Caminhos para um Real Digital on-chain compatível com o direito à privacidade e proteção de dados pessoais desde a concepção

Subeixo: direito e tecnologia da informação

Aline Cruvinel[1]
Jeff Prestes[2]

Resumo

O objetivo do presente artigo é levantar os pontos de contato entre *Central Bank Digital Currencies* (CBDCs), privacidade, proteção de dados, sigilo bancário, open finance e o projeto do Real Digital de uma perspectiva do ordenamento jurídico da União Europeia e do Brasil de proteção de dados pessoais. Visa abordar o que são técnicas que aumentam a proteção de dados, como funciona o mecanismo de *Zero Knowlegde Proof* e como ele se aplica ao projeto do Real Digital. O artigo analisou publicações do Parlamento Europeu, OCDE e leis brasileiras sobre privacidade, proteção de dados, sigilo bancário e *Open Finance*.

Palavras-chave: CBDCs; *privacidade; zero knowlegde proof; anonimização.*

Abstract

The objective of this article is to raise the points of contact between *Central Bank Digital Currencies* (CBDCs), privacy, data protection, banking secrecy, open finance, the Real Digital project from a perspective of the legal system of the European Union and Brazil for the protection of personal data. It aims to address what are techniques that increase data protection and how the Zero Knowlegde Proof mechanism works and how it applies to the Real Digital project. This article analyzed publications of the European Parliament, OECD and Brazilian laws on privacy, data protection, banking secrecy and Open Finance.

Keywords: CBDCs*; privacy; zero knowlegde proof; anonymization.*

1 aline.cruvinel@mackenzista.com.br. Mestranda em direito político e econômico pela Universidade Presbiteriana Mackenzie.
2 jeffprestes@gmail.com. Professor e profissional de tecnologia especialista em Blockchain.

1 Desafios das CBDCS e origem do princípio da autodeterminação informativa

As maiores economias do mundo enfrentam hoje o dilema de como aproveitar o potencial das *Central Bank Digital Currencies* (CBDCs), sem prejudicar o direito fundamental à privacidade a proteção de dados pessoais e o sigilo bancário. É natural que uma nova tecnologia coloque o regulador diante de um novo *trade-off*. Em que medida seria viável reduzir a privacidade de dados pessoais para usufruir dos benefícios de um sistema transparente, descentralizado e facilmente auditável? O Banco da Inglaterra, em seu *paper*[1] (2023, p. 15), publicado em 7 de fevereiro de 2023, assim expõe a questão:

> A libra digital teria as mesmas (ou mais fortes) proteções de privacidade que contas bancárias, cartões de débito ou cheques. Os detalhes pessoais dos indivíduos seriam conhecidos por seu provedor de carteira do setor privado da mesma forma que são para provedores de contas bancárias hoje (e sujeitos às mesmas proteções de privacidade). Mas os detalhes pessoais dos indivíduos não seriam conhecidos pelo governo ou pelo Banco da Inglaterra. (tradução livre).

No Brasil, a cultura da privacidade e proteção de dados pessoais foi majoritariamente importada da União Europeia. Essa cultura encontra suas raízes no princípio da autodeterminação informativa, por meio do qual o indivíduo possui a prerrogativa de conhecer e controlar como seus dados pessoais serão utilizados, por quem e para quais finalidades.

Na ocasião do relevante julgamento do caso do censo pela Corte Constitucional Alemã (*Bundesverfassungsricht*), em 1983[2], cunhou-se o entendimento de que o Estado não pode concentrar em si uma imensa quantidade de dados pessoais para usar em finalidades abertas, diante do potencial para causar restrição às liberdades individuais e aos direitos fundamentais dos cidadãos.

Desse entendimento, decorre a obrigação de que o Estado, ou qualquer controlador de dados pessoais, se atenha às finalidades para as quais os dados foram coletados, dando transparência desses propósitos publicamente. Sem isso, o titular de dados pessoais perde o controle dos motivos para os quais seus dados foram coletados e se vê diante de uma hipervigilância irrestrita.

Essa discussão se intensificou entre União Europeia e EUA após o ataque terrorista de 11 de setembro 2001, quando a NSA começou a violar a privacidade de cidadãos americanos ou não, em prol de uma irrestrita carta branca para garantir a segurança nacional conforme revelado por Edward Snowden[3] em 2013.

No Brasil, têm-se como fundamentos da Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) elencados no art. 2º, dentre outros, a autodeterminação informativa e o respeito à privacidade. No mesmo artigo, também se encontra como fundamento o

1 UK. **The digital pound**: a new form of money for households and businesses? Disponível em: https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper. Acesso em: 14 mar. 2023.

2 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

3 DOCUMENTÁRIO Citizenfour. Disponível em: https://www.youtube.com/watch?v=upg9hweFRpw. Acesso em: 14 mar. 2023.

desenvolvimento econômico/tecnológico e a inovação. O legislador quis contemplar tanto a privacidade do titular quanto o desenvolvimento tecnológico/inovação, tornando legítimo o uso de dados pessoais dentro dos limites estabelecidos pela lei para alavancar novas tecnologias e soluções inovadoras.

Trazendo para o contexto financeiro, a privacidade também é regulada pela Constituição Federal de 1988, pela Resolução Conjunta nº 1/2020[4] do Banco Central que regula o *Open Finance* e pela Lei Complementar nº 105/2001, que dispõe sobre o sigilo bancário. O *Open Finance* vincula o compartilhamento de dados bancários entre instituições ao consentimento livre, inequívoco e informado do titular. Já o sigilo bancário é um direito fundamental garantido pela Constituição Federal, passível de ser afastado apenas para a proteção do interesse público, por exemplo, em apuração de qualquer ilícito criminal (art 1°, § 4º), infrações administrativas (art. 7º) e procedimento administrativo fiscal (art. 6º).

Ao contrário da legislação californiana[5] de proteção de dados pessoais que expressamente prevê dados financeiros como dados pessoais sensíveis, a LGPD não imputa às transações financeiras necessariamente a categoria de dado pessoal ou mesmo dado pessoal sensível.

Entretanto, o conceito amplo de dado pessoal trazido pelo art. 5º, inciso I, é abrangente o suficiente para abarcar com tranquilidade as movimentações financeiras feitas por um cidadão brasileiro ou qualquer dado bancário capaz de tornar identificável uma pessoa física.

Diante disso, surge a obrigação de observar todo o regramento das leis de proteção de dados pessoais no Brasil ou leis estrangeiras quando dados pessoais de estrangeiros forem tratados.

2 Tensão entre privacidade e blockchain

O uso de uma tecnologia DLT para o projeto do Real Digital que envolva dados pessoais gera uma tensão preliminar com o ordenamento que se construiu até hoje. Em julho de 2019, o Parlamento da União Europeia publicou estudo[6] enfrentando a aparente incompatibilidade entre o Regulamento Geral de Proteção de Dados da União Europeia e DLTs. Nesse estudo, o Parlamento reconhece que o uso de DLTs pode trazer maior controle para o titular de dados pessoais contemplando o exercício do seu direito à autodeterminação informativa. Entretanto, alguns cuidados precisam ser observados para garantir a anonimização dos dados e não apenas a pseudoanonimização[7]. A anonimização seria o caminho mais seguro para o tratamento de dados, uma vez que, sem a identificação

4 BRASIL. Congresso Nacional. **Resolução Conjunta nº 01/2020 do Banco Central do Brasil e do Conselho Monetário Nacional**. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_P.pdf. Acesso em: 14 mar. 2023.

5 ESTADOS UNIDOS. **Lei de Privacidade do Consumidor da Califórnia de 201**8. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

6 Can distributed ledgers be squared with European data protection law? Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 15 mar. 2023.

7 Definição dada pelo art. 4º, item 5 do Regulamento Geral sobre a Proteção de Dados 2016/679: Pseudonimização – o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 14 mar. 2023.

do titular, não há risco à privacidade. Porém é muito comum achar que os dados estão anonimizados quando, na verdade, usando informações adicionais, é plenamente possível identificar um titular.

Para transacionar tokens do Real Digital ou mesmo CBDCs entre bancos, ainda que em uma rede permissionada restrita a instituições financeiras selecionadas, é necessário implementar ferramentas disponíveis no estado da arte que sejam capazes de proteger os titulares tornando-os anônimos.

Isso porque (i) os dados na *blockchain* são considerados pseudoanonimizados, ou seja, utilizando meios técnicos, é possível conhecer quem são os donos das transações financeiras realizadas por uma chave pública; (ii) caso os dados pessoais não sejam anonimizados, seria necessário cumprir com todas as obrigações da LGPD, garantir o direito dos titulares, tais como oposição ao tratamento, eliminação de dados e retificação, bem como coletar o consentimento livre, inequívoco e informado do titular de dados pessoais para o compartilhamento com outros bancos de forma a atender às regras vigentes do *Open Finance*; (iii) ainda que não diretamente identificadas, as transações financeiras poderiam gerar um perfil comportamental de uma determinada carteira que poderia ser facilmente utilizada por instituições financeiras visando direcionar ou inibir o acesso a produtos e serviços bancários pelo titular de dados pessoais gerando dano relevante.

É preciso mapear e analisar com cuidado, na fase de testes, quais dados pessoais estão envolvidos em um projeto de uma CBDC ou tokens do Real Digital e quais podem ser mantidos *off-chain* para garantir maior privacidade e controle tanto do titular quando do banco. Já os dados pessoais que forem tratados *on-chain*, precisam observar mecanismos de autorregulação para garantir privacidade, autodeterminação informativa e liberdade para os usuários que estão realizando operações lícitas e gozam de direito à privacidade e ao sigilo bancário.

O conceito de *Privacy by Design* criado por Ann Cavoukian[8] é uma das ferramentas para pensar uma solução tecnológica que tenha imbuída em seu desenho a proteção dos dados pessoais. É fato que o conceito foi desenvolvido nos anos 1990 para a estrutura de Web2. Porém, os conceitos são amplos e podem encontrar sua aplicação também para soluções WEB3.

Além do conceito de *Privacy by Design* de Ann Cavoukian, é possível pensar em ferramentas que tragam privacidade ao desenho de uma solução de maneira mais específica. São as chamadas *Privacy Enhancing Technologies* (PET).

Doneda (2019, p. 290) conceitua *Privacy Enhancing Technologies* (PET) como "basicamente qualquer meio tecnológico desenhado para atuar na arquitetura tecnológica da privacidade – impossibilitando, limitando ou mesmo facilitando uma determinada ação".

8 CAVOUKIAN, Ana. **Privacy by Design The 7 Foundational Principles**. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 16 mar. 2023.

A OCDE[9] e o Parlamento Europeu[10] apontam que o uso de *Zero Knowlegde Proof* teria a capacidade de garantir a privacidade desde a concepção de um projeto *on-chain (privacidade by design)*, gerando o necessário *compliance* com o GDPR e consequentemente com a LGPD. No capítulo seguinte explicaremos o que é *Zero Knowlegde Proof* e como essa ferramenta pode assegurar privacidade à rede blockchain do Banco Central.

3 Entendo zero-kwonledge proofs ou ZKP (Protocolo de Prova de Zero Conhecimento) e seu uso na rede blockchain do BACEN

Com base na Wikipedia, a definição de *Zero Knowledge Proof* (ZKP) seria:

> [...] *zero knowledge proof* ou protocolo de zero conhecimento é um método que o atestador pode provar a um verificador que uma dada afirmação é verdadeira enquanto o atestador evita transmitir qualquer informação adicional senão a que a afirmação é realmente verdadeira. A essência do zero-knowledge proof é que é trivial atestar que uma entidade possui o conhecimento de uma certa informação simplesmente revelando-a; o desafio é provar possuir tal informação sem revelar a mesma ou quaisquer informações adicionais.

A tecnologia ZKP pode ser amplamente utilizada em diferentes campos, como votações ou transferências financeiras anônimas em projetos CBDC, em que é difícil garantir essa anonimidade em bancos de dados públicos, como *blockchains*.

Mixers são contratos inteligentes que, aliados à ZKP, são usados para anonimizar transações em *blockchains* baseadas em EVM, públicas ou permissionadas.

3.1 Contexto

Por conta da sua natureza, todas as transações em *blockchain* são compartilhadas aos membros da rede. Se você possui algum ETH na sua conta, você não pode transferi-lo anonimamente porque o registro da transferência fica em um livro caixa ou banco de dados aberto.

Como anonimizar as transações? Os *Mixers* resolveram esse problema de privacidade quebrando a conexão entre os endereços das contas do destinatário e do remetente usando ZKP.

Neste artigo, demonstramos que o uso de ZKP estruturado em um *Mixer* pode trazer privacidade aos projetos CBDC (*Central Bank Digital Currency*) ou Moeda Digital do Banco Central. Pois, hoje, anonimizar as transações é um dos maiores entraves para o início de projetos CBDC pelos bancos centrais pelo mundo.

9 OCDE. **Emerging privacy-enhancing technologies Current regulatory and policy approaches**. Disponível em: https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm. Acesso em: 16 mar. 2023.

10 UE. **Report on Blockchain:** a forward-looking trade policy. Disponível em: https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html. Acesso em: 16 mar. 2023.

Desse modo, no banco de dados do Projeto-Piloto do Banco Central para o Real Digital as transações precisam perder a associação pública entre o destinatário e o remetente, tornando as transações anonimizadas.

Como funciona um *Mixer*? Para você anonimizar uma de suas transações usando um *Mixer,* você deve depositar uma pequena quantidade de Real Digital (ou um token ERC20) no contrato do *Mixer*. Depois de alguns blocos, você ou outra pessoa pode sacar este 1 Real Digital com uma conta diferente. A inovação aqui é que ninguém, além dos interessados, pode associar a conta remetente e a conta destinatária. Se centenas de contas depositarem 1 Real Digital de um lado, e outras centenas de contas sacarem de outro, ninguém será capaz de seguir o caminho da movimentação de Real. O desafio tecnológico é que as transações nos contratos inteligentes também são públicas como quaisquer outras transações em *blockchain*. É neste ponto que ZKP se torna relevante.

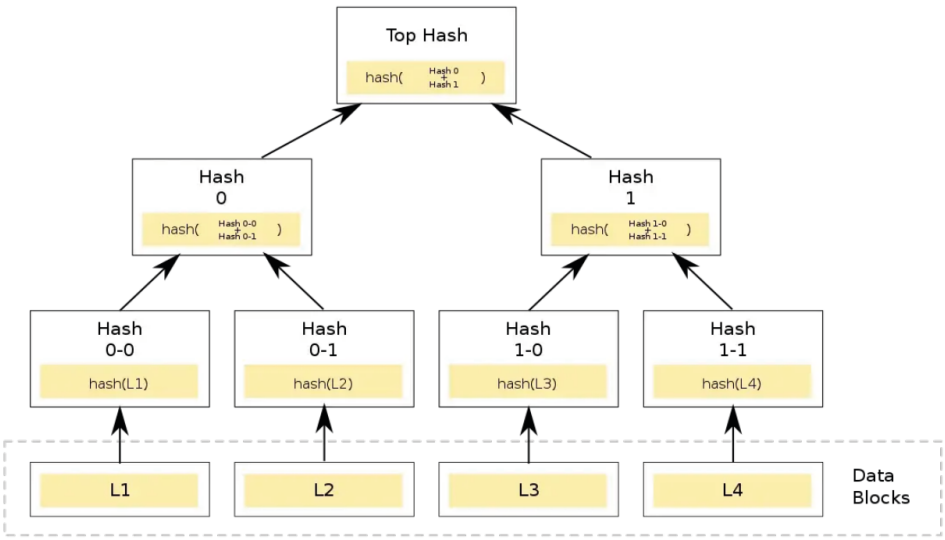
Quando você deposita seu 1 Real no contrato inteligente do *Mixer*, você pode prover um "registro". Esse registro é armazenado no contrato inteligente. Quando o destinatário saca 1 Real do outro lado, ele tem de fornecer um "anulador" e uma prova ZKP. O "anulador" possui esse nome pois, após o saque, ele anula o registro de depósito e, assim, evita que o destinatário da transação saque duas ou mais vezes o valor definido no registro.

O anulador é rastreado pelo contrato inteligente do Mixer, de maneira que somente podemos realizar um saque por anulador. O anulador tem um identificador único, que é a conexão com o registro, e a prova garante essa conexão, mas ninguém sabe a qual registro este anulador está conectado (exceto os donos das contas remetente e destinatária da transação).

Resumindo: nós podemos provar que um registro é designado ao nosso anulador, sem revelar o registro.

Parece fácil, não? Mas vejamos a parte tecnológica.

Primeiro precisamos entender um item usado pelo Mixer e projetos similares: a árvore Merkle.

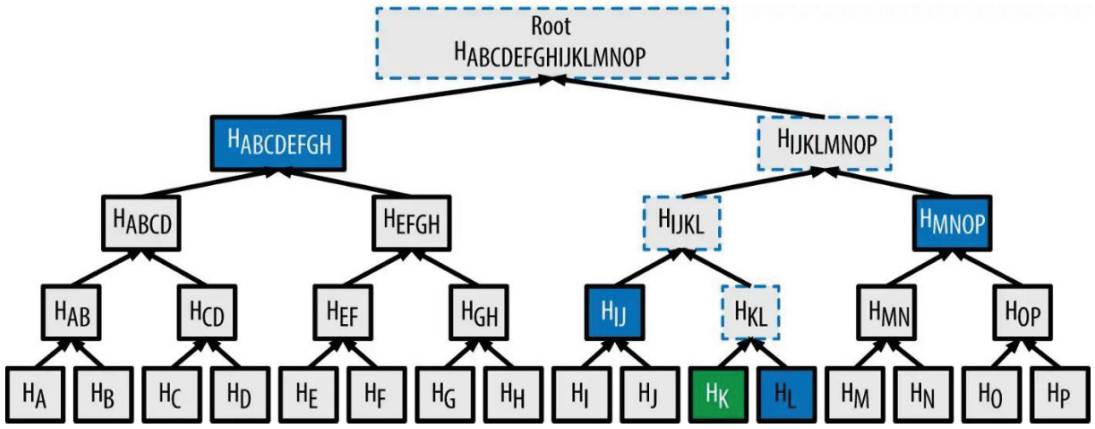


Uma árvore *Merkle* é uma árvore de *hashes*. Para quem não conhece, *hash* é uma identificação única para qualquer informação digital.

Em uma árvore *Merkle* as folhas são os elementos ou informações, e todos os galhos (ou nós) são *hashes* de suas ramificações (ou nós filhos). A raiz da árvore (apresentada na imagem acima de ponta-cabeça) é a raiz *Merkle* – que representa todo um conjunto de informações. Se você adicionar, remover, ou mudar qualquer informação em uma folha da árvore, a raiz *Merkle* vai mudar. Em resumo: a raiz *Merkle* é um identificador único do conjunto de informações distribuídas nas folhas.

Mas como podemos usá-la?

Existe uma outra coisa chamada prova *Merkle*. Se eu tenho uma raiz *Merkle*, você pode me enviar uma prova *Merkle* que atesta que uma informação que está em seu conjunto é representada pela raiz *Merkle*. A figura a seguir mostra como funciona.



Se você quiser me provar que *hash* de K está no conjunto de informações que compõem a árvore, você deve me enviar os *hashes* de L, K, IJ, MNOP, ABCDEFGH – lembrando que H na imagem acima quer dizer "*Hash* de".

Usando esses *hashes*, eu posso calcular a raiz *Merkle*. Se a raiz *Merkle* é a mesma raiz que tenho, eu posso ficar tranquilo que o *hash* de K está na árvore. E onde podemos usar isso?

Um exemplo simples é uma lista de clientes pré-aprovados e com permissão para realizar uma transferência. Imagine um contrato inteligente realizando esse controle de uma

base de 1.000 clientes. O contrato inteligente até pode armazenar toda essa base, mas uma solução computacionalmente mais otimizada seria construir uma árvore *Merkle*, e armazenar somente a raiz. Se alguém quiser executar a transferência, basta enviar a prova *Merkle*, neste caso a lista de 10 *hashes*, que podem ser facilmente verificadas pelo contrato inteligente.

Novamente: uma árvore *Merkle* é usada para representar um conjunto de elementos/informações com um único *hash* – a raiz *Merkle*. A existência de um elemento pode ser provada pela prova *Merkle*.

A próxima coisa que temos de entender é a prova ZKP. Para gerar uma prova ZKP, você precisa de um circuito. Um circuito é algo como um pequeno programa de computador que tem entradas e saídas de dados públicos e entradas de informações privadas. Essas entradas de dados privados são aquelas informações que você não revela para verificação. São sigilosas. Com os circuitos, nós podemos provar que a saída de informação foi gerada a partir das entradas, privadas e/ou públicas. Por isso chamamos ZKP de Protocolo de Prova de Zero Conhecimento.

O código fonte de um circuito se parece com isso:

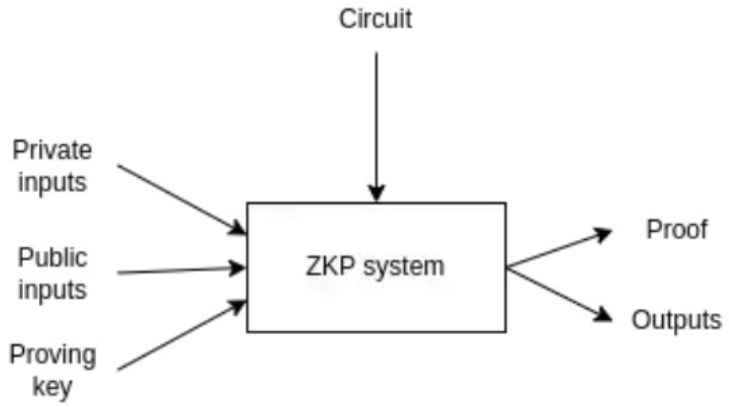
```
pragma circom 2.0.0;

include "node_modules/circomlib/circuits/bitify.circom";
include "node_modules/circomlib/circuits/pedersen.circom";

template Main() {
  signal input nullifier;
  signal output nullifierHash;

  component nullifierHasher = Pedersen(248);
  component nullifierBits = Num2Bits(248);

  nullifierBits.in <== nullifier;
  for (var i = 0; i < 248; i++) {
    nullifierHasher.in[i] <== nullifierBits.out[i];
  }

  nullifierHash <== nullifierHasher.out[0];
}

component main = Main();
```

Usando esse circuito, nós podemos provar que nós sabemos a fonte de um dado *hash*. Esse circuito tem apenas uma entrada, o anulador, e uma saída, o *hash* do anulador. A acessibilidade padrão das entradas de dados é privada, e as saídas são públicas. Esse circuito usa duas bibliotecas Circomlib. A primeira é a *bitlify*, que contém funções de manipulação de bits; a segunda é pedersen, que contém o gerador de *hash* Pedersen. Lembrando que *hashes* são identificadores únicos de informações digitais.

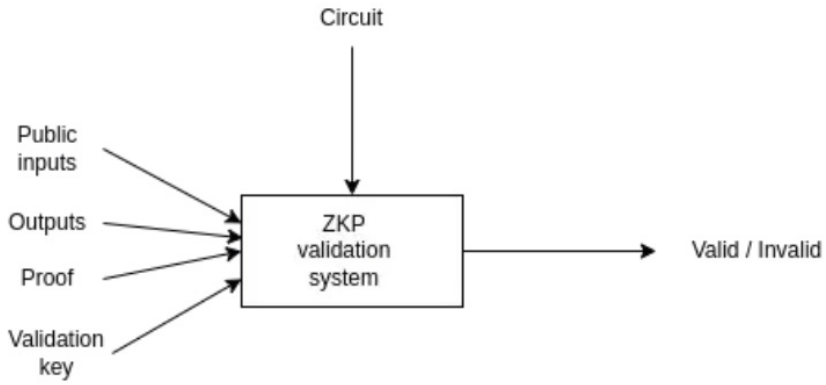
O gerador de *hash* Pedersen é uma função que é executada de maneira eficiente dentro de circuitos ZKP. Neste exemplo, no corpo do template Main, nós preenchemos o *hasher* com informações digitais e executamos a função para ele gerar o *hash*.

Para gerar a prova que conhece a informação, uma das coisas que você vai precisar é de uma "*proving key*", ou podemos traduzir como chave de credibilidade. Esta é a parte mais sensível de ZKP, porque utilizando a fonte de dados que foi usada para gerar a chave de

credibilidade, qualquer um pode gerar provas "*fake*" ou falsas. Essa fonte de informação é chamada de "lixo tóxico", e tem de ser removida a qualquer custo. Por essa razão existe uma "cerimônia" para geração da chave de credibilidade. A cerimônia tem muitos participantes, e todo participante contribui com alguma informação genérica para gerar a chave. Contudo, se houver ao menos um participante honesto, a geração de uma chave de credibilidade segura está garantida. Usando entradas de dados privadas e uma chave de credibilidade, o sistema ZKP pode executar o circuito e gerar a prova e a saída de dados.



Existe também uma chave de validação ("*validation key*") para cada chave de credibilidade. O sistema de validação usa as entradas públicas (caso existam), as saídas e a chave de validação para validar a prova, como mostra o diagrama a seguir.

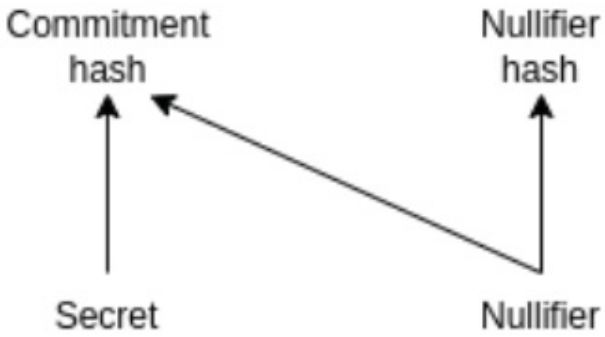


Snarkjs é uma ferramenta completa para manusearmos todos esses artefatos descritos. Gerar a chave de credibilidade e de verificação por meio da cerimônia e, com elas, a ferramenta também gerar a prova ZKP e validá-la. Ela também pode gerar um contrato inteligente para a verificação, que pode ser usada por um outro contrato inteligente para validar a prova ZKP.

3.2 Uso do ZKP no contexto do Real Digital.

Nós reunimos neste ponto tudo para entender como um *Mixer* funcionava e como poderemos criar algo similar dentro do projeto-piloto do Real Digital. Vamos chamar este projeto de RD. Quando você deposita 1 Real no contrato inteligente do RD, você tem de prover um *hash* de registro. Ele será armazenado na árvore *Merkle* do RD. Quando alguém for sacar esse 1 Real com uma conta diferente, o sacador tem de fornecer duas provas ZKP. A primeira prova que a árvore *Merkle* contém é o seu registro. Esta é a prova ZKP da prova *Merkle*. Mas isso só não é suficiente, porque você precisa fornecer o anulador, que é a chave única do registro. O contrato inteligente do RD armazena-o e garante que ninguém poderá sacar o dinheiro depositado novamente.

A singularidade do anulador é garantida pela função de geração do registro. O registro é gerado de um anulador e o segredo pela criação do *hash*. Se você alterar o anulador, então o registro irá mudar. Dessa forma, o anulador pode ser usado somente para um registro. Por conta da natureza unidirecional da geração do *hash*, dados => *hash*, não é possível associar o registro ao anulador, mas podemos gerar um ZKP para isso.



Após toda essa teoria, vejamos como seria o possível código do circuito do RD.

```
include "../node_modules/circomlib/circuits/bitify.circom";
include "../node_modules/circomlib/circuits/pedersen.circom";
include "merkleTree.circom";

// computes Pedersen(nullifier + secret)
template CommitmentHasher() {
    signal input nullifier;
    signal input secret;
    signal output commitment;
    signal output nullifierHash;
    component commitmentHasher = Pedersen(496);
    component nullifierHasher = Pedersen(248);
    component nullifierBits = Num2Bits(248);
    component secretBits = Num2Bits(248);
    nullifierBits.in <== nullifier;
    secretBits.in <== secret;
    for (var i = 0; i < 248; i++) {
        nullifierHasher.in[i] <== nullifierBits.out[i];
        commitmentHasher.in[i] <== nullifierBits.out[i];
        commitmentHasher.in[i + 248] <== secretBits.out[i];
    }
    commitment <== commitmentHasher.out[0];
    nullifierHash <== nullifierHasher.out[0];
```

```
}

// Verifies that commitment that corresponds to given secret and nullifier is included in the
merkle tree of deposits
template Withdraw(levels) {
    signal input root;
    signal input nullifierHash;
    signal private input nullifier;
    signal private input secret;
    signal private input pathElements[levels];
    signal private input pathIndices[levels];
    component hasher = CommitmentHasher();
    hasher.nullifier <== nullifier;
    hasher.secret <== secret;
    hasher.nullifierHash === nullifierHash;
    component tree = MerkleTreeChecker(levels);
    tree.leaf <== hasher.commitment;
    tree.root <== root;
    for (var i = 0; i < levels; i++) {
        tree.pathElements[i] <== pathElements[i];
        tree.pathIndices[i] <== pathIndices[i];
    }
}

component main = Withdraw(20);
```

Para melhor entendimento, é interessante recordar que, neste artigo, usamos o termo registrar/registro para o termo commit em inglês.

O primeiro template é o *CommitmentHasher*. Ele tem duas entradas – o anulador e o segredo – que são dois números randômicos de 248-bits. O *template* calcula o *hash* do anulador e calcula o *hash* do registro, que é o *hash* do anulador e o segredo.

O segundo *template* é o *Withdraw*, que lida com o saque. Ele tem duas entradas de dados públicos, a raiz *Merkle* e o *hash* do anulador (*nullifierHash*). A raiz *Merkle* é necessária para verificar a prova *Merkle* e o *hash* do anulador é para o contrato inteligente do RD armazená-lo. Os *inputs* privados são o anulador, o segredo e os caminhos dos ramos da árvore *Merkle* para os elementos e índices da prova *Merkle*. O circuito verifica o anulador, gerando o registro a partir do próprio anulador e do segredo e também verifica a prova *Merkle* fornecida. Se tudo estiver correto, a prova ZKP é gerada e poderá ser verificada pelo contrato inteligente do RD.

O verificador é gerado pelo circuito. Ele é usado pelo contrato inteligente do TC para verificar a prova ZKP por meio do *hash* do anulador e da raiz *Merkle*.

A forma mais fácil de usar o contrato inteligente do RD será por meio de carteiras de criptoativos personalizadas para a rede *blockchain* do projeto-piloto do Real Digital do Banco Central, onde não só os cálculos das provas ZKP seriam gerados, mas também onde todo o controle de acesso a essa mesma rede seria feito.

O protocolo de Prova de Zero Conhecimento, ZKP, é relativamente novo no mundo *cripto*. A matemática envolvida é realmente complexa e difícil de entender. Contudo, ferramentas como *snarkjs* e *circom* facilitam o seu desenvolvimento.

4 Conclusão

Como apresentado no presente artigo, a tecnologia ZKP tem o potencial para ajudar o Banco Central do Brasil em seu projeto de CBDC e Real Digital, bem como outros bancos centrais pelo mundo a contornar a tensão entre privacidade e blockchain.

O desafio de equilibrar o direito fundamental à privacidade e à proteção de dados pessoais e o interesse público na prevenção à lavagem de dinheiro e ilícitos financeiros precisa encontrar sua exata medida. Para que isso aconteça, é crucial testar, desde o início, a aderência do sistema aos princípios da LGPD e GDPR, bem como mecanismos adicionais de Privacy Enhancing Technologies (PET) com reconhecido potencial para garantir anonimização das transações, exemplo da tecnologia ZKP apresentada neste artigo.

A celebrada inovação do universo cripto precisa caminhar ao lado da liberdade dos indivíduos de se verem livres para transacionar seus ativos com um intermediário que respeite sua autonomia fazendo valer os valores fundamentais do Estado Democrático de Direito.

References

BANK OF ENGLAND AND HM TREASURY. **The digital pound**: a new form of money for households and businesses? 2023. Disponível em: https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper. Acesso em: 24 mar. 2023.

DOCUMENTÁRIO Citizenfour. Disponível em: https://www.youtube.com/watch?v=upg9hweFRpw. Acesso em: 14 mar. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

BRASIL. Congresso Nacional. **Resolução Conjunta nº 01/2020 do Banco Central do Brasil e do Conselho Monetário Nacional**. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_P.pdf. Acesso em: 24 de março de 2023.

BRASIL. Congresso Nacional. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 mar. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Lei de Privacidade do Consumidor da Califórnia de 2018**. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode= CIV&title=1.81.5. Acesso em: 24 mar. 2023.

CAVOUKIAN, Ana. **Privacy by Design The 7 Foundational Principles.** 2009. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 24 mar. 2023.

OCDE. **Emerging privacy-enhancing technologies Current regulatory and policy approaches**. Disponível em: https://www .oecd.org/publications/emerging-privacy-enhancing-technologies- bf121be4-en.htm. Acesso em: 24 mar. 2023.

UNIÃO EUROPEIA. **Report on Blockchain**: a forward-looking trade policy. 2018 Disponível em: https://www.europarl.europa.eu /doceo/document/A-8-2018-0407_EN.html. Acesso em: 24 mar. 2023.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de Dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal- content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 24 mar. 2023.

UK. **The digital pound**: a new form of money for households and businesses? Disponível em: https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper. Acesso em: 14 mar. 2023.