

Blockchain e o futuro da confiança nas transações

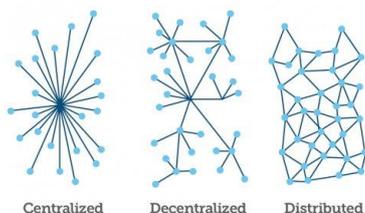
As tecnologias emergentes - aquelas com potencial para criar ou transformar o ambiente de negócios nos próximos anos, mas que ainda não se consolidaram - vêm ganhando cada vez mais espaço na discussão sobre o futuro dos negócios e da sociedade como um todo.

De acordo com o Liga Ventures - Liga Insights Emerging Technologies, essas novas tecnologias despertam grande interesse e são distribuídas em sete categorias:

- Inteligência Artificial / Machine Learning / Deep Learning / ChatBots
- Realidade Aumentada
- Big Data e Analytics
- Blockchain e Criptomoedas
- Cleantechs e Smart Cities
- Drones e Vants
- IoT (Internet das Coisas)

Afinal, o que é Blockchain?

Blockchain é uma tecnologia que permite, por meio de técnicas criptográficas, trazer maior confiança e agilidade nas transações. Funciona como um livro-razão (ledger) distribuído e compartilhado, que contém todas as transações processadas no sistema sem a necessidade de uma autoridade central e confiável para validar as informações (a validação é feita por meio do consenso dos participantes da rede).



Fonte: <http://uk.businessinsider.com/what-is-blockchain-2016-3>

Mas o Blockchain não é uma tecnologia nova. É uma combinação de tecnologias comprovadas e aplicadas de uma nova maneira (internet, criptografia de chave privada e protocolo). O resultado é um sistema para transações digitais que não precisa de um terceiro para intermediá-las (desintermediação).

Sua primeira e mais conhecida implementação foi o Bitcoin, em 2009, permitindo realizar transações e estabelecer confiança, sem intermediários. Todo o funcionamento desse sistema *peer-to-peer* está descrito no artigo de Satoshi Nakamoto intitulado: "Bitcoin um sistema de dinheiro eletrônico de pessoa a pessoa" (www.slideshare.net/rodrigoHenrik/bitcoin-um-sistema-de-dinheiro-eletronico-pontoaponto).

E apesar das muitas críticas com relação ao Bitcoin, é importante ressaltar que os problemas detectados aconteceram em função da implantação da tecnologia e não de sua segurança ou quebra de criptografia.

Como funciona o Blockchain

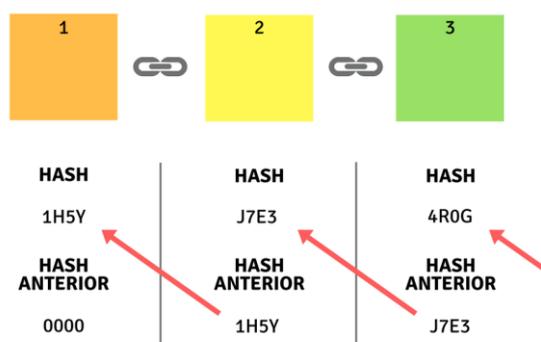


Fonte: <http://blog.simply.com.br/wp-content/uploads/2016/05/blockchain-como-funciona.png>

O conceito de Blockchain é normalmente apresentado explicando como o bitcoin funciona, pois ambos estão intrinsecamente ligados, e um pouco da história do bitcoin sempre ajuda a entender a tecnologia. No entanto, o Blockchain vai além do Bitcoin, sendo aplicável a qualquer transação online de ativos digitais.

Ao se realizar uma transação, ela é armazenada em uma estrutura fixa chamada bloco, assim como as novas transações que geram novos registros devem também ser inseridas em novos blocos.

Dentro da rede, o conjunto de transações registradas em um bloco funciona como um banco de dados. Uma vez que o bloco está completo e alocado de acordo com a sequência de tempo, é enviado por meio da rede, onde é ligado à cadeia.



As transações são validadas por nós da rede com o propósito de fornecer um consenso sobre a transação.

Mas, além do conjunto de transações, é preciso que cada bloco tenha um código que o liga ao anterior (afinal eles estão conectados em cadeia), bem como um código próprio que serve para conectá-lo ao seguinte. Para isso, é realizada a mineração, ou seja, os computadores conectados à rede Blockchain competem entre si na resolução de um problema matemático (o nível de dificuldade dos desafios é ajustado pela própria rede).

Fonte: <http://blog.ringa.com.br/wp-content/uploads/2018/02/blockchain.png>

O resultado do cálculo feito com essa fórmula gera um código chamado *hash*. Cada bloco possui uma *hash* (chave exclusiva) calculada com base no conteúdo preciso de todas as transações. Quando o novo bloco é postado no livro razão, ele está vinculado ao anterior usando suas respectivas chaves de *hash*, formando uma cadeia totalmente rastreável e verificável.

Os blocos possuem, além da sua própria hash, a chave do anterior. Dessa forma, um processo de verificação conseguirá perceber quando um bloco não é legítimo, pois o código *hash* deste será diferente dos registrados. O mecanismo de comunicação criptografada (relembrando, aquele método de chaves privadas e públicas) impede que essa rede seja invadida. Para entender melhor, assista ao vídeo disponível em <https://anders.com/blockchain/>.

Benefícios

Entre os principais benefícios do Blockchain podemos destacar:

- Segurança e imutabilidade - garantidas pela criptografia e estrutura em forma de cadeia de blocos;
- Disponibilidade - estrutura distribuída e descentralizada permite que o sistema continue funcionando mesmo que um ou mais nós caiam;

- Confiabilidade - como os dados não podem ser apagados ou alterados, as transações registradas ali são legítimas e íntegras;
- Transparência e Privacidade - as transações são públicas mas os mecanismos de criptografia garantem que os usuários do sistema não sejam identificados;
- Eliminação de intermediários;
- Processos de Transação mais rápidos;
- Custos operacionais mais baixos em comparação com sistemas computacionais centralizados.

Tipos de Blockchain

Há 02 (dois) tipos de Blockchain:

- Aberto ou Público - qualquer pessoa pode acessar o sistema, enviar transações ou participar do processo de consenso;
- Fechado ou Privado - há algumas restrições quanto às formas de participação

Aplicabilidade do Blockchain

Suas aplicações são inúmeras:

- Setor financeiro - hipotecas, pagamentos, transferências e financiamentos;
- Setor público - registro de ativos, identificação do cidadão, registros médicos, cadeia de fornecimento de medicamentos, processos de auditoria e combate a fraudes eleitorais;
- Setor de varejo - cadeia de suprimentos, programas de fidelidade e compartilhamento de informações (fornecedores - varejistas);
- Setor de seguros - origem de risco, processamento de sinistros e histórico de uso;
- Setor de manufatura - cadeia de suprimentos e rastreamento de peças.

Para Ricardo P. Alves, da Accenture Strategy, as aplicações focadas em governo são o segundo maior destino em investimentos no mercado de Blockchain

Mas para sua utilização é preciso verificar alguns critérios básicos para auxiliar a classificação dos processos elegíveis. O Blockchain pode ser usado em:

- Processos extremamente complexos (e lentos) que mantenham uma cadeia de validação em vários níveis;

- Transações que exijam rastreabilidade;
- Transações que exijam registros únicos e não alteráveis;
- Processos de identidade;
- Necessidade de aumento (ou estabelecimento) da relação de confiança entre os membros da rede de negócios;
- Novos modelos de negócio.

Há uma série de iniciativas importantes do uso de Blockchain em soluções governamentais que visam a redução dos custos transacionais e a transformação do governo em uma organização digital.

Levando em consideração a fase de aprendizado do Blockchain, é importante, antes de qualquer atitude, analisar os riscos envolvidos e entender se o Blockchain irá de fato atender ou resolver o desafio ao qual o projeto se propõe a solucionar.

Um exemplo de implementação desta tecnologia no Brasil é a plataforma MUDAMOS – ferramenta para a assinatura de projetos de Lei de iniciativa popular, de forma segura e simples.

Opções de plataforma de Blockchain disponíveis é o que não faltam! O ideal é escolher aquela que mais se adequa ao negócio.

Implementações do Blockchain

Após o *boom* das criptomoedas, surgiram centenas de ofertas no mercado.

Com propostas parecidas ou iguais ao Bitcoin, mas que vão também além das criptomoedas e suportam contratos inteligentes (Smart Contracts), temos:

- Ripple - surgido em 2012, é focado em um Blockchain Privado e possui um algoritmo de consenso próprio;
- Ethereum - criado em 2015, tem uma implementação de proof-of-work e é um Blockchain Público

Em setembro de 2015, foi lançado o Consórcio R3CEV, formado por diversos gigantes da indústria financeira, com foco em desenvolver tecnologias de Blockchain privado que atendam aos bancos. Mais tarde, ainda em 2015, a Linux Foundation lançou o consórcio Hyperledger, composto por empresas de diversos segmentos e suportado por gigantes da tecnologia, como IBM e Intel.

A plataforma Ethereum é a mais rica em termos de casos de uso, com centenas de implementações diferentes.

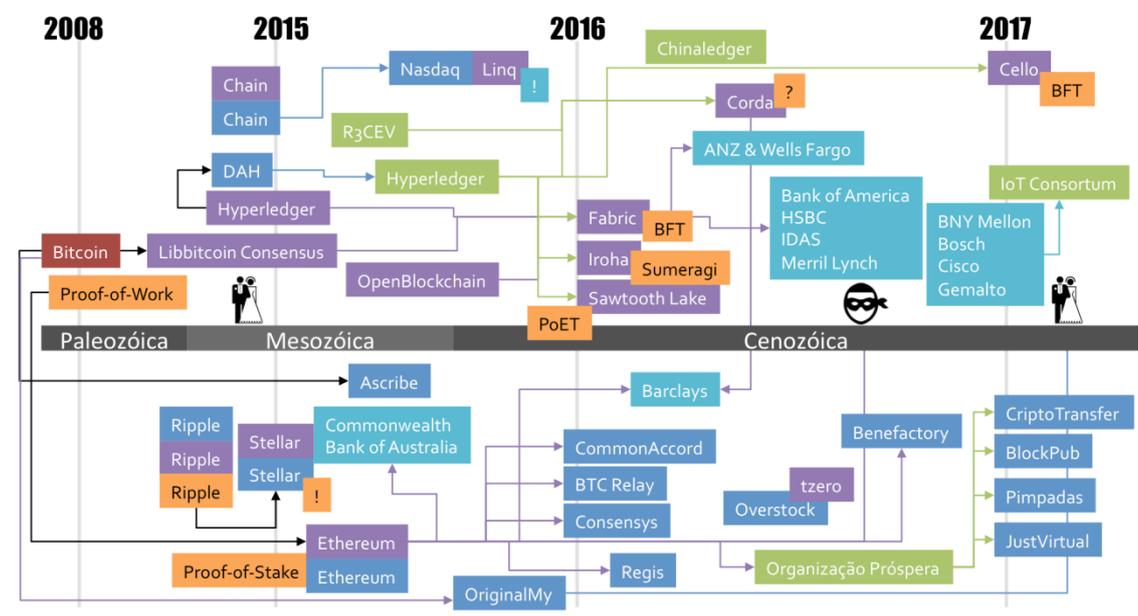
As ilustrações a seguir trazem um quadro comparativo entre os principais cases de Blockchain no momento e a evolução da plataforma ao longo do tempo:

Group	Feature	Bitcoin's Blockchain	Ethereum	Chain	Corda	Ripple	Stellar	Fabric	Iroha
Consensus	Algorithm	Proof-of-Work	Proof-of-Work	Chain Protocol	Raft, BFT*	Ripple	Ripple	BFT	Sumeragi
Consensus	Mining	Yes	Yes	No	No	No	No	No	No
Smart Contract	Language	Script	Solidity	Ivy	Kotlin	Codium**	N/A	Chaincode	Chaincode
Smart Contract	Oracles	No	Yes	No	Yes	Yes	No	No	No
Code	License	MIT	GPL-3.0	AGPL-3.0	Apache 2.0	Misc	Apache 2.0	Apache 2.0	Apache 2.0
Type	Permission	Permissionless	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	N/A
Type	Public/Private	Public	Public	Private	Private	Private	Private	Private	Private
Currency	Currency	Bitcoin	Ether	No	No	XRP	N/A	No	No

* Corda doesn't implement distributed consensus. It is reached only between participating peers on a transaction.

** In a public post on their website, Ripple announced that they have discontinued the development of Codium

Fonte: https://cdn-images-1.medium.com/max/1500/1*F7M0pvpX0H50V_XntNs0ow.png



Fonte: https://cdn-images-1.medium.com/max/1600/1*6mMcb_f4Yjm-WjsH2MhtBQ.png

A evolução tecnológica acontece de forma exponencial e provoca muitas mudanças de paradigmas. Nesse sentido, é fundamental perceber o tamanho dessas mudanças e como isso nos afeta, assim como nosso papel nesse contexto.

Como acontece com qualquer nova tecnologia, é preciso analisar a aplicabilidade do Blockchain, além dos seus prós e contras. Do ponto de vista tecnológico, há ainda questões de escalabilidade da plataforma, métodos de validação, padronização de dados e integração dos sistemas. Em termos gerenciais, as questões incluem transformação do modelo de negócio, estrutura de incentivo e escala de maturidade da transação.

A tendência é que o Blockchain faça uma revolução nas transações digitais, assim como a Internet fez com as informações. Será que estamos prontos?

Referências Bibliográficas:

Tapscott, D. /. (2016). *Blockchain Revolution*. São Paulo: SENAI - SP.

<https://www2.deloitte.com/lu/en/pages/technology/articles/blockchain-proof-concept-solve-traceability-issues-art.html>. (s.d.).

(<https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html>)

(<https://www.infochain.com.br/>)

(Workshop IBM Hyperledger)

(<https://medium.com/@flobomn/blockchain-menu-8f5cbb8ca7d4>)

(<https://news.sap.com/brazil/2017/07/21/infografico-o-que-e-blockchain-e-quais-seus-beneficios-para-os-negocios/>)

(<https://www.infowester.com/blockchain.php>)

(<https://medium.com/futuro-exponencial/blockchain-uma-cronologia-c3a15d246fef>)