talk. Junho 2016. Disponível em: <https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy?language=en>. Acesso em: 18 jan. 2020.
XIA, Q.; SIFAH, E.; SMAHI, A.; AMOFA, S.; ZHANG, X.. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. **Information**. 2017. 8(2), 44. doi:10.3390/info8020044
XUAN, S.; ZHANG, Y.; TANG, H.; CHUNG, I.; WANG, W.; YANG, W.. **Hierarchically Authorized Transactions for Massive Internet-of-Things Data Sharing Based on Multilayer Blockchain**. Appl. Sci. 2019, 9, 5159.
YANG, J.; ONIK, M.; LEE, N.-Y.; AHMED, M.; KIM, C.S.. (2019). **Proof-of-**

Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. Applied Sciences, 9(7), 1370. doi:10.3390/app9071370

ZHANG, Rui; XUE, Rui; LIU, Ling. **Security and Privacy on Blockchain**. ACM Comput. Surv. 52, 3, art. 51, 2019. 34 p.. doi: https://doi.org/10.1145/3316481.

ZHENG, X.; ZHU, Y.; SI, X.. **A Survey on Challenges and Progresses in Blockchain Tech-nologies**: A Performance and Security Perspective. Appl. Sci. 2019, 9, 4731.

ZHENG, Z.; XIE, S.; DAI, H.; CHEN, X.; WANG, H.. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. **Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)**, Boston, MA, USA, 11–14 dez. 2017; pp. 557–564.

ZHU, Y.; QIN, Y.; ZHOU, Z.; SONG, X.; LIU, G..; CHU, W. C.C.. **Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control**. 2018. 2018 IEEE International Conference on Services Computing (SCC). doi:10.1109/scc.2018.00032