ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

CRIPTOMOEDAS, CRIPTOCRIME E CRIPTOINVESTIGAÇÃO

Vytautas Fabiano Silva Zumas[1]

RESUMO

As criptomoedas, chamados por alguns de criptoativos, estão cada vez mais presentes nas relações sociais e consequentemente nas práticas criminosas. Não necessariamente atreladas a crimes cibernéticos, que demandam alto grau de especialização por parte de investigadores, estão também conectadas a crimes patrimoniais, contra a pessoa, contra a honra e assim por diante. Num caso ou no outro, urge a necessidade da padronização dessas investigações, assim como melhor capacitação da Polícia Judiciária brasileira, proporcinando repressão eficiente e uniforme em todo o país.

Palavras-chave: *blockchain*; criptomoedas; criptocrime; criptoinvestigação; crime cibernético.

INTRODUÇÃO

A investigação criminal contemporânea deve acompanhar tendências e estar sempre lateralizada às novas tecnologias, pois se o crime é assim, sua repressão também o deve ser. A existência de criptomoedas no *iter criminis* causa espanto a investigadores mais tradicionais e representa verdadeira barreira no avanço para a solução de crimes.

Apontamos aqui a extrema necessidade de melhor capacitação das polícias brasileiras. Não para a criação de milhares de especialistas em crimes relacionados direta ou indiretamente a criptomoedas, mas para que a simples menção ao termo não seja vista como barreira instransponível na coleta de provas para determinação de materialidade e autoria delitiva.

Válido frisar que a anonimização relacionada à utilização de criptomoedas é um tanto relativa. O investigador mais atento e com conhecimento basilar no campo cibernético pode galgar grandes avanços nas investigações relacionadas ao tema com exponencial taxa de sucesso na resolução de crimes.

[1] Delegado de Polícia Civil do Estado de Goiás, tendo coordenado por dez anos o Grupo Especial de Repressão a Narcóticos e Grupo de Investigação de Homicídios da 11ª Delegacia Regional de Formosa. Exerceu suas atividades no Laboratório de Operações Cibernéticas do Ministério da Justiça e Segurança Pública e atualmente encontra-se mobilizado à Coordenação de Combate ao Crime Organizado da Diretoria de Operações no âmbito da Secretaria de Operações Integradas, também do MJSP. É professor e conteudista da Escola Superior da Polícia Civil do Estado de Goiás nas disciplinas Planejamento Operacional, Investigação de Homicídios, Investigação em Local de Crime, Interceptações Telefônicas e palestrante do tema Investigação e Telemática, de inimigas a grandes confidentes. É conteudista da disciplina de "INTELIGÊNCIA CIBERNÉTICA" do Curso de Aperfeiçoamento de Inteligência De Segurança Pública – CAISP, participou do Cyber Crime Investigation Course pela Gujarat Forensic Sciences University na cidade de Ghandinagar, Gujarat, Índia. Pertence ao corpo docente do Curso de Inteligência Cibernética da Diretoria de Inteligência da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública. E-mail: vytautas.zumas@yandex.com.

Seria por demais pretenciosismo suscitar o esgotamento do tema neste artigo. O objetivo recai na demonstração da importância e necessidade de adequação de técnicas investigativas e da legislação pátria (da capacitação de profissionais à efetiva utilização em casos concretos, persecução penal e ordenamento jurídico) aos avanços da tecnologia em diversas áreas, neste caso, no contexto das criptomoedas.

1 CONCEITO DE BLOCKCHAIN

Antes de mais nada, alguns paradigmas conceituais devem ser mitigados. Importante conceituar *blockchain*, desmistificar o que o circunda e, principalmente, demonstrar sua segurança.

Trata-se de técnica criada em 1991 para impedir que documentos/contratos eletrônicos não tivessem suas datas alteradas e que ganhou holofotes em 2009 quando o personagem (não sabe-se dizer se é uma pessoa ou grupo de pessoas) Satoshi Nakamoto o adaptou para a criação da Bitcoin.

Assim, importante diferenciação deve ser feita neste momento. *Blockchain* trata-se da técnica de autenticação de informações utilizada por diversas criptomoedas, como a *Bitcoin, Ethereum, Litecoin, etc*. Assim podemos dizer que o *Blockchain* é o livro (e a técnica) de registros das transações de criptomoedas e outras informações.

E o conceito de livro de registros (*ledger*) é literalmente a essência do *blockchain*, porém com algum tempero. Trata-se de um "livro escritura" virtual, aberto e distribuído para qualquer pessoa e que pode receber registros de transações entre duas partes de maneira eficiente, descentralizada, verificada e permanente.

Nick Furneaux[i] conceituou *blockchain* como "conceito de registros de contratos e transações em um livro escritura que é distribuído por vários nós em uma determinada rede" [2]. Verifica-se que características como aberto, distribuído e público são sempre inerentes à técnica discutida.

Uma vez "registrados" no bloco, os dados são de praticamente impossível alteração em razão das características assecuratórias inerentes ao *blockchain*, daí sua importantância na manutenção da integridade das informações ali registradas.

Verificamos então que *blockchain* e *Bitcoin* (entendida como criptomoedas em geral) são entidades completamente diferentes, mas umbilicalmente ligadas entre si, sendo este o motivo para sua confusão. A título de duplo esclarecimento (sobre a diferença conceitual e ligação umbilical) citamos, superficialmente, como as transações da criptomoeda são registradas nos blocos, assim como a segurança que a técnica oferece.

[2] "Concept of recording contracts and transactions in a ledger that is distributed across many nodes on a network".

O *blockchain* da *Bitcoin* contém, dentre outros, os detalhes da transação ocorrida, o emitente da ordem, seu receptor e a quantia transacionada. Por hora deixaremos de lado como o emitente e receptor são identificados, as *wallets*, assim como a questão das chaves pública e privada que permitem que a ordem ocorra.

Os blocos nas transações da *Bitcoin* contém ainda as "impressões digitais" virtuais de cada transação, conhecidas por *hash*. O dicionário computacional Tech Terms[ii] diz que:

> *Hash* é uma função para conversão de um valor em outro. Submeter dados a *hash* (ação conhecida por *hashing*) é prática comum em ciência da computação e é utilizado para diferentes propósitos como criptografia, compressão e indexação de dados. Pilar basilar da criptografia porque é o que torna possível mascarar o dado original com outro valor. [...] Uma boa função de *hash* criptográfico não é reversível, ou seja, não é possível calcular o dado criptografado através da engenharia reversa[3].

Os *hash* mantém a integridade dos dados do bloco, pois se as informações de alguma transação forem alteradas na tentativa de burlar, por exemplo o valor transmitido, o *hash* final do bloco também será alterado, tornando fácil a detecção de alterações naquele bloco e impedindo a confirmação (prova de trabalho) que ocorre ao final de cada bloco de transações.

Cada bloco contém ainda o *hash* do bloco anterior, fazendo com que o início de cada novo bloco seja marcado com o *hash* do bloco aterior. Segundo Satoshi Nakamoto: "Cada marca temporal inclui a marca temporal anterior no seu hash, formando uma corrente, com cada marca temporal reforçando a anterior".[iii] Essa fusão do bloco anterior ao mas recente é o que dá a idéia de elos de ligação, como em uma corrente.

Ao final, e ponto fundamental na razão para o uso do Blockchain nas transações de criptomoedas, está a inexistência de terceira entidade de confiança (*Trusted Third Party*) como nas transações convencionais, estando aí a essência da privacidade do tema. Nas criptomoedas os valores virtuais são transferidos *peer to peer – P2P* (ponto a ponto) sem a necessidade de um intermediário, como as instituições financeiras.

A garantia de que as transações realmente ocorreram e ocorreram da maneira demonstrada no bloco (emissor, receptor, valor, data e hora) reside no processo de mineração.

Tal processo consiste[iv]:

[3] "A hash is a function that converts one value to another. Hashing data is a common practice in computer science and is used for several different purposes. Examples include cryptography, compression, checksum generation, and data indexing.
Hashing is a natural fit for cryptography because it masks the original data with another value. A hash function can be used to generate a value that can only be decoded by looking up the value from a hash table. The table may be an array, database, or other data structure. A good cryptographic hash function is non-invertible, meaning it cannot be reverse engineered."

> Num sistema distribuído de consenso utilizado para confirmar transações pendentes incluindo-as no *blockchain*. Reforça a ordem cronológica no *blockhain*, protege a neutralidade da rede, e permite que diferentes computadores concordem no estado do sistema. Para serem confirmadas, as transações devem ser comprimidas em um bloco que obedeça a exigentes regras criptográficas que serão verificadas pela rede. Tais regras previnem que o bloco anterior seja modificado porque isso invalidaria todos os blocos subsequentes.[4]

Em suma, é possível afirmar que a técnica de *blockchain*, como utilizada nas criptomoedas, consiste em transações realizadas através de assinaturas (mediante chave criptográfica pública e privada), sendo registradas em "livro escritura" denominado *ledger* (daí a desnecessidade de moeda no sentido físico) que é totalmente público, aberto e descentralizado (todos têm acesso), com a desnecessidade de um terceiro como intermediário (*Trusted Third Party*) uma vez que são feitas P2P e verificadas pelo processo de mineração.

Importante ressaltar que o contexto das criptomoedas é apenas uma das inúmeras possibilidades de uso do sistema de *blockchain*. Podemos citar, a exemplo, registros médicos de um paciente durante toda sua vida, atos cartorários (como a "vida" de um determinado imóvel, impedindo assim que terceiros de má fé reivindiquem o imóvel como seu), a cobrança de impostos pelo governo, sendo impossível a cobrança em duplicidade ou a falta de cobrança, a cadeia e custódia em evidências coletadas em locas de crime e surpreendentemente, todo um processo eleitoral.

2 CRIPTOMOEDAS E O CRIME

A privacidade ofertada pela criptografia e todas outras nuances que o *blockchain* entrega às transações em criptmoedas tem cada vez mais chamado a atenção de criminosos que visam o patrimônio de suas vítimas ao mesmo tempo que visam sua anonimização no ato do pagamento.

Somado às características "obscuras" que circundam a utilização de moedas virtuais para fins ilícitos está o relativo desconhecimento do tema por parte daqueles atores envolvidos na persecução penal. A equação obscuridade mais desconhecimento tem se revelado manto protetor de criminosos, panorama este que deve mudar com urgência.

Para amenizar o problema, é importante saber que tal privacidade acaba sendo relativizada pelos próprios fundamentos do *blockchain*, a saber a publicidade, abertura e descentralização do *ledger*, ou seja, todos (todos mesmo) têm acesso aos blocos das transações e sabem de onde determinada quantia

[4] Mining is a distributed consensus system that is used to confirm pending transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks.

de criptomoedas veio e para exatamente onde foi. É questão de tempo até seu proprietário (muitas vezes o próprio criminoso) monetizar o conteúdo e retornar os dados, antes virtuais e pseudoanônimos, ao mundo real.

Tão relativa é a privacidade inerente às transações que existem métodos para mascarar a publicidade característica aos blocos. Para tanto, citamos os serviços de "Lavagem de Criptomoedas" conhecidas por *Tumblers* ou *Mixers*, que consistem no processo de utilização de serviço terceirizado para interromper a conexão entre emissores e receptores de criptomoedas[v]. O que fazem basicamente é receber suas criptomoedas e, mediante uma taxa, restituir o valor equivalente em criptomoedas que pertenciam a outras pessoas, ou seja, depositam suas criptomoedas em uma grande "lava roupas" junto a criptomoedas de outras pessoas e restituem o valor equivalente advindo de diferentes transações, permitindo assim uma interrupção na "escrituração" da moeda virtual. O serviço é legal desde que o proprietário da moeda virtual busque apenas sua anonimização para fins de privacidade.

Obviamente, em nosso país, caso o montante lançado no tambor dessa a "máquina" seja proveniente de infrações penais e o escopo para utilização de tal serviço for a ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade, estaríamos notadamente falando sobre o crime de lavagem e dinheiro previsto na Lei 9.613/98[vi].

O relatório da empresa *CipherTrace*, publicado em 2018, apontou crescimento em crimes envolvendo moedas virtuais, estimando que cerca de 1.3 bilhões de dólares foram lavados em ferramentas como os citados *Tumblers* de criptomoedas[vii].

Os números acima representam que o caminho para a investigação acerca do tema, conceituada aqui como criptoinvestigação, é longo e doloroso, porém sem volta.

3 DA NECESSÁRIA ESPECIALIZAÇÃO DAS INVESTIGAÇÕES

O investigador que, durante o cumprimento de um mandado de busca e apreensão no ano de 2020, depara-se com um pedaço de papel muito bem guardado contendo os dizeres: ***monkey – ball – garden – pencil – flower – door – bottle – lamp – air – book – rug – bag*** e não tem a menor idéia do que significa, deve se preocupar.

Não se trata aqui de dizer O QUE FAZER, mas sim de PORQUE SABER O QUE FAZER. Apontamos a gritante necessidade de conhecimento mínimo necessário para conduzir investigações contemporâneas. O mínimo treinamento no assunto possibilitaria o investigador deduzir que aquela sequência de 12 palavras aleatórias poderia conduzir aos fundos do criminoso no ambiente das

criptomoedas. Nem um centavo sequer poderia ser encontrado naquela residência, mas aquela sequência mnemônica de palavras aleatórias poderia representar, literalmente, milhões.

E vamos mais longe, extorsões e outros delitos praticados por meio de aplicativos de mensageria parecem situações corriqueiras, porém caso a vantagem ilícita seja demandada com o fornecimento de uma *wallet* de criptomoedas, até mesmo o investigador mais experiente precisa ter cuidado.

A privacidade proporcionada pelas transações em criptomoedas, sem a necessidade de um terceiro de confiança (como uma instituição financeira) e sequer de uma conta bancária vinculada a dados de pessoas ou empresas tem sido amplamente utilizada por criminosos para obtenção do proveito dos crimes praticados.

Assim, é de suma importância que investigadores tenham a noção daquilo que procuram em uma investigação relacionada, mesmo que tenuamente, à utilização de criptomoedas. Não necessariamente porque devem saber analisar a fundo as carteiras, decifrar a criptografia SHA256 e serem capazes de compreender como funciona o processo de mineração dos blocos no *blockchain*. Obviamente isso seria fantástico, mas o conhecimento mínimo acerca tema (e em diversos outros ligados à investigação e tecnologia) pode proporcionar o início para o deslinde de vários crimes, antes vistos como insolucionáveis caso o agente não tivesse atento à "criptoinvestigação".

A importância da melhor capacitação acerca do tema rompe o espectro de Polícia Judiciária. Não há, atualmente, procedimento padrão para busca e apreensão de *wallets* e respectiva quantidade de criptmoedas atreladas a elas, assim como falta legislação específica acerca do tema. Tal lacuna técnica e jurídica corrobora com a importância da especialização ora sugerida, aqui especificamente não apenas por investigadores, mas também no âmbito da *persecutio criminis* como um todo e pelo Poder Legislativo Federal.

Ao final, e não menos importante, está a necessária capacidade do investigador de reproduzir em juízo os passos da investigação e esclarecer ao magistrado e membro do Ministério Público dúvidas que porventura sejam ventiladas, assim como ter a firmeza necessária para responder a perguntas técnicas por vezes formuladas pela defesa.

Por óbvio não visamos em sucinto trabalho a especialização de leitores no tema, mas tão somente acentuar a importância de atualização das técnicas de investigação usuais para que o trabalho da Polícia Judiciária acompanhe a evolução do crime e métodos utilizados por criminosos.

CONSIDERAÇÕES FINAIS

As técnicas investigativas convencionais devem andar ao lado de novas metodologias já inseridas nas novas facetas do crime. Delitos não necessariamente cometidos no ambiente cibernético

podem remeter ao contexto das criptomoedas como, por exemplo, a obtenção da vantagem patrimonial almejada. O pagamento do resgate de um sequestro exigido em criptomoedas eleva a outro nível não só o leque de possibilidades de técnicas investigativas, mas também demonstra que os criminosos do mundo real (e não apenas do virtual) já se aproveitam da anonimização relativa no escopo de cada vez mais eivarem-se dos braços da lei.

Assim, é de bom alvitre que investigadores deixem sua zona de conforto e deem o primeiro passo no aprendizado dos mecanismos que redundam as criptomoedas para que a simples exigência de valor indevido em Bitcoins (por exemplo) não se transforme em um ciclope comedor de carne humana e afugente aqueles menos esclarecidos.

Por outro lado, a capacitação oferecida pelo Estado deve estar à altura daquilo que enfrentam nos dias atuais. Policiais devem ter a seu alcance não só o treinamento (e legislação) mínimos necessários para combater o crime moderno, mas também permitir a mudança de *mindset* investigativo tradicional, quebrando assim paradigmas atrelados a crimes cometidos com ou através da tecnologia.

REFERÊNCIAS

BITCOIN. **How does Bitcoins work?** Disponível em: https://bitcoin.org/en/how-it-works. Acesso em: 25 abr. 2020.

BRASIL. **Constituição Federal.** Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 abr. 2020.

BRASIL, Lei nº 9.613 de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. **In: Diário Oficial da República Federativa do Brasil**, Brasília, DF, 4 mar. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 25 abr. 2020.

CRYPTALKER. **10 Best Bitcoin Tumbler (Mixer) Services**. Disponível em: https://cryptalker.com/best-bitcoin-tumbler. Acesso em: 25 abr. 2020.

CRYPTOBUZZ. **$1.3 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers**. Disponível em: https://cryptographybuzz.com/cryptocurrency-laundered-bitcoin/. Acesso em: 25 abr. 2020.

FURNEAUX, Nick. Investigating **Cryptocurrencies:** Understanding, Extracting, and Analyzing Blockchain Evidence. Indianapolis: Wiley, 2018.

NAKAMOTO, Satoshi. **Bitcoin:** Um Sistema de Dinheiro Eletrônico Ponto a Ponto. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf. Acesso em: 25 abr. 2020.

TECH TERMS. **The Computer Dictionary**. Disponível em: https://techterms.com/definition/hash. Acesso em 25 abr. 2020.

[i] FURNEAUX, Nick. **Investigating Cryptocurrencies**: Understanding, Extracting, and Analyzing Blockchain Evidence. Indianapolis: Wiley, 2018. p.39

[ii] TECH TERMS. **The Computer Dictionary**. Disponível em: https://techterms.com/definition/hash. Acesso em: 25 abr. 2020.

[iii] NAKAMOTO, Satoshi. **Bitcoin:** Um Sistema de Dinheiro Eletrônico Ponto a Ponto. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf. Acesso em: 25 abr. 2020.

[iv] BITCOIN. **How does Bitcoins work?**. Disponível em: https://bitcoin.org/en/how-it-works. Acesso em: 25 abr. 2020.

[v] CRYPTALKER. **10 Best Bitcoin Tumbler (Mixer) Services**. Disponível em: https://cryptalker.com/best-bitcoin-tumbler. Acesso em: 25 abr. 2020.

[vi] BRASIL, Lei nº 9.613 de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 4 mar. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm . Acesso em: 25 abr. 2020.

[vii] CRYPTOBUZZ. **$1.3 Billion in Cryptocurrency Laundered Through Bitcoin Tumblers.** Disponível em: https://cryptographybuzz.com/cryptocurrency-laundered-bitcoin/. Acesso em: 25 abr. 2020.