DOI: 10.5748/19CONTECSI/PSE/ESD/6934

TAXONOMIA DO MODELO DE APLICAÇÕES DESCENTRALIZADAS BASEADAS EM BLOCKCHAIN

Jeffson Celeiro Sousa ; http://orcid.org/0000-0003-1654-1912
Universidade Federal do Pará

Alan Tony Souza Veloso ; http://orcid.org/0000-0002-0905-0771
Universidade Federal do Pará

Elder Bruno Evaristo Correa ; http://orcid.org/0000-0002-4031-6857
Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPQD

Billy Anderson Pimheiro ; https://orcid.org/0000-0002-2317-6258
Amachains - Amazônia Blockchain Solutions

TAXONOMY OF THE BLOCKCHAIN-BASED DECENTRALIZED APPLICATIONS MODEL

ABSTRACT: cryptocurrencies introduced and pushed the concept of Blockchain allowing the decentralized registration of information with the support of a network of untrusted participants. Using these concepts, a new model for building decentralized applications emerged, called Dapps (Decentralized Applications), which, besides being scalable, provides security and forms of incentives for participation. Despite the great attention that Dapps have received from the developer community and the innovation system, their definition is still imprecise. This paper aims to define and conceptualize Dapps and underlying technologies, as well as to propose a taxonomy that allows their classification. A study of the main Dapps proposed or recently developed using the proposed taxonomy is also presented. The definitions and the taxonomy proposed in this paper will enable a better understanding of the challenges potentials of Dapps in the context of the scientific community and industry

Keywords: taxonomy, blockchain, Decentralized Applications.

TAXONOMIA DO MODELO DE APLICAÇÕES DESCENTRALIZADAS BASEADAS EM BLOCKCHAIN

RESUMO: as criptomoedas introduziram e impulsionaram o conceito de Blockchain permitindo o registro descentralizado de informações com o suporte de uma rede de participantes não confiáveis. Utilizando esses conceitos surgiu um novo modelo para construir aplicações descentralizadas, chamado de Dapps (aplicações descentralizadas), que, além de escalável, provê segurança e formas de incentivos à participação. Apesar da grande atenção que as Dapps têm recebido por parte da comunidade de desenvolvedores e do sistema de inovação, sua definição ainda é pouco precisa. Este artigo procura definir e conceituar as Dapps e tecnologias subjacentes, bem como propor uma taxonomia que permita sua classificação. Também é apresentado um estudo sobre as principais Dapps propostas ou desenvolvidas recentemente, utilizando a taxonomia proposta. As definições e a taxonomia proposta neste artigo permitirão uma melhor compreensão dos desafios potenciais das Dapps no contexto da comunidade científica e indústria.

Palavras-chave: Taxonomia, blockchain, aplicações descentralizadas

1 INTRODUÇÃO

O crescente uso de tecnologia da informação e o esforço da comunidade em direção a cidades inteligentes tem fomentado a Computação Urbana (CoUrb) – infraestruturas que apoiam ambientes urbanos na prestação de serviços computacionais avançados aos cidadãos. Entre os principais focos da CoUrb destacam-se a melhoria dos serviços prestados à população (expedição de documentos, pagamento de impostos, etc.) e a integração digital de serviços (tal como em cidades inteligentes). Nesse contexto, a migração de serviços públicos para o meio digital traz à mesa de discussão questões de anonimidade e privacidade, uma vez que os usuários passam a depender mais dos serviços providos, tornando mais evidente a necessidade de auditoria e análise de riscos em sistemas.

Aliada à migração de serviços governamentais para o meio digital, observou-se também um aumento no interesse da indústria e da academia pelo desenvolvimento de moedas criptográficas (entre elas o *Bitcoin*), e de sua tecnologia base *blockchain*. *Blockchain* permite que informações sejam armazenadas de forma descentralizada, de forma anônima, com alta disponibilidade e de forma auditável (Frizzo-Barker et al., 2020). No âmbito da moeda virtual *Bitcoin*, uma das mais famosas implementações de moedas digitais, um *blockchain* é a estrutura de dados que representa uma entrada de contabilidade financeira ou um registro de uma transação. Tais entradas são geralmente chamadas de *tokens*, e representam uma quantidade de recursos digitais que podem ser transferidos para outra pessoa. Cada transação é assinada digitalmente, visando garantir sua autenticidade e integridade, de forma que o próprio registro e as transações persistidas pelo *token* sejam consideradas invioláveis (Kiff et al., 2020).

Com o sucesso de *Bitcoins*, logo se percebeu que era possível criar *blockchains* para outras finalidades: controle de mídias, contratos, documentos, etc. e várias iniciativas criadas nesse sentido. Uma dessas iniciativas -- *Ethereum* -- se destacou ao habilitar o *upload* e execução de aplicações no *blockchain*. Seus mantenedores se baseiam em todas as premissas técnicas e matemáticas de *blockchain* para aferir que as aplicações derivadas a partir desta são isentas de *downtime*, censura e fraudes. Mais importante, garante-se que estas aplicações executam exatamente como programadas (Abuhashim & Tan, 2020), propriedade similar àquela garantida por plataformas de computação confiável. As aplicações que executam sobre uma rede *blockchain* são chamadas de DAPPs (*Decentralized Applications*) e são formadas, principalmente, por partes lógicas executadas no *blockchain*, denominadas de smart contracts (Abuhashim & Tan, 2020).

A habilidade dos contratos inteligentes de expressar lógica de uma forma aberta, confiável e verificável, torna-os uma solução para estabelecer confiança e controle entre entidades pertencentes a diferentes domínios (Raval, 2016). Considerando a relevância das *Dapps* e a falta de uma categorização especifica para o tema, propõe-se uma taxonomia para as *Dapps*, classificando-as e ressaltando os pontos comuns existentes nas diferentes aplicações, além de mostrar suas divergências conceituais e de implementação.

O artigo está organizado como segue. A Seção 2 trata sobre a fundamentação teórica que apresenta os principais conceitos sobre *blockchain e Dapps*. A seção 3 fala sobre alguns trabalhos que tratam de formas de organizações taxonômicas e as diferentes de classificação que as envolvem. A Seção 4 introduz a taxonomia proposta no escopo do artigo, especificando as características das *Dapps* e definindo as categorias taxonômicas

utilizadas. Na Seção 5 discute-se uma classificação de Dapps existentes de acordo com a taxonomia proposta. A Seção 6 conclui o artigo com considerações finais e perspectivas de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Um aplicativo centralizado é de propriedade de uma única empresa. O software de aplicativo para um aplicativo centralizado reside em um ou mais servidores controlados pela empresa. Como usuário, você interagirá com o aplicativo baixando uma cópia do aplicativo e enviando e recebendo dados do servidor da empresa.

Um aplicativo descentralizado (também conhecido como dApp ou dapp) opera em uma rede *blockchain* ou *peer-to-peer* de computadores. Ele permite que os usuários se envolvam em transações diretamente uns com os outros, em vez de depender de uma autoridade central. O usuário de um dApp pagará ao desenvolvedor uma quantia em criptomoeda para baixar e usar o código-fonte do programa. O código-fonte é conhecido como contrato inteligente, que permite que os usuários concluam transações sem revelar informações pessoais.

É nesse contexto que esta seção apresenta os principais conceitos sobre Dapps, além de apresentar trabalhos que já se propuseram a classificar de alguma forma as moedas criptográficas.

2.1 Blockchain

Blockchain funciona como um livro de registros aberto (*open*) e descentralizado, permitindo pagamentos em moedas que não são emitidas nem controladas por uma autoridade central. Nesse contexto, são a própria rede de usuários e a "teia" de trocas quem conferem valor e credibilidade aos pagamentos feitos apoiando-se na *blockchain*.

Figura 1. Funcionamento de uma *blockchain*

Fonte: Elaboração própria (2021).

A figura 1 ilustra o conceito. Além de permitir a implementação de moedas virtuais, *blockchain* pode ser utilizado para assegurar outras transações entre usuários de uma rede. Nesse caso, *blockchain* confere confiabilidade na realização de transações entre entidades distribuídas e mutuamente não confiáveis, sem a necessidade de uma entidade intermediária confiável por ambos. *Blockchain* permite ainda implementar de forma efetiva

contratos inteligentes (*smart contracts*) (Zheng et al., 2020) na rede -- contratos automatizados, com execução realizada pela rede, seguindo as condições criadas pelo usuário. Assim, ações podem ser executadas por meio de instruções lógicas, gerando como produto ativos (*assets*) reconhecidos como válidos no mundo real. Ou seja, quando alcançada uma condição pré-estabelecida (programada), o contrato é executado automaticamente gerando uma ação pré-estabelecida como saída.

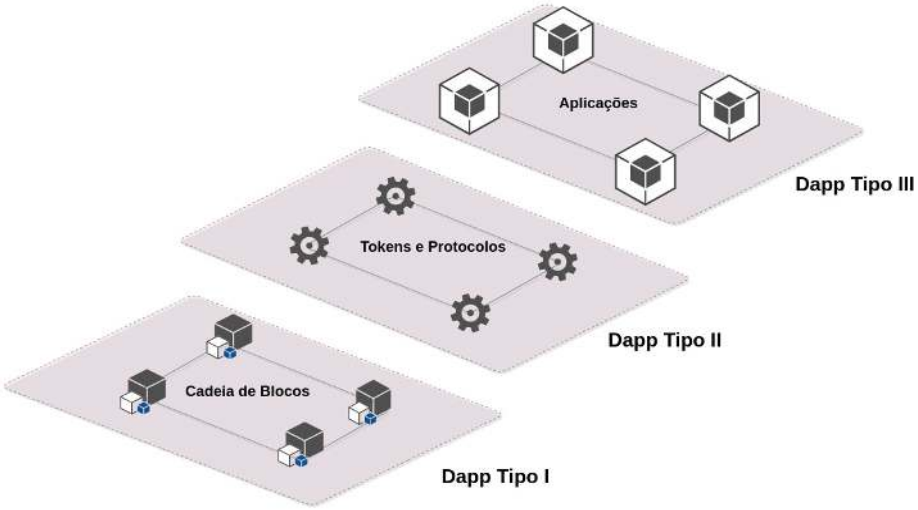
O conceito de contratos inteligentes foi desenvolvido antes do *blockchain*, com base nos mesmos estudos do cientista e jurista Nick Szabo. Szabo propôs que era possível formalizar de forma segura a relações entre elementos de uma rede pública, através do uso de interfaces de usuários e protocolos (Nagothu et al., 2018). Nesse contexto, surge a ideia de *Blockchain Thinking*, que é a maneira de formular pensamentos usando como base os processos *blockchain*. A aplicação dessa visão permite, por exemplo, a resolução de problemas relacionados à confiança entre entidades pertencentes a diferentes domínios. Em outras palavras, o *blockchain* é usado como um mecanismo confiável de consenso entre as partes (Hassan & De Filippi, 2021). Usar *blockchain* com um conector via *software* para elementos de diferentes domínios é uma abordagem que permite criar uma alternativa descentralizada para os atuais compartilhamentos de dados centralizados. A vantagem é que essa abordagem melhora a transparência e a rastreabilidade das informações trocadas pelos diferentes domínios (Zheng et al., 2020).

2.2 Aplicações Descentralizadas (Dapps)

Segundo essa definição, para uma aplicação ser considerada uma *Dapp* devem ser atendidos quatro critérios. A primeira demanda abertura total da aplicação, tanto no sentido de código aberto como na especificação do protocolo, que deve se adaptar às novas demandas, mas restrito a um consenso dos usuários sobre essas mudanças. O segundo critério determinado que todos os dados e registros de operações deva ser armazenado de uma *blockchain* pública e descentralizada. O terceiro critério diz respeito à existência de um *token* (por exemplo, *bitcoin*), o qual é necessário para acessar a aplicação. Esse *token* serve de remuneração para qualquer contribuição pelo esforço computacional realizado pelos membros em manter o sistema. O quarto critério determina que os tokens sejam gerados por algoritmos criptográficos que agem como prova da contribuição ou esforço realizado pelos participantes do sistema.

A definição acima pode ser flexibilizada e entendida de forma mais ampla. Por exemplo, embora ela cite explicitamente o uso de *blockchain*, aceita-se que uma *Dapp* seja baseada em outros sistemas distribuídos públicos, desde que mantidos os demais critérios. A definição proposta afirma ainda a necessidade de utilizar *blockchains* públicas nas *Dapps*. No entanto, no presente artigo considera-se também a utilização de redes privadas e híbridas, pois se vislumbra que dessa forma a classificação utilizada permitirá melhor abstração e cobertura. A anatomia e nomenclatura das *Dapps* ainda não estão consolidadas, uma vez que a área se encontra em constante evolução, e requer mais esforços para padronização. O presente artigo apresenta-se como um esforço nesse sentido.

Figura 2. Tipos de Dapps.



Fonte: Elaboração própria (2021).

As *Dapps*, como apresentado na figura 2, podem ser organizadas em 3 tipos. *Dapps* tipo I possuem sua própria blockchain; essas são de mais baixo nível, e dão suporte para a criação das *Dapps* do tipo II. *Dapps* tipo II, por sua vez, são protocolos que manipulam tokens para realizar suas funções. Com o uso de *Dapps* tipos I e II é possível criar *Dapps* tipo III; essas implementam funções mais relacionadas às necessidades dos usuários. Desta forma, teremos poucas *Dapps* do tipo I, seguidas de um número maior das do tipo II, e um número mais elevado de *Dapps* tipo III. O sucesso e a flexibilidade das *Dapps* provocaram um aumento no número de casos de uso aplicando a tecnologia nos mais variados campos. Os parágrafos a seguir discutem os casos mais promissores.

Aplicações financeiras: Com o avanço e popularização das pesquisas envolvendo *blockchain*, bancos, empresas e grupos de *startups* lançaram esforços para explorar oportunidades como permitir o desenvolvimento de novas bolsas de valores que facilitam a negociação de uma grande variedade de ativos, não apenas instrumentos financeiros.

Internet das coisas: IoT engloba o mundo dos sensores, movendo objetos como veículos e realmente qualquer dispositivo que tenha incorporado a eletrônica para se comunicar com o mundo exterior, combine isso com *blockchain* - um padrão de arquitetura de *ledger* distribuído (DLT), juntos eles podem facilitar todo o ciclo de vida de dispositivos e aplicações IoT e provar ser a junção para os processos de negócios para agir sobre esses eventos. Considere o seguinte cenário - um bloqueio privado para um carro conectado sem driver que permitirá interações seguras e em tempo real do carro, começando com a inicialização do carro, autenticação do *driver*, contratos inteligentes para trocar informações de seguros e informações de manutenção e informações de localização em tempo real para monitorar a segurança.

Computação em nuvem: Tendo como principal desenvolvedora nesse seguimento envolvendo *blockchain* e *cloud*, a *Microsoft* usa *blockchain* como um serviço (*blockchain-as-a-service*, BaaS), aluga serviços e espaço para startups desenvolverem e criarem aplicações em cima da nuvem da *Microsoft Azure*.

Automação de contratos: Parte da ideia de automatizar as relações através de um protocolo de confiança, ou seja, seria o uso de uma tecnologia digital para incorporar regras de

negócios em um contrato, incluindo a execução automatizada de cláusulas contratuais. Usando o *blockchain*, os contratos inteligentes podem ser customizados de contrato para contrato, estreitando transações ao cortar contrapartes e intermediários.

RFID (Radio-Frequency Identification): É um sistema composto, basicamente, de uma antena, um transceptor, que faz a leitura do sinal e transfere a informação para um dispositivo leitor, e também um transponder ou etiqueta de RF (rádio frequência), que deverá conter o circuito e a informação a ser transmitida. Estas etiquetas podem estar presentes em pessoas, animais, produtos, embalagens, enfim, em equipamentos diversos. Agora imaginem essa tecnologia se baseando no princípio de *blockchain*, gerando um controle seguro, tudo sendo registrado ao modo que nada possa ser alterado, além de levar em consideração a velocidade das transações. A diversidade de empresas de grande porte (como consórcio R3, que seria um conglomerado de mais de 70 bancos, a IBM e etc.) que estão em busca de consenso em relação ao uso do protocolo de confiança que é o *blockchain*, afim de se ter uma seguridade e estabilidade, visando a troca de valores, informações, dados, arquivos em tempo real.

Registro de imóveis: Talvez seja o serviço mais recente proposto na rede *blockchain*, que visa facilitar a compra, venda e troca de imóveis através de verificação dos contratos e registros do usuário que esteja disposto a negociar o imóvel que seja registrado na rede, excluindo a burocracia que é a negociação de bens e de imóveis atualmente, tudo envolvendo um grande registro imobiliário.

3 TRABALHOS RELACIONADOS

Até o presente momento, a literatura contempla apenas taxonomias para *blockhain* (Capar et al., 2004), a qual é limitada ao não categorizar *Dapps*. Apesar de a taxonomia existente aborda satisfatoriamente as características das *blockchains*, o artigo que a descreve não apresenta uma metodologia clara, que seja detalhada e atualizada, levando em consideração característica de acesso, modelos e tipos de *blockchain* para determinação de uma taxonomia embasada, e não classifica as *blockchains* existentes, sendo um ponto positivo na taxonomia proposta.

Outro contexto de definição taxonômicas em *blockchain* está atrelado ao contexto de cadeias de verificação de suprimentos no contexto do agronegócio, onde é abordado Características de rastreabilidade e gestão, tomando como princípios riscos nas cadeias de suprimentos agro alimentícios, gerenciamento, interrupção, avaliações e o processo que envolve o transporte (Imbiri et al., 2004). Outro exemplo claro de definições muitos especificas de cenários que utilizam redes blockchain.

A pesquisa (Hameed et al., 2022) abrangente a última geração de tecnologias baseadas em aplicativos da indústria 4.0, com foco em possíveis requisitos de design, segurança e privacidade de aplicativos, bem como ataques correspondentes a sistemas *blockchain* com possíveis contramedidas, ou seja, mostra o cenário atual de desafios encontrados em aplicações desenvolvidas visando um modelo de gestão atualizado.

O trabalho (Fridgen et al., 2018) tem como motivação o contexto de *blockchain* voltado as ofertas iniciais de moedas (ICOs). Muitos desses empreendimentos de *crowdfunding* são muito bem-sucedidos, outros não. No entanto, apesar dos crescentes investimentos em ICOs, ainda não há conhecimento teórico suficiente nem uma compreensão abrangente dos

diferentes tipos de modelos de negócios e as implicações para esses ecossistemas baseados em *tokens*, apresentando uma taxonomia de *startups* baseadas em *blockchain* do mundo real. a taxonomia proposta nesse trabalho mira nas questões como modelos de negócios baseados em *tokens*, gerencia e tipos variados de estruturas de ecossistemas de startups.

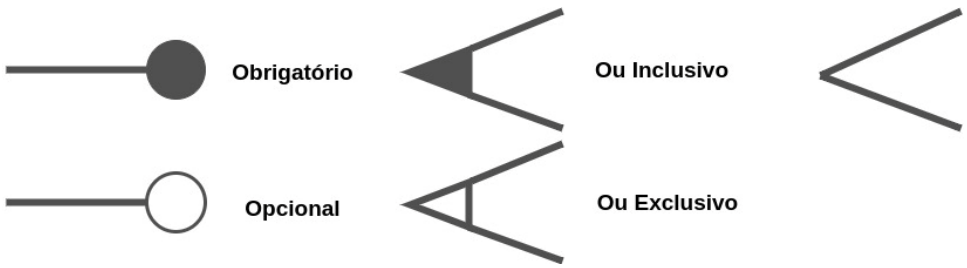
Para formular a taxonomia proposta no escopo do presente artigo, considerou-se ainda como fonte de informações sobre Dapps o livro *Decentralized Applications*: *Harnessing Bitcoin's Blockchain Technology* (Rayal, 2016). Esse livro é importante nesse contexto por, entre outros, abordar questões importantes sobre nomenclatura e diferenciação entre aplicações descentralizadas e distribuídas.

4 TAXONOMIA DAS DAPPS

Nesta seção apresenta-se uma categorização de *Dapps*, que servirá para criar a base taxonômica proposta no escopo do presente artigo. É importante destacar que a taxonomia para um dado campo do conhecimento mostra o domínio neste campo em termos que são fáceis de entender, comunicar, ensinar, aprender e trabalhar. Desta forma, uma taxonomia pode ser usada para classificar de maneira eficiente e efetiva um determinado campo, tornando esta classificação um artefato para meta análise computacional por outros pesquisadores além de identificar lacunas na literatura que consequentemente apontam direções de pesquisa (Kang et al., 1990).

O método de análise de domínio orientado a características *Feature-Oriented Domain Analysis, FODA)* (Kang et al., 1990), foi utilizado para criar a taxonomia proposta. O foco principal do método FODA é a identificação de características proeminentes ou distintivas em domínios específicos, em nosso caso, as *Dapps*. As características são os atributos de um sistema que afeta diretamente os usuários finais, que precisam tomar decisões sobre a disponibilidade de funcionalidade no sistema e precisam entender o significado destas características para usar o sistema. Um diagrama de características é um conjunto hierárquico de recursos. As relações entre um recurso principal e suas características filho são categorizadas como: (e) - todas as sub-características devem ser selecionadas; ou exclusivo - apenas uma sub característica pode ser selecionada; ou inclusivo - uma ou mais podem ser selecionadas; obrigatórias - características que são necessárias ao funcionamento do sistema; e opcionais - recursos que são opcionais. A figura 3 apresenta a simbologia para representar os diagramas de recursos.

Figura 3. Legenda do Modelo de Características.

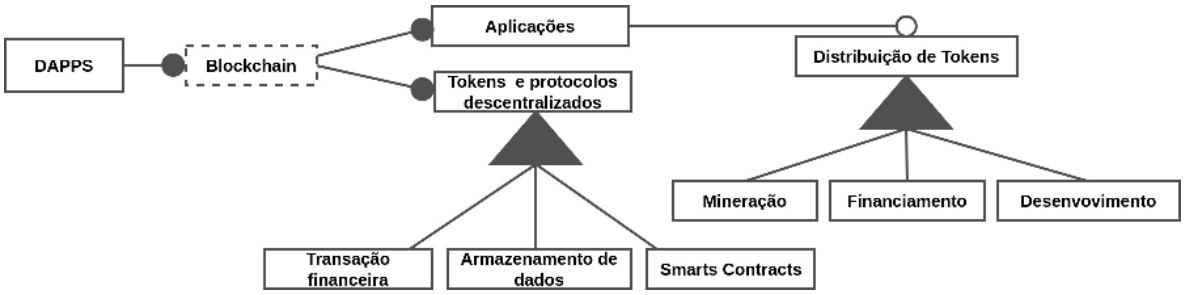


Fonte: Elaboração própria (2021).

4.1 CATEGORIAS TAXONÔMICAS

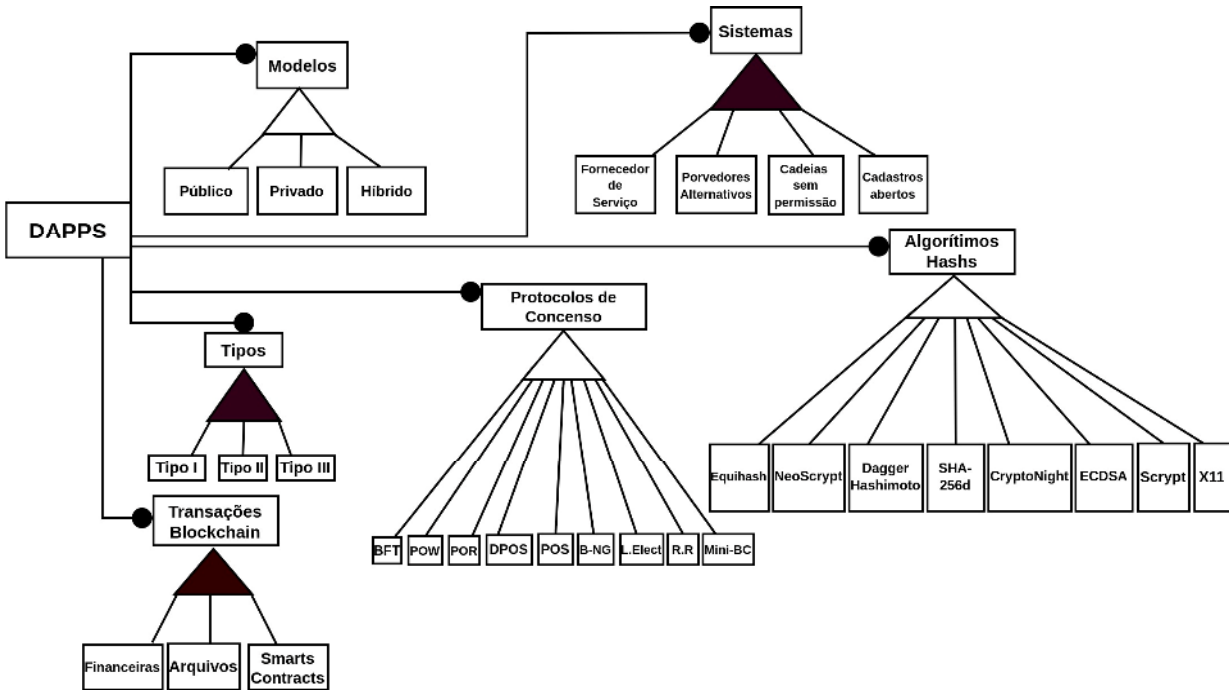
A escolha das características usadas para criar as categorias foi realizada usando a definição de *Dapps* apresentada em (Nijsse & Litchfield, 1990). Substituímos os tipos de *Dapps* utilizadas pelas respectivas características funcionais que definem cada tipo. Especificamente, o Tipo I é definido pelas *blockchains* em si, o Tipo II pelos *tokens* e Protocolos Descentralizados e o Tipo III pelas aplicações que são armazenadas e executadas de forma descentralizada.

Figura 4. Estrutura do conjunto de Características das Dapps



Fonte: Elaboração própria (2022).

Figura 5. Estrutura detalhada de Características Blockchain.



Fonte: Elaboração própria (2022).

A figura 4 apresenta as características funcionais da *Dapps* utilizando o diagrama de características definido no FODA (Kang et al., 1990). Na Figura 5 é apresentada a continuação do diagrama anterior, porém em maior nível de detalhamento quanto as *blockchains*. Cada uma das características é explicada em seguida.

4.2 TOKENS E PROTOCOLOS DESCENTRALIZADOS

São as funcionalidades oferecidas sobre as *blockchains* e normalmente disponibilizadas através de uma API (Johnson et al., 2015). Estas funcionalidades estão relacionadas a três tipos de uso para a cadeia de blocos:

Transações financeiras: Se resume em transações de ativos financeiros entre os nós da rede, de forma segura, transparente e descentralizada;

Armazenamento de dados: um exemplo desse tipo de transação está relacionado a aplicações de streaming, usando uma plataforma de serviço (Saas), que através de banco de dados descentralizados, podem trocar informações e dados entre os que estiverem registrados na rede;

Smart contracts: São transações que funcionam como contratos inteligentes que se auto executam baseado em regras entre as partes, que geram consenso e confiança mútua, sem necessidade de intermediários.

4.3 APLICAÇÕES

São aplicações que são armazenadas na própria rede e são executadas pelos usuários através do acesso a blocos criptografados armazenados na rede. Quando estas aplicações utilizam *tokens*, a distribuição deste pode acontecer de 3 formas:

Mineração: Neste modelo os tokens são distribuídos para aqueles que contribuem mais para a operação da *Dapp*;

Financiamento: Os *tokens* são distribuídos para as pessoas que ajudaram a financiar o desenvolvimento inicial da Dapps;

Desenvolvimento: Os *tokens* são gerados usando um mecanismo predefinido e são disponíveis, como forma de contrapartida, para os desenvolvedores da *Dapp*.

4.4 BLOCKCHAIN

São as redes P2P, com mecanismos de consenso, que usam criptografia para tornar as informações permanentes e que armazenam os blocos na forma de empilhamento. Sua implementação é dada através da criação de um *software* que age como mais um nó dentro da rede *blockchain*:

- Modelos de redes Blockchain

→ Permissionado Público: Somente nós que foram autenticados podem ingressar na rede. Os membros devem concordar com o consenso e somente nós validados podem fazer parte desse consenso. Os leitores também devem ser autenticados ou podem ser usados apenas por nós específicos;

→ Permissionado Privado: Os nós também precisam se autenticar para ingressar na rede, que possui permissões para persistir dados e manter a rede, eles são centralizados em uma ou mais organizações confiáveis cuja função é adicionar novos blocos à cadeia após a verificação. O processo de leitura pode ser feito publicamente para nós autenticados ou restrito a conjuntos confiáveis;

→ Não-permissionado: São redes blockchain de acesso aberto sem autenticação, ou seja, qualquer usuário pode criar uma carteira e usá-lo. Consiste em um ledger transparente no qual qualquer par na rede pode se tornar mineradores e tentar validar blocos como *Bitcoin e Ethereum*.

Em suma, a classificação de *blockchains* é importante para possibilitar a customização de aplicativos, diferentes regras de acesso para sistematizar a organização do modelo de rede de acordo com as necessidades da aplicação. Ao projetar uma rede *blockchain*, se um modelo de rede inadequado for escolhido, a privacidade do usuário pode ser comprometida ou os dados podem ser muito restritos.

- Protocolos (mecanismos) de Consenso

Os mecanismos de consenso blockchain fornecem benefícios através de um conjunto de ferramentas que geram um consistente e consolidado número reduzido de erros, onde esses mecanismos geram dados de referência quase em tempo real e os participantes têm a flexibilidade para mudar as descrições dos ativos que possuem dados (Miers et al., 2015). São eles:

→ *Proof-of-work* (POW): Usado como mecanismo de consenso o *proof-of-work*, prova de entrega ao poder computacional recompensada em caso de sucesso na transação, nos cálculos criptográficos complexos. É recompensado o minerador que for mais rápido;

→ *Proof-of-retrievability* (POR): Tem como função armazenar dados distribuídos de recursos de mineração, ou dados arquivísticos;

→ *Proof-of-stake* (POS): Enquanto no *proof-of-work* o minerador é recompensado por provar a sua capacidade computacional, no *proof-of-stake* ele precisa provar que é detentor de várias criptomoedas para ser remunerado. O dado preocupante é que se algum milionário adquirir no mercado uma parcela gigantesca das moedas, o consenso ficará sob seu domínio, e a descentralização estará comprometida. Com base nisso, pensou-se em modelos mais democráticos que pudessem favorecer a redução de gastos com a computação;

→ *Delegate proof-of-stake* (DPOS): Este método de consenso que vem sendo testado em algumas criptomoedas de maneira aparentemente satisfatória. Nesse protocolo, o computador da comunidade com mais criptomoedas é eleito para fazer a mineração, sendo o lucro obtido dividido com a comunidade. Essa iniciativa visa evitar a centralização por uma única pessoa detentora de muitas moedas;

→ *Byzantine fault tolerance*, BFT: Esse mecanismo oferece uma garantia de consistência muito mais forte e menor latência, mas para um número menor de participantes;

→ *Leader elec*t: Por esse modelo, elege-se um líder para ser seguido por todas as máquinas (similar ao Paxos);

→ *Round-robin*: As máquinas são selecionadas de forma aleatória para fazer a mineração de blocos;

→ Consenso proprietário: Mecanismo bastante usado em modelos privados, onde visa a segurança e total anonimato do usuário;

→ *Mini-blockchain*: Esse mecanismo tem como função o equilíbrio entre todos os endereços, gerando equiparidade entre os nós da rede, além de gerar atualizações de transações periodicamente, fazendo com que se descarte transações muito antigas que só estão consumindo recurso;

→ *Bitcoin-NG*: Sua função é gerar uma divisão entre operação de bloco em dois planos: eleição de líder e serialização de transações. Uma vez que um líder é selecionado, ele pode serializar transações até a seleção do próximo líder. A eleição líder no *Bitcoin-NG* é orientada para o futuro e garante que o sistema possa processar continuamente as transações.

- Modelos de sistemas

→ Fornecedor de sistemas: Esse sistema funciona a partir de uma plataforma baseada em *blockchain*, que fornece ambiente para desenvolvimento de ferramentas voltadas a governos e tribunais dentro de uma jurisdição, e monopólios empresariais, um exemplo desse sistema é o projeto *Ripple*;

→ Provedores alternativos: Funciona para bancos, pagamentos *on-line* ou provedores de computação em nuvem. Qualquer sistema centralizado é um único ponto de falha para seus usuários. No entanto, onde existem provedores alternativos, a falha de um provedor de serviço único afeta apenas seus usuários, e os usuários podem mudar os provedores ou usar vários provedores. Um dos exemplos desse sistema é a nuvem da *Microsoft Azure* e recentemente a IBM lançou seu projeto em nuvem *blockchain*, baseado em código livre;

→ Cadeias sem permissão: O sistema sem permissão trabalha de forma pública, fazendo que o usuário não precisa de algum tipo de permissão para se registrar, exemplos desse sistema seria o *Bitcoin e o Ethereum*;

→ Cadastros abertos: São sistemas que fazem o cadastro de novos usuários. Embora seja aberto, dependendo do modelo *blockchain* usado, faz-se necessário que a autorização seja dada de forma consensual pelos registrados no bloco; após essa liberação, o usuário consegue efetuar/validar transações na rede.

É possível realizar um paralelo da taxonomia apresentada com o padrão de projeto MVC, sendo a *blockchain* como *Model* oferecendo serviços de comunicação e consenso de forma segura, os *tokens* e Protocolos descentralizados como *Control*, adicionando funcionalidades sobre a *blockchain* e as aplicações como *View*, que utiliza as funcionalidades criadas pelas outras camadas para criar serviços para os usuários.

5 CLASSIFICAÇÃO DAPPS

O processo de escolha das *Dapps* foi através da listagem das moedas com maior volume de troca em uma casa de câmbio[1], adicionalmente outras moedas foram inseridas devido a sua relevância em contexto específicos, como a *SolarCoin* que foi projetada para trabalhar com energias renováveis (Tian et al., 2022).

A Figura 6 apresenta a classificação das *Dapps* utilizando a taxonomia proposta. As seguintes Dapps foram classificadas: Bitcoin (Rosenberger, 2018), Terracoin (Aggarwal & Kumar, 2021), Ethereum (Ferretti & D'Angelo, 2020), FreiCoin (Bieliauskas, 2019), Monero (Li et al., 2019), SolarCoin (Tian et al., 2022), Hyperledger (Aggarwal & Kumar, 2021), Zcash (Silfversten et al., 2020), CargoChain (Hellani et al., 2021), Omni (Strehle & Steinmetz, 2020), Dash (Mosley et al., 2022), Litecoin (Van Hieu et al., 2021), AnonCoin (Henry et al., 2018), Warranteer (Attaran & Gunasekaran, 2019), Genecoin (Thiebes et al., 2020), IBREA (Veuger, 2017), Ripple (Amores-Sesar et al, 2020), Feathercoin (Attah, 2019), DigitalNote (Yu et al., 2019), MultiChain (Ismailisufi et al., 2019), Cryptonite (Suarez et al., 2019) e Permacoin (Aggarwal & Kumar, 2021) totalizando 22 *Dapps*. Em seguida iremos descrever com maiores detalhes o uso da classificação para três *Dapps* escolhidas, baseada na sua importância para a comunidade e ao uso das três macros categorias propostas.

5.1 BITCOIN

Embora o fenômeno *Dapps* tenha começado com métodos de pagamento e certificação de dados (para os quais já existem padrões de blocos), sua influência e alcance estão atingindo uma grande variedade de setores industriais. Variedade essa que acabou gerando classificações acerca de suas especificidades e limitações, como seria o caso do tipo I, que se encaixa na mais conhecida entre as criptomoedas, atuando na área financeira ao possuir sua cadeia própria de blocos.

A tecnologia inovadora permite recriar as características do dinheiro físico no mundo digital. Mas com uma particularidade notável, porque o *Bitcoin* é simultaneamente uma moeda digital e um sistema de pagamentos. Isso nunca ocorreu na história financeira da humanidade. É certo que não é reconhecido nem emitido por nenhum estado. Moeda estrangeira, por definição, jamais será. Mas tem funcionado como dinheiro para muitas pessoas, algo inexplicável para a maioria dos economistas, cujas teorias não admitem uma moeda produzida livremente pelo mercado (Cunha, 2019).

5.2 ETHEREUM

A intenção da *Ethereum* é criar um protocolo para a construção de aplicações descentralizadas. A *Ethereum* fornece aos desenvolvedores uma camada fundamental: uma cadeia de blocos com uma linguagem de programação integrada de Turing, permitindo que qualquer pessoa escreva contratos inteligentes e aplicativos descentralizados onde eles podem criar suas próprias regras arbitrárias de propriedade, formatos de transação e funções de transição do estado.

[1] http://poloniex.com

Fazendo uso de sistemas de *tokens*, existem três tipos de aplicativos no *Ethereum*, como: Aplicações financeiras, proporcionando aos usuários formas mais poderosas de gerenciar e contratar contratos usando seu dinheiro; Aplicações semi-financeiras , onde o dinheiro está envolvido, mas também há um forte lado não monetário para o que está sendo feito; Aplicativos como a votação *on-line* e a governança descentralizada que não são financeiras (Modi, 2018).

5.3 SAFE NETWORK

A rede SAFE funciona a partir da integração de blocos próprios de aplicações do tipo I e usa a tecnologia de registros através de *tokens* do tipo II, gerando assim uma plataforma de compartilhamento de arquivos de forma descentralizada.

Ela é uma rede de desenvolvimento que permite a criação de aplicações rápidas e seguras que ajudam a garantir privacidade, segurança e liberdade digitais para todos, além de gerar acesso de aplicações, armazenamento de dados e comunicação baseadas no protocolo p2p, funcionar com o propósito de compartilhamento de recursos de máquinas que estejam registradas na rede SAFE, fazendo com que se tenha maior poder de armazenamento em escala global (Makridakis & Christodoulou, 2019).

5.4 HYPERLEDGER

O projeto *Hyperledger* é um projeto de *blockchain* de código aberto e ferramentas relacionadas lançadas pela *Linux Foundation* em 2015 (Aggarwal & Kumar, 2021). A visão da *Hyperledger* é que a tecnologia blockchain tem o potencial de impactar quase todos existem áreas de atuação. Diante dessa visão, eles acreditam que no futuro, em vez de grandes *blockchains* operando entre empresas, haverá muitos *blockchains* interconectados, cada um sintonizado e adaptado para uma finalidade específica. O projeto *hyperlegder* é composto por vários módulos de implementação e desenvolvimento de acordo com várias lógicas de negócio, tais como:

- *Fabric*: uma plataforma para criar soluções de contabilidade distribuída Arquitetura modular que oferece alta confidencialidade, flexibilidade, Elasticidade e escalabilidade.

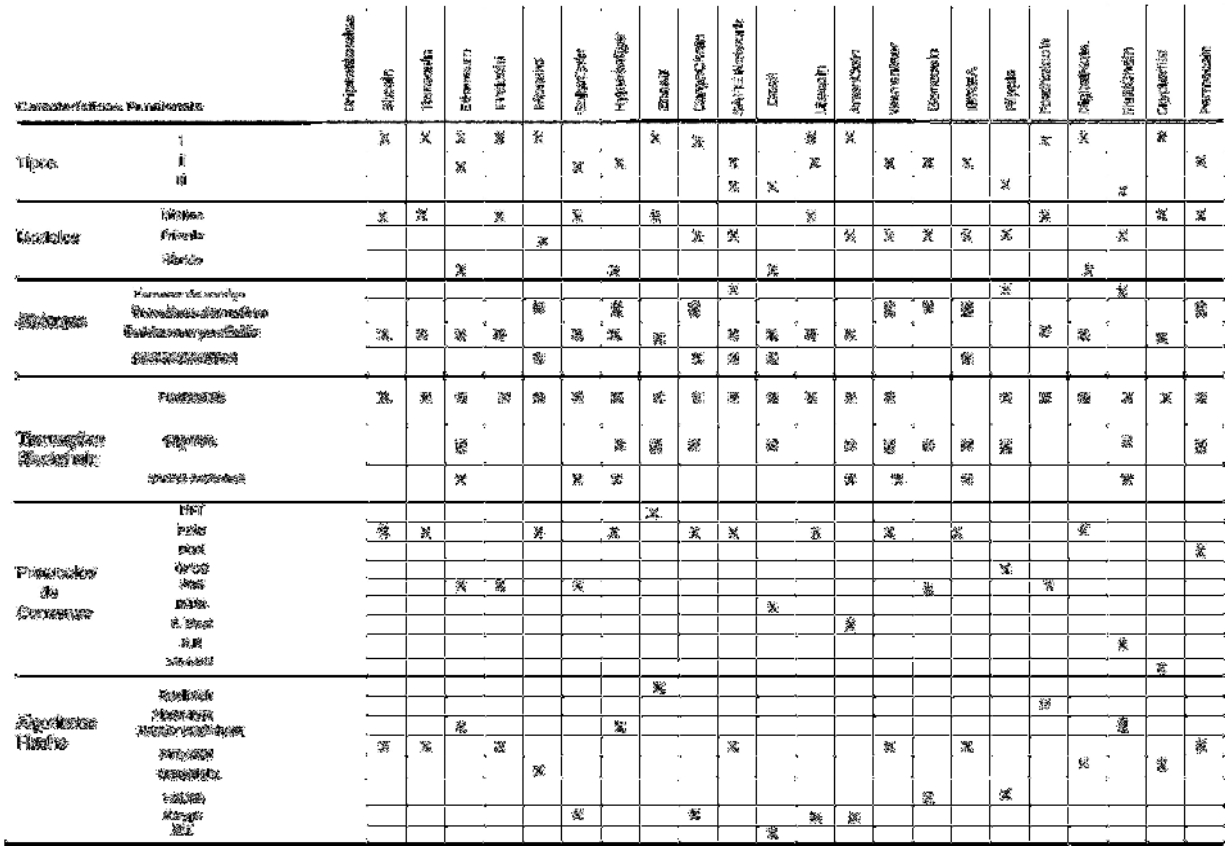
- *Burrow*: cliente *blockchain* modular com intérprete de contrato inteligente Licença desenvolvida em parte de acordo com a especificação da máquina virtual (VM) *Ethereum*.

- *Indy*: livro-razão distribuído que fornece ferramentas, bibliotecas e componentes Reutilizável criado para identidades descentralizadas.

- *Iroha*: Uma estrutura blockchain com design simples e fácil de incorporar em projetos de infraestrutura empresarial.

- *Sawtooth*: Uma plataforma modular para criar, implantar e executar registros distribuídos.

Figura 6 - Classificação das Dapps.



Fonte: Elaboração própria (2021).

Dentre outras bibliotecas e ferramentas que garantem a variedade de tecnologias que compõem o projeto. Os *frameworks* e ferramentas disponíveis da plataforma, facilitam o embasamento e utilização da tecnologia *Blockchain* por diferentes modelos de indústria. Desta forma, revela-se a versatilidade do uso da tecnologia *Blockchain* e também das possibilidades de desenvolvimento a partir do *Hyperledger*.

É interessante as discussões acerca de vantagens e desvantagens sobre o uso e desenvolvimento de estudos voltados às dapps, como por exemplo:

- Vantagens

→ Promove a privacidade do usuário

→ Resiste à censura

→ Plataforma flexível permite o desenvolvimento de dApp

- Desvantagens

→ Experimental, pode não ser capaz de dimensionar

→ Desafios no desenvolvimento de uma interface amigável

→ Difícil fazer as modificações de código necessárias

Em suma, as discussões trazidas neste trabaho, está estreitamento ligado a exposição da complexidade que permeia a redes blockchains, especificamente as aplicações descentralizadas. Para Para apoiar esse entendimento, este artigo contribui com uma classificação sistemática e rigorosa, porém expondo de forma clara como os conceitos e definições se apoiam na infraestrutura que é executada por trás de todas as aplicações. A diretriz descentralizada é resultado de uma nova metodologia orientada a dados que estrutura a complexidade de modelagem de sistemas descentralizados na fase de projeto e, portanto, pode apoiar a inovação da comunidade empresarial e de computação distribuída. Seu valor na educação está na melhor compreensão e comparação do design de livros distribuídos.

Assim, as contribuições deste artigo podem explicar e fornece novos insights para pesquisadores, profissionais e empreendedores sobre quais escolhas no espaço de design de sistemas DLT têm maior impacto, onde há espaço para inovação e quais sistemas têm características competitivas ou designs compartilhados.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

As *Dapps* são uma releitura da tecnologia p2p adicionando toda a questão de segurança e consenso que é inserida através de *blockchain*. A análise da literatura mostrou que este é o primeiro trabalho que desenvolve uma taxonomia especifica para *Dapps*.

A forma de manipular os blocos de dados dentro de uma *Dapp* é classificada, na nossa taxonomia, fora da *blockchain*, ou seja, ela não é uma característica intrínseca da blockchain e sim uma característica adicionada quando existe a manipulação de tokens e de protocolos descentralizados por parte das *Dapps* do tipo II.

Através do uso da taxonomia é possível escolher melhor qual tipo de *Dapp* pode ser usada como base para desenvolvimento de novos projetos uma vez que as características de cada uma estão organizadas e separadas por categoria.

Como trabalhos futuros, pretende-se disponibilizar um sistema online de classificação de *Dapps*, usando a taxonomia proposta, que possa ser manipulado de forma colaborativa, criando com isso uma base constantemente atualizada sobre *Dapps*. Outro tópico de pesquisa interessante é a classificação qualitativa das categorias exposta na nossa taxonomia, permitindo saber com maior facilidade qual categoria é mais interessante para um determinado projeto.

7 REFERÊNCIAS

Abuhashim, A., & Tan, C. C. (2020, July). Smart contract designs on blockchain applications. *2020 IEEE Symposium on Computers and Communications* (ISCC) (pp. 1-4).

Aggarwal, S., & Kumar, N. (2021). Cryptocurrencies. *Advances in Computers,* Vol. 121, pp. 227-266.

Aggarwal, S., & Kumar, N. (2021). Hyperledger. *Advances in Computers* Vol. 121, pp. 323-343.

Amores-Sesar, I., Cachin, C., & Mićić, J. (2020). Security analysis of ripple consensus. *ArXiv:2011.14816 [Cs]*.

Attah, E. (2019, April 24). *Five most prolific 51% attacks in crypto: Verge, Ethereum Classic, Bitcoin Gold, Feathercoin, Vertcoin*. CryptoSlate. https://cryptoslate.com/prolific-51-attacks-crypto-verge-ethereum-classic-bitcoin-gold-feathercoin-vertcoin/

Attaran, M., & Gunasekaran, A. (2019). Consumer goods and retail industry. *Applications of blockchain technology in business* (pp. 59-61). Springer, Cham.

Bieliauskas, R. (2019, January). Invisible BlockChain and Plasticity of Money–Adam Smith Meets Darwin to Buy Crypto Currency. *Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers* (Vol. 339, p. 289).

Capar, I., Ulengin, F., & Reisman, A. (2004). A taxonomy for supply chain management literature. *SSRN Eletronic Journal*, 10.2139/ssrn.531902.

Cunha, M. de C., Fº. (2019). Bitcoin: uma tentativa de construção da confiança por meio da tecnologia. *Revista de Informação Legislativa*, 56(221), 37-60.

Ferretti, S., & D'Angelo, G. (2020). On the ethereum blockchain structure: A complex networks theory perspective. *Concurrency and Computation: Practice and Experience*, *32*(12), e5493.

Fridgen, G., Regner, F., Schweizer, A., & Urbach, N. (2018). Don't Slip on the Initial Coin Offering (ICO): A Taxonomy for a Blockchain-enabled Form of Crowdfunding. In 26th European Conference on Information Systems (ECIS).

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029.

Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. *Journal of Industrial Information Integration*, 26, 100312.

Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, 10(2), 1-10.

Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. *Logistics*, 5(3), 46.

Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy*, 16(4), 38-45.

Imbiri, S., Rameezdeen, R., Chileshe, N., & Statsenko, L. (2021). A novel taxonomy for risks in agribusiness supply chains: a systematic literature review. *Sustainability*, 13(16), 9217.

Ismailisufi, A., Popović, T., Gligorić, N., Radonjic, S., & Šandi, S. (2020, February). A private blockchain implementation using multichain open source platform. *2020 24th International Conference on Information Technology* (IT) (pp. 1-4). IEEE.

Johnson, L., Isam, A., Gogerty, N., & Zitoli, J. (2015). Connecting the Blockchain to the Sun to Save the Planet. *SSRN Eletronic Journal*, 10.2139/ssrn.2702639.

Kang, K. C., Cohen, S. G., Hess, J. A., Novak, W. E., & Peterson, A. S. (1990). Feature-oriented domain analysis (FODA) feasibility study. Technical Report. Software Engineering Institute, Carnegie Mellon University.

Kiff, M. J., Alwazir, J., Davidovic, S., Farias, A., Khan, M. A., Khiaonarong, M. T., ... & Zhou, P. (2020). A survey of research on retail central bank digital currency. *SSRN Eletronic Journal*, 10.2139/ssrn.3639760.

Li, Y., Yang, G., Susilo, W., Yu, Y., Au, M. H., & Liu, D. (2019). Traceable monero: Anonymous cryptocurrency with enhanced accountability. *IEEE Transactions on Dependable and Secure Computing*, 18(2), 679-691.

Makridakis S, Christodoulou K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet*. 11(12):258.

Miers, C. C., Koslovski, G. P., Pillon, M. A., Simplício Jr, M. A., Carvalho, T. C., Rodrigues, B. B., & Battisti, J. H. (2019). Análise de mecanismos para consenso distribuído aplicados a Blockchain. *XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, (São Paulo: Sociedade Brasileira de Computação, 1-49).

Modi, R. (2018). Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain. *Packt Publishing Ltd*, 222p.

Mosley, L., Pham, H., Guo, X., Bansal, Y., Hare, E., & Antony, N. (2022). Towards a systematic understanding of blockchain governance in proposal voting: A dash case study. *Blockchain: Research and Applications*, 3(3), 100085.

Nagothu, D., Xu, R., Nikouei, S. Y., & Chen, Y. (2018, September). A microservice-enabled architecture for smart surveillance using blockchain technology. *2018 IEEE international smart cities conference* (ISC2) (pp. 1-4). IEEE.

Nijsse, J., & Litchfield, A. (2020). A taxonomy of blockchain consensus methods. *Cryptography*, 4(4), 32.

Raval, S. (2016). *Decentralized applications: Harnessing Bitcoin's blockchain technology*. O'Reilly Media, Inc.

Rosenberger, P. (2018). Satoshi Nakamto. *Bitcoin und Blockchain* (pp. 25-34). Springer Vieweg, Berlin, Heidelberg.

Silfversten, E., Favaro, M., Slapakova, L., Ishikawa, S., Liu, J., & Salas, A. (2020). *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*. RAND Corporation.
https://www.rand.org/pubs/research_reports/RR4418.html

Strehle, E., & Steinmetz, F. (2020). Dominating OP returns: the impact of omni and veriblock on bitcoin. *Journal of Grid Computing*, 18(4), 575-592.

Suarez, S., Astor, M. A., Russoniello, A., Bezeira, A. M., Pereira, W., & CICORE, C. (2019). Instalacion y Configuracion de una Red Privada para la Mini-Blockchain Cryptonite.

Thiebes, S., Kannengießer, N., Schmidt-Kraepelin, M., & Sunyaev, A. (2020). Beyond data markets: Opportunities and challenges for distributed ledger technology in genomics. *Proceedings of the 53nd Hawaii international conference on system sciences*.

Tian, Y., Minchin, R. E., Chung, K., Woo, J., & Adriaens, P. (2022). Towards Inclusive and Sustainable Infrastructure Development through Blockchain-enabled Asset Tokenization: An Exploratory Case Study. *IOP Conference Series: Materials Science and Engineering* 1218(1), 012040. IOP Publishing.

Tönnissen, S., Beinke, J. H., & Teuteberg, F. (2020). Understanding token-based ecosystems–a taxonomy of blockchain-based business models of start-ups. *Electronic Markets*, 30(2), 307-323.

Van Hieu, D., Luan, P. H., Hong, T. T., & Khai, L. D. (2021, April). Hardware implementation for fast block generator of Litecoin blockchain system. *2021 International Symposium on Electrical and Electronics Engineering* (ISEE) (pp. 9-14). IEEE.

Veuger, J. (2017). Attention to disruption and blockchain creates a viable real estate economy. *Journal of US-China Public Administration*, 14(5), 263-285.

Yu, Z., Au, M. H., Yu, J., Yang, R., Xu, Q., & Lau, W. F. (2019, February). New empirical traceability analysis of CryptoNote-style blockchains. *International Conference on Financial Cryptography and Data Security* (pp. 133-149). Springer, Cham.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105, 475-491.