TECNOLOGIAS DE CONTABILIDADE DISTRIBUÍDAS (DLTS): EVOLUÇÃO, DIFERENÇAS, SIMILARIDADES E VANTAGENS

DISTRIBUTED LEDGER TECHNOLOGIES (DLTS): EVOLUTION, DIFFERENCES, SIMILARITIES AND ADVANTAGES

Reginaldo José da Rosa 1
Rogério Hermínio da Silva 2
Roderval Marcelino 3
Vilson Gruber 4

Resumo: *As novas tecnologias da informação e comunicação (NTICs), vem alterando a forma de vida e trabalho das pessoas e organizações. Entre estas tecnologias emergentes, algumas vem sendo destaque como por exemplo: Inteligência Artificial, Big Data e tecnologias de contabilidade distribuídas (DLTs). As DLTs são a base das criptomoedas, sendo a mais famosa o Bitcoin, baseado na tecnologia Blockchain. O objetivo deste artigo é discutir as diferenças, evolução, similaridades e vantagens das DLTs. Para isto uma breve descrição das principais DLTs é apresentada. Por fim uma análise comparativa foi efetuada. A metodologia utilizada foi a realização de uma pesquisa sistêmica pelas palavras chaves Blockchain e Tangle. Posteriormente através de uma pesquisa exploratória o estudo foi ampliado com as tecnologias Ethereum, Hyperledger e Hashgraph. O resultado foi uma linha do tempo e duas tabelas que possibilitou identificar a evolução, diferenciação e similaridades entre as DLTs estudadas.*

Palavras-chave: *DLT. Blockchain. Tangle. Ethereum. Hyperledger.*

Abstract: *The new information and communication technologies (NICTs) have been changing the way of life and work of people and organizations. Among these emerging technologies, some have been highlighted as for example: Artificial Intelligence, Big Data and Distributed Ledger Technologies (DLTs). DLTs are the basis of cryptocurrency, the most famous of which is Bitcoin, based on Blockchain technology. The purpose of this article is to present the differences, evolution, similarities and advantages of DLTs. For this a brief description of the main DLTs is presented. Finally, a comparative analysis has been made. The methodology used was the performance of a systemic search by the key words Blockchain and Tangle. Subsequently through an exploratory research the study was expanded including Ethereum, Hyperledger and Hashgraph. The result was a timeline and two tables that allowed to identify the evolution, differentiation and similarities between the DLTs studied.*

Keywords: *DLT. Blockchain. Tangle. Ethereum. Hyperledger.*

1 Mestre em Tecnologias da Informação e Comunicação, UFSC. Lattes: http://lattes.cnpq.br/0867818249544967. ORCID: https://orcid.org/0000-0003-0207-0056. E-mail: rjrosa72@gmail.com

2 Graduado em Gestão de TI, Universidade Federal de Santa Catarina. Lattes: http://lattes.cnpq.br/8848143720129694. ORCID: https://orcid.org/0000-0002-6781-8902. E-mail: rogerioherminio@outlook.com.br

3 Doutor em Engenharia, UFRGS. Lattes: http://lattes.cnpq.br/0122916218414168. ORCID:https://orcid.org/0000-0002-5489-0171. E-mail: roderval.marcelino@ufsc.br

4 Doutor em Engenharia, Universidade Federal de Santa Catarina. Lattes: http://lattes.cnpq.br/5501474017902654. ORCID: https://orcid.org/0000-0003-4092-8578. E-mail: vilson.gruber@ufsc.br

Introdução

Atualmente existem mais de 2.000 criptomoedas, sendo a *Bitcoin* de maior notoriedade e trouxe o tema ao alcance da grande massa. Em 2017 a cotação da moeda teve uma elevação superior 1.700%, trazendo seu valor para US$17.549,00 no mês de dezembro, porém em 30 de abril de 2019 sua cotação caiu para US$5.378,62 uma volatilidade muito alta (BUYBITCOINWORLDWIDE, 2019).

Para tentar identificar quais criptomoedas estão bem posicionadas além do *Bitcoin*, em 15 de maio de 2019 realizou-se uma consulta nas principais criptomoedas por ordem de capital de mercado: *Bitcoin*, *Ethereum*, XRP, *Bitcoin Cash*, *Litecoin*, EOS, *Binance Coin*, *Tether*, *Stellar*, *Cardano*, *Tron*, *Monero*, *Dash*, *Bitcoin* SV e IOTA (COINMARKETCAP, 2018).

Como o *Bitcoin* continua sendo a principal moeda em ordem de capital, esta será utilizada como referência de comparação. O *Bitcon* possui como base o protocolo *Blockchain*, o qual possui algumas deficiências, sendo uma delas apresentar baixa performance de escalabilidade da rede onde o torna vulnerável à criação de falsas transações utilizando computação quântica. Pensando no futuro e suprir estas lacunas surgiram novas DLTs e algumas variações do *Blockchain*, entre elas estão *Ethereum*, *Tangle*, *Hyperledger* e *Hashgraph*. Estes protocolos possibilitam a criação de um livro razão distribuído (*Ledger*), onde permite que as transações realizadas possuam características como imutabilidade, descentralização e dispensa de um órgão regulador, pois a validação ocorre pelo consenso dos participantes da rede (KUO; KIM; OHNO-MACHADO, 2017).

Devido estas características das DLTs, além da utilização em criptomoedas o mercado tem procurado aplicar estes protocolos para resolver problemas de negócio, buscando otimização de recursos e eliminação de intermediários. Os contratos inteligentes, por exemplo, podem ser utilizados para solucionar alguns destes problemas.

Este artigo apresenta através de uma tabela o comparativo entre as seguintes DLTs: *Blockchain*, *Ethereum*, *Tangle*, *Hyperledger* e *Hashgraph*, abordando itens como sua resistência ao quantum, cobrança de taxas, escalabilidade, taxa de transferência e contratos inteligentes. Em uma segunda tabela são confrontados os principais algoritmos de consenso: *proof of stake, proof of works, proof of elapsed time, simplified byzantine fault tolerance e proof of authority*, tratando itens como funcionamento e exemplos de utilização. E por fim, através de uma linha do tempo apresenta a evolução das tecnologias DLT estudadas.

Método da Pesquisa

Este estudo originou-se da necessidade da comparação entre as tecnologias DLTs: *Blockchain* e *Tangle*. Através de buscas exploratórias definimos o construtor (*Blockchain and* IOTA) como estratégia de busca. No dia 22 de agosto de 2018 foi efetuada uma consulta nas bases *Web of Knowlwdge(WoS), Scopus* e IEEE, onde foi encontrado dois artigos em cada. Em seguida realizou-se uma validação inicial e identificado que um destes artigos estava repetido. Desta forma eliminando um destes artigos esta pesquisa resultou em um total de cinco artigos, após a leitura, efetuou-se uma análise complementar através de busca em websites encontrando três artigos adicionais. Além destes artigos a pesquisa foi complementada com links de websites conforme tabela 1.

Tabela 1. Resultado da Pesquisa nas bases de dados.

Base de Dados	Quantidade de Artigos
IEEE	*2*
Scopus	*2*
Websites	*25*
WoS	*2*

Fonte: Autores.

Após a revisão bibliográfica efetuada, foi desenvolvida uma linha do tempo para melhor compreensão da cronologia das DLTs estudadas. Além da linha do tempo foi desenvolvidos dois quadros, um deles comparando as características das DLTs e o outro apresenta um comparativo dos principais algoritmos de consenso.

Fundamentação Teórica das DLTs

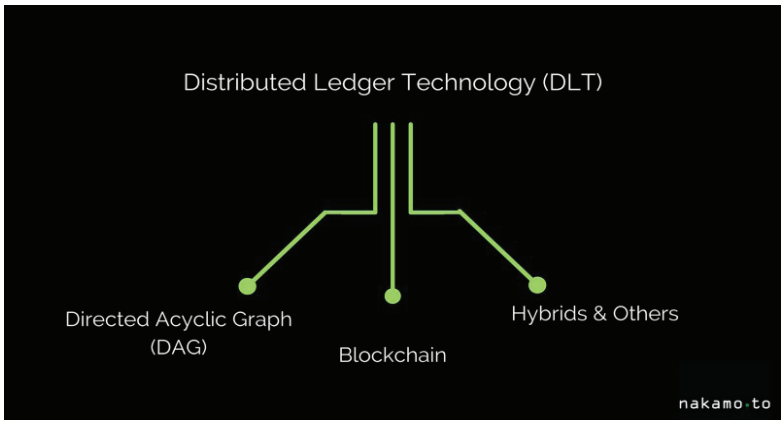
Tecnologias de Contabilidade Distribuídas

As DLTs são um livro de registros descentralizados, ou seja, um banco de dados distribuídos que possui diversos participantes conhecidos ou desconhecidos, tornando-o difícil de ser violado pois cada participante possui uma cópia de todos os registros. Além disto possui características como: dispensar a dependência de agentes reguladores, obter consenso e imutabilidade das transações e dados (KUO; KIM; OHNO-MACHADO, 2017).

As DLTs são um conjunto de dados distribuídos em vários locais, usando redes P2P[1], onde todas as alterações no *Ledger* são refletidas em todas as cópias da rede (FLOREA, 2018).

É possível encontrar definições onde o *Blockchain* é confundido com DLT, isto se dá porque o *Blockchain* foi a primeira implementação funcional de uma DLT. A figura 1 mostra que o *Tangle* e *Blockchain* são DLTs, embora o *Tangle* (representado na imagem por DAG) não seja um *Blockchain*, como será apresentado mais a diante.

Figura 1. Tipos de DLTs.



Fonte: (THAKE, 2018)

A seguir serão detalhadas as tecnologias: *Blockchain*, *Ethereum*, *Hyperledger*, *Tangle* e *Hashgraph*.

Blockchain

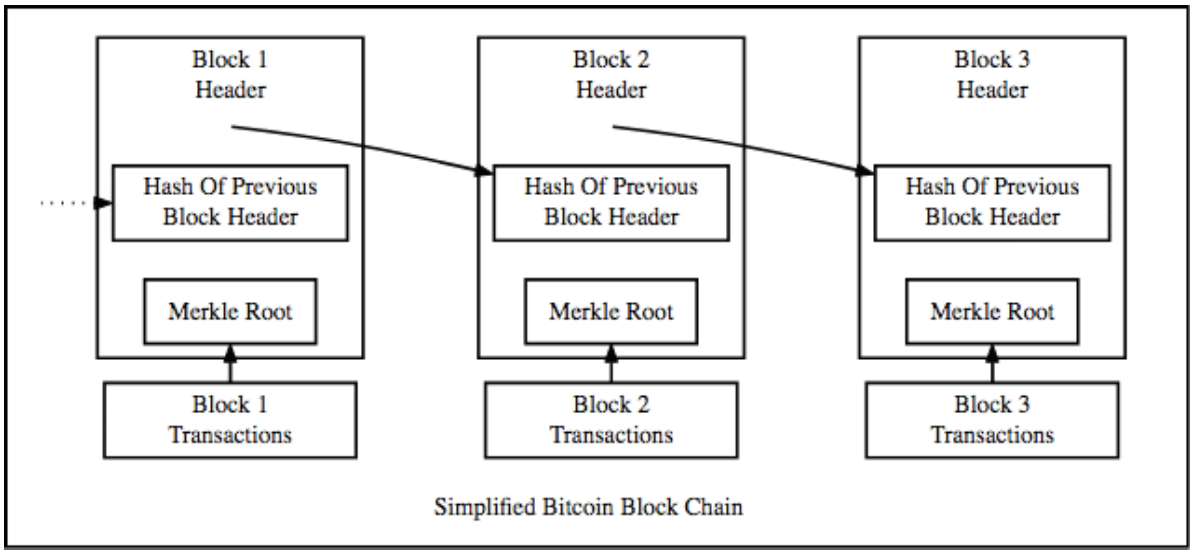
A tecnologia *Blockchain* foi introduzida em 2008 por Nakamoto (2008), como uma plataforma para transações seguras e anônimas, usando uma rede descentralizada de computadores ou dispositivos.

O *Blockchain* alcança o consenso usando funções criptográficas com dificuldade crescente, utilizando o poder computacional da rede mantida pelos mineradores, participantes que disponibilizam seus computadores para verificar, transmitir e registrar as transações no *Ledger*. A segurança é fornecida usando o *hash*[2] criptográfico resultante do bloco anterior como ponto de partida para o próximo bloco, gerando assim a cadeia de blocos, como visto na figura 2.

1 P2P designativo de uma rede em que os computadores comunicam e trocam dados entre si diretamente, sem a necessidade de um servidor central a gerir essa comunicação; posto a posto, ponto a ponto, par a par.

2 A função *hash* fornece segurança e integridade a informação, pois uma simples alteração no texto original resulta em um novo *hash* totalmente diferente. Não importando o tamanho da entrada, a saída terá sempre o mesmo tamanho (UPADHYAYA; SHARMA; ARUN, 2017)

Figura 2. Esquema simplificado de um Blockchain.

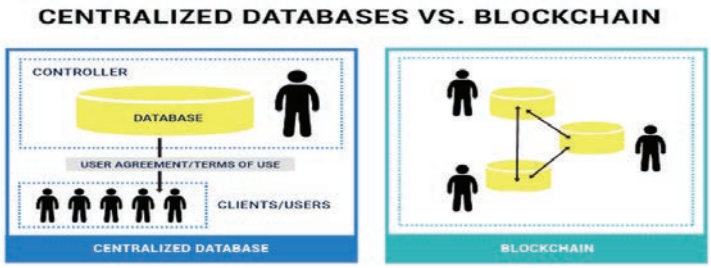


Fonte: (ISOIN, 2019)

A característica mais importante da tecnologia *Blockchain* é a imutabilidade dos dados. Uma vez que um bloco tenha sido validado pela rede, seu *hash* resultante é usado no próximo bloco. Se um participante tentar alterar um bloco existente e o transmitir para a rede, este não será aceito, já que ele altera seu *hash* calculado e assim necessita alterar todos os *hashes* de blocos subsequentes. A rede rejeitará tal alteração, desde que a capacidade computacional da rede permaneça neutra. A Figura 3 ilustra a diferença entre uma *Blockchain* e uma base de dados centralizada (NAKAMOTO, 2008).

Wahab, Barlas e Mahmood (2018) destacam que as principais características do *Blockchain* são: Imutabilidade, distribuída, criptografada, confiabilidade e consenso.

Figura 3. Base de dados centralizada x Blockchain



Fonte: (BLOCKSPLAIN, 2018)

Com o aumento do uso da rede *Blockchain* surgiram algumas limitações ou desvantagens: o incremento da dificuldade da função de *hashing*, que resulta em altos tempos de transação, consumo de energia elétrica e de processamento (FLOREA, 2018). Isso levou ao desenvolvimento de *Blockchains* alternativos, com diferentes abordagens para validação de blocos, como a *Ethereum*, *Hyperledger* e também outros modelos. O *Tangle* é uma nova abordagem de DLT para aplicativos distribuídos e com dispositivos de internet das coisas (IoT).

A arquitetura do *Blockchain* sobretudo possui alguns pontos que receberam críticas: Necessita de mineração, além desta atividade concentrar-se na mão de poucos, estes estão localizados principalmente na China; Necessita de alto poder de processamento e consumo de energia; Tarifação por transações; O tempo médio para uma transação entrar na rede é de 10 minutos, podendo levar mais de 1 hora para aparecer no *Ledger*.

Problemas de segurança relatados: Gasto em dobro, ataque de 51%, Mineração Egoísta

e não resistência a computação quântica.

Ethereum

De acordo com Maltawinds (2018) Vitalik Buterin foi o criador da *Ethereum*, em janeiro de 2014, uma variante do *Blockchain*. Ele implementou o contrato inteligente[3], além da criptomoeda Éther.

Segundo a Blockgeeks (2018) o *Ethereum* inaugurou a segunda geração do *Blockchain* com a implementação dos contratos inteligentes. Estes são facilmente programáveis, que o torna simples, mas vulnerável a erros de programação (intencionais e não intencionais), permitindo ataques de *hackers* e tornando-o menos seguro. Para que o contrato funcione é necessário programá-lo e gerar os aplicativos denominados *Dapps*. O protocolo ERC20 foi especificado com intuito de permitir a interoperabilidade de aplicativos e plataformas. O mesmo possui algumas fragilidades, pois requer algumas sequencias de códigos e pressupõem que os programadores não cometerão erros. Novas especificações mais seguras já foram implementadas como o ERC233 e ERC777, porém o ERC20 continua sendo o mais utilizado. A figura 4 representa um esquema do funcionamento de um contrato inteligente (MOLECKE, 2018). Para que os contratos inteligentes sejam executados é necessário utilizar a Máquina Virtual *Ethereum* (EVM), e o programador gerar seu código na linguagem *Solidity* (muito parecida com *JavaScript*), que após compilado gerará o *bytecode* de nível de máquina. Outras linguagens como a *Serpent* também podem ser utilizadas desde que gerem os *bytecode* EVM.

Assim como o *Ethereum* é uma variante do *Blockchain*, existe a NEO que é uma variante da própria *Ethereum*. Estas variantes surgem com propósitos diferentes ou mesmo para corrigir algumas deficiências das originárias. O NEO é considerado o *Ethereum* da China, utilizando a mesma EVM, porém com flexibilidade na linguagem de programação, permite uso do Java, Go, C# e *JavaSctipt*.

Figura 4. Infográfico do funcionamento de um Contrato Inteligente

Fonte: (ROSIC, 2018b)

A *Ethereum* pretende implementar duas soluções para resolver problemas de performance do *Blockchain*: prova de participação ou *Proof of Stake* (PoS) e a fragmentação (*Sharding*) (MALONEY, 2018). Isso permitirá que os usuários realizem mais transações sem congestionamentos e lentidão, além de torná-la ainda mais segura e mais rápida que qualquer outra moeda pública baseada em *Blockchain* (MALONEY, 2018). São dois projetos distintos, mas que estão sendo trabalhados de forma conjunta devido suas estruturas. A previsão para entrega do PoS é para o final de 2019 e o *Sharding* para 2020. A equipe de desenvolvimento tem chamado o projeto de *Ethereum* 2.0.

3 Contratos inteligentes não estará disponível no núcleo do protocolo, mas em desenvolvimento como uma camada adicional.

Blockchain permissionada

Blockchain permissionadas ou privadas, são implementações de *Blockchain* com limitações de acesso, seu desenvolvimento foi focado nas instituições financeiras. Exemplos de redes permissionadas: Corda, *HyperLegder*, *Quorum*, *Ethereum* permissionado. Já foram relatados problemas de segurança, já que alguns usuários podem ter permissão para a inclusão de registros. (WAHAB; BARLAS; MAHMOOD, 2018).

Como o mercado corporativo vem demandando de pesquisas sobre o *Blockchain*, algumas soluções estão sendo apresentadas:

A Accenture criou um protótipo de um recurso que permite a *Blockchain* ser editada em circunstâncias excepcionais para resolver erros humanos, acomodar exigências legais e regulatórias. Esta implementação oferece um recurso no qual qualquer edição feita em um bloco deixa uma "cicatriz" imutável, indicando que o bloco foi alterado (WAHAB; BARLAS; MAHMOOD, 2018).

O JPMorgan Chase está considerando tornar o *Quorum* sua plataforma *Blockchain* de contratos inteligentes em sua própria empresa que é executada no *Ethereum* (COINTELEGRAPH, 2018).

A Corda é uma ferramenta altamente especializada para utilização nas instituições financeiras. Sua característica chave é que a plataforma não usa *Blockchain* no sentido usual da palavra. Em vez disso, são utilizados nós notários especiais. As transações feitas em Corda não são transmitidas para todos os participantes. As entradas no banco de dados estão disponíveis apenas para os membros da rede que têm o direito de visualizá-los e gerenciá-los (BTCSOUL, 2018).

O *Hyperledger Fabric* é um exemplo de implementação de uma estrutura projetada para atender aos seguintes requisitos corporativos: alto desempenho, Alta Resiliência e Privacidade (BLOCKGEEKS, 2019).

Hyperledger

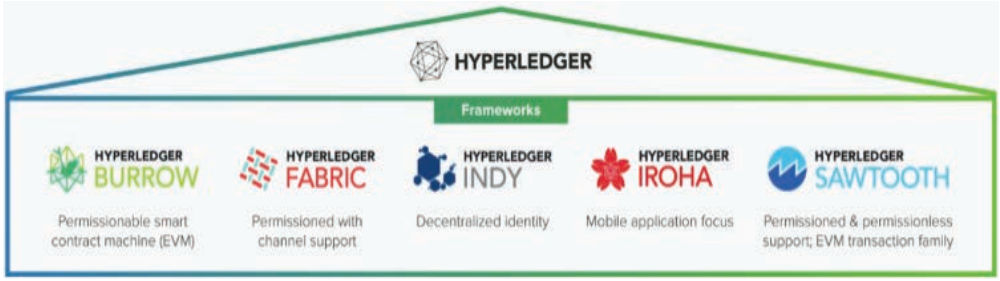
Fundada em dezembro de 2015 pela Fundação Linux, conta com mais de 100 membros. Entre estes membros estão algumas das gigantes de diversos segmentos, como: Airbus, Daimler, IBM, Fujitsu, SAP, Huawei, Nokia, Intel, Samsung, Deutsche Börse, American Express, JP Morgan, BNP Paribas e Well Fargo (AMEER ROSIC, 2018a).

Em seu planejamento foi definido que o *Hyperledger* não irá criar sua própria moeda, mas servirá para criar aplicações industriais da tecnologia *Blockchain*, por meio de uma estrutura distribuída de código aberto de nível corporativo.

Como um HUB para o desenvolvimento de *Blockchain* industrial aberto, a figura 5 apresenta diversos projetos suportados pela Fundação Linux: *Hyperledger Burrow, Hyperledger Fabric, Hyperledger Indy, Hyperledger Iroha* e *Hyperledger Sawtooth* (ROSIC, 2018a).

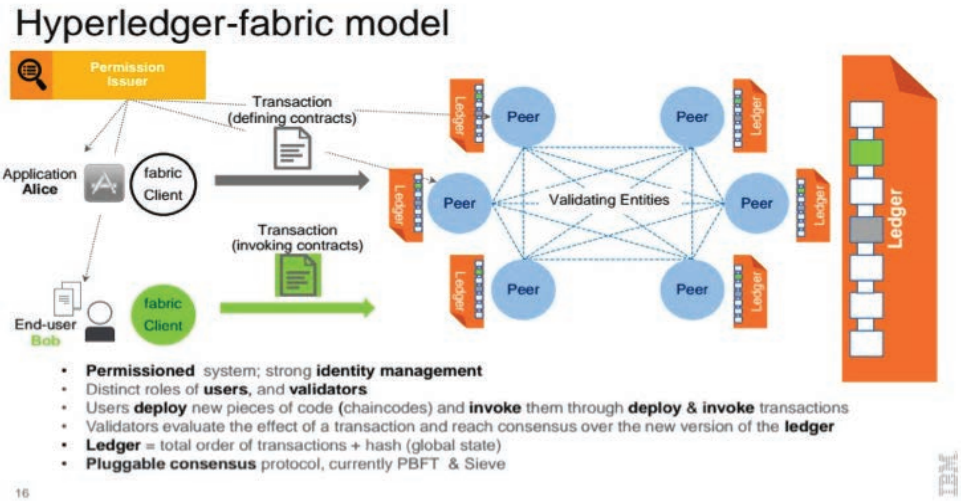
O *Hyperledger Fabric* da IBM, foi projetado para que as empresas criem suas próprias redes *Blockchain* e pode escalar até 1000 transações por segundo. Seu *framework* foi desenvolvido na linguagem GO e seu contrato inteligente chama-se *Chaincode*. Os contratos são executados no *container Docker*, similar a EVM do *Ethereum*. Sua estrutura permite interagir com a rede pública ou privada. Não necessariamente é uma *Blockchain* permissionada, mas este é seu grande trunfo, devido a sua privacidade e escalabilidade, pois diferentemente do projeto inicial de Satoshi, separa os mineradores e nós de consenso. Para aumentar a eficiência o *Fabric* possui uma quantidade menor de nós e permite cálculos paralelos. A figura 6 apresenta um modelo conceitual do *Hyperledger Fabric*.

Figura 5. Guarda chuva dos projetos Hyperledger da Fundação Linux



Fonte: (HYPERLEDGER, 2018)

Figura 6. Modelo conceitual do Hyperledger Fabric



Fonte: (ROSIC, 2018a)

Tangle

Conceituado em 2014 por David Sonstebo, Sergey Ivancheglo, Dominik Schiener e Dr. Serguei Popov. O *Tangle* é um novo tipo de DLT, que visa mitigar duas das questões mais importantes das atuais soluções *Blockchain*: altas taxas de transação e alto tempo de processamento. Fornece um modelo de transação sem taxas para a realização de micropagamentos[4] utilizando os dispositivos IoT (FLOREA, 2018).

O *Tangle* é considerado uma evolução da DLT, voltada para o domínio da IoT, é construído no *Directed Acyclic Graph* (DAG) uma estrutura de dados baseados em grafos com NÓS ou vértices representando cada transação, e promete resolver boa parte das principais desvantagens do *Blockchain* (WAHAB; BARLAS; MAHMOOD, 2018).

A principal vantagem dessa abordagem é a escalabilidade da rede, enquanto no *Blockchain* isto está se tornando um problema, pois a velocidade da rede diminui com o aumento das transações. No *Tangle* é completamente o oposto, quanto mais transações na rede, maior a velocidade. Em vez de encadear as transações de forma linear, elas são armazenadas de maneira semelhante a um grafo. A figura 7 mostra a diferença entre o *Tangle* e *Blockchain* (BURGER, 2018).

No *Tangle*, transações recém-anexadas são chamadas de "dicas". Como cada nova transação faz referência a duas transações anteriores, a rede selecionará duas dicas não confirmadas, às quais a nova transação se anexará. As duas transações são validadas por suas assina-

4 Micropagamentos se referem a pagamentos de valores baixos, cujo as taxas são altas, até mais altas que os valores a serem pagos, isso inibe este tipo de transação. Atualmente já existem criptomoedas com taxas muito baixas tornando esta operação viável (BENGHI, 2018).

turas. Se as dicas são validadas, a nova transação é anexada ao *Tangle*, mas também confirma todas as outras transações ligadas pelas duas pontas, gerando um caminho de validação. Isso aumenta a confiança de todas as transações do caminho de validação. Quanto mais transações forem adicionadas, maiores serão os níveis de certeza de confirmação no caminho de transações. As dicas são escolhidas aleatoriamente utilizando um método chamado *Markov Chain Monte Carlo* (MCMC).

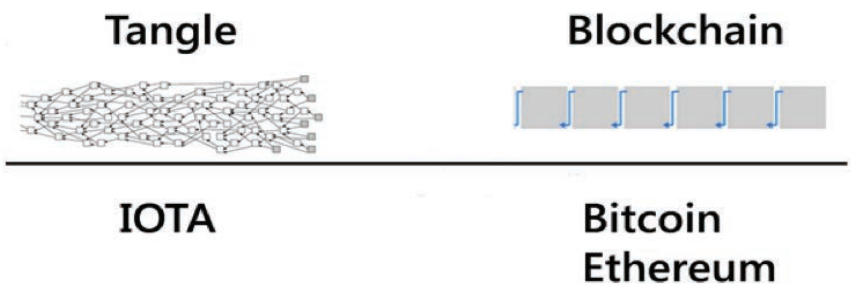
Uma coisa muito importante a ser observada que diferencia o *Tangle* de outros sistemas do tipo *Blockchain*, é que os cálculos da *Proof of Work* (POW) devem ser feitos localmente pelo dispositivo que inicia a transação (cliente), mas eles também podem ser delegados ao NÓ que o dispositivo está conectado e é somente executada ao gerar a nova transação.

A taxa zero é possibilitada pois todo participante da rede faz algum trabalho computacional, não necessitando de mineradores, porque não requer alto poder computacional.

Outras características do *Tangle*: baixo poder de processamento para inserir e validar transações; baixo consumo de tempo para validação do consenso; resistência a computação quântica; altamente escalável.

Sobre os contratos inteligentes, a fundação IOTA sua mantenedora, sinaliza que não apoia seu desenvolvimento com suporte nativo, poderá ser disponibilizado como uma camada adicional (ROTTMANN, 2018).

Figura 7. Representação do Tangle e Blockchain



Fonte: (BURGER, 2018)

Hashgraph

O *Hashgraph* usa um método totalmente diferente de compartilhar informações e estabelecer consenso, a fofoca. Um participante da rede é obrigado a compartilhar todas as informações sobre transações com múltiplos outros nós selecionados aleatoriamente (BAIRD; HARMON; MADSEN, 2018). No *Blockchain* o *hash* do bloco anterior é armazenado no novo bloco, todavia no *Hashgraph* o próximo nó combinará as informações recebidas com as informações de outros participantes e adicionará informações sobre novas transações que retransmitirá até que todos estejam cientes das informações criadas no início. Neste caso, além das informações da transação, data e hora são passadas também as informações sobre os receptores anteriores, caracterizando assim a fofoca sobre a fofoca (SCHUEFFEL, 2018).

No *Hashgraph* com a fofoca sobre fofoca é criado um mecanismo de consenso inteiramente novo, o chamado voto virtual. Como cada nó da rede tem uma cópia do histórico de transações juntamente com informações sobre quem mais recebeu as informações, todo participante pode calcular qual seria a reação dos outros nós, pois conhece a decisão um do outro sem nunca ter votado.

No *Blockchain* tradicional a comunidade gasta muito poder computacional com os cálculos para o PoW que reduz a velocidade de mineração. Isso faz com que seja necessário investir muito em hardware e energia elétrica para minerar. No *Hashgraph* e em algumas variantes de moedas virtuais, esse problema não existe, pois foi eliminada há necessidade de PoW (MOREIRA, 2018).

Mas o *Hashgraph* é uma tecnologia proprietária, criada em 2016 por Leemon Baird e pelo time da Swirlds. Até o momento o *Hashgraph* só foi implementado em ambientes privados. Seus desenvolvedores afirmam que ela é muito rápida, permitindo mais de 250.000 transações por segundo, porém como não foi implementado em ambiente público, estará sujeito aos mesmos desafios de outras tecnologias DLTs, como segurança e desempenho.

A Swirlds possui os direitos de propriedade intelectual no algoritmo de consenso de *Hashgraph* e caso as empresas o utilizem em uma rede privada estarão sujeitas a pagamento de taxas à proprietária, todavia se utilizar a plataforma pública nenhuma licença será solicitada. Sendo uma tecnologia proprietária a empresa não permite que seu código seja utilizado para criação de novas variantes, mas os desenvolvedores são livres para criar seus *Dapps* ou contratos inteligentes sobre a plataforma *Hedera*, utilizando a linguagem *Solidity*, 100% compatível com os contratos já criados em outras plataformas (BAIRD; HARMON; MADSEN, 2018).

Resultados e Discussões

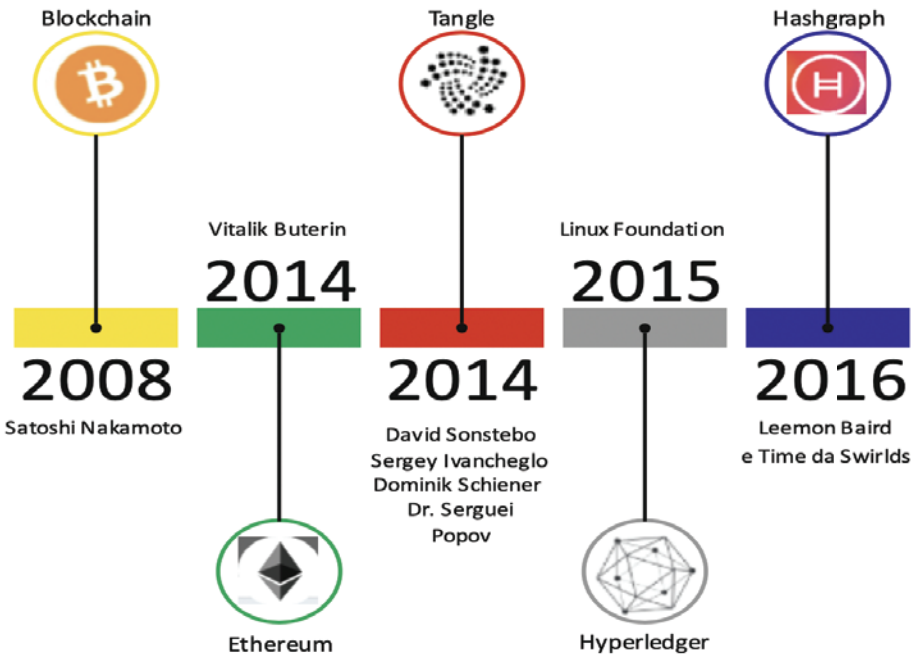
Neste estudo foi descoberto que a primeira tecnologia de DLT funcional foi o *Blockchain* e se popularizou com a criptomoeda *Bitcoin*. Para entender melhor como foi o seu surgimento e adaptação, foi construída uma linha do tempo conforme a figura 8 para apresentar de forma cronológica os protocolos estudados: *Blockchain, Ethereum, Tangle, Hyperledger* e *Hashgraph.*

O *Blockchain* introduziu uma tecnologia nova no mercado com sua estrutura que permite eliminar os intermediários em uma transação através do consenso obtido com o uso dos trabalhos realizados pelos mineradores. Com suas características de imutabilidade dos dados, aplicação de *hash* e distribuída, chamou a atenção de toda comunidade e do mercado.

O *Ethereum* surgiu com a intenção de ser uma versão melhorada do *Blockchain*, adicionando a funcionalidade de contratos inteligentes, maior escalabilidade e performance. Em termos de performance o *Ethereum* está buscando implementar até 2020 um algoritmo de consenso com performance superior que é o PoS. O *tangle* surge com o propósito de eliminar as taxas de transação, permitindo os micropagamentos, além de eliminar a vulnerabilidade a computação quântica.

Em relação ao *Hyperledger*, este foi desenvolvido para ambiente empresarial como uma *Blockchain* permissionada, e em seu planejamento foi definido que não será utilizado para criar criptomoedas.

Figura 8. Linha do tempo das DLT estudadas



Fonte: Autores.

Por último o *Hashgraph* elimina os cálculos computacionais PoW, sendo que possui uma forma de consenso própria, com a expectativa de atingir 250.000 transações por segundo 10 vezes mais que a VISA (BLOCKSPLAIN, 2018).

De acordo com a linha do tempo elaborada pode-se evidenciar que nos últimos doze anos houve evolução significativa nas tecnologias DLTs. O *Blockchain* por exemplo em 2008 introduziu a segurança para transações de forma distribuída. Com a utilização do *Blockchain* em larga escala, novas tecnologias computacionais surgiram para mitigar problemas de segurança, performance, escalabilidade e aplicações empresarias.

Através do quadro 1 foram apresentadas quais tecnologias atendem ou não as principais características apresentadas neste artigo. Para aplicação pensada em uma resistência a computação quântica, que ainda está em desenvolvimento, as tecnologias *Tangle* e *Hashgraph* são as mais indicadas. Já pensando em baixo custo com taxas de transações o *Hyperledger* e o *Tangle* são os mais indicados, o *Hashgraph* mesmo não possuindo taxas de transação está sujeito a licenciamento sendo que não é código livre. No quesito escalabilidade o destaque fica para o *Tangle*, devido sua tecnologia, quanto maior o número de nós maior a performance o contrário do *Blockchain* onde quanto maior o número de blocos menor a performance. Para utilização de contratos inteligentes o *Ethereum* foi o que introduziu a tecnologia e o *Hyperledger* foi desenvolvido com perfil corporativo.

Quadro 1. Comparação das tecnologias DLT apresentadas neste artigo

CARACTERÍSTICAS	BLOCKCHAIN	ETHEREUM	HYPERLEDGER	TANGLE	HASHGRAPH
Resistência ao Quantum	Não	Não	Não	Sim	Sim
Sem taxas	Não	Não	Sim	Sim	Sim
Escalável	Não	Não	Sim	Sim	Sim
Taxa de transferência	Baixa	Média	Média	Alta	Alta
Contratos inteligente	Não	Sim	Sim	Sim	Sim

Fonte: Autores.

Todas as criptomoedas ou tecnologias permissionadas precisam de algum tipo de algoritmo de consenso para garantir que as transações são válidas.

Quadro 2. Comparativo entre os principais algoritmos de consenso

Algoritmo de Consenso	Como é seu funcionamento	Exemplos de onde é utilizado
Proof of Stake	No caso do PoS, o algoritimo *"Prof of Stake"* é uma generalização do mecanismo *Proof of Work*, no *PoS* os nós são conhecidos como "validadores" e ao invés de minerarem o *Blockchain*, eles validam a transação e como retorno recebem uma taxa. Os validadores com maior quantidade de moedas possuem maior poder de aprovarem o próximo bloco e serem recompensados. No caso das moedas que utilizam PoS, as mesmas não utilizam mineração sendo que todas as moedas são criadas desde o primeiro dia (EDX, 2018).	*DASH, NEO, PIVX, OkCash, Stratis, Reddcoin*
Proof of Works	O Algoritmo de consenso *PoW,* é utilizado em criptomoedas como o *Bitcoin* para resolver um quebra-cabeça computacional para que assim possa ser criado o próximo bloco do *Blockchain*. O processo é conhecido como mineração, e todos os nós engajados na resolução deste bloco são mineradores. A iniciativa de mineração se dá por retorno financeiro, onde os mineradores que estão competindo recebem como retorno 12,5 *Bitcoins* no caso da mineração de *Bitcoin* e 5 ETC no caso da mineração de Ethereum, além de uma pequena taxa de transação (EDX, 2018).	*Bitcoin, Ethereum, Litecoin, Dogecoin*

Proof of Elapsed Time	No *Proof of Elapsed Time*, cada participante na rede de Blockchain precisa esperar um tempo randômico, sendo assim o primeiro participante a finalizar a espera se torna o líder do próximo bloco (RILEE, 2018).	*Sawtooth*
Simplified Byzantine Fault Tolerance	O *Simplified Byzantine Fault Tolerance* é um algoritmo de consenso que resolve o problema geral de *Byzantine* para ambientes assíncronos. O *Simplified Byzantine Fault Tolerance*, assume que menos de um terço dos nós são maliciosos. Para cada bloco ser adicionado na corrente, um líder é selecionado para ser encarregado de ordenar as transações. Esta seleção deve ser suportada por ao menos 2/3 de todos os nós, que devem ser conhecidos pela rede.	*Hyperledger*
Proof of Authority	Neste tipo de algoritmo os blocos são validados por contas aprovadas, conhecidas como validadores. Os validadores deixam um programa executando em seus computadores e assim recebem algumas moedas como recompensa. A prova de autoridade nada mais é do que uma prova de participação mais restrita, onde a participação somente será permitida se você for um validador (HOSE, 2018).	*Vechain*

Fonte: Autores.

Estes algoritmos garantem que todos os participantes na rede venham a possuir exatamente os mesmos dados além de prevenir a manipulação de dados por atores maliciosos (EDX, 2018). O quadro 2 acima apresenta um comparativo entre os cinco principais algoritmos de consenso, com um breve resumo de suas aplicações, fazendo um relacionamento de exemplos práticos de sua utilização.

Considerações Finais

Este artigo teve como objetivo estudar as DLTs, apresentando as diferenças, similaridades e vantagens de cada um dos protocolos estudados (*Blockchain*, *Ethereum*, *Tangle*, *Hyperledger* e *Hashgraph*). Estes protocolos podem coexistir sendo que um único não é solução para todos os problemas, estes devem ser escolhidos de forma cautelosa de acordo com sua aplicação e necessidade. Com base neste estudo, conclui-se que o *Tangle* é o único que não é considerado uma *Blockchain* e indicado para o ambiente de IoT. Já para uso nas corporações indica-se o *Hyperledger*, por possuir características que remetem a uma melhor performance e por possui contratos inteligentes. O *Ethereum* tem ênfase para utilização de contratos inteligentes no domínio das redes públicas. O *Hashgraph* por ser uma tecnologia proprietária e a mais recente não recomendamos para uso corporativo. Como exemplo prático da utilização das DLTs podemos citar: controle de transações financeiras, logística de precisão, saúde, agricultura, leilões, todas utilizando contratos inteligentes.

A linha do tempo apresenta a evolução das DLTs ocorrida na última década, trazendo características como: imutabilidade, descentralização e dispensa de um órgão regulador também para as aplicações corporativas. Alguns entusiastas estão considerando que as DLTs serão tão importantes para as transações como a internet é para a informação hoje (MANO, 2017).

Houve dificuldade de encontrar publicações comparativas entre o *Tangle* e as demais tecnologias DLTs, possivelmente devido o *Tangle* não usar a mesma arquitetura *Blockchain*. Outra dificuldade foi de localizar publicações cientificas referente às DLTs, desta forma a maioria das referências são de pesquisa exploratória na web.

As tecnologias de DLT podem ser ótimas aliadas aos negócios principalmente devido a segurança embarcada, como a rastreabilidade e imutabilidade.

Referências

BAIRD, L.; HARMON, M.; MADSEN, P. H.: A Governing Council & Public Hashgraph Network: **The trust layer of the internet**. 2018. Disponível em: <https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf>. Acesso em: 17 jan. 2019.

BENGHI, F. **Você já ouviu falar sobre micropagamentos?** 2018. Disponível em: <https://blog.cedrotech.com/o-que-sao-micropagamentos-e-como-se-beneficiar/>. Acesso em: 02 maio 2019.

BLOCKGEEKS. **A Deeper Look at Different Smart Contract Platforms**. Disponível em: <https://blockgeeks.com/guides/different-smart-contract-platforms/>. Acesso em: 05 ago. 2018.

_____. **What Are Enterprise Blockchains?** Disponível em: <https://blockgeeks.com/guides/enterprise-blockchains/>. Acesso em: 16 ago. 2019.

BLOCKSPLAIN. **Blockchain speeds & the scalability debate.** Disponível em: <https://blocksplain.com/2018/02/28/transaction-speeds/>. Acesso em: 29 ago. 2018.

BTCSOUL. **Grupo R3 introduz plataforma Corda v.1.0.** Disponível em: <https://www.btcsoul.com/noticias/grupo-r3-introduz-plataforma-corda-v-1-0/>. Acesso em: 02 set. 2018.

BURGER, A. **IOTA Tangle Takes the Blocks Out of Peer-to-Peer, Distributed Ledger Networks.** Disponível em: <http://microgridmedia.com/iota-tangle-takes-blocks-peer-peer-distributed--ledger-networks/>. Acesso em: 15 ago. 2018.

BUYBITCOINWORLDWIDE**. Buy Bitcoin Worldwide.** Disponível em: <https://www.buybitcoinworldwide.com/pt-br/preco/>. Acesso em: 30 abr. 2019.

COINMARKETCAP. **CoinMarketCap**. Disponível em: <https://coinmarketcap.com/pt-br/all/views/all/.>. Acesso em: 01 ago. 2018.

COINTELEGRAPH. Presidente da CFTC dos EUA: **Precisamos testar o Blockchain porque estamos "quatro anos atrasados".** Disponível em: <https://br.cointelegraph.com/news/u-s-cftc--chair-we-need-to-test-blockchain-because-we-are-four-year>. Acesso em: 01 set. 2018.

EDX. **Blockchain-for-Business - An Introduction to Hyperledger Technologies.** Disponível em: <https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/course/.>. Acesso em: 05 ago. 2018.

FLOREA, B. C. Blockchain and Internet of Things data provider for smart applications. In: **MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING, 17914987**., 2018, Budva. 2018 7th Mediterranean Conference on Embedded Computing (MECO). Budva: Ieee, 2018. p. 1 - 4.

HOSE, A. **Rolling your own Proof-of-Authority Ethereum consortium.** Disponível em: <https://blog.enuma.io/update/2017/08/29/proof-of-authority-ethereum-networks.html>. Acesso em: 14 ago. 2018.

HYPERLEDGER. Disponível em: <https://www.hyperledger.org>. Acesso em: 22 ago. 2018.

ISOIN. **Blockchain, la última revolución tecnológica**. Disponível em: <http://www.isoin.es/blockchain-la-ultima-revolucion-tecnologica/>. Acesso em: 20 ago. 2019.

MALONEY, C. Ethereum Sharding Slated for 2020: **ETH Foundation Researcher Justin Drake.** Disponível em: <https://www.ccn.com/ethereum-sharding-slated-for-2020-ethereum-foundation-researcher-justin-drake>. Acesso em: 16 ago. 2018.

MALTAWINDS. **Erc20-tokens-the-origin-story**. Disponível em: <http://maltawinds.com/2018/08/14/erc20-tokens-the-origin-story/>. Acesso em: 20 set. 2018.

MANO, C. **Blockchain é "tão revolucionária quanto a internet".** 2017. Disponível em: <https://exame.abril.com.br/revista-exame/blockchain-e-tao-revolucionaria-quanto-a-internet/>. Acesso em: 7 set. 2017.

MOLECKE, R. How To Learn Solidity: **The Ultimate Ethereum Coding Tutorial.** Disponível em: <https://blockgeeks.com/guides/solidity/>. Acesso em: 05 ago. 2018.

MOREIRA, E. **Descubra o que é Hashgraph, o substituto do blockchain**. Disponível em: <https://transformacaodigital.com/o-que-e-hashgraph-o-substituto-do-blockchain/>. Acesso em: 05 ago. 2018.

KUO, T.; KIM, H.; OHNO-MACHADO, L. Blockchain distributed ledger technologies for biomedical and health care applications. **Journal Of The American Medical Informatics Association.** Cary, p. 1211-1220. 08 set. 2017.

NAKAMOTO, S. **A Peer-to-Peer Eletronic Cash System**. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.221.9986>. Acesso em: 31 out. 2008.

RILEE, K. **Understanding Hyperledger Sawtooth - Proof of Elapsed Time**. Disponível em: <https://medium.com/kokster/understanding-hyperledger-sawtooth-proof-of-elapsed-time--e0c303577ec1>. Acesso em: 18 ago. 2018.

ROSIC, A. **Hyperledger-fabric model**. Disponível em: <https://blockgeeks.com/guides/hyperledger/>. Acesso em: 15 ago. 2018a.

_____. Smart Contracts: **The Blockchain Technology That Will Replace Lawyers.** Disponível em: <https://blockgeeks.com/guides/smart-contracts/>. Acesso em: 03 set. 2018b.

ROTTMANN, R. **About Smart Contracts in IOTA.** Disponível em: <https://medium.com/@ralf/about-smart-contracts-in-iota-626d2bd3619e>. Acesso em: 16 ago. 2018.

SCHUEFFEL, P. Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph: A High-Level Overview and Comparison. **Ssrn Electronic Journal.** Rochester, p. 1-8. mar. 2018.

THAKE, M. **What's the difference between blockchain and DLT?** Disponível em: <https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd>. Acesso em: 22 ago. 2018.

UPADHYAYA, V.; SHARMA, M.; ARUN, A. **Think Blockchain**. 2017. 209 p.

WAHAB, A; BARLAS, M; MAHMOOD, W. Z. C.: A Framework to Authenticate Academic Verifications Using Tangle. **Journal Of Software & Systems Development**. King Of Prussia, p. 1-14. 24 maio 2018. Disponível em: <http://ibimapublishing.com/articles/JSSD/2018/370695/>. Acesso em: 17 maio 2019.

Recebido em 6 de dezembro de 2019.
Aceito em 30 de março de 2020.