**VII Forum da Internet**

**Título:** Blockchain para Interesse Público

Apresentação

Priscila fez apresentação da mesa de abertura com a pergunta: como a Blockchain pode ser usada no setor público e privado e quais os impactos para a sociedade?

Pedro

Quando este workshop foi pensado, houve uma preocupação em fazê-lo realmente multissetorial. Como primeiro da mesa, e representante do setor acadêmico, ficou encarregado de fazer uma base conceitual. Algumas noções básicas e os principais desafios que blockchain e smart contracts terão que enfrentar ou já estão enfrentando para se tornarem tecnologias viáveis foram apresentados. Em sua apresentação, Pedro colocou esse questionamento para iniciar esse debate sobre interesse público e blockchain: Uma das principais funções do governo é assegurar autenticidade de certos documentos. Todo o arcabouço jurídico do governo foi criado para confiarmos nele. Por exemplo cartórios, a justiça. Com o tempo outros atores alcançaram um alto grau de confiança, mas em geral é no governo que mais confiamos. Mas eu também foi feito um questionamento: Se o governo é sempre confiável, e se podemos confiar sempre nele. E mesmo que seja, pergunta-se se apenas a confiança entre as partes é suficiente, se é possível contar só com ela. Isso vai variar de contexto jurídico e nacional mas permanece o questionamento.

Ao perguntar se alguém não tem familiaridade com a tecnologia, 5 pessoas da plateia se manifestam e Pedro traz uma definição breve com dinâmica: se todo mundo aqui tivesse que comprovar a propriedade de um objeto e que pudesse trocar esse objeto e que toda vez que pudesse trocar esse objeto, todo mundo precisasse concordar que o objeto foi trocado, haveria um consenso. Então se ele passasse o controle para Priscila, todo mundo ia ver que o controle foi passado, que o controle agora é dela, e se alguém falasse que não é dela, a coletividade iria levantar contra isso e dizer não. Houve um consenso concordando que o controle agora é dela.

Foi explicado de uma forma bem simplificada: a relação de livro razão, de transações, que uma é uma blockchain: um livro de registro distribuído que envolve transações e consenso. Então numa definição objetiva: Um livro distribuído, imutável, público e criptografado.

Outra coisa que a blockchain torna viável apesar de não ter sido criada com a invenção do blockchain, são os smart contracts, que são basicamente um contrato que se auto executa. Eles se tornam viáveis na tecnologia blockchain porque foi só com a tecnologia descentralizada que ela trouxe, que a ideia de smart contracts ficou realmente factível. Esse conceito é central para toda a discussão. A diferença entre eles e um contrato tradicional é o que diferencia a discussão para o interesse público. A partir dele você elimina a necessidade de terceiros. Elimina a necessidade de confiança.

De certa forma um contrato jurídico é quase uma linguagem de programação mas escrita de forma mais rebuscada, e tão difícil de ler quanto para quem não é da área. Foi explicado o que se queria dizer por computador virtual distribuído. Imagina um computador na nuvem que não

está em nenhum servidor específico, está distribuído assim como o torrent. Seria possível executar um programa nesse computador virtual peer-to-peer pagando uma determinada taxa em ether, ou bitcoin, ou outro recurso. Ele funciona como um grande computador na nuvem que ninguém tem controle sobre ele. Como ninguém tem controle sobre ele, ele não pode ser desligado, ele só executa os contratos nele.

Smart contracts é como o contrato jurídico com códigos.

O contrato tradicional: contrata-se uma pessoa para fazer um serviço para você por 500 mil reais, ela faz o serviço e esse é o input, pagam-se os 500 mil e é outro input. Todavia, no contrato tradicional é necessária uma pessoa para interpretar e decidir se o serviço foi feito de acordo com o combinado ou não. E se não foi, aquilo vai ser judicializado. Em alguns casos, por exemplo de registro de imóveis, mesmo depois que a justiça tenha decidido que foi tudo realizado, ainda existe uma burocracia para garantir que aquilo saiu do nome de uma pessoa e foi para outra pessoa, que é significativo.

Nos smart contracts ele funciona com dois inputs dados, o computador já interpreta pra ver se ele foi realizado de acordo com o combinado, já executa, e então pode ter duas consequências, ou executa ou não executa. O contrato não tem requisitos subjetivos. No momento que você assina ele se executa automaticamente. Essa é a maior força e uma das maiores fraquezas do smart contract.

Nem todo smart contract é um contrato jurídico tradicional. Se você usa ele de maneira meramente instrumental, dentro da sua empresa para automatizá-la, o smart contract não é um contrato jurídico tradicional. Todavia, se existem duas vontades distintas envolvidas, o smart contract também pode ser um contrato jurídico.

Alguns riscos dos smart contracts: eles são extremamente inflexíveis, irretroativos e de alto custo de reparo. Recorrer é difícil. Mesmo se o indivíduo aceita a pagar o custo, nem sempre a conseguirá de volta o que foi acordado.

Algumas das coisas que o tornam relevante: ele torna tudo transparente, a nível de interesse público, tudo estará aberto para todo mundo acessar. O uso em licitações, quanto mais complexo a licitação mais difícil de dizer quem vai ganhar aquela licitação objetivamente. Também existe muita corrupção por meio da licitação, que pode ser combatida através do uso de smart contracts.

Pedro definiu a aplicação da blockchain para interesse público em 3 níveis: os casos em que a blockchain pode substituir o direito, são em lacunas onde não foi construído uma arquitetura jurídica em que as pessoas podem confiar certamente no sistema vigente. Por exemplo o sistema de microcréditos, o registro de imoveis em países subdesenvolvidos, que faz ser muito difícil saber de quem é essa propriedade. A aplicação da blockchain vai ser acessória para garantir a aplicação do direito. Na blockchain é praticamente impossível fraudar.

E por fim é blockchain como complemento, você usa a blockchain para dar mais robustez para levar a níveis maiores. Em geral o custo são altos demais para pequenos valores. A blockchain permite que você escale isso massivamente.

Gabriel Aleixo

Gabriel considerou importante deixar claro para estimular o uso da blockchain para interesse público explicar que não é necessário entender como funciona blockchain para entender o que é possível fazer com ela.

Blockchain é ao mesmo tempo o nome dado a uma base de dados distribuída e também o nome que dado para a base de dados em si, e o nome utilizado para a tecnologia que mantém as múltiplas cópias dessa base de dados em consenso. Entendendo isso, é possível entender porque a blockchain tem o potencial de redefinir relações de confiança em qualquer ponto da sociedade, em qualquer setor.

No novo paradigma que a blockchain nos consegue prover, o espectro de utilização é muito amplo. Do mesmo jeito que o bitcoin não depende de banco ou governo central para existir, ele só precisa dos milhares de usuários que o transacionam.

Quais os 2 grandes trunfos que a blockchain resolve: por 26 anos se achou que seria impossível criar o que a blockchain nos permite criar. No termo técnico, blockchain resolve uma questão prática dos generais bizantinos que dizia que seria impossível estabelecer consenso em uma rede distribuída sem que houvesse um centralizador. Se fosse traduzir o que é posto nesse problema, é impossível utilizar a tecnologia para fazer com que duas pessoas que não se conhecem consigam confiar umas nas outras sem remeter a um terceiro de confiança. Essas instituições existiam por uma questão tecnológica, se acreditava até então. Como é que vai se existir o provimento de bens públicos sem que o governo a partir de impostos recolhidos, consiga coordenar essas expectativas e prover bens públicos. Como se pode garantir que uma sendo comprada de alguém, é dela, sem um cartório responsável por isso? Como fazer uma transferência para um site como Alibaba onde se compra algo na China, sem ter um banco pra fazer isso?

O que a blockchain resolve é justamente essa camada de confiança, e o que a blockchain nos permite criar também de forma inédita, entende-se o bitcoin como uma versão digital do ouro do que do dinheiro. Ela nos permitiu replicar a escassez do mundo físico no mundo digital. Então blockchain é uma tecnologia que nos permitiu fazer com que estranhos consigam conversar e consiga confiar um nos outros sem que instituições públicas ou privadas sejam necessárias para parte destes processos de auditoria de confiança.

Blockchain não é panaceia, não vai acabar com bancos, governos ou outra coisa. Essas instituições vão se modernizar. Mas é possível conseguir a replicação e conseguir estabelecer uma tecnologia descentralizada no qual os registros não podem ser duplicado.

O bitcoin está na nuvem, está numa nuvem descentralizada. É como se fosse uma moeda escritural. É um ativo que é um registro. Quando alguém manda bitcoin daqui para o Japão por exemplo, está anexando bitcoin na transação e a enviando. Do mesmo jeito que quando alguém vende sua casa para outrem, este alguém não leva a sua casa para a pessoa, ela vai até o cartório, registra no cartório e transfere a posse daquele bem para uma pessoa, assim é com o bitcoin, assim é com qualquer ativo que consegue ser digitalizado e transacionado via blockchain.

Aleixo considera interessante termos essas duas coisas: blockchain como camada de confiança e como forma de transacionar ativos, bens ou qualquer coisas que podem ser representadas na forma de um registro digital.

Ele costuma usar o exemplo do Everledger em que se utiliza a blockchain para registrar cada etapa da cadeia de suprimentos de diamantes com registros em blockchain. porque registrar cada etapa de transação é interessante, porque entende-se a consequência de se guardar, gravar uma informação na blockchain, entende-se não somente porque esse é um caso de interesse público mas porque muitos outros podem ser explorados. Qualquer informação uma vez armazenada no blockchain, qualquer informação se torna acessível, transparente, imutável e segura.

Existem blockchain de cores e sabores distintas mas o que faz que tenham valor para o interesse público é o fato de que uma vez armazenada na blockchain ela se torna acessível, transparente, imutável e segura.

O sistema quando está baseada em blockchain ele não cai. a base de dados que constitui o sistema.

imutabilidade: blockchain são bases de dados infraudáveis porque o custo de se fraudar é maior do que o benefício de se ajudar a rede.

Se alguém consumir um alimento orgânico terá que olhar o selo lá colocado dizendo que aquilo é orgânico e precisará confiar que aquilo é orgânico. Num futuro muito próximo a blockchain vai se ligar à IoT, e não será possível colocar uma informação fraudulenta. O sensor vai falar que o alimento ficou 15 dias no armazém quando deveria ter ficado só 7.

Gabriel fechou sua apresentação falando do case da Mudamos+.

Bernardo

Uma das coisas importantes a se entender é a questão da arquitetura. Na verdade blockchain é uma tecnologia é um pouco antiga. o que acontece é que ela começou a ficar famosa depois de ser usada para bitcoin. Na verdade é uma tecnologia que permite uma troca peer-to-peer.

É a arquitetura C2C. Focar em moedas é ver a ponta do iceberg. Então entende-se que blockchain é uma plataforma, uma camada informacional que permite transacionar de forma privada e escalada graças a ledger, ao consenso e aos smart contracts, que são a lógica do negócio do que deve acontecer dentro da blockchain.

Então basicamente os smart contractas são a lógica que deve acontecer dentro do ecossistema da blockchain. Então novamente a partir daí, pode-se aplicar essas plataformas dentro dessas arquiteturas de B2B e B2C. Onde entram os conceitos de rede permissionada, uma rede que depende de uma permissão para que uma pessoa entre nela para interagir.

Dentro de uma rede permissionada os participantes se conhecem, portanto não se precisa de algoritmos para transacionar. Não se precisa minerar a informação. Dentro de uma blockchain comissionada a arquitetura de consenso é muito mais fácil. Cada organização que pertence a essa plataforma

Bernardo considera que as redes de IoT são a próxima mina de ouro dos hackers. Hoje como as redes acabam não sendo muito protegidas, hé possível facilmente entrar para fraudar essas redes. Com blockchain eles não entrarão com tanta facilidade.

Serão os dispositivos que irão se auditar. A operação também será regulada dentro do blockchain. O smart contract irá tomar controle.

Mas dentro do âmbito de IoT uma das plataformas que está começando a surgir é o Iota. Essa arquitetura permite que pagamentos sejam feitos de forma automática. Uma máquina consigue contratar um serviço e fazer o pagamento de um drone para que ele pegue uma coca-cola num local e este drone leve o produto até o consumidor.

Vanessa Almeida

Vanessa explica que não é só o Brasil que está passando pelo governo.

Vemos o blockchain como uma possibilidade de reconstruir confiança. Os bancos vão continuar existindo, então vemos a blockchain como a tecnologia que pode refazer isso.

Duas características que Vanessa considera que podem refazer essa confiança: ser inviolável, então já que as pessoas não confiam no governo, pode-se usar a blockchain para dar transparência às informações. Para as informações de governo que deveriam ser todas públicas, então a blockchain parece ser essa ferramenta para refazer a confiança.

Para outras aplicações, isso pode ser essencial. Transferência de dinheiro em muitos casos vai ser assim.

O que o KFW já fez com o bitcoin. Eles entendem que a questão da transparência e confiança é muito importante, e criaram uma forma de transação na África. Então a KFW quer que ele seja usada em transações na África.

O dinheiro sai do KFW e vai para o cliente. quando o dinheiro chega no cliente, o registro está visível para todo mundo, então ninguém mais precisa confiar na KFW. O dinheiro vai e o fornecedor entra no workflow e dá ok nesse dinheiro do workflow. Então se aumenta a transparência. Ainda é uma prova de conceito. Não é um piloto. O próximo passo que eles querem dar é um piloto rodando em produção.

A gente vê o KFW como um piloto que pode ser rodado no Fundo Amazônia. O objetivo do Fundo Amazônia é proteger a floresta amazônica. A Noruega entende que o mundo precisa defender a Amazônia. O BNDES opera esse fundo.

O FKW quer ir além e transformar o Fundo Amazônia no criptotoken para ter ainda mais confiança. Um token digital é liberado, e esse token digital é enviado para o cliente. e passa a ter um rastreio total do dinheiro. Por que é bom porque esse dinheiro está sendo usado para tentar desenvolver o país. Então todos querem saber por onde esse dinheiro está passando . A gente consegue ver por onde está passando, fazer políticas públicas. O criptotoken é a nossa visão de longo prazo que pode impactar drasticamente o desenvolvimento do país. Vai diminuir o  custo de auditoria, mapear cadeia produtiva entre outros impactos.

FIM DA MESA.

Perguntas:

Diogenes, Youth: Blockchain é uma tecnologia notavel e a imutabilidade e inalterabilidade são as principais características. Mas na Europa muitos tem falado do direito ao esquecimento e a eficiência do blockchain no cotidiano. Qual a implicação da lei do direito ao esquecimento na aplicação do blockchain uma vez que os usuários não podem alterar os registros. Como ultrapassar essa barreira que está surgindo?

Vanda: eue stou envolvida nesse negoico dia 30/11 vamos fazer um ICO. O que me ineteressa é um outro. Eu inivisto em startup na cadeia industrial. Como é que está isso no mercado mesmo, quem está andando, que volumen, que estatisticas nós temos. E pro bndes se eles estão pensando em logica de linhas para quem está investindo nessa área. Tenho conversado cmom a turma de tecnologia mas essa caracteristica é um pouco diferente das fintech, se tem umaprevisão de pensar nessa área.

Bruno Bioni: Necessariamente essa arquitetura terá imutabilidade. É uma coisa com direitos pessoais. A noção de dados pessoais perpassa pelo fato de que há um direito de retificação. Isso não é algo novo? Não é uma panaceia. Então podia pensar em quais setores a gente aplicaria blockchain pensando nesse direito de proteção de dados pessoais.

Henrique, Lapin, Brasília: A gente vai tratar de uma blockchain pública ou privada, permissionada ou não. Vocês veem possível uma blockchain privada do governo? Porque me parece que uma blockchain privada no governo talvez implique nessa questão da confiança.

Gabriel Aleixo: Depende. Não existe uma verdade absoluta. Os casos de uso estão sendo criados enquanto a gente fala aqui. É uma pergunta muito comum que é feita, por exemplo num caso de uso, colocam-se informações, e se tiver que mudar um dado que fica lá pra sempre. Por exemplo, falando de criptografia de chave pública. Quando se manda uma mensagem criptografada, a chave é a chave que eu me identifico. E se um computador for compromissado, perdido. Como se faço pra falar para o mundo que aquela chave não vale mais? A possibilidade é de revogar uma chave. É como se qualquer informação assinada pudesse falar que aquela chave não pertence mais a você. Essa seria uma forma de você fazer. Ver como funciona a revogação de dados privados, revogar uma informação a partir do momento que ela não vale mais. Não podemos perder de vista que blockchain temuma flexibilidade grande. Não tem nada ver se a rede é pública ou privada, mas eu consigo permissionar uma informação. Não é porque a rede é publica que todos os seus dados são públicos. É possível rastrear qualquer coisa no blockchain muito facilmente. É possível ver tudo sobre todos. Essa preocupação, hoje muito mais mainstream, tem raízes no movimento cyberpunk. Então não por acaso já se tem toda a lógica do blockchain. Os serviços que agregam valor não é porque a chave é publica que eu não posso Noque isso pode ter de bom e de ruim,

Bernardo: Basicamente a parte de redes comissiondas, o governo entra no papel de regulador. Dentro de uma rede comissionada, precisa-se de alguém que cumpra o papel de regulador. Então o papel dentro de redes permissionadas, do governo, acaba sendo como regulador.

Publicidade também está bastante ativda pela segurança dos dados para os diferentes publishers. Um caso interessante em termos de estatais, Dubai é a primeira cidade inteligente totalmente conectada por blockchain.

Pedro: O problema do direito ao esquecimento se mantém igual como já está se revelando na Internet, mas numa escala e dificuldade maior.