

REVISTA TÓPICOS

TECNOLOGIA BLOCKCHAIN: TRANSPARÊNCIA E CREDIBILIDADE NOS PROCESSOS GOVERNAMENTAIS

DOI: 10.5281/zenodo.10720455

Marcelo de Andrade e Silva¹

RESUMO

O presente paper tem como objetivo geral apresentar um estudo sobre a maneira que o Blockchain pode vir a fomentar o nível de credibilidade e confiança nos processos governamentais dando maior transparência em suas ações. Vale salientar que é uma nova tecnologia e que a mesma há uma enorme necessidade de ser melhor difundida empresarialmente e até mesmo para a sociedade civil para entender melhor seus recursos e aplicabilidades e um melhor desenvolvimento relacionado aos seus aspectos legais. A metodologia utilizada para o desenvolvimento desse paper foi uma pesquisa bibliográfica acerca do objeto em estudo, bem como acrescida de conhecimento adquirido nos materiais ofertados pela disciplina de Tecnologia de Blockchain e temos por pretensão expor seus aspectos conceituais, funcionamento, segurança e aplicações buscando facilitar um melhor entendimento por parte do leitor. Por fim demonstraremos como essa tecnologia pode demonstrar a transparência no poder público no que tange as votações, repasses financeiros e licitações e

REVISTA TÓPICOS - ISSN: 2965-6672

REVISTA TÓPICOS

contratos através dos contratos.

Palavras-chave: Tecnologia Blockchain, Governo, Credibilidade, Segurança.

ABSTRACT

This paper has the general objective of presenting a study on how Blockchain can foster the level of credibility and trust in government processes, providing greater transparency in their actions. It is worth mentioning that it is a new technology and that there is a huge need for it to be better disseminated in business and even for civil society to better understand its resources and applicability and a better development related to its legal aspects. The methodology used for the development of this paper was a bibliographical research about the object under study, as well as added knowledge acquired in the materials offered by the Blockchain Technology discipline and we intend to expose its conceptual aspects, operation, security and applications, seeking to facilitate a better understanding by the reader. Finally, we will demonstrate how this technology can demonstrate transparency in public power regarding voting, financial transfers and bids and contracts through contracts.

Keywords: Blockchain Technology, Government, Credibility, Security.

1 Introdução

Desde o período Iluminista, no século XVII, que se vem à tona as discussões acerca sobre os Segredos de Estado, no qual os pensadores sempre questionavam que as informações governamentais não deveriam ficar restritas à elite da sociedade e sim era um direito que o povo também

REVISTA TÓPICOS - ISSN: 2965-6672

REVISTA TÓPICOS

tinha. Com a formação da nova geopolítica diversas Constituições conceberam aos cidadãos o direito à informação, mas muitas delas eram restritas aos resultados dos trabalhos acadêmicos até meados do final do século XX.

Ressaltamos aqui que em 1966 houve um fato importante nos Estados Unidos que foi a assinatura da FOIA – Ato de Liberdade da Informação que estabeleceu a publicação para a sociedade diversas informações restritas ao governo. Essa questão houve uma maior difusão com a vinda da internet e com os softwares livres.

Um outro período marcante foi em 2007 que no Estado da Califórnia – EUA houve um encontro no qual criaram os princípios de dados abertos do governo e que em 2009, no governo de Barack Obama foi assinado o Memorando de Transparência e Governo Aberto que teve como finalidade tornar como patrimônio público a informação do governo federal e que estas deveriam estar disponíveis no portal de dados abertos americanos e, diversos governos seguiram o modelo adotado pelos Estados Unidos e outros criaram suas legislações específicas.

O OGP - Open Government Partnership, foi criado em 2011 no qual tiveram como premissa o comprometimento dos governos em adotarem medidas para abertura das informações governamentais. No Brasil, o Diário Oficial da União (DOU) foi por muito tempo a fonte oficial dos dados desde o período da República e também pelo Governo Militar e que a partir de 2000 alguns mecanismos de fiscalização dos gastos do governo federal foram

REVISTA TÓPICOS

criados como a CGU – Controladoria Geral da União, a Lei de Responsabilidade Fiscal e o Portal da Transparência no ano de 2004

Em 2009 através da Lei Complementar nº 131, foi determinado que as três esferas governamentais disponibilizassem em tempo real e meio eletrônico as suas execuções financeiras e orçamentárias e em 2011 foi aprovada a LAI - Lei de Acesso à Informação (Lei nº 12.527), que regulamenta o direito ao acesso às informações públicas e no final desse mesmo ano o Brasil aderiu a OGP se comprometendo em implantar medidas para melhoria e ampliação da divulgação dos dados governamentais.

Percebemos então que através desses movimentos houve uma crescente em busca de um modelo ideal de transparência na administração pública, orçamentos, pagamentos para acesso de toda a sociedade

Depois desse período começou um crescente interesse pela utilização da tecnologia blockchain ganhando uma atenção maior nos últimos anos que inicialmente era muito mais estudada e entendida pelo meio acadêmico para a utilização do Bitcoin como um novo modelo de moeda que surgia como alternativa ao modelo tradicional das transações financeiras e que atualmente entende-se que essa tecnologia que está por trás do Bitcoin oferece muito mais que a aplicação em moedas criptográficas.

Conforme Barber et al (2012) houve a publicação de um artigo através de uma lista específica de e-mails através de um remetente com nomenclatura de Satoshi Nakamoto no qual despertou um grande interesse mundial entre os programadores no qual descrevia como uma moeda digital funcionava e

REVISTA TÓPICOS

era controlada por um protocolo cuja a validação das operações financeiras eram feitas de maneira distribuída pelos nós de uma rede P2P permitindo que essa moeda circulasse sem a regulação e funcionamento através de uma instituição financeira e nem da necessidade de uma autoridade que valide as operações.

Com a popularização da tecnologia, algumas altcoins (criptomoedas) começaram a surgir e atualmente algumas moedas digitais começaram a ser construídas sobre o blockchain como exemplo temos o Ethereum, uma plataforma de smart contracts, o Follow My Vote, para realização de votações e o BitHealth para acompanhamento de registros de pacientes. Há também ao redor do mundo o Distributed Ledger – livro de registro distribuído que possui uma grande quantidade de aplicações para diversos propósitos construídos com a tecnologia blockchain.

De acordo com Aranha et al (2013) como seria se todos os repasses governamentais fossem realizados por moeda digital com registro no livro razão? Ou se todos os contratos e licitações fossem feitos com o uso da tecnologia blockchain? Se as eleições fossem realizadas através do uso dessa tecnologia substituindo a urna eletrônica?

Entretanto percebemos que há uma infinidade de possibilidades de uso da tecnologia blockchain pela esfera governamental, mas que há a necessidade de existir uma maior maturidade técnica, legal e financeira para explorar todo o potencial que oferece.

2 Conceitos Importantes sobre a Tecnologia Blockchain

REVISTA TÓPICOS - ISSN: 2965-6672

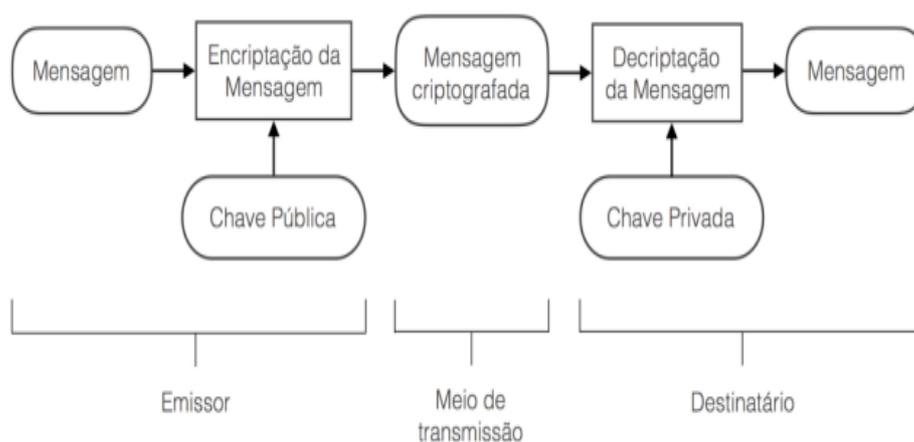
REVISTA TÓPICOS

Visando um melhor entendimento acerca do tema buscamos elucidar nessa seção alguns conceitos relacionados a tecnologia blockchain como a criptografia de chave pública, inserção, difusão e validação dos registros realizados pela tecnologia tendo como referência os bitcoins.

2.1. Criptografia de chave pública

Conhecida também por criptografia assimétrica tem como requisito a utilização de duas chaves nas quais uma é pública para criptografar e outra é privada para decodificar as mensagens conforme modelo abaixo

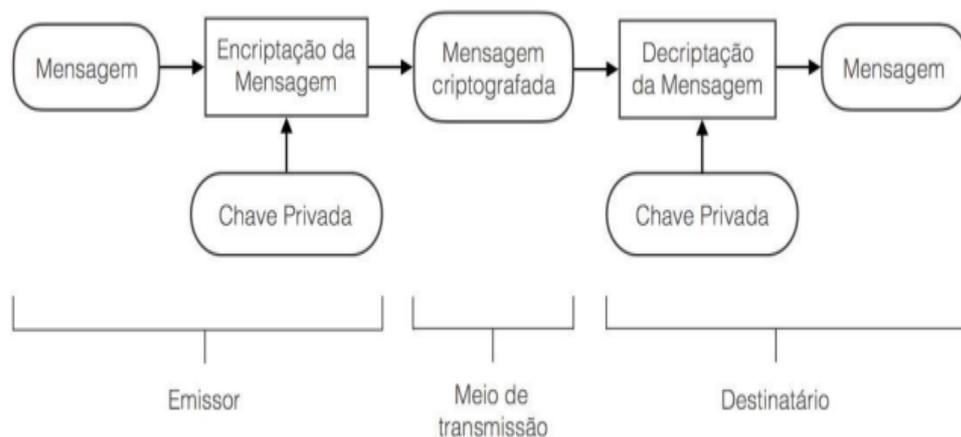
Figura 01 – Criptografia de Chave Pública



Fonte: Salomaa (1996)

Figura 02 – Criptografia de Chave Privada

REVISTA TÓPICOS



Fonte: Salomaa (1996)

No sistema de criptografia assimétrica divulga-se abertamente a chave pública para que todos possam se comunicar com o dono da chave e até mesmo verificar se uma mensagem enviada pelo proprietário é autêntica, já a chave privada é mantida em segredo que por sua vez somente a pessoa que possui acesso a ela poderá decodificar e até mesmo autenticar a mensagem por meio de sua assinatura digital.

De acordo com Impagliazzo (1989) a diferença entre os caminhos de ida e volta da operação que a criptografia está embasada é o que define a segurança do sistema de criptografia assimétrica sendo que quanto maior for a diferença mais eficiente será o algoritmo. Atualmente um dos sistemas considerados mais seguro e eficiente para as aplicações de blockchain é a Criptografia de Curvas Elípticas.

2.2 Função Flash

REVISTA TÓPICOS - ISSN: 2965-6672

REVISTA TÓPICOS

Essa função matemática tem as propriedades de uma eficiência computável, sua entrada pode ser qualquer tamanho e sequência de caractere e a saída possui sequência de tamanho fixo.

Na tecnologia blockchain as utilizações de função flash é a árvore de Merkle – árvores binárias de hash que de acordo com Okupski (2014) essa estrutura admite uma verificação rápida das entradas iniciais da função reduzindo a representação de todas as entradas em um único hash.

2.3 Assinatura Digital

Esta é uma aplicação criptográfica aplicada aos meios digitais os mesmos princípios de uma assinatura convencional com as suas propriedades essenciais como a autenticidade e o endosso. Contudo a finalidade é que esta não possa ser usada de má fé e nem em documentos que não a cabem, contudo, quando nos reportamos a assinatura digital espera-se as mesmas condições e com o uso da criptografia assimétrica pode-se fornecer essas duas características da assinatura convencional. Com o uso do conceito da função hash também pode-se tornar a assinatura digital mais eficiente criptografando e permitindo a sua validação.

Como na essência do blockchain não se há a intenção da confidencialidade se há cadeias de registros públicos, mas a autenticidade é essencial para o funcionamento da tecnologia portanto a criptografia é nela utilizada como assinatura e não como encriptação da mensagem de acordo com Okupski (2014).

REVISTA TÓPICOS

3 Funcionamento do Blockchain

Vamos apresentar como é a forma de funcionamento dos protocolos do blockchain tendo como referência o bitcoin para um melhor entendimento.

Sabemos que o blockchain é uma cadeia de registros imutáveis, públicos e distribuídos.

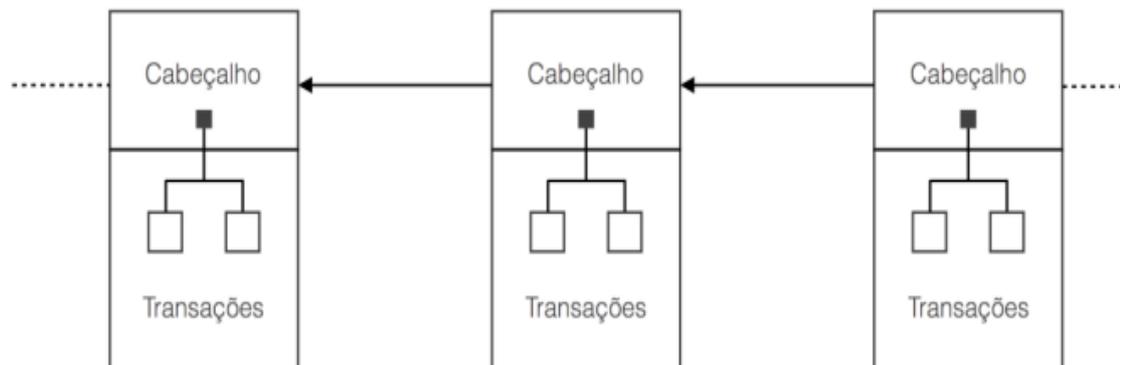
3.1 A cadeia de blocos

Conforme Narayanan (2016) o blockchain está estruturado na forma de blocos encadeados com suas respectivas áreas de transações onde estão as transações de um determinado bloco e uma área de cabeçalho onde há o hash do cabeçalho do bloco anterior e todas as transações presentes na raiz da Árvore de Merkle, sendo assim cada bloco é ligado ao anterior formando uma cadeia de blocos.

De acordo com Okupski (2014) A árvore de Merkle possui a capacidade de permitir a detecção de quaisquer alterações nas transações portanto cada vez que novos cabeçalhos (nós) são inseridos na rede cresce a dificuldade em alterar um registro do blockchain.

Figura 03 – Cadeia de blocos do Blockchain

REVISTA TÓPICOS



Fonte: Okupski (2014)

3.2 Questões de segurança

Walport (2016) define muito bem o conceito de segurança como “coisas que devem acontecer acontecem; e o coisas que não devem acontecer, não acontecem. Com o blockchain não é diferente”. Essa tecnologia vem constantemente sendo pesquisada quanto sua segurança e há uma corrente que ressalta que não se é possível ter um nível satisfatório no que tange essa questão porem outros pesquisadores afirmam que poucas tecnologias possuem a segurança que o blockchain promove.

Quanto aos ataques não há registro de sucesso desde a implementação do primeiro blockchain em 2009 (Eyal e Sirer, 2014). Quanto as Chaves e Aleatoriedade, com a utilização da Assinatura Digital com Curvas Elípticas promove grande eficiência e dificuldade de vulnerabilidade do algoritmo.

No que diz respeito a confidencialidade e anonimato a identificação do usuário de blockchain é realizada por terceiros que aplicam suas regras de

REVISTA TÓPICOS

identificação ao protocolo da tecnologia conforme as regras conhecidas como KYC (Know Your Customer). Porém vale salientar que não são regras do blockchain e sim particulares que promovem um alto nível de transparência e rastreabilidade das transações.

4 Aplicação da Tecnologia na Administração Pública

Na seção anterior apresentamos os pressupostos teóricos referentes à tecnologia blockchain e buscamos explicar como ela funciona. Nessa seção vamos apresentar algumas possíveis aplicações na administração pública visando deixar mais transparente e com maior legitimidade as ações governamentais utilizando o governo federal como base. Segundo Walport (2016) a tecnologia blockchain promove ao governo redução de erros, fraudes, corrupção, entre outros além de potencializar a melhoria de relacionamento entre o cidadão e governo quanto a confiança, transparência e divulgação dos dados, além de que com a utilização dos contratos inteligentes haverá uma melhoria quanto as prestações de conta, eficiência e consonância.

Vamos apresentar duas aplicabilidades que possibilitariam um aumento bem significativo em relação a transparência na administração pública.

4.1 Repasses de verbas em moeda digital

Uma das mais óbvias aplicações do blockchain na esfera pública, mas possivelmente muito difícil seria a implementação do uso de moedas digitais para pagamentos a serem realizados e repasses de verbas, e

REVISTA TÓPICOS

ressalta-se que os benefícios dessa implantação de uma moeda digital é a transparência e a criptografia traz isso à realidade, porém há desafios tecnológicos a serem enfrentados quanto a esses repasses realizados pelo governo.

No que tange aos benefícios em relação a transparência há alguns tipos de repasses como os relativos as empresas prestadoras de serviços, os repasses para as instituições de caridade e ONG's, os repasses para os Estados e Municípios e os repasses para os partidos políticos.

A expectativa que se tinha em relação ao Portal da Transparência era que qualquer pessoa pudesse acessar e verificar os valores mas observamos que a realidade é muito diferente em virtude principalmente das pedaladas e que com a utilização das moedas digitais qualquer cidadão poderia acessar e verificar os valores reais repassados para cada instituição em virtude de não poder desassociar a execução do registro porque o valor que foi registrado no blockchain é o repasse financeiro que foi realizado dando mais lisura do processo para a comunidade.

Walport (2016) afirma que não há somente os benefícios ligados à transparência quanto a utilização das moedas digitais, mas também como a ausência de limites geográficos, a conformidade com a finalidade do repasse, a inclusão de pessoas que não possuem acesso a bancos tradicionais.

Quanto aos aspectos tecnológicos o governo possuirá grandes dificuldades, principalmente econômico e legal, mas há alguns países que já estão com

REVISTA TÓPICOS

essa tecnologia já em desenvolvimento e até mesmo em utilização nos quais devem ser considerados para mitigar o processo de implantação aqui no Brasil.

Outro possibilidade limitante quanto ao blockchain pelas administrações públicas são o Blockchain Não Permissionados que permite que qualquer pessoa possa inserir informações na cadeia dos registros e o Blockchain Permissionado que possuem proprietários e que quando há adição de registro haverá a checagem quanto a integridade do livro-razão por operadores confiados, sejam departamentos governamentais ou instituições financeiras que farão a manutenção da cadeia dos registros e cabe ressaltar que quando existem diferentes departamentos validando esse registro gera um maior nível de confiança quanto ao modelo convencional que estes compartilham informações por papéis.

4.2 Contratos e licitações com tecnologia de contrato inteligente (smart contract)

Outra aplicabilidade do blockchain são os contratos inteligentes que nada mais são que linhas de códigos executados com as transações que são realizadas no blockchain que carregam informações utilizadas pelo script do contrato permitindo a realização de nova transação, emissão de alerta, entre outros e estão relacionados com outra área da tecnologia como a Internet das Coisas (IoT, do inglês Internet of Things).

No que tange a gestão pública há algumas maneiras que os contratos inteligentes poderiam ser utilizados para transmitir maior transparência

REVISTA TÓPICOS

como o controle de percentual de arrecadação a ser designado para uma finalidade específica saindo da gestão humana e sendo gerenciada por linhas de códigos. A certificação de cumprimento de cláusulas de contrato permitiria que o pagamento desses contratos fosse realizado mediante a evolução da construção ou prestação de serviço e resultados através de sensores, balança digital e até mesmo a Radio-Frequency Identification (RFID). Outra maneira seria com o registro eletrônico de ponto dos servidores públicos, tornando público os horários de trabalho dos servidores, deputados, senadores, ministros e os salários pagos mediante o registro das horas laboradas.

Existem outras formas de aplicação de contratos inteligentes no governo com a utilização de plataformas como Ethereum, o Eris, o bitcoin, o Clearmatics entre outros.

5 Considerações Finais

Sabemos que tem muito para ser pensado, entendido e desenvolvido através dessa tecnologia para que seu funcionamento seja proveitoso em diversas áreas da sociedade, porém há a necessidade de que a tecnologia blockchain seja eficiente e segura quanto aos aspectos econômicos, legais e tecnológicos.

Esse paper buscou elucidar a tecnologia blockchain historicamente o seu desenvolvimento, seu funcionamento e suas aplicações na administração pública buscando a credibilidade e transparência das informações prestadas

REVISTA TÓPICOS

pelos governos federal, estadual, municipal e Distrito Federal, mas há a necessidade de cuidados quanto a sua regulação e pesquisa.

Sabemos que todos os problemas quanto a transparência da administração pública não será resolvida com a utilização dessa tecnologia, mas existem diversos benefícios por ser uma ferramenta de grande potencial e que o interesse mundial pela utilização dessa tecnologia na administração pública deverá crescer cada vez mais no que tange ao desenvolvimento de aplicações que buscam realizar essa integração e que existem diversas ferramentas que desenvolvem aplicativos sobre a tecnologia blockchain a exemplo temos a utilização de contratos inteligentes.

REFERÊNCIAS BIBLIOGRÁFICAS

Aranha et al; (2013). Vulnerabilidades no software da urna eletrônica brasileira. Departamento de Ciência da Computação - Universidade de Brasília. Versão 1.0.2. 31 de março de 2013.

Barber et al (2012). Bitter to better - how to make bitcoin a better currency. Palo Alto Research Center, University of California, Berkeley.

Eyal, Ittay; Sirer, Emin G. (2014). Majority is not enough: Bitcoin mining is vulnerable. Department of Computer Science, Cornell University, Nova York, USA.

Impagliazzo, Russell. (1989). One-way functions are essential for complexity based cryptography. Dept. of Math., California Univ., Berkeley, CA, USA.

REVISTA TÓPICOS - ISSN: 2965-6672

REVISTA TÓPICOS

Narayanan et al. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.

Okupski, Krzysztof (2014). Bitcoin developer reference. In: Eindhoven.

Valente, Luiz. (2015). PF toca 9.400 inquéritos sobre desvios de verba pública. Disponível em: <http://www1.folha.uol.com.br/poder/2015/12/1717091-pf-toca-94-mil-inqueritos-sobre-desvios-de-verba-publica.shtml>. Acessado em 26/05/2023

Walport, Mark. (2016). Distributed Ledger Technology: beyond block chain||. A report by the UK Government Chief Scientific Adviser. Information Policy Team, The National Archives, Kew, London.

Salomaa, Arto. (1996). Public Key Cryptography||. 2ª ed. Ed. Springer

¹ Bacharel em Turismo pela UNIFACS – Universidade Salvador, MBA em Gestão Empresarial pela ESTÁCIO. MBA em Gestão de Pessoas pela Universidade Cruzeiro do Sul, MBA em MKT e Vendas pelo Centro Universitário DomBosco e Mestre em Administração pela Must University.

E-mail: marcelodeandradeesilva@gmail.com