São Paulo, Brazil
October 29-30, 2018

The Tenth International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C201803 or http://dx.doi.org/10.5769/C2018003

Smart Contracts baseados em blockchain na cadeia de custódia digital: uma proposta de arquitetura

Benedito Cristiano Ap.Petroni[1], Rodrigo Franco Gonçalves[2]

(1) Universidade Paulista, Email: cristiano@petroni.com.br
(2) Universidade Paulista, Email: rofranco212@gmail.com

Abstract: O desenvolvimento tecnológico e a evolução de ferramentas computacionais se faz presente e necessária em todas as áreas do conhecimento. Especificamente o trabalho realizado por peritos em áreas que envolvem sistemas e tecnologia da informação, invariavelmente necessitam de coleta de informações – evidências digitais, que formarão a cadeia de custódia para posterior análise e consultas pelos operadores do direito em demandas judiciais. No entanto, métodos forenses tradicionais utilizados por peritos para coleta, armazenamento e verificação podem não ser adequados para evidências digitais, como tempo, tipo e meio de coleta. A proposta deste artigo é um modelo de arquitetura para o desenvolvimento de objetos integrados a smart contracts aplicados numa plataforma blockchain, e com isso permitirá a formação de uma cadeia de custódia digital. Essa cadeia de custódia digital poderá estar disponível pelo tempo que for necessário – característica inerente da tecnologia blockchain, para: análise de peritos na confecção de laudos periciais, consultas futuras pelos operadores do direito como magistrados para verificações de jurisprudência, e de advogados em pesquisas para utilização de provas emprestadas. Além disso, espera-se estimular trabalhos adicionais no campo da perícia forense computacional, em particular na manutenção de uma cadeia de custódia digital nas mais variadas esferas jurídicas.

Key words: Smart Contracts, Blockchain, Cadeia de Custódia.

I. Introdução

As primeiras quatro décadas da internet nos trouxeram o e-mail, a world wide web, as pontocom, as mídias sociais, a internet móvel, o Big Data, a computação em nuvem e os primórdios da Internet das Coisas [2]. Neste cenário, a tecnologia Blockchain surgiu junto com a criptomoeda Bitcoin em meados de 2008 com a publicação do artigo “Bitcoin: A Peer-to-Peer Eletronic Cash System” por Satoshi Nakamoto, tendo porém seu lançamento em código aberto somente em 2009. No artigo publicado por Satoshi Nakamoto foi criado um conceito inovador, que tratava da criação de um sistema monetário digital, distribuído e baseado em blocos criptografados destinados a criptografia das autenticações das transações realizadas, [3]. O Blockchain é um livro-razão seguro, compartilhado e distribuído que facilita o processo de registro e acompanhamento de recursos sem a necessidade de uma autoridade confiável centralizada. É permitido com isso, que duas partes se comuniquem e troquem recursos em uma rede peer-to-peer, na qual as decisões distribuídas são tomadas pela maioria, e não por

uma única autoridade centralizada [5]. Em sua essência, o blockchain é uma tecnologia que grava transações permanentemente de uma maneira que não podem ser apagadas depois, somente podem ser atualizadas sequencialmente, mantendo um rastro de histórico sem fim [4], e cada participante da rede torna-se proprietário do bloco criado, mantendo consigo uma cópia. Desta forma, qualquer intenção em apagar determinado conteúdo torna-se praticamente improvável. Anteriormente, ao surgimento da tecnologia blockchain, questões de confiança e integridade em transações derivava de indivíduos, intermediários ou de outras organizações que atuam de acordo com a direção do senso da justiça, de maneira logica até os dias de hoje monetizam pelo serviço. Os proponentes do blockchain acreditam que a confiança deveria ser livre, e não estar nas mãos de forças centrais que a taxam ou a controlam de uma maneira ou de outra com taxas, direitos, acessos ou permissões [4], com isso, a substituição de selos, carimbos ou assinaturas que, persiste no Brasil desde o período colonial [17], por exemplo, utilizando-se da tecnologia de smart contracts – tecnologia apoiada no blockchain, específicos teria a garantia e a integridade, confiança e segurança do documento no formato de objeto de uma determinada rede, através do blockchain. O aumento da regulamentação, o cibercrime e a fraude estão inibindo a expansão de tecnologias em segmentos industriais e para enfrentar esses desafios, a tecnologia blockchain poderá permitir cadeias de valor mais ágeis, inovações de produtos mais rápidas, relacionamentos mais estreitos com os clientes e integração mais rápida com tecnologias, oferecendo custo de negociação mais baixo com uma plataforma confiável, monitorada e sem a intervenção de terceiros que podem não agregar valor direto. Facilitará com isso o uso de smart contracts na geração de compromissos e acordos com recursos de segurança cibernética robustos e inerentes [15]. Este artigo possui cinco seções. A segunda seção examina a cadeia de custodia, as tecnologias, blockchain e smart contracts que trabalhando em conjunto, podem permitir o armazenamento de evidências digitais. A terceira seção apresenta a proposta de uma arquitetura passo a passo, para construção de um novo sistema de armazenamento de evidências digitais utilizando smart contracts sobre a plataforma blockchain passíveis de acompanhamento por tempo indeterminado, desde a fase de coleta das evidências, validação pelos operadores do direito, a utilização pelo perito e a possibilidade de se utilizar como fonte confiável de provas emprestadas – recurso jurídico submetido ao contraditório que será avaliada pelo magistrado. A quarta seção discute os requisitos tecnológicos necessários e restrições de utilização atualmente. A última seção conclui este Artigo.

2. Preliminares

A. Cadeia de Custódia

A cadeia de custódia nos processos judiciais é utilizada para manter a história cronológica das evidências digitais, sendo de fundamental importância no trabalho do perito judicial para a apuração dos fatos. A evidência digital pode ser um arquivo com ou sem uma extensão, alguns arquivos, uma partição em um disco rígido, o disco rígido inteiro, um dispositivo de memória flash USB, discos CD / DVD / Blue Ray, links de internet, conexões peer to peer, e qualquer outra mídia removível. Os computadores costumam ser usados para fornecer evidências digitais em um caso porque contêm muitas informações. Também podem conter informações sobre dispositivos como cartões de memória USB, telefones celulares, câmeras digitais e discos rígidos portáteis [9]. A cadeia de custódia, considerada adequada, deve incluir informações sobre como as evidências são coletadas, transportadas, analisadas, preservadas e tratadas, [6], sendo que basicamente descreve o 'evidence continuum', fornecendo prova de manuseio adequado e justificando ações executadas em qualquer item de evidência, [8]. A responsabilidade dos peritos envolvidos na manutenção da cadeia de custódia possui várias implicações, como questões éticas e morais pois o destino de possíveis vítimas e réus muitas vezes dependem dos resultados das perícias. Desta forma, a integridade da evidência digital desempenha um papel importante no processo de investigação forense. Uma vez coletadas, as amostras digitais recebidas como evidências, serão analisadas e verificadas e todo o seu

resultado será apresentado no formato de um laudo pericial que será apreciado pelos operadores do direito no processo judicial. Desta forma, o manuseio das evidências digitais devem ser realizadas de forma cautelosa, para evitar futuras alegações de adulteração ou má conduta que possam comprometer decisões futuras. Porém, existe uma dificuldade em considerar artefatos digitais como evidências sendo legalmente relevantes ou admissíveis, uma vez que a falta de recursos forenses, no ambiente da cadeia de custódia ainda permite que usuários mal-intencionados possam alterar, ocultar, ou eventualmente apagar conteúdos [7]. Algumas ferramentas de coleta de informações para que o perito faça a coleta de evidências digitais foram projetadas com foco apenas na melhor maneira de recuperar as informações do destino e de maneira isolada. A atenção dada aos requisitos legais, de integridade e cadeia de custódia, bem como a aceitação jurídica com a recuperação de tais informações, tem sido inadequada e a orientação sobre os assuntos existe apenas em manuais escritos por juristas [8], não existindo com isso, um método que permita armazenar e realmente aferir a integridade, segurança e validade de evidências digitais coletadas. O ideal seria a adoção de um procedimento e/ou mecanismo que comprove de maneira segura o momento em que exista acesso a evidência por pessoas habilitadas, em qualquer estágio da investigação forense. O advento da era da Internet nos traz muita conveniência, porém disputas sobre transações de rede e cibercrimes também estão aumentando, requerendo com isso que evidências digitais legais sejam adequadas, eficazes e persuasivas para fornecer apoio [10] ao perito, bem como manterem-se íntegras. O crime tornou-se um grande negócio, e as Nações Unidas estimam que o crime organizado transacional obtém um lucro e mais de 2 trilhões de dólares por ano. O dinheiro vem de roubo de propriedade intelectual, pornografia infantil, roubo de identidade e claro do cibercrime [1].

B. Blockchain

As aplicações envolvendo blockchain e smart contracts sugere a criação de um livro-razão digital, sendo executado sobre um protocolo para todas as transações, permitindo que todos os participantes na rede editem um ledger – livro-razão, de forma segura, e posteriormente compartilhe e distribua aos demais computadores da grande rede [11]. A base tecnológica das transações na plataforma blockchain podem fornecer um mecanismo importante para transferências além daquelas que envolvem moedas. O processo de validação pela sequencias de blocos, utilizado pelo blockchain ocorre da seguinte maneira: o bloco anterior da transação faz parte da criação do bloco subsequente e o registro e autenticação da transação é replicada por todos os participantes da rede, numa estrutura conhecida como ledger, que dentre outras características, funciona semelhante a um livro de registros, conforme pode ser observado na Figura 1 a seguir

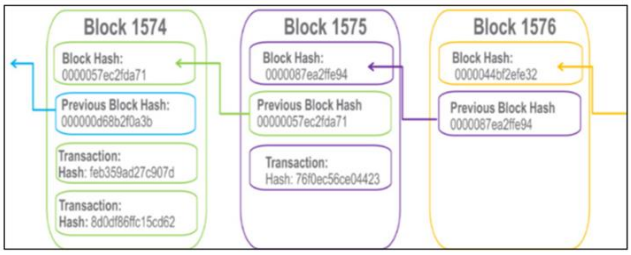

Figure 1. IBM[1] -Blockchain For Dummies, Edição Limit. da IBM, p. 14.

Verifica-se que, cada bloco contém um hash (também conhecido como data zero ou identificador único) com lotes de data e hora de transações recentes e o hash do bloco que vão sendo adicionados ao ledger através das validações dos usuários da rede. Desta forma, a plataforma blockchain está se tornando um protocolo de confiança que busca estabelecer um conjunto de regras – na forma de cálculos distribuídos – que asseguram por exemplo, a integridade e a segurança dos dados trocados entre vários dispositivos sem passar por uma terceira parte confiável. Portanto, um blockchain é

[1] Fonte: WILEY & SONS, J. Inc., Blockchain for dummies, 1ed., River St.– Hoboken NJ: Wiley Brand, 2017.

uma estrutura de dados distribuída que é replicada e compartilhada entre os membros de uma rede. Como resultado de como os nós na rede, por exemplo Bitcoin (os chamados mineradores) anexam transações validadas, mutuamente acordadas, a blockchain do Bitcoin abriga o ledger autoritário de transações que estabelece quem possui o que [12]. A ciência da criptografia é usada em múltiplos lugares para garantir a segurança para uma rede blockchain, e ele repousa sobre três conceitos básicos [4]

- Hashing: impressão digital única que ajuda a verificar que uma informação não foi alterada, sem a necessidade de realmente analisa-la;
- Chaves: usadas em uma combinação mínima de duas uma pública e outra privada;
- Assinaturas digitais: oriundas de algoritmos matemáticos usados para provar a autenticidade de umas mensagem ou documento digital;

C. Smart Contracts

Um smart contract ou contrato inteligente é um programa executado no protocolo blockchain e tem sua execução correta imposta pelo protocolo de consenso [13], e este consenso advém dos demais computadores – podendo ser mais um somente ou vários conectados a rede. Computacionalmente, um smart contract pode codificar qualquer conjunto de regras representadas em uma determinada linguagem de programação sobre um protocolo de transação computacional, no caso o blockchain, e a partir disto executar seus termos contratuais minimizando a necessidade de intermediários, podendo assim diminuir fraudes e arbitrariedades. Em um sentido mais amplo sobre smart contracts baseados em blockchain surge da discussão sobre a propriedade inteligente, que significam transações em cadeia que vão além de simples transações de compra / venda de moeda e podem ter instruções mais extensas incorporadas a elas [14], e dentro de um universo amplo de opções, a possibilidade da utilização de objetos que compõem uma determinada cadeia de custódia possam ter seu contrato inteligente validado por operadores do direito e posteriormente disponibilizados na rede. Um contrato inteligente não pode ser alterado depois que o código é definido, sendo que o código (programa fonte) funciona como um acordo, disponível para qualquer um usar, portanto, sendo possível sua utilização graças às linguagens de programação completas [16]. Com relação aos ativos que podem ser controlados por smart contracts e blockchain, estes podem ser: uma casa, um carro, dinheiro, terrenos ou propriedades intelectuais e moedas. Todos os direitos podem ser rastreados e negociados em uma rede com o blockchain, reduzindo os custos de risco, cortes ou todos os custos operacionais.

3. Arquitetura Proposta

Experimentos envolvendo a aplicação de smart contracts sobre blockchain possuem resultados robustos em algumas aplicações como:

- Automação da função de fornecedor no sistema de energia usando smart contracts baseados em blockchain, [20];
- Soluções com blockchain e smart contracts para Big Data [21];
- Blockchain e smart contracts aplicados a Internet das Coisas [22];
- Modelo de criptografia e privacidade utilizando blockchain e smart contracts [23];
- Controle de transporte de produtos médicos com smart contracts e blockchain [24].

Tecnicamente, pericias digitais tem sido caracterizadas como uma abordagem científica para a identificação, coleta, validação, preservação e subsequente análise de evidências digitais [18], todavia, projetos específicos envolvendo aplicações de smart contracts baseados em blockchain ainda nesta área pode-se afirmar inexistentes. Toda evidência digital gerada, armazenada e coletada deve ser preservada de maneira completa, formando assim uma cadeia de custódia, antes da fase de análise para posterior confecção de um laudo pericial. Conforme apontado por [19], a manutenção de uma cadeia de custódia, deve ocorrer de acordo com 4 princípios:

- Nenhuma ação tomada pelos responsáveis na aplicação da lei, pessoas agentes não devem alterar os dados que posteriormente podem ser invocados no tribunal;
- Em circunstâncias em que uma pessoa ache necessário acessar dados originais, esta deva ser competente para fazê-lo e ser capaz de fornecer evidências que expliquem a relevância e as implicações de suas ações;
- Registros de todos os processos aplicados à evidência digital deve ser criado e preservado. Um terceiro independente deve ser capaz de examinar esses processos e obter o mesmo resultado, sem alterar as informações;
- O perito responsável pela investigação tem a responsabilidade geral de garantir que a lei e esses princípios sejam cumpridos;

Portanto, em análise preliminar, um smart contract baseado em blockchain apresenta um potencial considerável para garantir que as evidências – transformadas em objetos na cadeia de custódia possuam integridade e segurança para além do trabalho do perito, bem como o seu devido armazenamento. Estas evidências quando apresentadas aos operadores do direito serão transformadas em objetos através dos smart contracts para validação e consultas pelo período de tempo necessário ao deslinde da questão jurídica em discussão. Em tempo, talvez o período de armazenamento possa ser considerado eterno. Atualmente, a análise de evidências digitais utilizando aplicações forenses tem sido utilizadas para questões pontuais de soluções caso a caso, sempre realizadas somente pelo perito que, utilizando-se de softwares específicos não deixando a disposição dos demais envolvidos na lide jurídica. Assim, a necessidade de soluções robustas, seguras e que mantenham a integridade poderão ser acessadas pelos operadores do direito como magistrados, advogados e colaboradores da justiça tornou-se inevitavelmente necessária. Desta forma, o desenvolvimento de uma solução que deva ser tecnicamente distribuída, não tendo comprometida a segurança e sua integridade possa atender as deficiências em níveis de habilidades específicas de operação das interfaces de usuários [18] para manipulação durante o tempo do processo. A arquitetura proposta – criação de smart contracts baseados em blockchain para a cadeia de custódia digital deverá considerar e abordar ameaças nos três tipos distintos de análise [18], transformando-os em objetos integrados em smart contracts:

- Mídia: Examinando mídias físicas para evidências digitais;
- Código: Revisão de software para verificação de conteúdo malicioso;
- Rede: analise o tráfego de rede e os registros para identificar e localizar responsáveis;

Como a correta identificação das evidências digitais a serem armazenadas que formarão a cadeia de custódia, o processo inicial deverá ser um roteiro que irá mostrar como as evidências foram coletadas, analisadas e preservadas para serem apresentadas como provas no tribunal [6] e posteriormente auxiliar na geração dos laudos periciais pelos peritos e demais manifestações processuais bem como procura de provas de outros processos – a prova emprestada. A seguir serão demonstradas todas as etapas que irão compor a arquitetura sugerida neste trabalho. Inicialmente, a Figura 2, ilustra o processo em que o perito apresenta a justiça as evidências digitais coletadas, podendo estas serem oriundas de mídias, redes de computadores, dumps de memória e etc.

Figura 2: Etapa de apresentação das evidências digitais pela justiça[2]

Na sequencia, após o perito apresentar as evidências digitais que deverão compor a cadeia de custódia, incluindo documentação sobre como

[2] Fonte: Dos autores.

os dados são coletados, transportados, analisados, preservados e tratados (prestando atenção especial, por exemplo, em evidências internacionais). Esta informação é importante na verificação de dados eletrônicos, uma vez que pode ser facilmente alterada se as devidas precauções não forem tomadas [6]. Os componentes desta cadeia de custódia devidamente aprovados, serão transformados em objetos – integrados através de smart contracts. Os smart contracts podem assumir muitas formas, neste caso, utilizará uma forma simplificada do padrão do modelo Ethereum [25]. A Figura 3 ilustra a criação de um objeto, mídia DVD, como componente de uma cadeia de custódia apresentada pelo perito, pertencente a um referido número de processo.

```
// Mídia referente ao processo hipotético de número 1099939-81.2018.8.26.0554
contract Mídia 01 {
mapping(address => DVD_Proc_1099939-81.2018.8.26.0554) public dvds; // more state definitions
function vote(uint proposal) {

DVD_Proc_1099939-81.2018.8.26.0554 sender = dvds[msg.sender];

if (sender.dvds)

throw;
sender.dvds = true;
sender.DVD_Proc_1099939-81.2018.8.26.0554 = proposal; proposals[proposal].procCount += sender.weight;

}

// more operation definitions
```

Figura 3: Código fonte para a criação do smart contract de mídia contendo evidências digitais[2]

Do código fonte gerado e apresentado na Figura 3 anterior, o próximo passo será a criação efetiva do smart contract, ou seja, a sua preparação para posterior disponibilidade na plataforma blockchain, ilustrado pela Figura 4 a seguir:

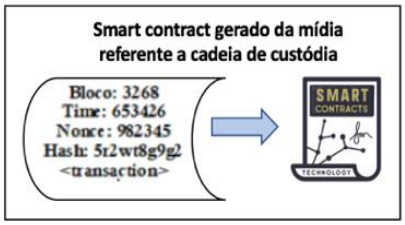

Figura 4: Smart contract criado da mídia contendo evidências digitais[2]

Após a criação do smart contract, caberá aos operadores do direito disponibilizá-lo na plataforma blockchain. Na proposta desta arquitetura, o processo de validação, que já ocorrera conforme ilustrado na Figura 2, convalidará a disponibilização na plataforma blockchain que atenderá aos princípios citados em [19], atenderá os requisitos especificados em [6], [7] e [10]. Com a criação dos smart contracts os operadores do direito poderão disponibilizá-los na plataforma blockchain, conforme ilustrado na Figura 5 a seguir:

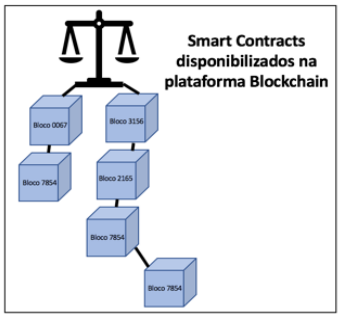

Figura 5: Smart contract disponibilizados na plataforma blockchain contendo evidências digitais[2]

Uma vez disponibilizados pelos operadores do direito, todos os smart contracts contendo os objetos da cadeia de custódia com as evidências digitais, poderão a qualquer tempo e lugar serem consultados. Portanto, em breve síntese e ilustrado pela Figura 6 a seguir, é apresentado todo o fluxo operacional – desde a recepção das evidências digitais pela justiça junto ao perito, o processo de validação, geração de smart contracts e a sua disponibilização na plataforma blockchain.

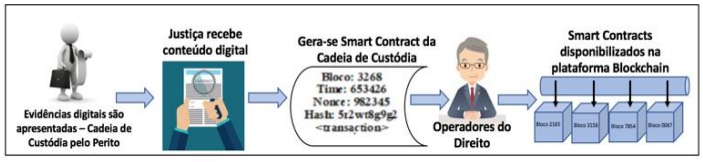

Figura 6: Proposta de arquitetura para disponibilizar a cadeia de custódia[2]

4. Discussão: requisitos e restrições

A disruptiva tecnologia blockchain executando smart contracts de fato, oferece uma gama de oportunidades e ideias para novas implementações e desafios aos atuais e se não antigos modelos de negócios, não diferente para a área do direito. Profissionais da área de tecnologia e escritores de ficção científica há muito tempo imaginavam um mundo onde uma

rede global ininterrupta de sensores conectados a internet poderiam capturar todos os eventos, ações e mudanças na Terra [2]. Desta forma, considerando as tecnologias blockchain e smart contracts com suas capacidades, estas permitirão que várias áreas colaborem, troquem unidades de valor reconfigurando todos seus processos de negócios. A a área do direito pode ter seus processos – atualmente morosos e onerosos como é sabido, sendo executados numa plataforma distribuída, parcimoniosa e que possa, ao mesmo tempo centralizar todas e quaisquer questões processuais (cíveis, criminais e trabalhistas) nas mais variadas esferas (municipais, estaduais e federais) em num ambiente totalmente descentralizado e seguro. A relação entre evidência e confiança, para dados digitais não deve ser adulterada e sempre poderá ser rastreada [26], sendo consideradas juntamente com a segurança, os requisitos necessários em se tratando da formação de uma cadeia de custódia digital. Ao mesmo tempo, deve-se analisar de maneira sistemática que toda a infraestrutura tecnológica, conceitos de capacitação e mão de obra, a própria confiança das instituições – Tribunais e Fóruns, em relação a redes distribuídas, devam ser revistas para que deixem de ser uma restrição mas sim aliados tecnológicos para o bem da sociedade.

V. Conclusão

A arquitetura proposta - criação de smart contracts baseados em blockchain na cadeia de custódia digital, poderá portanto, armazenar quaisquer evidências digitais coletadas por peritos, oriundas de questões judiciais – processos, e terão como elementos primordiais a integridade, a confiança e segurança. Atualmente é necessário a adequação de evidências digitais em todas as suas formas, uma vez que são cada vez mais complexas e pouco compreendidas de maneira geral estando constantemente transformadas em novas formas e funções que devem ser explicadas [18] para todos os interessados diretos e indiretos. Devem ser acessadas independentemente de prazos e conteúdos, assim, poderão tornar-se acessível a todos os envolvidos nas lides processuais – operadores do direito para consultas em casos de jurisprudência como advogados e magistrados bem como a peritos. Com esta tecnologia, também será permitido aos operadores do direito a consulta e utilização na prática sobre o conceito de prova emprestada , onde a prova – resultado de análise de evidências de um determinado fato e produzida em um processo através de documentos, testemunhas, confissão, depoimento pessoal, mas principalmente por exame pericial, poderá ser utilizada em outro processo, sem a necessidade atual de certidões e morosidade na procura.

Referências

[1] Goodman, Marc Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso – São Paulo: HSM Editora, 2015.

[2] Tapscott, Don, Alex T., Blockchain: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. – São Paulo: SENAI-SP Editora, 2016.

[3] Nakamoto, Satoshi, Bitcoin: A peer-to-Peer Electronic Cash, [online] Disponível em : https://bitcoin.org/bitcoin.pdf <Acessado em 07/24/2018>.

[4] Mougayar, William. Blockchain para negócios: promessa prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books, 2017

[5] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," in IEEE Communications Surveys & Tutorials.

[6] J. Ćosić and M. Bača, "(Im)proving chain of custody and digital evidence integrity with time stamp," The 33rd International Convention MIPRO, Opatija, 2010, pp. 1226-1230.

[7] F. Cohen, “Forensic methods for detecting insider turning behaviors,” in 2012 IEEE Symposium on Security and Privacy Workshops, 2012, pp. 150–158.

[8] D. A. Flores and A. Jhumka, "Implementing Chain of Custody Requirements in Database Audit Records for Forensic Purposes," 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, 2017, pp. 675-682.

[9] J. Rajamäki and J. Knuuttila, "Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement," 2013 European Intelligence and Security Informatics Conference, Uppsala, 2013, pp. 198-203.

[10] G. Chen, "Digital evidence evaluation system based on computer system environment analysis," 2014 IEEE International Conference on Progress in Informatics and Computing, Shanghai, 2014, pp. 606-609.

[11] Sachchidanand Singh; Nirmala Singh, Blockchain: Future of financial and cyber security, 2016 - IEEE Conference Publications, 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016 pp: 463 – 467.

[12] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[13] Szabo, N.: 'Smart contracts'. Available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html 1997, <accessado em 24/09/2018>

[14] Swan, Melaine, Blockchain: Blueprint for a new economy. 1.ed. - Eua: O'Reilly Media, Inc., 2015

[15] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels and B. Amaba, "Blockchain technology innovations," 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, 2017, pp. 137-141.

[16] R. Beck, "Beyond Bitcoin: The Rise of Blockchain World," in Computer, vol. 51, no. 2, pp. 54-58, February 2018.

[17] Souza, D.C.P., A burocracia vista do cartório: uma análise antropológica da burocracia estatal, Dissertação (Mestrado) Universidade Federal de São Carlos, 115 f. 2007.

[18] G. Palmer, "A road map for digital forensic research," DFRWS Technical Report, New York 2001, [Accessado em 25/09/2018]. [Online]. Disponível em: http://bit.ly/28YEaXP

[19] Association of Chief Police Officers. (2012) Good Practice Guide for Digital Evidence. [Accessado em 25/09/2018] [Online]. Disponível em: https://goo.gl/UUHFwQ

[20] Thomas, Lee, et al. (2017). Automation of the supplier role in the GB power system using blockchain-based smart contracts. CIRED - Open Access Proceedings Journal. 2017. 2619-2623

[21] Karafiloski E., A. Mishev, "Blockchain solutions for big data challenges: A literature review," IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Ohrid, 2017, pp. 763-768.

[22] Christidis K., M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, IEEE Access, vol. 4, pp. 2292-2303, 2016.

[23] Kosba, A., et al, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858.

[24] Bocek, T., B. B. Rodrigues, T. Strasser, B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, 2017, pp. 772-777.

[25] Ethereum https://github.com/ethereum <accessado em 24/09/2018>

[26] B. Wen, Z. Luo and Y. Wen, "Evidence and Trust: IoT Collaborative Security Mechanism," 2018 Eighth International Conference on Information Science and Technology (ICIST), Cordoba, 2018, pp. 98-9.