Blockchain

Jonath Wesley Herdt
jonathherdt@edu.univali.br
Universidade do Vale do Itajaí
Itajaí, SC, Brasil

Figure 1: Conceito de Blockchain

ABSTRACT

Blockchains são contadores digitais à prova de violação e à prova de violação implementados de forma distribuída (ou seja, sem um repositório central) e geralmente sem uma autoridade central (ou seja, um banco, empresa ou governo). Em seu nível básico, eles permitem que uma comunidade de usuários registre transações em um livro razão compartilhado dentro dessa comunidade, de forma que, sob a operação normal da rede blockchain, nenhuma transação possa ser alterada depois de publicada. Este documento fornece uma visão geral técnica de alto nível da tecnologia blockchain, com alguns casos de uso, mais detalhadamente sobre contratos inteligentes.

KEYWORDS

blockchain, contratos inteligentes

ACM Reference Format:
Jonath Wesley Herdt. 2018. Blockchain. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUÇÃO

Blockchains são registros digitais a prova de alteração e violação, implementados de uma maneira distribuída e geralmente sem uma autoridade central. Em seu nível mais básico, blockchains permitem uma comunidade de usuários gravar transações em registros compartilhados dentro daquela comunidade, de modo que, sob operação normal do rede blockchain nenhuma transação pode ser alterada uma vez publicada. Em 2008, a ideia do blockchain foi combinado com várias outras tecnologias e conceitos de computação para criar criptomoedas: dinheiro eletrônico protegido por mecanismos criptográficos em vez de um repositório central ou autoridade. [9]

Essa tecnologia se tornou amplamente conhecida em 2009 com o lançamento da rede Bitcoin, a primeira de muitas criptomoedas modernas. Com Bitcoin e sistemas semelhantes, a transferência de informações digitais que representam dinheiro eletrônico ocorrem em um sistema distribuído. Os usuários do Bitcoin podem assinar digitalmente e transferir seus direitos a essas informações para outro usuário e o blockchain do Bitcoin registra essa transferência publicamente, permitindo que todos os participantes da rede verifiquem independentemente a validade das transações. O blockchain Bitcoin é mantido e gerenciado de forma independente por um grupo distribuído de participantes. Isso, junto com os mecanismos criptográficos, torna o blockchain resiliente a tentativas de alterar o registros posteriormente (modificando blocos ou forjando transações). A tecnologia Blockchain permitiu o desenvolvimento de muitos sistemas de criptomoeda, como Bitcoin e Ethereum. Por causa disso, a tecnologia blockchain é frequentemente vista como vinculada ao Bitcoin ou possivelmente às soluções de criptomoeda em geral. No entanto, a tecnologia está disponível para uma ampla variedade de aplicações e está sendo investigada para uma variedade de setores. [9]

2 CARACTERÍSTICAS

A confiança necessária em uma rede de blockchain é possibilitada por quatro características-chave da tecnologia de blockchain, descritas abaixo:

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

- Registros: A tecnologia utiliza de um registro apenas de anexo para fornecer histórico transacional completo. Ao contrário dos bancos de dados tradicionais, as transações e os valores em um blockchain não são substituídos.
- Segurança: Blockchains são criptograficamente seguros, garantindo que os dados contidos nos registros não tenham sido adulterados e que sejam atestáveis.
- Compartilhamento: Os registros são compartilhados entre vários participantes. Isso fornece transparência entre os participantes do nó na rede blockchain.
- Distrubuição: Blockchains podem ser distribuídos. Isso permite dimensionar o número de nós de uma rede blockchain para torná-la mais resistente a ataques de malfeitores. Ao aumentar o número de nós, a capacidade de um mau ator impactar o protocolo de consenso usado pelo blockchain é reduzida.

Para redes blockchain que permitem que qualquer pessoa crie contas anonimamente e participe (chamadas de redes blockchain sem permissão), esses recursos oferecem um nível de confiança entre as partes sem nenhum conhecimento prévio uma da outra; essa confiança pode permitir que indivíduos e organizações façam transações diretamente, o que pode resultar em transações sendo entregues mais rapidamente e com custos mais baixos. Para uma rede blockchain que controla mais rigidamente o acesso (chamadas de redes blockchain permitidas), onde alguma confiança pode estar presente entre os usuários, esses recursos ajudam a reforçar essa confiança. [9]

3 EXEMPLOS DE UTILIZAÇÃO

Embora a ideia funcione extremamente bem para Bitcoin e outras criptomoedas, existem muitas outras aplicações úteis da tecnologia blockchain. [6]

O uso de contratos inteligentes em um blockchain pode fornecer maior transparência para clientes e provedores de seguros. Registrar todas as reivindicações em um blockchain evitaria que os clientes fizessem reivindicações duplicadas para o mesmo evento. Além disso, o uso de contratos inteligentes pode acelerar o processo de recebimento de pagamentos pelos reclamantes.

As transações imobiliárias exigem uma tonelada de papelada para verificar as informações financeiras e a propriedade e, em seguida, transferir as escrituras e títulos para novos proprietários. O uso da tecnologia blockchain para registrar transações imobiliárias pode fornecer um meio mais seguro e acessível de verificação e transferência de propriedade. Isso pode acelerar as transações, reduzir a papelada e economizar dinheiro.

Se as informações de identidade pessoal são mantidas em um blockchain, o uso da tecnologia pode garantir que ninguém vote duas vezes, apenas os eleitores qualificados podem votar e os votos não podem ser adulterados. Além do mais, pode aumentar o acesso à votação, tornando-o tão simples quanto pressionar alguns botões em seu smartphone. Ao mesmo tempo, o custo de conduzir uma eleição diminuiria substancialmente.

4 BLOCKCHAIN E CONTRATOS INTELIGENTES

[8] introduziu o conceito de "Contratos inteligentes", que combinam protocolos de computador com interfaces de usuário para executar os termos de um contrato. Devido ao blockchain, os contratos inteligentes estão se tornando mais populares, pois podem ser utilizados mais facilmente aplicando blockchains em comparação com a tecnologia disponível na época de sua invenção, 20 anos atrás.

Esta abordagem inovadora pode, por exemplo, substituir advogados e bancos que estiveram envolvidos em contratos para transações de ativos, dependendo de aspectos predefinidos [3]. Os contratos inteligentes também podem ser usados para controlar a posse de propriedades. Essas propriedades podem ser tangíveis (por exemplo, casas, automóveis) ou intangíveis (por exemplo, ações, direitos de acesso). Um exemplo proeminente para a tecnologia blockchain que trata os contratos inteligentes como cidadãos de primeira classe é Ethereum, que é um sistema descentralizado originalmente proposto por [2]. Uma taxonomia de sistemas de consenso descentralizados e uma visão geral dos diferentes tipos de sistemas é fornecida por [5]. Ethereum pode ser visto como uma extensão do blockchain Bitcoin para suportar um escopo mais amplo de aplicações. Assim, a tecnologia blockchain permite estabelecer contratos usando criptografia e substituir terceiros (por exemplo, um notário) que foram necessários para estabelecer a confiança no passado. O Blockchain pode interromper todo o processo de transação ao executar contratos automaticamente de maneira econômica, transparente e segura [3]. Os componentes arquitetônicos da tecnologia blockchain, sua interação, bem como um framework para análise de implicação de sistemas blockchain para ecossistemas digitais é proposto por [4].

O setor financeiro está até se perguntando se grande parte de seus negócios atuais pode ser substituída pelo blockchain. Isso pode ser ilustrado pelo processo de pagamento. Se as pessoas pagarem as mercadorias com cartão de crédito hoje, a liquidação ocorre após um atraso de vários dias. Utilizando o blockchain, essa liquidação atrasada se tornaria redundante, pois o pagamento pode ser feito em tempo real adicionando nos registros. [7]

5 DAUTIN

A Dautin é uma empresa que surgiu com foco na inovação e na tecnologia, tendo como objetivo, ser uma alternativa ao processo de autenticações e registros de documentos de forma digital, através das criações de provas de autenticidade e dos “smart contracts”, conhecidos como contratos inteligentes, contemplando para o seu cliente um cenário totalmente desburocratizado, descentralizado e com um custo inferior aos métodos convencionais. A Dautin tem grandes diferenciais e funcionalidades:

- Compartilhamento de arquivos entre usuários, modo público ou privado;
- Possibilidade de armazenamento;
- Conta exclusiva para sua empresa;
- Cadastro dos seus clientes na conta empresarial;
- Opções de planos e pacotes;
- Aplicativo sincronizado com suas informações;
- Equipe de suporte exclusivo;
- Valores acessíveis;

- Comodidade e segurança;

A Dautin oferece serviços de Autenticação (geração de prova de autenticidade) de documentos, registros de contratos (vários signatários) e de criação de identidade blockchain, utilizando como tecnologia para isso a rede blockchain.

6 NECESSIDADE DO USO DE BLOCKCHAIN

Um dos principais benefícios proporcionados pelos contratos inteligentes é a redução de custos relacionados à transação comercial e a redução de tempo, trazendo mais segurança e eficiência aos processos. Isso acontece porque esse formato de negócio não requer a atuação de intermediários para a formalização de acordos efetuados via internet, contrariamente ao que ocorre nas compras feitas por meio de websites que cobram taxas e, consequentemente, encarecem os valores do serviço ou produto.

Outra vantagem da implantação desse recurso tecnológico é a otimização do processo de gestão de contratos. Como o fluxo contratual passa a ser completamente gerido por um software, todos os trâmites burocráticos que normalmente fazem parte desse tipo de transação são eliminados. Além disso, eventuais erros humanos que poderiam ser cometidos por colaboradores são extintos.

O alto nível de proteção de informações que confere confiabilidade ao processo de contratação é mais um importante diferencial propiciado pela utilização dos smart contracts. A segurança de dados que caracteriza esse tipo de operação comercial maximiza o sigilo das transações efetuadas, garante a integridade informacional, e evita a possibilidade de surgimento de fraudes.

De todo modo, apesar de o conceito de contrato inteligente ter nascido juntamente com a blockchain, e algumas de suas características, como a imutabilidade, serem dependentes da blockchain. Ainda é possível idealizar algo parecido com um contrato inteligente, utilizando um banco de dados governado por um terceiro confiável, com componentes de auto execução.

7 CONCLUSÃO

Os campos de aplicação para blockchains parecem ser múltiplos, especialmente em áreas que historicamente dependeram de terceiros para estabelecer um certo grau de confiança. [1] suggests that politics and the entire society might be restructured by the blockchain. Many functions might become obsolete if people started to organize and protect the society using decentralized platforms.

Enquanto os cientistas da computação se concentram principalmente nos desafios técnicos e criptográficos desta área, os pesquisadores da área de Engenharia de Sistemas de Informação e Negócios têm a oportunidade de focar no design de mercado, nas questões de confiança e privacidade, e na respectiva não adoção da nova tecnologia. . Além disso, essa inovação disruptiva pode mudar muitos modelos de negócios existentes, criar novos e pode ter impactos severos em setores inteiros. Portanto, a pesquisa na interseção de tecnologia, mercados e modelos de negócios é certamente valiosa.

REFERENCES

[1] M. Atzori. 2015. Blockchain technology and decentralized govenance: Is the state still necessary? *Work Pap* (2015).

[2] V. Buterin. 2014. A next-generation smart contract and decentralized application platform. *White Pap* (2014).

[3] J. Fairfield. 2014. Smart contracts, Bitcoin bots, and consumer protection. *Wash Lee L Rev Online* (2014).

[4] F. Glaser. 2017. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. *: Proceedings of the 50th Hawaii International Conference on System Sciences* (2017).

[5] F. Glaser and L. Bezzenberger. 2015. Beyond Cryptocurrencies-A Taxonomy of Decentralized Consensus Systems. *Proceedings of the 23rd European Conference on Information Systems* (2015).

[6] Adam Levy. 2021. 15 Applications for Blockchain Technology. *The Motley Fool* (2021).

[7] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 2017. Blockchain. *Business Information Systems Engineering* (2017).

[8] N. Szabo. 1997. Formalizing and Securing Relationships on Public Networks. *First Monday* 2, 9 (1997). https://doi.org/10.5210/fm.v2i9.548

[9] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. 2018. *Blockchain Technology Overview.* U.S. Department of Commerce.