



RNP

ORGANIZAÇÃO SOCIAL DO MCTI

Relatório de Visão de Futuro

Comitê Técnico de Blockchain (CT-BLOCKCHAIN)

Dezembro de 2020

Coordenadora do CT-Blockchain

Fabiola Gonçalves Pereira Greve, Dra. (UFBA)

Assistente Técnico do CT-Blockchain

Allan Edgard Silva Freitas, Dr. (IFBA)

Coordenador RNP

Renato Duarte Rocha, Esp (RNP)

Diretor Adjunto de e-Ciência e Ciberinfraestrutura Avançada

Leandro Neumann Ciuffo, Me. (RNP)

Autores

Alberto Paradisi, Dr. (CPqD)
Allan Edgard Silva Freitas, Dr. (IFBA)
Antônio Augusto Rocha, Dr. (UFF)
Billy Anderson Pinheiro, Dr. (Amachains)
Fabiola Gonçalves Pereira Greve, Dra. (UFBA)
Glauber Dias Gonçalves, Dr. (UFPI)
Igor Machado Coelho, Dr. (UFF)
Luis Carlos Erpen De Bona, Dr. (UFPR)
Marcela Ribeiro Gonçalves, Esp (Multiledgers)



1. Introdução

Blockchain é uma tecnologia de grande potencial disruptivo, pois cria digitalmente uma rede de confiança descentralizada, permitindo o estabelecimento de transações entre as partes sem a necessidade de intermediários. Ela oferece um arcabouço seguro, resiliente, e transparente para a realização das transações na Internet. O potencial de transformação é imenso e aplicações descentralizadas estão surgindo a partir desta tecnologia em inúmeros setores: finanças, saúde, artes, educação, varejo, governo, além da própria computação: protocolos de redes, nuvem e névoa, cidades inteligentes, etc.

Para que a tecnologia blockchain evolua e contribua para o bem-estar da sociedade é preciso difundi-la, formar pessoas, promover o desenvolvimento tecnológico e o empreendedorismo, além do diálogo e aliança entre academia, governo, indústria e agências de fomento. Nesse contexto, é fundamental a articulação de uma rede de cooperação em pesquisa e desenvolvimento tecnológico para o fomento do ecossistema no Brasil.

O Comitê Técnico em Blockchain (CT-Blockchain) é um comitê de caráter consultivo criado pela Rede Nacional de Ensino e Pesquisa (RNP) em 2020, cujo foco é construir uma visão de futuro sobre a atuação da RNP neste domínio. Ele visa fomentar o ecossistema, prospectar tecnologias e acompanhar os principais avanços técnico-científicos em blockchain e suas aplicações.

O CT-Blockchain contempla uma parcela ativa de pesquisadores e especialistas, com atuação destacada no domínio da tecnologia blockchain, nos mais diversos setores da academia, indústria, governo e terceiro setor, agregando pessoas dentro e fora do ecossistema RNP. A sua participação é feita a partir de convites públicos e direcionados aos especialistas, de maneira a termos uma representatividade e abrangência significativas considerando o cenário de blockchain no Brasil.

1.1. Escopo e limitações

A visão de futuro aqui apresentada considera as contribuições dos cerca de 100 membros do CT-Blockchain, de mais de 50 instituições distintas. Ela agrega visões distintas desses diversos membros, que possuem experiência em blockchain e são oriundos de diferentes classes de instituições (universidades e institutos, centros de pesquisa, governo, terceiro setor, start-ups etc.), mas não necessariamente representam a visão institucional das suas organizações. A construção da visão é apresentada de forma distribuída em eixos, como detalhado na metodologia, os quais integram-se entre si.

2. Metodologia

Ao longo de 2020, o CT-Blockchain realizou reuniões periódicas abertas à comunidade, nas quais se discutiram as diferentes perspectivas associadas ao tema. Considerando as diferentes facetas e perspectivas da tecnologia blockchain, optamos pela discussão temática em torno de seis principais eixos:

- *Aplicações*
- *Desenvolvimento Tecnológico*

- *Educação*
- *Identidade Digital Descentralizada*
- *Infraestrutura*
- *Governança e Padrões*

De forma aberta, a partir da comunidade ativa no CT-Blockchain, grupos de trabalho (GTs) atuaram em reflexões conjuntas para cada uma das seis temáticas, com coordenação de membros representativos da comunidade que atuaram como facilitadores para a condução de cada grupo de trabalho.

As reuniões do CT-Blockchain incluíram desde apresentações temáticas, a apresentações convidadas e aproximação com iniciativas internacionais (caso da LACChain) e participação em eventos externos, com debates envolvendo comunidades externas: WGID com SBSEG 2020, Fórum RNP 2020, WRNP 2020, ENCCLA 2020 etc.

Os grupos de trabalho também realizaram reuniões próprias, e, quando necessário, houve reuniões envolvendo mais de um grupo de trabalho com temáticas específicas. Além disto, dinâmicas foram realizadas pela coordenação geral junto aos facilitadores de cada grupo, alinhando as expectativas quanto ao trabalho desenvolvido no CT.

Cada grupo de trabalho apresentou a sua visão de futuro e um conjunto de reflexões sobre a temática na forma de um capítulo de obra em construção pelo CT-Blockchain. O presente documento de visão de futuro apresenta uma visão sintética e integrada destes esforços conjuntos.

3. Panorama / Contexto

A blockchain e as tecnologias de registro distribuído DLTs (*distributed ledger technologies* ou *DLTs*) oferecem uma rede de confiança digital, com potencial para o desenvolvimento de aplicações distribuídas descentralizadas. Ela alicerça suas bases em elementos da segurança computacional - em especial as funções *hash* e criptografia de chave assimétrica - e da computação distribuída tolerante a falhas - em especial o consenso distribuído - oferecendo um arcabouço seguro, escalável e confiável para a realização de transações entre pares que não se conhecem, sem a necessidade de entidades centralizadoras para validação. O registro das transações é mantido num livro-razão distribuído (*distributed ledger*), que é replicado, mas único, oferecendo uma base comum e transparente, imutável e passível de verificação e auditoria [Greve et al. 2018].

As tecnologias de blockchain e registro distribuído tem potencial para mudar as relações comerciais entre os países e seus cidadãos, bem como o papel dos bancos e a relação com órgãos governamentais de controle financeiro.

Blockchain reúne conceitos consagrados em outras áreas e domínios de conhecimento da Ciência da Computação, particularmente de sistemas distribuídos tolerantes a falhas, segurança, redes P2P, criptografia, entre outros. Muitos desafios tecnológicos e científicos emergem de tal definição, entretanto não se transparecem as razões que realmente tornam disruptivas as tecnologias derivadas desse conceito.

Por trás do singelo fato da possibilidade de se fazer registros de forma distribuída e confiável, encontra-se uma mudança importante que é o deslocamento dos agentes que provêem confiança em nossa sociedade. O advento das criptomoedas e ativos digitais são exemplos desse potencial e vêm causando uma disrupção no sistema financeiro internacional.

Um dos primeiros casos de uso da tecnologia blockchain foi a moeda virtual bitcoin, que nasceu no meio uma grande crise confiança global do sistema de crédito em 2008, segundo Edelman, e se posiciona como uma nova tentativa de mudança da estrutura de confiança do sistema financeiros que surgiu na idade média e foi aperfeiçoado pela dinastia dos Médicis durante o século 15.

Apesar das transformações tecnológicas, incluindo a Internet, desde aquela época essas instituições não mudaram radicalmente, pois seu fundamento é a confiança em uma família dinástica ou em uma instituição. Percebemos que desde a idade média a sociedade se hierarquiza em torno de entidades que são "fontes confiáveis" a fim de realizar registros de informações e que essas entidades passaram ilesas a cinco séculos de desenvolvimento tecnológico. Não há como negar o caráter transformador de uma tecnologia que promete acabar com as fontes de confiança centralizada e seus carimbos, dando mais liberdade (e privacidade) ao cidadão detentor da moeda a ser gasta. Neste contexto, blockchain propõe um modelo descentralizado que funda a chamada internet da confiança.

Blockchain vem transformando diversas indústrias além da financeira, uma das primeiras a colher frutos do uso da tecnologia foi a Cadeia de Suprimentos, onde cada ator do sistema registra informações no processo, onde consegue identificar o membro e o rastreamento de um item circulante dentro da cadeia. Além de compartilhar dados verificáveis e transparentes, ele permite ainda garantir o controle de qualidade específicas de produtos ao longo de todo processo, tal como temperatura de transporte de um produto armazenado em caminhão refrigerado.

Outro uso muito promissor está na área de Blockchain for Goods, ou questões de bem-estar social, onde os contratos inteligentes podem permitir uma melhor automatização de serviços, principalmente em áreas onde não se queira a assimetria de informações, e garantindo uma autenticidade da mesma. O uso em votações, dados médicos, gestão de identidades para refugiados, entre outros.

Mercados relacionados onde hoje existem terceiros de confiança para que uma transação ou negócio seja executado, desse modo a desintermediação elimina riscos com centralizações, baixa eficiência e alto custo de transação. Nesse aspecto as DAO's podem ser boas soluções, através dos contratos inteligentes, formando novos modelos de negócios e criação de diferentes tipos de ativos, tal qual estamos vendo surgir com as DE-FI e NFT's.

Há diferentes aspectos a tratar quanto aos desafios e perspectivas do uso da blockchain para a comunidade do ecossistema RNP em particular e para o cenário nacional, de forma ampla. Isto motivou uma abordagem por eixos temáticos, que tratam desde aspectos organizacionais a aspectos tecnológicos, bem como a necessidade de articular e capacitar para melhor potencializar o uso da Blockchain.

3.1. Eixos Temáticos do Comitê Técnico

Governança entende o papel disruptivo da Blockchain na relação entre entidades e da mudança importante do deslocamento dos agentes que provêm confiança na sociedade, e se propõe a refletir nos desafios de diferentes níveis da governança da Blockchain e como a RNP pode atuar como líder e facilitadora, considerando seu papel histórico de indução da Internet brasileira. A promoção da Governança entre as diversas entidades e o estabelecimento de padrões e protocolos comuns é essencial para o ecossistema Blockchain, pois esse depende de colaboração e cooperação entre as partes para que haja compartilhamento seguro e transparente.

Identidade Digital Descentralizada propõe a partir da experiência em identidade da RNP, desde ICP-Brasil, e das iniciativas em diferentes países, um caminho para identidade digital descentralizada (IDD) no Brasil e um

papel para RNP neste processo. A IDD permite a propriedade e o resgate do controle dos dados para o indivíduo e entidades, coisas e organizações, contribuindo dessa maneira para o direito do indivíduo (instituições) à privacidade dos seus dados.

Educação tem como foco contribuir para formar e capacitar pessoas em blockchain ao redor do país, das mais variadas maneiras. Formar especialistas e desenvolvedores na área é essencial para a apropriação da tecnologia e desenvolvimento de novas aplicações inovadoras. Assim, esse eixo estabelece as bases para a formação de pessoas em diversos níveis, e explora um modelo de referência em blockchain considerando cursos de graduação e pós-graduação, para além de formações pontuais e especializadas em ações da própria RNP.

Infraestrutura computacional para blockchain deve atender aos modelos de negócios e aos requisitos das aplicações que as utilizam. Assim, esse eixo elabora uma taxonomia para tais infraestruturas, indica casos de uso, e estabelece um diagrama de processos, que devem ser utilizados com os requisitos mapeados para a escolha da infraestrutura adequada a cada cenário de aplicação.

Desenvolvimento Tecnológico reflete questões do desenvolvimento de nossas próprias aplicações, considerando o contexto e ecossistema nacionais, em que a academia é o território propício, mediado pela RNP, como laboratório para a experimentação de novas tecnologias.

Aplicação contribui para o mapeamento das diferentes necessidades, contextos, requisitos e particularidades de aplicações que façam uso da blockchain. Além disso, identifica os desafios de engenharia para o projeto, desenvolvimento e implantação de aplicações da tecnologia blockchain, dado as suas diferentes configurações e variantes. O eixo oferece ainda uma visão crítica das aplicações blockchain que são viáveis e estratégicas para os setores da indústria, serviços e governos, buscando contribuir para o desenvolvimento tecnológico e científico nacional.

4. Recomendações

4.1. Problemas, Desafios e Dores identificadas

- Apoiar a pesquisa e o desenvolvimento tecnológico em Blockchain;
- Estabelecer infraestrutura compartilhada de rede blockchain;
- Definir modelos de governança adequados ao uso destes recursos;
- Alinhar políticas públicas e legislação;
- Estimular formação e capacitação de pessoas;
- Utilizar o potencial da blockchain em cenários de identidade digital descentralizada;
- Apoiar o desenvolvimento de aplicações inovadoras para o uso da Blockchain.
- Divulgar ações e estabelecer plataformas oficiais de comunicação.

4.2. Tendências tecnológicas e aplicações emergentes

A tecnologia blockchain permite desta forma a construção de possibilidades de inovação incremental e mesmo disruptiva no ecossistema RNP, revolucionando a forma como serviços e aplicações podem ser fornecidos por meio de uma nova relação e forma de mediação de confiança entre partes interessadas.

4.2.1. Ações de curto ou médio prazo com o potencial de estender os serviços da RNP

Seguem as ações traçadas para o fomento da tecnologia blockchain:

- Interagir com atores de governo, academia, indústria e terceiro setor para fortalecimento do ecossistema;
- Formar alianças nacionais e internacionais;
- Contribuir para o estabelecimento de políticas públicas e legislações adequadas ao uso da tecnologia;
- Capacitar recursos humanos e divulgar a tecnologia e seus artefatos.
- Estabelecer uma rede experimental (testbed);
- Construir coletivamente padrões de governança;
- Fomentar o desenvolvimento de serviços de identidade digital descentralizada;
- Identificar e solucionar desafios de pesquisa e tecnológicos;
- Fomentar o desenvolvimento de aplicações descentralizadas em benefício da sociedade.
- Estruturar e difundir canais oficiais de comunicação

4.2.2. Ações disruptivas de médio ou longo prazo, com o potencial de criar novos produtos ou serviços

Para além das ações traçadas num curto e médio prazo, seguem as ações complementares para a consolidação do uso e benefícios associados à tecnologia blockchain:

- Ofertar serviços de identidade digital descentralizada baseada em blockchain;
- Estabelecer uma infraestrutura de serviços e aplicações em blockchain que favoreça o ecossistema da RNP;
- Integrar a infraestrutura com redes nacionais e internacionais de blockchain;
- Fomentar o desenvolvimento de aplicações disruptivas baseadas na tecnologia blockchain, tais como identidade digital descentralizada, notariação, compartilhamento, gestão segura de dados, diploma digital etc;
- Apoiar empreendedorismo

5. Visão de futuro do CT

A visão de futuro expressa neste documento vislumbra possibilidades de alianças com diferentes iniciativas, com reflexões sobre como mediar as relações, bem como a oferta de base tecnológica

adequada para a experimentação de protocolos de base para a blockchain, bem como frameworks, serviços de base, como identidade digital descentralizada, e aplicações. Tais ações em conjunto com demais de fomento ao desenvolvimento tecnológico e a capacitação de pessoas permitirá ao ecossistema RNP incorporar as diferentes possibilidades tecnológicas e disruptivas apresentadas a partir da blockchain.

5.1. Curto prazo (1 ano)

Estabelecimento de Alianças e Governança. A interlocução com alianças como Alastria, LACChain, EBSI e Tradelens, entre outras, é importante, uma vez que estas iniciativas estão consolidando um novo momento na utilização da tecnologia, em que as redes não estão só com foco nas aplicações, mas em todo o ambiente que as compõem. Essas novas redes estruturam sua governança dentro e fora das redes, criando elementos que atraiam novos usuários e que permitam inovação, cooperação e colaboração no desenvolvimento de novos modelos de mercado e produto, além de conduzir grupos para promoção de políticas e padronizações com a contribuição de múltiplos setores permitindo o desenvolvimento de regulação.

Instâncias de plataformas de blockchain. A infraestrutura disponível para o ecossistema RNP deve permitir o uso, desenvolvimento e experimentação em blockchain. Ela deve permitir desde provas de conceitos focadas em aplicações até a possibilidade de experimentação em tecnologias de blockchain. As provas de conceito não recorrem a modificações em plataformas blockchain, podendo desta forma compartilhar a mesma instância de plataforma com outras aplicações. Já a experimentação tem foco nas plataformas blockchain, de tal maneira que estas plataformas serão modificadas e instanciadas na própria infraestrutura. Como implicação direta, o compartilhamento de uma mesma instância de plataforma por mais de uma aplicação pode não ser o desejável. A possibilidade de ambiente de simulação permanente pode ser utilizada para facilitar a comparação e eventual adoção de soluções blockchain.

A criação de uma rede experimental blockchain pela RNP pode orientar os requisitos para criação de redes de propósito específico. É esperado um mapeamento mínimo das necessidades do ecossistema envolvido para definir o formato da rede experimental e sua governança, e possibilitar que todos os atores envolvidos possam alcançar melhor seus resultados.

A RNP pode, por meio de parcerias, prover serviços e aplicações baseadas em blockchain que agreguem valor à comunidade, como serviços de identidade digital descentralizada e diploma digital.

Disseminação e Capacitação. Disseminar o conhecimento gerado por meio das atividades do CT-Blockchain, apresentando-as de forma clara à RNP e à comunidade nacional. Em paralelo, ações de reflexão para a melhor formação dos estudantes, em nível de graduação e pós-graduação, tais como o estabelecimento de um currículo mínimo, devem ser realizadas. Além disso, há que se fomentar a realização de eventos científicos na área para o estímulo e troca de conhecimentos, a exemplo do WBlockchain (Workshop em Blockchain: Teoria, Tecnologia e Aplicações), evento satélite do SBRC, em que já participam diversos membros do CT. No curto prazo, pretende-se aprofundar essa sinergia do CT com a comunidade do WBlockchain.

Na graduação em áreas correlatas à Ciência da Computação, a formação de pessoas requer o refinamento e proposição de um currículo de referência em Blockchain e suas aplicações. O CT-Blockchain deve mediar recomendações à Sociedade Brasileira de Computação de tal forma que os documentos de referência da área ("Referenciais de Formação" e "Currículos de Referência") contemplem diretamente as seguintes tecnologias: algoritmos de consenso, tecnologia blockchain e suas aplicações.

Na pós-graduação, pode-se promover a criação de componentes eletivos sobre blockchain e Identidades Digitais. Para isso, além de criar conteúdo didático de qualidade, recomenda-se promover eventos científicos

e escolas regionais sobre a temática. Também é possível pensar a articulação de programas de pós-graduação, em rede, dedicados ao tema, sejam estes profissionais ou acadêmicos.

5.2. Médio prazo (2 - 5 anos)

Fortalecimento da Governança. Em médio prazo, espera-se um amadurecimento maior em torno dos ecossistemas de blockchain, bem como passos concretos para consolidação das ações necessárias. Espera-se um novo alinhamento em relação aos objetivos já conquistados pela RNP e pela comunidade nacional, bem como novos objetivos elencados no caminho. Já é possível vislumbrar, neste prazo, formação de pessoal qualificado em nível de pós-graduação, bem como através de ações e cursos oferecidos pelo mercado.

Oferta de Redes e Infraestrutura de Serviços. Deve-se convergir no uso da rede de blockchain proposta, permitindo ambientes de teste, validação e produção, bem como usufruto das vantagens associadas à integração com iniciativas como LACChain e Rede Brasileira de Blockchain (RBB).

A criação de um ecossistema próprio para as experimentações junto a universidades, tendo a possibilidade que startups, pequenos e médios negócios se beneficiem da tecnologia pode ser um caminho para a difusão e aceleração das descobertas que essa nova internet do valor nos propõe. A construção desse ambiente que agiliza a capacidade de interação entre diferentes áreas e conecta diferentes estratégias e necessidades, com segurança e controle, pode ser vista como uma solução.

Desenvolvedores e pesquisadores necessitam de plataformas com a escala adequada para realizar experimentação e coletar dados, de modo a explorá-los para gerar conhecimento útil. Ao mesmo tempo, é necessário desenvolver nossas próprias aplicações, considerando o contexto e ecossistema nacionais, com suas necessidades próprias e peculiaridades. Nesse sentido, as Universidades são o território propício, pois já vêm funcionando desde a criação da RNP como laboratórios para a experimentação de novas tecnologias. A disponibilização de uma infraestrutura compartilhada e aberta aliada à experimentação em cenários reais pode alavancar de maneira significativa os efeitos das tecnologias de *distributed ledgers* e outras supracitadas.

Fomento ao Desenvolvimento de Aplicações Estratégicas em Diversos Níveis. O fomento ao desenvolvimento de aplicações inovadoras em Blockchain que usem o ecossistema compartilhado é esperado, podendo evoluir na oferta de serviços à comunidade RNP. Em especial, deve-se fomentar o uso de Identidade Digital Descentralizada baseada em Blockchain articulando o desenvolvimento de diferentes tipos de aplicação no Ecossistema RNP. Considerar que existem iniciativas de desenvolvimento com diferentes níveis de maturidade, desde provas de conceitos até a aplicações em operação.

Evolução na Capacitação e Apoio às Atividades de P&D. A evolução do currículo de referência e o incremento de ações na pós-graduação, além de ações de formação inicial e continuada em Blockchain, baseados neste material de referência, por meio da Escola Superior de Redes, são ações importantes do ponto de vista de capacitação de pessoas em médio prazo.

Em alinhamento entre os grupos de trabalho, seria interessante nesta etapa dispor do uso experimental em nível nacional do Sandbox comunitário proposto, além dos fins de experimentação e prototipação, para capacitação de pessoas.

Assim, entende-se que o apoio a atividades de P&D, fortalecendo a formação de pessoas em Blockchain, e o uso experimental por meio de infraestruturas compartilhadas, bem como a articulação de parceiros,

estabelecendo modelos de governança e alinhando políticas públicas necessárias, são vistos como mecanismos importantes para potencializar a Blockchain no cenário brasileiro.

5.3. Longo prazo (6 - 10 anos)

A longo prazo, espera-se que os objetivos aqui listados já tenham se cumprido, mesmo que parcialmente, e que já exista uma comunidade nacional bem estabelecida, em torno do tópico de Blockchain. Diversas iniciativas lançadas no momento, em nível nacional e internacional, já devem começar a dar frutos e modificar de forma irreversível alguns setores da economia, bem como a forma como compreendemos e utilizamos a tecnologia Blockchain.

Referências

1. REVOREDO, Tatiana. **Blockchain: Tudo O Que Você Precisa Saber**. 2020
2. ___. **Blockchain, a Nova Internet da Confiança**, publicação EdUFBA 2021
3. Trust Barometer da Edelman. Acessível em <https://www.edelman.com.br/estudos/edelman-trust-barometer-2021>
4. GREVE, Fabíola Greve et al. **Blockchain e a Revolução do Consenso sob Demanda**. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos, 2018.

