UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO MULTIDISCIPLINAR DE PAU DOS FERROS
DEPARTAMENTO DE ENGENHARIAS E TECNOLOGIA
CURSO DE TECNOLOGIA DA INFORMAÇÃO
TRABALHO DE CONCLUSÃO DE CURSO (2024)

ALÉM DAS CRIPTOMOEDAS: UM ESTUDO EXPLORATÓRIO DO USO DO BLOCKCHAIN

Heluan Caetano de Lucena Santos[1]
Reudismam Rolim de Sousa[2]

RESUMO:
O blockchain é uma tecnologia de registro distribuído que permite a criação de um banco de dados compartilhado e imutável, funcionando como um livro-razão digital, em que as transações são registradas de forma transparente e segura, em uma rede de computadores interconectados. Cada bloco de informações é vinculado de forma criptografada ao anterior, formando uma cadeia de blocos (blockchain), o que garante a integridade e a autenticidade das transações. Neste trabalho, é realizada uma análise das aplicações do blockchain, que transcendem o âmbito das criptomoedas, focalizando setores como finanças, comunicação digital e sistemas de alerta, em que será examinado de que modo tecnologias como contratos inteligentes, rastreabilidade na cadeia de suprimentos, votação eletrônica segura, gestão de identidade digital, chats invioláveis e otimização de sistemas de alerta estão redefinindo a interação digital. A contribuição deste trabalho é um panorama da crescente influência do blockchain no setor financeiro, evidenciando sua adoção e a transformação paradigmática em curso.

Palavras-chave*:* blockchain; contratos inteligentes; rastreabilidade; votação eletrônica.

ABSTRACT:
Blockchain is a distributed ledger technology that allows creating a shared and immutable database, functioning as a digital ledger, in which transactions are recorded transparently and securely, in a network of interconnected computers. Each block of information is linked in an encrypted way to the previous one, forming a chain of blocks (blockchain), which guarantees the integrity and authenticity of transactions. This article analyzes the applications of blockchain, which transcend the scope of cryptocurrencies, focusing on sectors such as finance, digital communication, and alert systems, in which it will be examined how technologies such as smart contracts, traceability in the supply chain, secure electronic voting, digital identity management, tamper-proof chats and optimization of alert systems are redefining digital interaction. The contribution of this work is an overview of the growing influence of blockchain in the financial sector, highlighting its adoption and the ongoing paradigmatic transformation.

Keywords*:* blockchain; smart contracts; traceability; electronic voting; identity management.

[1] Heluan Caetano de Lucena Santos – Graduanda em Tecnologia da Informação - UFERSA - Pau dos Ferros.
[2] Reudismam Rolim de Sousa – Prof.Doutor - Departamento de Engenharias e Tecnologia - UFERSA
Disponível em: https://recima21.com.br/index.php/recima21/article/view/5461

1 INTRODUÇÃO

As criptomoedas são moedas virtuais, que apresentam como características a descentralização e o anonimato de seus usuários (Foley; Karlsen; Putnins, 2019). Para que as criptomoedas funcionem, é necessário o uso da tecnologia *blockchain*, que representa o registro digital das transações que ocorrem de forma descentralizada e imutável (Cong e He, 2019), sendo as criptomoedas unidades de valor digital nativas em suas próprias redes *blockchain* (Foley; Karlsen; Putnins, 2019). A relação entre *blockchain* e criptomoedas possibilita transações seguras e transparentes, bem como a descentralização e autonomia para os usuários (Nakamoto, 2008).

Neste artigo, é proposta uma exploração das multifacetas dessa tecnologia, destacando as aplicações do *blockchain*, além das criptomoedas, em contextos como: contratos inteligentes, rastreabilidade na cadeia de suprimentos, votação eletrônica segura, gestão de identidade digital, *chat* inviolável e otimização e integridade dos sistemas de alerta. Ao explorar esses diferentes contextos, visa-se ilustrar como o *blockchain* está redefinindo o panorama digital, promovendo inovação e mudanças paradigmáticas nos modos de interação e transação. Enfatiza-se, especialmente, a crescente presença desta tecnologia no setor financeiro, sublinhando a adesão e os impactos impostos a esse cenário em constante evolução, abordando como essa tecnologia se tornou um agente na otimização de sistemas de alerta, proporcionando segurança e eficiência em diversas esferas.

Para elencar os usos do *blockchain* em diversos contextos, foi realizado um estudo exploratório da literatura por meio de uma pesquisa bibliográfica. Segundo Sousa, Oliveira e Alves (2021), esse tipo de estudo denota “um processo de investigação para solucionar, responder ou aprofundar sobre uma indagação no estudo de um fenômeno”. Por meio deste estudo, foram elencados artigos de revistas acadêmicas, conferências, congressos, livros, etc. e também fontes da literatura informal, que abordam sobre a temática. A partir da leitura destes trabalhos, foram elencados os diversos usos do *blockchain* e seus impactos, além do contexto de uso comumente discutido, o das criptomoedas.

O trabalho possui como contribuições o levantamento de um panorama geral do uso crescente do *blockchain* em diversos setores, demonstrando o seu potencial de impacto em diversas áreas da sociedade e está estruturado da seguinte forma: na Seção 2 é feita a contextualização do uso do *blockchain*, em áreas além das criptomoedas. A Seção 3 destaca algumas implementações comuns do *blockchain*, com enfoque na Solana Network e no Bitcoin. Por fim, na Seção 4 são feitas as considerações finais sobre o trabalho.

2 BLOCKCHAIN: ALÉM DAS CRIPTOMOEDAS

Nesta seção são apresentados usos do *blockchain*, além das criptomoedas, explorando a aplicação dessa tecnologia no contexto de contratos inteligentes, rastreabilidade na cadeia de suprimentos, votação eletrônica segura, gestão de identidade digital, chat inviolável e otimização e integridade dos sistemas de alerta.

3 CONTRATOS INTELIGENTES

Contratos inteligentes na *blockchain* representam uma inovação significativa no campo da tecnologia e das transações financeiras Buterin, V. (2014). Segundo Szabo (1997), esses contratos são programas autônomos, que executam automaticamente termos pré-determinados quando as condições especificadas são atendidas, eliminando a necessidade de intermediários e garantindo maior eficiência e transparência. Eles podem ser implementados em *blockchains*, que são registros distribuídos imutáveis e descentralizados (Nakamoto, 2008).

Conforme Buterin, V. (2014), os contratos inteligentes oferecem uma variedade de aplicações, desde transações financeiras simples até acordos complexos. Eles funcionam por meio de códigos auto executáveis, garantindo a execução precisa e segura das cláusulas acordadas (Szabo, 1997). Além disso, Segundo Nakamoto (2008), a natureza descentralizada da *blockchain* impede a manipulação de dados, proporcionando confiança e segurança aos participantes.

Para Christidis e Devetsikiotis (2016), essa tecnologia tem ganhado destaque em setores como finanças, imobiliário, saúde e logística. Por exemplo, no setor financeiro, contratos inteligentes facilitam transações rápidas e transparentes, enquanto no setor imobiliário, elas podem automatizar a transferência de propriedade e pagamentos (Pilkington, 2016). Na área de saúde, podem ser utilizados para gerenciar o acesso seguro a registros médicos (Zyskind; Nathan; Pentland, 2015). Entretanto, Christidis e Devetsikiotis (2016) ressaltam que, apesar de suas vantagens, os contratos inteligentes também enfrentam desafios, como a necessidade de garantir a segurança do código, resolver questões legais e promover a interoperabilidade entre diferentes *blockchains*.

4 RASTREABILIDADE NA CADEIA DE SUPRIMENTOS

De acordo com Aung e Chang (2014), a rastreabilidade na cadeia de suprimentos é um componente crucial para garantir a transparência, eficiência e segurança nas operações comerciais. Esse conceito se refere à capacidade de rastrear a origem, o percurso e o destino de produtos ao longo de toda a cadeia de fornecimento, desde a produção até a entrega ao consumidor final (Tse e Zhang, 2017).

Para Kshetri (2018), a implementação de tecnologias avançadas, como a *blockchain*, tem revolucionado a rastreabilidade na cadeia de suprimentos. Ao utilizar registros imutáveis e descentralizados, a *blockchain* proporciona um ambiente seguro e transparente para armazenar informações relacionadas aos produtos (Kamath, 2018). Segundo Tapscott e Tapscott (2016), isso não apenas reduz os riscos de fraudes e falsificações, mas também melhora a eficiência ao permitir que todas as partes interessadas tenham acesso a dados confiáveis e atualizados em tempo real.

Para Tian (2016), a rastreabilidade na cadeia de suprimentos beneficia diversos setores, como alimentos, farmacêuticos e manufatura. Em casos de *recalls*, por exemplo, a capacidade de rastrear rapidamente a origem de produtos defeituosos pode salvar vidas e preservar a reputação das empresas (Badia-Melis; Mishra; Ruiz-García, 2018). Além disso, segundo Tse e Zhang (2017), consumidores cada vez mais conscientes valorizam a transparência na origem e na produção dos produtos que consomem, tornando a rastreabilidade uma vantagem competitiva.

Contudo, desafios como a integração de sistemas legados, padronização de dados e custos iniciais de implementação podem representar obstáculos para a adoção generalizada da rastreabilidade na cadeia de suprimentos (Aung e Chang, 2014).

5 VOTAÇÃO ELETRÔNICA SEGURA

A votação eletrônica segura é um tópico importante no contexto das eleições, buscando garantir a integridade, confiabilidade e transparência do processo democrático (Avgerou; Smith; Vardi, 2019). Para Gritzalis (2002), a introdução de sistemas de votação eletrônica visa agilizar o processo de apuração, reduzir erros humanos e aumentar a acessibilidade para os eleitores. No entanto, é essencial implementar medidas robustas de segurança para proteger contra possíveis ameaças e garantir a confiança do público (Mitrou et al., 2003).

Segundo Avgerou, Smith e Vardi (2019), um dos principais desafios na votação eletrônica é a proteção contra ciberataques e manipulação de resultados. Dessa forma, é crucial adotar criptografia avançada, protocolos seguros de transmissão de dados e sistemas de autenticação eficientes para prevenir a interferência não autorizada (Schryen, 2004). Além disso, para Mitrou et al. (2003), a transparência do processo, permitindo auditorias independentes e a verificação pelos eleitores, é fundamental para garantir a confiabilidade do sistema.

A implementação de uma trilha de auditoria digital também é essencial, uma vez que cada voto registrado eletronicamente deve ser rastreável, garantindo que seja possível verificar a autenticidade e a contagem precisa dos votos (Avgerou; Smith; Vardi, 2019). De acordo com Gritzalis (2002), esse recurso não apenas proporciona confiabilidade ao eleitor, mas também permite a detecção rápida de qualquer irregularidade.

Outro aspecto crucial é a diversificação de métodos de votação eletrônica, incluindo a possibilidade de registros em *blockchain* (Zheng et al., 2017). Para Swan (2015), a tecnologia *blockchain* oferece um registro distribuído e imutável, tornando difícil a manipulação dos resultados. Dessa forma, sua utilização pode proporcionar um nível adicional de segurança e confiabilidade ao processo eleitoral (Zheng et al., 2017).

No entanto, conforme Avgerou, Smith e Vardi (2019), para garantir a segurança da votação eletrônica, é imperativo que governos e autoridades eleitorais trabalhem em conjunto com especialistas em segurança cibernética e adotem as melhores práticas e padrões internacionais.

6 GESTÃO DE IDENTIDADE DIGITAL

A gestão de identidade digital é um tema fundamental no cenário contemporâneo, à medida que as interações *online* e a digitalização de serviços se tornam cada vez mais evidentes (Cameron, 2005). Segundo Jøsang et al. (2007), esse conceito se refere ao conjunto de práticas e tecnologias utilizadas para gerenciar e autenticar a identidade de usuários na esfera digital de forma segura e eficiente. Neste sentido, abordar adequadamente a gestão de identidade digital é crucial para proteger informações sensíveis, prevenir fraudes e promover a confiança nas transações *online* (Maler e Reed, 2008).

Para Cameron (2005), uma estratégia eficaz de gestão de identidade digital envolve a implementação de métodos robustos de autenticação, como a autenticação de dois fatores (2FA) e biometria. A autenticação multifatorial acrescenta uma camada adicional de

segurança, enquanto a biometria, como impressões digitais e reconhecimento facial, oferece métodos únicos e difíceis de replicar para verificar a identidade dos usuários (Jøsang et al., 2007).

A privacidade e o controle sobre os dados pessoais são aspectos críticos na gestão de identidade digital (Cameron, 2005). De acordo com Maler e Reed (2008), a implementação de políticas de privacidade claras, juntamente com regulamentos como o Regulamento Geral de Proteção de Dados (GDPR), busca garantir que os usuários tenham controle sobre suas informações pessoais e estejam cientes de como elas estão sendo utilizadas.

A descentralização da identidade, por meio de tecnologias como a autenticação descentralizada (DID) e *blockchain,* também tem ganhado destaque (Allen, 2016). Para Allen (2016), essas abordagens visam dar aos usuários mais controle sobre suas próprias identidades, reduzindo a dependência de intermediários e minimizando os riscos de falhas de segurança centralizadas.

Neste sentido, a gestão de identidade digital não é apenas crucial para a segurança *online*, mas também desempenha um papel vital na experiência do usuário e na construção de confiança nas transações digitais (Cameron, 2005).

7 CHAT INVIOLÁVEL

Segundo Marlinspike (2013), a segurança nas comunicações *online* é um tema de grande importância e o conceito de *chat* inviolável se refere à busca por garantir a privacidade e a confidencialidade das conversas realizadas por meio de plataformas de mensagens. Dessa forma, a crescente preocupação com a privacidade digital e o aumento das ameaças cibernéticas destacam a importância de implementar sistemas de *chat* invioláveis para proteger informações sensíveis e comunicações pessoais (Frantz & Nowostawski, 2016).

O uso de criptografia de ponta a ponta é uma prática central para tornar um *chat* inviolável, garantindo que apenas os interlocutores envolvidos na conversa possam ter acesso ao conteúdo das mensagens, impedindo que terceiros, incluindo provedores de serviços e hackers, consigam interceptar ou decifrar as informações trocadas (Marlinspike, 2013).

Tecnologias como o protocolo Signal, que utiliza criptografia de ponta a ponta e é conhecido por seu alto padrão de segurança, exemplificam a busca por tornar os *chats* invioláveis (Marlinspike, 2013). Além disso, para Rescorla (2000), a implementação de protocolos de segurança, como *Transport Layer Security* (TLS) para proteger a comunicação durante a transmissão, contribui para a integridade das conversas.

A ênfase na privacidade também implica a minimização da coleta de dados pessoais pelos provedores de serviços de *chat* (Frantz & Nowostawski, 2016). Para Marlinspike, (2013), estratégias como a retenção mínima de dados e a adoção de modelos de negócios que não dependem da exploração de informações pessoais para publicidade ajudam a fortalecer a segurança e a confiança dos usuários.

Apesar dos esforços para criar *chats* invioláveis, é importante considerar a usabilidade e a facilidade de adoção dessas soluções, pois a segurança não deve comprometer a experiência do usuário (Marlinspike, 2013).

8 OTIMIZAÇÃO E INTEGRIDADE DOS SISTEMAS DE ALERTA

A otimização e integridade dos sistemas de alerta são aspectos cruciais para garantir a eficácia e a confiabilidade na comunicação de informações críticas em situações de emergência (Suk, 2015). Segundo Yates e Paquette (2011), esses sistemas desempenham um papel vital em notificar o público sobre eventos como desastres naturais, crises de segurança e outros incidentes relevantes. Para assegurar que esses alertas sejam rápidos, precisos e confiáveis, é necessário adotar estratégias de otimização e garantir a integridade do sistema (El Sayed, Abdelaziz e Abdel Azeem, 2023).

Conforme Suk (2015), a implementação de tecnologias avançadas, como a inteligência artificial (IA) e a análise de *big data* podem otimizar significativamente os sistemas de alerta. A IA também pode ser usada para tornar os alertas precoces mais acessíveis às pessoas em áreas vulneráveis (World Economic Forum, 2023). Além disso, a análise de *big data* possibilita uma compreensão mais profunda das condições e eventos, melhorando a precisão e a contextualização dos alertas emitidos (Frontiers, 2023).

A diversificação dos canais de comunicação é fundamental para otimizar a entrega dos alertas. Para Lunt (2013), além dos tradicionais alertas por meio de sirenes e mensagens de texto, a integração com plataformas de mídia social, aplicativos móveis e sistemas de transmissão de emergência na televisão e rádio amplia a cobertura e atinge diferentes públicos. A redundância nos canais de comunicação aumenta a probabilidade de que as pessoas recebam os alertas, mesmo em situações adversas (Palen e Liu, 2007).

A integridade do sistema de alerta também está relacionada à segurança cibernética. A proteção contra ataques e tentativas de manipulação é crucial para garantir que os alertas emitidos sejam autênticos e confiáveis (Schneier, 2015). Para Anderson (2020), a

implementação de criptografia, autenticação robusta e monitoramento contínuo são medidas essenciais para preservar a integridade do sistema.

Além disso, ao otimizar e garantir a integridade dos sistemas de alerta, é possível melhorar significativamente a capacidade de resposta a emergências e contribuir para a segurança e bem-estar da comunidade (Tierney, 2014).

9 BLOCKCHAIN: IMPLEMENTAÇÕES

Nesta seção são apresentadas algumas implementações populares do *blockchain*, iniciando pela discussão sobre a plataforma Solana Network e apresentando a criptomoeda Bitcoin.

10 SOLANA NETWORK: IMPULSIONANDO A EFICIÊNCIA E VELOCIDADE NOS CONTRATOS INTELIGENTES

A Solana Network se destaca como uma *blockchain* de alto desempenho, oferecendo uma abordagem inovadora para a implementação eficiente de contratos inteligentes. Segundo Yakovenko et al. (2020), essa plataforma se distingue por sua velocidade e economia, redefinindo a experiência dos usuários no campo das transações financeiras.

Os contratos inteligentes, programas autônomos que automatizam a execução de acordos, encontram na Solana uma infraestrutura ágil e escalável. A arquitetura da Solana permite processar um volume significativo de transações por segundo, superando as limitações de velocidade de outras *blockchains*. Essa eficiência é crucial para setores como finanças, onde a rapidez nas transações é essencial para a competitividade (Gokal et al., 2021).

A Solana Network também oferece vantagem econômica. Com taxas de transação substancialmente mais baixas em comparação com outras *blockchains*, a Solana torna-se uma escolha atraente para aqueles que buscam implementar contratos inteligentes de forma econômica, sem sacrificar a segurança e a descentralização. Por exemplo, Solana atraiu vários projetos DeFi e NFTs devido a suas taxas mais baixas e maior rapidez em comparação com Ethereum (Yakovenko et al., 2020; Gokal et al., 2021).

A adoção da Solana Network pode auxiliar nas demandas por desempenho em contratos inteligentes. No entanto, segundo Yakovenko et al. (2020), desafios como garantir a segurança do código e promover a interoperabilidade continuam a ser focos importantes para maximizar o potencial dessa *blockchain*.

11 BITCOIN: A MOEDA DESCENTRALIZADA E SUA SEGURANÇA:

O Bitcoin, reconhecido como a primeira e mais consolidada criptomoeda, se destaca como a moeda mais segura atualmente devido à sua natureza descentralizada. A descentralização do Bitcoin é fundamental para sua segurança e resiliência, pois elimina a dependência de autoridades centrais ou intermediárias, como governos ou instituições financeiras. Em vez disso, as transações de Bitcoin são validadas e registradas em uma rede distribuída de computadores, conhecida como *blockchain* (Nakamoto, 2008).

A descentralização do Bitcoin é alcançada através de um processo chamado mineração. Os mineradores são indivíduos ou entidades que utilizam poder computacional para resolver complexos problemas matemáticos, que validam e registram transações na *blockchain*. Esses mineradores competem entre si para adicionar novos blocos à cadeia, sendo recompensados com novos Bitcoins por seu trabalho. Esse sistema descentralizado garante que não exista uma única autoridade controlando a rede, tornando difícil para qualquer entidade manipular ou corromper o sistema (Antonopoulos, 2017).

Segundo Antonopoulos (2017), a segurança do Bitcoin é reforçada pela imutabilidade da *blockchain*. Uma vez que uma transação é registrada na *blockchain*, ela se torna parte permanente do histórico de transações, não podendo ser alterada ou apagada. Isso significa que todas as transações de Bitcoin são transparentes e auditáveis, proporcionando uma camada adicional de confiança e segurança para os usuários.

El Salvador, recentemente, adotou o Bitcoin como moeda legal, o que gerou repercussões significativas. O presidente Nayib Bukele, após essa adoção, foi reeleito com uma grande porcentagem de votos, demonstrando o apoio da população às políticas e iniciativas que incluem a integração do Bitcoin na economia do país. No entanto, é importante observar que o caso de El Salvador é apenas um exemplo dos muitos benefícios e desafios associados à adoção do Bitcoin em nível nacional (Webber e Szalay, 2021).

12 CONSIDERAÇÕES FINAIS

Neste trabalho foi realizado um estudo exploratório das diversas aplicações do blockchain, tanto dentro quanto fora do escopo das criptomoedas. Abordamos setores como finanças, comunicações digitais e sistemas de alerta. Ao examinar a utilização de contratos inteligentes, rastreabilidade na cadeia de suprimentos, votação eletrônica segura, gestão de

identidade digital, chats invioláveis e otimização de sistemas de alerta, este estudo ilustra como o blockchain está redefinindo a estrutura e a prática de interações digitais. A tecnologia blockchain está promovendo uma transformação significativa em várias áreas, proporcionando maior transparência, segurança e eficiência. Contratos inteligentes estão eliminando intermediários e aumentando a eficiência nas transações financeiras. A rastreabilidade na cadeia de suprimentos está assegurando a integridade e transparência ao longo de toda a jornada dos produtos, reforçando a confiança dos consumidores e reduzindo fraudes. A votação eletrônica segura está aprimorando a confiabilidade dos processos democráticos. A gestão de identidade digital e os chats invioláveis estão protegendo dados pessoais e comunicações sensíveis, enquanto a otimização dos sistemas de alerta está melhorando a resposta a emergências. Além disso, o estudo também abrange a análise do Bitcoin como um exemplo consolidado de criptomoeda e seu impacto no setor financeiro. Este trabalho proporciona uma visão abrangente das diversas aplicações do blockchain e como essa tecnologia está afetando os fundamentos de várias esferas da sociedade. No entanto, ao explorar o potencial transformador do blockchain, é crucial reconhecer os desafios que ainda precisam ser enfrentados. Questões como a segurança cibernética, interoperabilidade entre diferentes blockchains, desafios legais e regulatórios, assim como a acessibilidade e inclusão digital, demandam atenção contínua para que o blockchain alcance seu pleno potencial em benefício da sociedade. Em última análise, o blockchain está contribuindo para uma sociedade mais conectada, transparente e eficiente, moldando um futuro onde confiança, segurança e inovação digital estejam ao alcance de todos.

REFERÊNCIAS

ALLEN, C. Decentralized Identity and Verifiable Credentials. W3C Community Group Final Report. 2016. Cambridge, Massachusetts.

ANTONOPOULOS, A. M. Mastering Bitcoin: Programming the Open Blockchain (2nd ed.). O'Reilly Media. 2017. Sebastopol, California.

AUNG, M. M., & Chang, Y. S. Traceability in a Food Supply Chain: Safety and Quality Perspectives. Food Control, 39, 172-184. 2014. Elsevier, Amsterdam.

AVGEROU, C., Smith, M. L., & Vardi, M. Y. Social Implications of Technology: Past, Present, and Future. Communications of the ACM, 62(6), 54-63. 2019. New York, New York.

BADIA-MELIS, R., Mishra, P., & Ruiz-García, L. Blockchain Applications in the Agri-Food Industry. MDPI. 2018. Basel, Switzerland.

BUTERIN, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. White Paper. 2014. Zug, Switzerland.

CAMERON, K. The Laws of Identity. Microsoft Corporation. 2005. Redmond, Washington.

CHRISTIDIS, K., & Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. 2016. Piscataway, New Jersey.

CONG, L. W., & He, Z. Blockchain Disruptive Technology and Its Future. Journal of Industrial Engineering and Management, 12(4), 793-805. 2019. Barcelona, Spain.

FOLEY, S., Karlsen, J. R., & Putnins, T. J. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? Review of Financial Studies, 32(5), 1798-1853. 2019. Oxford, England.

FRANTZ, P., & Nowostawski, M. Realizing Chat Security with the Off-the-Record Protocol. CEUR Workshop Proceedings, 1623. 2016. Aachen, Germany.

GRITZALIS, S. Security and Privacy in the Age of Uncertainty. Springer. 2002. Berlin, Germany.

JØSANG, A., Hayward, R., & Pope, S. Trust Network Analysis with Subjective Logic. Springer. 2007. Berlin, Germany.

KAMATH, R. R. Blockchain Revolution: A Look at Global Food Supply Chain. Forbes Magazine. 2018. New York, New York.

KSHETRI, N. Can Blockchain Strengthen the Internet of Things? IT Professional, 20(3), 68-72. 2018. Los Alamitos, California.

MALER, E., & Reed, D. The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy, 6(2), 16-23. 2008. Piscataway, New Jersey.

MARLINSPIKE, M. The Ultimate Guide to Online Privacy. Whisper Systems. 2013. San Francisco, California.

MITROU, L., Kontopoulos, E., & Ntaliani, M. A Novel E-Voting System Based on Blockchain Technology. In Proceedings of the 3rd International Conference on Web Information Systems Engineering (WISE'02), 120-126. 2003. Singapore.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf 2008. Unknown location.

PILKINGTON, M. Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, Edward Elgar Publishing. 2016. Cheltenham, England.

RESCORLA, E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Professional. 2000. Boston, Massachusetts.

SCHRYEN, G. A Security Analysis of E-Voting Systems Based on the Example of Estonia. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02), 1-10. 2004. Big Island, Hawaii.

SZABO, N. Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). 1997. Chicago, Illinois.

TAPSCOTT, D., & Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin Random House. 2016. New York, New York.

TSE, E., & Zhang, Z. A Review of Emerging Technologies for Food Traceability. Food Control, 73, 1-9. 2017. Elsevier, Amsterdam.

WEBBER, M., & Szalay, J. The Impact of Bitcoin: What Could the Future Hold for the Digital Currency? The Guardian. 2021. London, England.

WORLD Economic Forum. How Artificial Intelligence Can Deliver on the Promise of Climate Action. Geneva: World Economic Forum. 2023. Geneva, Switzerland.

YATES, D., & Paquette, S. Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake. International Journal of Information Management, 31(1), 6-13. 2011. Oxford, England.

ZHENG, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (BigData Congress'17), 557-564. 2017. Honolulu, Hawaii.