Avaliação do uso de *Smart Contracts* para Sistema de Saúde Colaborativa*

Vinícius Branco[1], Bruno Lippert[1], Henry C. Nunes[1], Roben C. Lunardi[1,2], Avelino F. Zorzo[1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre, Brasil.

[2]Instituto Federal de Educação Ciência e Tecnologia do Rio Grande Sul (IFRS)
Porto Alegre, Brasil.

Abstract. *Blockchain emerged as a solution for data integrity, non-repudiation, and availability in different industry sector. Data sensitive scenarios, such as health care, can have benefits from those blockchain properties. Consequently, different researches proposed the adoption of blockchain in health care applications. However, few are discussed about incentive methods to be attractive to new users. Also, few are discussed about performance during code executions in blockchains. In order to tackle these issues, this work presents the preliminary evaluation of TokenHealth, an application for collaborative health with gamification and token-based incentives. The proposed solution is implemented using the Ethereum blockchain with Solidity smart contracts programming language.*

Resumo. *A tecnologia de blockchain surgiu como uma solução para integridade, não-repúdio e disponibilidade de dados para os diferentes setores da indústria. Cenários sensíveis a dados, como a área da saúde, podem se beneficiar dessas propriedades de blockchains. Consequentemente, diferentes pesquisas propuseram a adoção de blockchain em aplicações de saúde. No entanto, pouco é discutido sobre métodos de incentivo para serem atraentes para um novo usuário. Além disso, pouco é discutido sobre o desempenho durante a execução de códigos em blockchains. A fim de abordar essas questões, este trabalho apresenta a avaliação preliminar do TokenHealth, um aplicativo para saúde colaborativa com incentivos baseado em gamificação e tokens. A solução proposta é implementada usando o blockchain Ethereum com linguagem de desenvolvimento de smart contracts Solidity.*

1. Introdução

O conceito de *Blockchain* foi inicialmente introduzido para manter registro das transações da criptomoeda *Bitcoin* [Nakamoto 2008]. Contudo, atualmente, a *Blockchain* passou a ser utilizada na solução de uma série de diferentes problemas, tais como, serviço de DNS [Chang and Svetinovic 2016], armazenamento e execução de trechos de código [Ethereum 2017], controle de

*O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal Nível Superior – Brasil (CAPES) – Código de Financiamento 001, pelo IFRS e pela DB Server. Ainda, o trabalho foi desenvolvido em conjunto com a TokenHealth.

transações [Min et al. 2016], voto eletrônico [Moura and Gomes 2017], controle de direitos autorais [Kishigami et al. 2015]. Muitas destas diferentes aplicações são originadas graças as características de resiliência (devido ao caráter descentralizado da rede), não-repúdio (através do uso de assinatura digitais nas transações) e também pela imutabilidade. Portanto, *blockchain* provê confiabilidade nos dados que por ela são mantidos.

Especialmente no contexto de dados sobre a saúde, alguns estudos sugerem a aplicação de *blockchains* para garantir a integridade e disponibilidade dos dados [Azaria et al. 2016, Mettler 2016, Guo et al. 2018]. Dentre alguns problemas, podem ser citados dados que muitas vezes não são registrados corretamente, que podem estar desatualizados, e até, em muitos casos, não ficam sobre a posse dos pacientes [Azaria et al. 2016]. Ainda, a falta de interoperabilidade de sistemas pode levar a registro duplicados e a realização desnecessária de novos exames médicos [Azaria et al. 2016]. Além disso, a falta de mecanismos de controle de acesso aos dados pode comprometer o negócio de empresas do ramo de saúde [Mettler 2016]. Devido a natureza dos dados, e especialmente após a Lei Geral de Proteção de Dados [BRASIL 2018] ter entrado em vigor no Brasil, a privacidade dos dados dos usuários passa a ter ainda mais impacto no negócio das empresas do setor de saúde [Guo et al. 2018].

Apesar das pesquisas na área de *blockchain* proporem soluções na área da saúde para armazenamento de dados digitalizados [Mertz 2018], controle de acesso aos dados [Rifi et al. 2017], compartilhamento de dados [Xia et al. 2017], pouco se discutiu sobre soluções com métodos de incentivos para usuários. Métodos de incentivo, seja através de bonificação ou de gamificação, vem atraindo muita atenção e sendo adotados em diversos sistemas que utilizam *blockchain* [M. Parizi and Dehghantanha 2018]. Isto ocorre devido a capacidade da execução de código de forma distribuída através do uso de *smart contracts*, também conhecidos como contratos inteligentes [Zyskind et al. 2015].

Portanto, este trabalho tem como objetivo apresentar e avaliar o projeto TokenHealth, um sistema de saúde colaborativo com métodos de incentivo utilizando *blockchain* e *smart contacts*. Desta forma, o sistema possui os aspectos de integridade, resiliência e disponibilidade, além de apresentar métodos de incentivos para a adesão dos usuários. Ainda, tem-se como objetivo a utilização de *smart contracts*, para garantir que as regras de negócio fiquem disponíveis, íntegras e estejam protegidas contra usuários maliciosos. Para avaliar o desempenho em diferentes ambientes, utilizou-se como base tanto a rede de testes (Ropsten) e instância privada da Ethereum [Ethereum 2017], uma das mais populares *blockchains* com suporte a *smart contracts*.

O artigo está organizado da seguinte forma. A Seção 2 apresenta e relaciona alguns trabalhos com a solução apresentada. A Seção 3 apresenta a solução conceitual do sistema, relatando o seu funcionamento, detalhes de como os *smart contracts* são utilizados no projeto, bem como relata as tecnologias utilizadas, principais pontos sobre a implementação e as limitações da solução. A Seção 4 apresenta os resultados preliminares obtidos. Por fim, a Seção 5 apresenta as considerações finais e trabalhos futuros.

2. Referencial Teórico

Com o sucesso da Bitcoin, outras *blockchains* começaram a surgir com propostas diferentes e novas tecnologias. A Ethereum, assim como outras *blockchains* que possuem

uma criptomoeda (como o Bitcoin e o Litecoin) associada, utiliza o *Proof-of-Work* (PoW) como algoritmo de consenso [Tschorsch and Scheuermann 2016]. O algoritmo de consenso é um mecanismo utilizado para garantir que a adição de dados segue uma lógica de negócio pré-combinada. Isso se faz necessário pela *blockchain* funcionar em uma rede descentralizada *peer-to-peer* (p2p) onde os nodos participantes não são confiáveis, podendo agir de forma maliciosa. O algoritmo de consenso garante que os dados gerados por qualquer nodo nesse ambiente não-confiável são dados confiáveis.

A natureza dos dados gerados e da logica de negócio pré-combinado funcionam de acordo com a aplicação da *blockchain*, uma das possibilidades de aplicação são os *smart contracts*. Na *blockchain* esses *smart contracts* possuem modelos diferentes, mas funcionam como programas que podem ser processados pela rede da *blockchain*, dando flexibilidade para uma *blockchain* poder processar qualquer aplicação implementada em *smart contract*. Como são processados na *blockchain*, são decentralizados, o que pode trazer benefícios para aplicações. Outras vantagens são a imutabilidade das informações geradas, transparência do funcionamento e a auditabilidade das computações feitas.

No caso da Ethereum, cada nodo possui uma máquina virtual, chamada de Ethereum Virtual Machine (EVM), que pode processar *bytecodes* representando *smart contracts*. Os usuários podem fazer solicitações especiais para a rede, com chamadas para esses *smart contracts*, permitindo que eles alterem seu estado ou solicitar informações sobre o estado atual dos *smart contracts*. Os nodos vão processar essas solicitações com o *bytecode* do *smart contract* em questão na sua EVM e o estado resultante do *smart contract* será armazenado na *blockchain* [Ethereum 2017].

Em um trabalho realizado por Rouhani *et al.* [Rouhani and Deters 2019], discute-se questões de segurança e desempenho da execução de *smart contracts*. Por exemplo, cita-se diferentes trabalhos que tentam medir o desempenho de *smart contracts*. Por exemplo, são citadas algumas métricas como número de transações por segundo, tempo para a execução de contratos e tempo de atualização de estado do bloco. Para fim de medição, neste trabalho, será adotado o tempo médio para realização de cada contrato.

3. Prova de Conceito: TokenHealth

O sistema TokenHealth[1] é um sistema que visa promover a saúde, através de uma ferramenta colaborativa, com métodos de incetivos (*tokens*) e gamificação (sistema de reputação). Para validar a ideia, optou-se por implementar uma prova de conceito de um fluxo de vacinação. Esta prova de conceito visa cobrir todo ciclo de vacinação, desde a solicitação de vacina, lembrete de reaplicação, aplicação de vacina, e gamificação/incentivos.

Ainda, esta prova de conceito tem como pilares a integridade, disponibilidade, e transparência, funcionalidades estas que podem ser obtidas através da adoção de *blockchain*. Adicionalmente, as regras de negócio utilizam a linguagem *Solidity* para desenvolvimento de *smart contracts*. Desta forma, propôs-se um modelo genérico de funcionamento, onde usuários podem manter atualizados seu registros de vacinas e receber bonificação ao cuidar da saúde. A Figura 1 apresenta uma visão geral do funcionamento e fluxo dos principais componentes do sistema e a interação com os atores envolvidos.

[1]Direitos Autorais e uso do modelo de negócio explícito neste artigo são de propriedade dos seus idealizadores: Diego Pirolla, Reider Arnaud Bernucio e Sérgio Spacov.

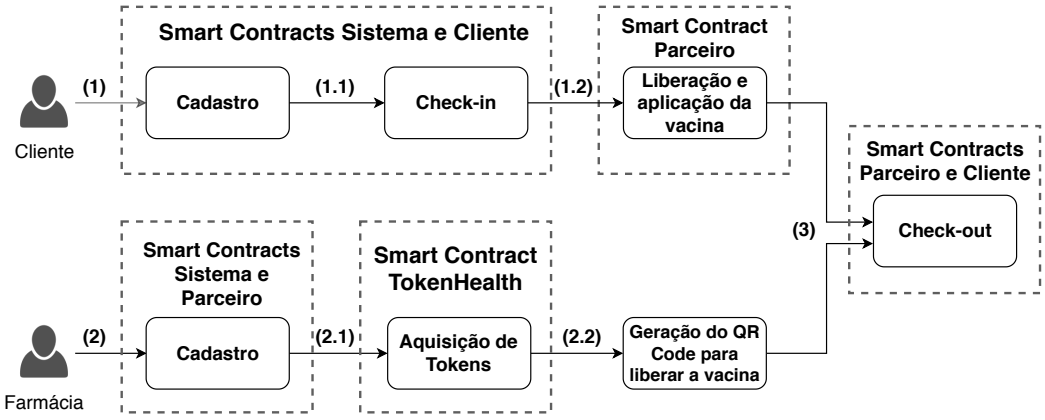

Figura 1. Fluxo do sistema de vacinação

O fluxo do sistema TokenHealth depende de dois atores: *(i)* o cliente que deseja se vacinar ou a um dependente e *(ii)* um local de vacinação (na Figura 1 é utilizada uma farmácia como exemplo de local de vacinação). A proposta deste fluxo é conectar clientes e empresas de vacinação, estimulando que o cliente mantenha sua grade de vacinas atualizada. Além disso, os clientes podem ser bonificados com *tokens*, os quais podem ser utilizados para receber descontos em outras compras, assim, fidelizando o cliente às empresas que utilizam o sistema TokenHealth. Para isto, utilizou-se da tecnologia *blockchain*, mais especificamente da *blockchain* Ethereum, que permite criar transações que persistem dados seguindo regras de negócio, além de permitir enviar *tokens*, uma forma de "criptomoeda", que permite gerar valor de troca.

O fluxo é iniciado com o cadastro, tanto do cliente quanto da empresa, (fluxo 1 e 2, respectivamente na Figura 1). O cliente, utilizando os *smart contracts* "Sistema e Cliente", informa seus dados pessoais, cadastra seus dependentes e as vacinas que já foram recebidas por cada um. Em um outro fluxo, a farmácia, informa nos *smart contracts* "Sistema e Parceiro", seus dados, endereço e registra as vacinas que possui disponíveis. Com os cadastros finalizados, a farmácia pode realizar a aquisição dos *tokens* que serão transferidos aos clientes como bonificação, fluxo 2.1 na Figura 1. O cliente pode, por exemplo, verificar quais vacinas devem ser aplicadas, selecionar um parceiro que disponibilize a vacina desejada e realizar o *check-in* no mesmo, podendo escolher entre pagar o valor integral da vacina e receber *tokens*, ou, usar seus *tokens* para receber um desconto no valor da vacina, fluxo 1.1 na Figura 1.

Após o *check-in* ser realizado, o cliente deve deslocar-se até a farmácia, onde um atendente do estabelecimento poderá visualizar o *check-in* no sistema "Parceiro TokenHealth". Desta forma, sendo possível gerar um QR Code único para o fluxo atual, para que o cliente, no aplicativo TokenHealth, faça a leitura e confirme a liberação da vacina para aplicação, fluxo 2.2 e 1.2 na Figura 1. Assim que a vacina for aplicada, o atendente da farmácia, então poderá confirmar que o cliente recebeu a vacina no sistema "Parceiro TokenHealth"com o processo de *check-out*, fluxo 3 na Figura 1. O processo de *check-out* consiste em ambas as partes terem confirmado a realização completa do fluxo. Caso o cliente tenha optado pelo pagamento do valor integral da vacina, o parceiro realiza a confirmação e é enviado automaticamente os *tokens* para o cliente, realizando o processo de bonificação. Por outro lado, caso tenha optado por usar seus *tokens* como forma de

pagamento e receber um desconto no valor do produto, após a confirmação do parceiro, o cliente deverá, novamente, fazer a leitura de um QR Code para realização do *check-out* e o envio de *tokens* do cliente para o parceiro seja gerada automaticamente, efetuando o pagamento da vacina.

3.1. Implementação

Para desenvolvimento da solução foi escolhido um conjunto de tecnologias que pode ser dividido em dois grupos: (*i*) tecnologias utilizadas para o desenvolvimento da aplicação, como linguagens de programação, bibliotecas e *Application Programming Interface* APIs; e (*ii*) tecnologias utilizadas como infraestrutura.

Para o desenvolvimento da interface *web* da empresa, utilizou-se JavaScript. Esta linguagem foi escolhida por estar consolidada nesse ambiente e por possuir integração com as bibliotecas escolhidas, já, para o aplicativo do cliente, utilizou-se o *framework Flutter*, pois este gera aplicativos tanto para *Android* quanto para *iOS* com o mesmo código fonte. Adicionalmente, a linguagem Solidity foi escolhida para o desenvolvimento de *smart contracts*, linguagem esta utilizada por padrão pela *blockchain* Ethereum. Ainda, utilizou-se as bibliotecas *React.js*, para criação da interface *web* e *Web3.js* para conexão com a *blockchain*.

4. Avaliação Preliminar

Para avaliar a solução, utilizou-se a *Ropsten Test Net*, uma *blockchain* de teste da Ethereum que permite testar com facilidade os *smart contracts*, simulando a rede principal da Ethereum. Uma das principais vantagens está no fato de não ser necessário o uso da criptomoeda Ether da *blockchain* principal da Ethereum para realizar transações. Na *Ropsten* são utilizadas criptomoedas ”falsas”para viabilizar o teste de aplicações, e não é preciso manter uma infraestrutura para manter a *blockchain*, pois é mantida pelos próprios mineiros da rede. Ainda, realizou-se experimentos com uma instância privada da Ethereum.

A Tabela 1 apresenta as diferenças entre as redes da Ethereum para utilização em uma *Dapp*. Como pode ser observado na tabela, apenas na rede privada da Ethereum é possível regular a dificuldade inicial de mineração. Desta forma, pode-se adequar a dificuldade do algoritmo de PoW para produzir novos blocos em menor tempo. Ainda, tanto na instância privada da Ethereum, quanto na rede de teste da Ropsten, é possível gerar e executar *smart contracts* sem a necessidade de compra ou mineração de Ethers, diferentemente da rede principal. Todavia, para o desenvolvimento de um *Dapp*, somente na rede privada possui custo de infraestrutura para manter a *blockchain* para que sejam garantidos os requisitos de resiliência e consenso da solução.

	Ethereum (Principal)	**Ropsten (rede de testes)**	**Instância Privada**
Tempo de Mineração	>5 minutos	<1 minuto	<1 minuto
Dificuldade de Mineração	Alta	Média	Inicial Regulável
Custo Financeiro	Sim (Ethers)	Não	Sim (Infraestrutura)

Tabela 1. Diferenças das *blockchains* Ethereum para *Dapps*

Para avaliar os custos de manutenção do sistema, são apresentados os principais custos do sistema. Primeiramente, analisando a rede pública da Ethereum, analisou-se o custo em *gas* (taxa para execução de contratos). O maior custo, como apresentado na Tabela 2, é o somatório do custo para a criação do Cadastro do Usuário, correspondendo a um total de 0,002523 Ethers (ou 0,52983 dólares, usando a cotação média de 210 dólares por Ether, do dia 29/07/2019 [Coin Market Cap 2019]). Apesar desta função ser a que possui maior custo, ela deve ocorrer apenas 1 vez por usuário. O custo total para execução completa do ciclo de vacina (*check-in*, liberação e *check-out*) ficou em 0,00154 Ether (ou aproximadamente 0,3234 dólares).

Como contraponto, para execução em instância privada da Ethereum, pode-se utilizar serviços em nuvem com custos pré-definidos para a infraestrutura. Por exemplo, ao alocar 5 máquinas específicas para rodar nós Ethereum no Google Cloud Platform [Google Inc. 2019], o custo fixo mensal ficaria por volta dos 123,75 dólares (5 instâncias de 24,75 dólares). Vale destacar, que neste cálculo estão sendo considerados apenas os custos básicos da locação de máquinas virtuais e não estão sendo considerados os custos de manutenção e configuração do sistema.

	Ethereum (Principal)	**Instância Privada**
Custo por Cadastro	0,002523 Ethers(∼US$0,52983)	-
Custo por Ciclo	0,00154 Ethers (∼US$0,3234)	-
Custo Mensal	-	US$123,75

Tabela 2. Custos para Execução dos Smart Contracts

Para a avaliação preliminar do desempenho dos *smart contracs* da solução, utilizou-se da rede testes Ropsten e de uma instância privada no Google Cloud [Google Inc. 2019] com 2 núcleos de processamento, 8GB de memória e 80GB de armazenamento. Os testes foram repetidos 10 vezes, sendo apresentados os resultados da mediana das execuções. Tanto na instância privada, quanto na rede de testes Ropsten, obtiveram-se bons resultados quanto ao desempenho, como pode ser observado na Figura 2.

Se considerarmos a execução do Smart Contract para criação de conta do usuário, contrato com maior tamanho do *bytecode*, a execução teve desempenho similares, sendo executado em aproximadamente 18,1s segundos (mediana) na instância privada e 20,4s na Ropsten. Porém, o tempo de execução do Smart Contract para realizar checkin na rede da Ropsten é gerado em um tempo consideravelmente mais elevado (24,5s) do que na instância privada (9,6s). Todavia, não foi possível realizar comparação com a rede pública da Ethereum devido aos custos associados a compra de Ether.

5. Considerações Finais e Trabalhos Futuros

O cuidado com a saúde é sempre um tópico recorrente na sociedade, a cada dia surgem diversos avanços, técnicas novas e medicamentos, sendo assim é necessário criar meios de incentivar o cidadão a utilizá-los. Desta forma, neste artigo foi apresentada uma solução para sistemas de economia colaborativa para a saúde utilizando *blockchain*, exemplificando a usabilidade desta tecnologia com o objetivo de melhorar a saúde e prevenção de doenças através da gamificação e fidelização.

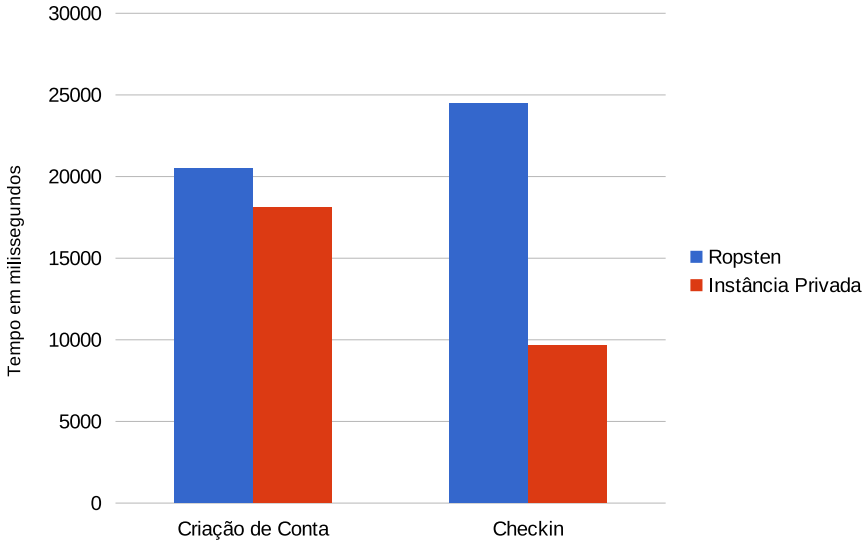

Figura 2. Desempenho para execução de Smart Contracts

Além disso, foram apresentados os *trade-offs* da utilização de *blockchain* em instâncias privadas ou em redes públicas de *blockchain*. Como demonstrado, os custos na rede pública da Ethereum são elevados quando o número de transações for alto. Porém, quando é escolhido utilizar instância privada, o custo de infraestrutura e pessoal devem ser levados em conta. Ainda, observou-se que o desempenho na rede de testes se aproximou com os valores obtidos na instância privada, porém não foram obtidos resultados com a rede pública da Ethereum.

Por fim, conclui-se que utilizar *blockchain* é uma alternativa para sistema de economia colaborativa para a saúde, pois torna o sistema seguro por prover a imutabilidade dos dados, garantia de que uma lógica de negócio deve ser seguida e possibilidade de gamificação ao concluir uma ação de saúde preventiva.

Pretende-se, como trabalhos futuros, expandir o sistema para abranger, além de vacinas, medicamentos, consultas médicas e outras práticas que levam a manutenção da saúde preventiva. Ainda, pretende-se ampliar os testes na rede pública da Ethereum.

Referências

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.

BRASIL (2018). Lei geral de proteção de dados (lgpd). Disponível em: ≪http://www.planalto.gov.br/ccivil03/Ato2015-2018/2018/Mpv/mpv869.htm≫. Acesso em 20 Jul. 2019.

Chang, T. H. and Svetinovic, D. (2016). Data analysis of digital currency networks: Namecoin case study. In *2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS)*, pages 122–125.

Coin Market Cap (2019). Cryptocurrencies by market capitalization. Disponível em: ≪https://coinmarketcap.com/≫. Acesso em 24 Jul. 2019.

Ethereum (2017). A Next-Generation Smart Contract and Decentralized Application Platform. Disponível em: https://github.com/ethereum/wiki/wiki/White-Paper. Acessado em: 20-07-2019.

Google Inc. (2019). Google cloud platform. Disponível em: ≪https://cloud.google.com/≫. Acesso em 24 Jul. 2019.

Guo, R., Shi, H., Zhao, Q., and Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*, 6:11676–11686.

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., and Akutsu, A. (2015). The blockchain-based digital content distribution system. In *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, pages 187–190.

M. Parizi, R. and Dehghantanha, A. (2018). On the understanding of gamification in blockchain systems. In *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 214–219.

Mertz, L. (2018). (block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE Pulse*, 9(3):4–7.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3.

Min, X., Li, Q., Liu, L., and Cui, L. (2016). A permissioned blockchain framework for supporting instant transaction and dynamic block size. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 90–96.

Moura, T. and Gomes, A. (2017). Blockchain voting and its effects on election transparency and voter confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, dg.o '17, pages 574–575, New York, NY, USA. ACM.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Disponível em: https://bitcoin.org/bitcoin.pdf. Acessado em: 20-06-2019*.

Rifi, N., Rachkidi, E., Agoulmine, N., and Taher, N. C. (2017). Towards using blockchain technology for ehealth data access management. In *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, pages 1–4.

Rouhani, S. and Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, 7:50759–50779.

Tschorsch, F. and Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., and Guizani, M. (2017). Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767.

Zyskind, G., Nathan, O., and Pentland, A. . (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184.