Opinião: Smart Blockchain Contracts

16 fev 2018 19:08

As implicações da tecnologia blockchain em smart contracts é explorada por Carina Branco, fundadora da Techlawyers by pbbr, neste artigo de opinião.

Por Carina Branco (*)

Desde que em 2009 Satoshi Nakamoto (cuja real identidade permanece em aberto) começou a "minar" moeda digital (no caso em concreto, bitcoin) que a tecnologia Blockchain tem granjeado cada vez mais seguidores.

Estamos essencialmente diante de uma base de dados distribuída, contida num livro de razão (ledger) que regista todas as transações ocorridas na rede distribuída (*peer-to-peer*) de nós.

As transações unanimemente aceites pelos nós que compõem a rede são confirmadas por uma chave encriptada (*hash*) e guardadas em "blocos", que se vão ligando permanente e irreversivelmente entre si. Pelo estabelecimento de regras de consenso na rede, a tecnologia Blockchain prometeu resolver o problema computacional da inevitabilidade de falhas de comunicação nos sistemas distribuídos (*problema dos dois generais*) e o problema do *gasto duplo*. Pela vinculação de um bloco a todos os demais blocos através da chave de encriptação - *hash* - se houver uma tentativa de fraude ou de um *gasto duplo*, tudo o que o sistema vai fazer é verificar o código desse bloco e da corrente que o antecede. O bloco que será validado e reconhecido será aquele que veio da cadeia mais longa, de maior poder computacional (ou *hashpower*), ficando o outro bloco órfão (fora da cadeia).

Esta forma de garantir a segurança das transações potenciou o alastramento da tecnologia a cada vez mais áreas e setores de atividade, entre as quais, a de "smart contracts" em que um protocolo computacional executa determinada transação (contrato). No caso do *Ethereum,* alguém, em determinada data, pode contratar de forma descentralizada e independente, o envio de uma certa quantia de *Ether* para um terceiro, ou - com recurso ao *Serviço Notarial de Prova de Existência* - certificar a existência de um documento, de uma invenção ou a posse de determinado material/dados em determinada data.

Os dados da transação identificados por um dos contratantes são carregados no *Ethereum* que executa o "contrato", com recurso a um programa/código computacional. Noutro tipo de soluções, um conjunto de *smart contracts* poderá permitir a concertação da execução de várias partes simples de um contrato complexo, por exemplo, a validação da celebração por um deles (por exemplo, pela via do controlo de identificação) e a execução de fluxos financeiros entre as partes, por outro.
Não querendo qualificar juridicamente um *smart contract,* até porque tal seria impossível no espaço disponível, a verdade é que queremos contribuir para a discussão e reflexão. Estaremos diante de uma confluência de vontades, ainda que apenas digitalmente expressas e manifestadas. Parece-nos factual e irrefutável.

Poderemos não estar diante de um contrato complexo, mas estaremos pelo menos, diante de aspetos de execução material (pela via computacional) de contratos, que até podem ter maior complexidade para além da que é executada pela via do *smartcontract*.

Considerando, por facilidade de raciocínio, que estaremos pelo menos diante de um contrato simples, desde logo, como deverão relevar os vícios da vontade? Por exemplo, se alguém executa uma transação sob coação? Como reverter a execução (programada, mas errada!) de um *smart contract* porque não se teve em conta um facto (morte, por exemplo) que deveria ser extintivo da obrigação?

No domínio da responsabilidade, considerando que a arquitetura Blockchain é em rede, geograficamente dispersa e opera a grande velocidade computacional, como poderemos estabelecer um nexo de causalidade entre o facto (data e local) ocorrido – na "rede" - e o evento danoso? Dever-se-ia considerar uma qualquer solidariedade entre os nós que constituem a rede? Deveremos prever uma qualquer responsabilidade pelo risco

na pessoa da entidade que opera a rede?

Por último, admitindo que por trás de cada máquina (ou de uma rede) estará, pelo menos por agora, o Homem, enfrentamos o desafio da garantia da privacidade dos seus dados pessoais (ou metadados) que questiona os alicerces da irreversibilidade, permanência e imutabilidade do *Ledger Blockchain*.

(*) Fundadora e Senior Tech & IT Counsel da Techlawyers, Techlawyers by pbbr