**As vantagens da aplicação e utilização do blockchain na privacidade**

De forma a entender os verdadeiros benefícios da blockchain na melhoria da privacidade, precisamos inicialmente de entender o conceito de privacidade. O dicionário Merriam-Webster define privacidade como o “estado de separação/distância de companhia ou observação”, situação que não ocorre frequentemente na proteção de dados pessoais.

Atualmente, a blockchain é uma das melhores soluções para a melhoria da privacidade de dados online, visto que o armazenamento da informação não é realizado numa só base de dados, mas sim num potencialmente infinito número de lugares e de forma encriptada como garantia de segurança. A incorporação desta tecnologia em diversos sistemas modernos (por exemplo de pagamento), fornece um maior controlo ao usuário relativamente à informação que partilha e com quem a partilha. (Hall 2018).

Estas técnicas de blockchain já estão a ser aplicadas em vários países, a Estónia por exemplo, moveu gradualmente todos os dados e informações acerca dos seus cidadãos para um sistema de blockchain distribuído, em Illinois (EUA) estão também a ser efetuados testes em sistemas baseados em blockchain, que incluem um registo de nascimento. Já na Singapura, está a ser considerada a implementação de um blockchain que visa a fornecer aos seus cidadãos uma maneira simples de interagir com os serviços do governo (Hall 2018).

Assim, há ainda muito trabalho a fazer para desviar o foco da tecnologia blockchain das cripto moedas e direcionar a sua atenção para aplicações no mundo real, como a garantia de privacidade e soluções de armazenamento (Hall 2018).

**Desafios (sociais) na aplicação e utilização dos sistemas de criptomoeda (blockchain)**

Ainda que tenha inúmeros benefícios, uma das grandes barreiras ao blockchain é também uma das maiores razões para a sua popularidade: a falta de suporte e controlo por parte das autoridades. De facto, é o carácter social da blockchain, em que cada usuário da rede tem um papel, que provoca, ocasionalmente, a pobre gestão e manuseamento de dados, tendo como consequências, no caso do sistema de moedas virtuais, por exemplo, em perda de dinheiro por parte de certos utilizadores, falhas de segurança e outros.

**- A possibilidade de perda da “wallet”**

Uma vez que não atuam terceiros confiáveis na gestão de carteiras virtuais de Bitcoin, se um utilizador perder a chave privada associada à sua carteira, todas as bitcoins contidas nesta serão perdidas para sempre, uma vez que não existe nenhum método que permite a recuperação desta moeda. A perda desta chave associada à “wallet”, muitas vezes associada a danos no disco rígido ou vírus que corrompem dados, pode facilmente levar à falência um investidor de Bitcoin em meros segundos (Conti et al. 2017).

**- A facilitação de atividade criminal**

O nível de anonimato e privacidade fornecido pelo sistema de Bitcoin, ainda que não inquebrável (como irá ser exposto mais à frente), é considerável, o que justifica a elevada utilização desta moeda nas transações e atividades ilícitas, como o mercado negro, lavagem de dinheiro, evasão a taxas (Conti et al. 2017) e ainda, como foi visto recentemente, com o “WannaCry”, em ataques de ransomware (Mathews 2018).

**Falhas de segurança nos sistemas de cripto moeda (blockchain)**

Apesar da grande quantidade de benefícios que advêm do uso do Blockchain, este está também exposto a diversas ameaças que afetam, especialmente, os sistemas reguladores de moedas virtuais.

É o modelo descentralizado e o ambiente incontrolável que garantem a popularidade de moedas como a Bitcoin e Ethereum, porém, estas são também algumas das razões pelas quais hackers e ladrões conseguem tão facilmente encontrar métodos para burlar transações realizadas nestes sistemas de cripto moeda (Conti et al. 2017).

Desta maneira, há diversas vulnerabilidades associadas à tecnologia Blockchain, que são evidenciadas pelos vastos tipos de ataque que ocorrem, nomeadamente: “Double Spending” (existindo também vários métodos para o facilitar), Ataques à rede da moeda, Ataques às “mining pools” e Ataques ao cliente. (Conti et al. 2017)

**- Double Spending**

Como o nome indica, “Double Spending” é o ato de gastar as mesmas bitcoins em múltiplas transações, e é realizado ao enviar rapidamente duas transações sucessivas, de modo a enganar o destinatário do pagamento, que consequentemente não será capaz de resgatar as moedas, perdendo, assim, o produto vendido. Atualmente, “Double Spending” é um dos grandes problemas de segurança do sistema de bitcoin, e, devido ao modo como a blockchain funciona, é e sempre será possível de realizar, mesmo com a rigorosa identificação e ordenação nas transações (Conti et al. 2017).

**Os problemas de privacidade e anonimato no blockchain**

No sistema bancário tradicional, é atingido o nível de privacidade requerido através da restrição de acesso às transações, ou seja, apenas as entidades envolvidas nestas transferências têm acesso às informações associadas a estas (Conti et al. 2017)

Devido à natureza do funcionamento da tecnologia blockchain, não é possível atingir privacidade e anonimato total, uma vez que, ao efetuar uma transação de dados, toda a informação respetiva a essa transferência é revelada a qualquer utilizador conectado à rede, ainda que esta não especifique a origem da transação e que esteja encriptada. Na rede Bitcoin, por exemplo, uma transação representa um pagamento, que é certificado por uma chave digital privada pertencente ao dono anterior dessa quantidade de bitcoin, após a transação, a posse da moeda é especificada numa outra chave, agora pública (Möser 2013).

Estas chaves, utilizadas na blockchain (neste caso no sistema Bitcoin) são endereços pseudónimos que tentam desvincular a transação da identidade do utilizador, porém, as transações têm que ser identificadas, de modo a evitar o “Double Spending”. Desta maneira, a ligação entre o utilizador e a transação pode ser rastreada através destas chaves, levando à origem da transferência e expondo a identidade desse mesmo utilizador (Conti et al. 2017).

**Propostas de melhoria de privacidade e anonimato do blockchain (mais especificamente Bitcoin)**

Perante todos os problemas de privacidade que surgem devido à estrutura natural pública do blockchain existem tecnologias que melhoram e aperfeiçoam os aspetos de privacidade desta corrente de dados, que podem ser divididos em três categorias: Peer-to-peer mixing protocols, que se baseiam na utilização de um serviço de “mixing” anónimo para misturar o rasto de transferências/transações de modo a confundir eventuais rastreadores, Distributed mixing networks, que usam também protocolos de “mixing”, facilitando também as transações e, finalmente, Altcoins, que podem ser moedas alternativas ou extensões à própria bitcoin, frequentemente mais seguras, oferecendo mais privacidade e anonimato nas transferências (Conti et al. 2017).

**Fontes**

Möser.2013. Anonymity of Bitcoin Transactions – <https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf>

Conti et al. 2018. A survey on privacy and security issues of Bitcoin - <https://arxiv.org/pdf/1706.00916.pdf>

Lee Mathews.2018. Boeing Is The Latest WannaCry Ransomware Victim - <https://www.forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim/#6df80a316634>

Merriam-Webster. Definition of privacy – <https://www.merriam-webster.com/dictionary/privacy>

Hall.2018.Benefícios do Blockchain - <https://www.theguardian.com/commentisfree/2018/mar/21/blockchain-privacy-data-protection-cambridge-analytica>