UNIVERSIDADE D
COIMBRA

Lara Micaela Pereira da Costa e Fonseca Trindade

INVESTIGAÇÃO DE SUPORTE TECNOLÓGICO PARA CRIPTOMOEDAS DE BANCOS CENTRAIS

Dissertação no âmbito do Mestrado em Engenharia Informática, especialização em Sistemas de Informação, orientada pelo Professor Doutor Paulo Rupino da Cunha, da Faculdade de Ciências e Tecnologia, e pelo Professor Doutor Manuel Paulo Albuquerque Melo, da Faculdade de Economia, e apresentada à Faculdade de Ciências e Tecnologia / Departamento de Engenharia Informática.

Junho de 2021

Faculdade de Ciências e Tecnologia
Departamento de Engenharia Informática

INVESTIGAÇÃO DE SUPORTE TECNOLÓGICO PARA CRIPTOMOEDAS DE BANCOS CENTRAIS

Lara Micaela Pereira da Costa e Fonseca Trindade

Dissertação no âmbito do Mestrado em Engenharia Informática, especialização em Sistemas de Informação, orientada pelo Professor Doutor Paulo Rupino da Cunha, da Faculdade de Ciências e Tecnologia e pelo Professor Doutor Manuel Paulo Albuquerque Melo, da Faculdade de Economia, apresentada à Faculdade de Ciências e Tecnologia / Departamento de Engenharia Informática.

Junho de 2021

1 2 9 0

UNIVERSIDADE D
COIMBRA

Resumo

Durante algum tempo, os reguladores monetários, a banca, e o setor financeiro em geral, mostraram-se bastante céticos sobre a possibilidade das criptomoedas poderem vir a mudar o cenário monetário e financeiro existente. Contudo, não podendo ignorar o recente paradigma das criptomoedas, os Bancos Centrais estão atualmente interessados na criação das suas próprias *Central Bank Digital Currencies* (CBDCs), que se apresentam como uma versão digital das moedas fiduciária nacionais, satisfazendo as mesmas funções de meio de pagamento, unidade de medida e reserva de valor. Sendo uma moeda centralizada e administrada pelo Banco Central de um país, contrariamente às criptomoedas, como a Bitcoin (emitida de forma distribuída), as CBDCs tendem a ter a mesma estabilidade que as moedas fiduciárias, pois os Bancos Centrais retêm o monopólio da sua emissão.

Numa primeira fase do trabalho desenvolvido, efetuámos a revisão sistemática de literatura para estudar as características e principais conceitos de base da Bitcoin e das moedas digitais de Bancos Centrais, Diem, DCEP, Digital Euro e E-krona, para o desenvolvimento de provas de conceito, tendo-se determinado que a privacidade e a confidencialidade são as características mais relevantes para o efeito.

Posteriormente, implementámos as provas de conceito para as CBDCs, com as características de privacidade e confidencialidade definidas, juntamente com uma demonstração do seu funcionamento. Para esse fim, houve necessidade de implementar um *webservice* e um *smart contract*, tendo-se utilizado os *softwares* Ganache (*blockchain* privada) e Metamask (*software* de carteiras).

Através da demonstração com as provas de conceito foi comprovado que as características de privacidade e confidencialidade são viáveis para utilização nas CBDCs.

Palavras-Chave

Moeda digital do Banco Central (CBDC), Criptomoedas, Privacidade, Confidencialidade, Provas de conceito

Abstract

For some time, monetary regulators, banks, and the financial industry in general have been very skeptical that cryptocurrencies could change the existing monetary and financial landscape. However, unable to ignore the recent cryptocurrency paradigm, Central Banks are currently interested in creating their own Central Bank Digital Currencies (CBDCs), which stand as a digital version of national fiat currencies, fulfilling the same functions of means of payment, unit of measure, and store of value. As a centralized currency managed by a country's Central Bank, unlike cryptocurrencies such as Bitcoin (issued in a distributed manner), CBDCs tend to have the same stability as fiat currencies, since Central Banks retain the monopoly on their issuance.

In the first phase of the work developed, we performed a systematic literature review to study the characteristics and main basic concepts of Bitcoin and the digital currencies of Central Banks, Diem, DCEP, Digital Euro and E-krona, for the development of proofs of concept, having determined that privacy and confidentiality are the most relevant characteristics for this purpose.

Subsequently, we implemented the proofs of concept for CBDCs, with the privacy and confidentiality features defined, along with a demonstration of their operation. For this purpose, there was a need to implement a webservice and a smart contract, and the software Ganache (private blockchain) and Metamask (wallet software) were used.

Through the demonstration with proofs of concept it was proven that the privacy and confidentiality features are viable for use in CBDCs.

Keywords

Centrak Bank Digital Currency (CBDC), Criptocurrency, Privacy, Confidentiality, Proofs of concept

Agradecimentos

Desejo expressar os meus agradecimentos a todos aqueles que possibilitaram a realização deste trabalho.

Em primeiro lugar, ao Professor Doutor Paulo Rupino da Cunha e ao Professor Doutor Manuel Paulo Albuquerque Melo pela confiança, disponibilidade e orientações ao longo desta dissertação.

De igual forma, agradeço ao Professor Doutor Helder Sebastião pela sua disponibilidade e esclarecimentos bastante pertinentes, que contribuíram para a continuação deste trabalho.

Aos meus pais e família, agradeço por sempre me acompanharem e apoiarem incondicionalmente, em especial ao longo deste percurso, por toda a força, carinho e amor que me deram.

Aos meus amigos, que de forma presencial ou virtual me incentivaram a continuar, em particular aos mais próximos, que me aconselharam e apoiaram em todos os momentos.

Índice

Acrónimos

AML	*Anti-Money Laundering*
BCE	Banco Central Europeu
BFT	*Byzantine Fault Tolerance*
CBDC	*Central Bank Digital Currency*
CBDCs	*Central Bank Digital Currencies*
DCEP	*Digital Currency Eletronic Payment*
DLT	*Distributed Ledger Technology*
KYC	*Know Your Costumer*
LibraBFT	*Libra Byzantine Fault Tolerance*
PBoC	*People's Bank of China*
PoA	*Proof-of-Authenticity*
PoS	*Proof-of-Stake*
PoW	*Proof*-of-Work
SMC	*Secure Multiparty Comunication*
SPAM	*Sending and Posting Advertisement in Mass*
ZKP	*Zero-Knowledge Proof*

Lista de Figuras

Lista de Tabelas

Capítulo 1
Introdução

Este documento surge no âmbito da dissertação "Investigação de suporte tecnológico para criptomoedas de bancos centrais" com o objetivo de documentar o trabalho realizado no âmbito da unidade curricular de Dissertação/Estágio em Sistemas de Informação. O estágio foi orientado pelo Professor Doutor Paulo Rupino da Cunha, da Faculdade de Ciências e Tecnologia, e pelo Professor Doutor Manuel Paulo Albuquerque Melo, da Faculdade de Economia.

Neste capítulo é feita a delineação do trabalho proposto, encontrando-se estruturado em quatro partes: motivação, objetivos, planeamento e estrutura da tese.

1.1 Motivação

O ano de 2009 representa um marco histórico para as criptomoedas. Até àquela data, as tentativas de desenvolvimento de criptomoedas esbarravam sempre no problema do *double-spending*, que permitia a utilização duma entidade monetária em diferentes transações. A única maneira de realizar os pagamentos, de forma confiável, era com a intervenção de um intermediário, que garantia que as operações eram feitas de forma correta. Após a introdução da primeira moeda digital, em 2009, sem o problema de *double-spending* a Bitcoin, baseada no conceito *peer to peer* (ponto a ponto) (Nakamoto, 2008), impulsionou uma tendência crescente no aparecimento de novas criptomoedas (também conhecidas por *altcoins*). Contudo, estas ainda não podem substituir perfeitamente as formas de moeda existentes por não cumprirem, simultaneamente, quatro requisitos fundamentais: alta eficiência (tempo de realização de operações), baixo custo de transações, escala e valor comercial suficiente (Han et al., 2019). Como, teoricamente, estes objetivos são mais fáceis de concretizar por entidades estatais, apesar de algum vazio regulamentar e descoordenação internacional, as agências internacionais, os Bancos Centrais e os governos têm prestado cada vez mais atenção às criptomoedas. O conhecimento adquirido, desde 2009, enformou a base para a concretização real das *Central Banck Digital Currencies* (CBDCs). Segundo Barontini & Holden (2019), no final de 2018, um total de 63 Bancos Centrais (representando aproximadamente 80% da população e 90% do produto mundial) estavam a analisar as implicações da emissão de CBDC, metade já estava a realizar experiências nesse sentido e um quarto já tinha ou estava previsto ter em breve autorização para a sua emissão (Barontini & Holden, 2019). Deste modo, as principais partes interessadas no desenvolvimentos de CBDC são os órgãos governamentais, instituições financeiras, provedores de tecnologia e infraestruturas financeiras e, em última instância, os utilizadores finais (Cheng et al., 2021). Dependendo do país, as motivações económicas e institucionais para a emissão de CBDC variam (Auer et al., 2020b). Tanto a segurança e eficiência dos pagamentos em criptomoedas, como o decréscimo na utilização de dinheiro são motivos para o estudo e desenvolvimento de CBDC (Godinho et al., 2020).

1.2 Objetivos

O objetivo do trabalho consiste em identificar características relevantes das criptomoedas e desenvolver provas de conceito para as CBDCs com essas particularidades, utilizando tecnologias como *blockchain* (tecnologia de registo distribuído) e *smart contract* (protocolo autoexecutável, que reforça a confiabilidade das transações online) (Godinho et al., 2020). A implementação das provas de conceito permite verificar a viabilidade da utilização daquelas características nas CBDCs, bem como contribuir para uma discussão mais ampla do assunto.

1.3 Planeamento

O estágio dividiu-se em dois semestres, com um total de 40 semanas, englobando várias etapas, entre as quais: compreensão do tema, investigação do estado da arte das diferentes criptomoedas, CBDCs e *stablecoins* e respetivas características, análise dos possíveis cenários que as CBDCs podem desenvolver e implementação e validação das provas de conceito dos cenários. Nesta secção são apresentadas as tarefas desenvolvidas nos dois semestres.

Primeiro Semestre

Os cronogramas das tarefas planeadas e executadas, relativamente ao primeiro semestre, estão representados nas Figuras 1 e 2, respetivamente. As discrepâncias entre o cronograma planeado e o executado são relativas à exigente compreensão da *blockchain* e tecnologia subjacente, que requereu pesquisa e entendimento dos seus fundamentos.

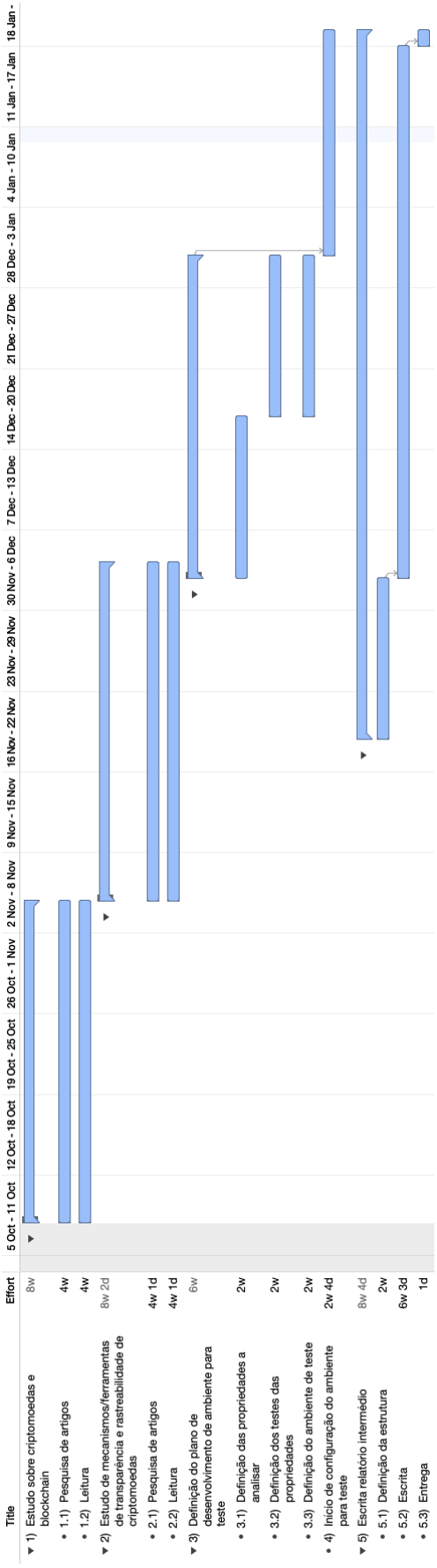


Figura 1 - Cronograma planeado para o primeiro semestre.

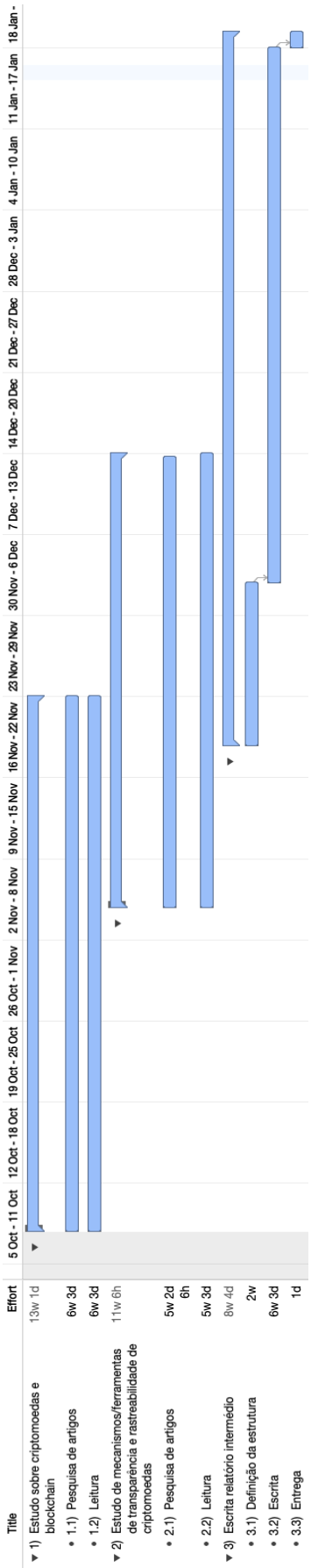


Figura 2 - Cronograma executado no primeiro semestre.

Segundo Semestre

Nesta sub-secção é apresentado o cronograma planeado e executado relativo ao segundo semestre, ilustrado respetivamente na Figura 3 e nas Figuras 4 e 5. Foi necessário dividir o cronograma executado devido à elevada amplitude temporal.

A tarefa quatro do cronograma planeado não foi colocada no cronograma final, devido ao desenvolvimento do estágio ter sido mais demorado do que o previsto, levando a que a elaboração daquela tarefa apenas pudesse ser realizada no mês de junho de 2021, não sendo um período de tempo suficiente para tal. As restantes discrepâncias, associadas ao segundo semestre, são relativas à complexidade de definição dos cenários que as CBDCs permitem implementar e ao desconhecimento da tecnologia *blockchain*, que requereu mais tempo do que o previsto para o seu entendimento.

A implementação das provas de conceito foi sujeita a uma dificuldade adicional relativa às tecnologias que iam ser utilizadas, por se encontrarem em desenvolvimento. No Capítulo 3 é explicado como foi superado o problema para a implementação das provas de conceito.

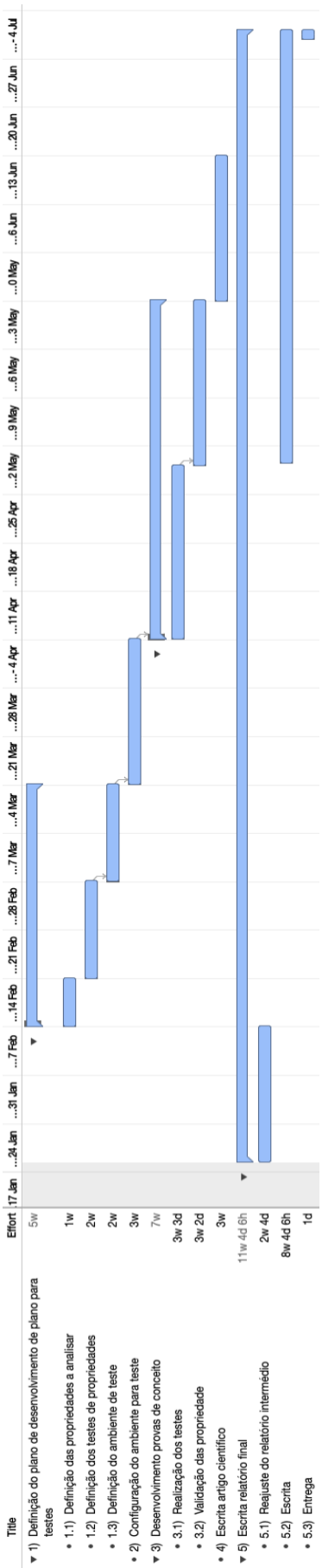


Figura 3 - Cronograma planeado para o segundo semestre

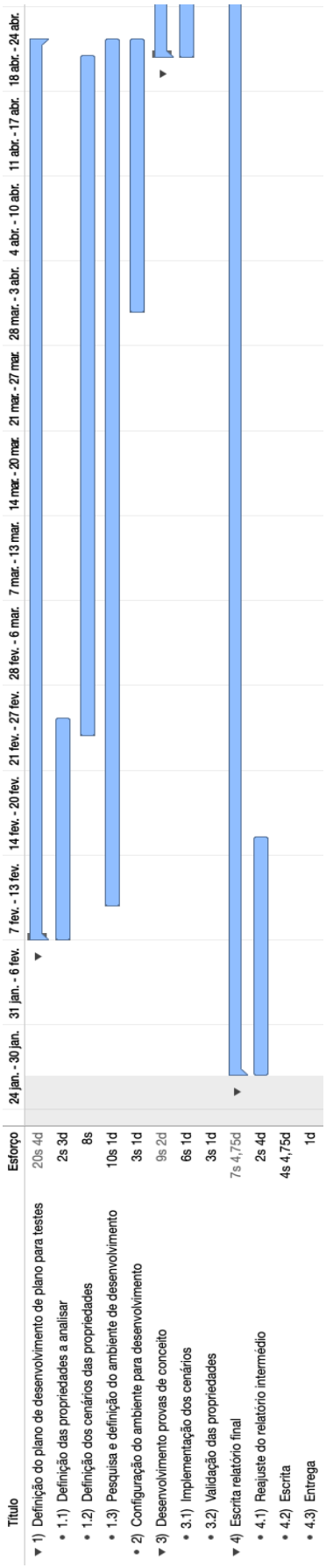


Figura 4 - Cronograma executado no segundo semestre – 1ª parte

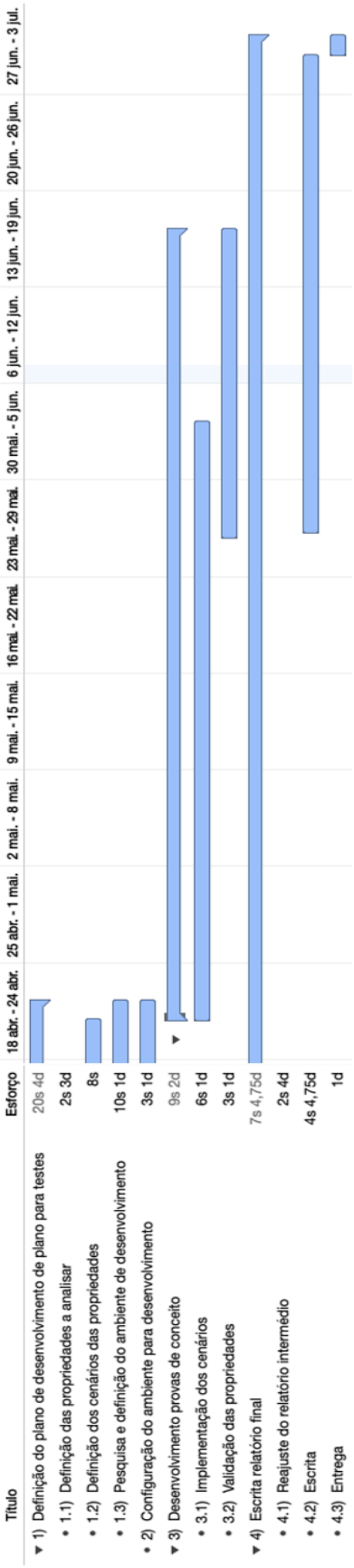


Figura 5 - Cronograma executado no segundo semestre – 2ª parte

1.4 Estrutura do documento

O trabalho realizado ao longo do primeiro e segundo semestres é apresentado neste documento estruturado em quatro capítulos. Para além da presente Introdução, onde é apresentada a motivação para a realização do trabalho, os objetivos subjacentes, o planeamento do trabalho para cada semestre e o cronograma do trabalho efetivamente cumprido, neste trabalho constam ainda os seguintes capítulos: Criptomoedas e CBDCs, Cenários, casos de uso e provas de conceito e Considerações finais.

No capítulo referente a criptomoedas e CBDCs é inicialmente descrita a metodologia usada para a recolha de informação, bem como as expressões de pesquisa utilizadas para o efeito. Posteriormente é realizada uma contextualização do estado de arte, análise das características e do funcionamento da Bitcoin e das CBDCs (Diem, Digital Currency Electronic Payment – DCEP, Digital Euro e E-krona). Posteriormente é explicado as características inerentes ao dinheiro digital e criptomoedas, de entre as quais a privacidade e confidencialidades como características fundamentais.

No terceiro capítulo, sobre os cenários de casos de uso e provas de conceito, são descritos todos os cenários para que as CBDCs possam obter privacidade e confidencialidade com os respetivos atores envolvidos, são apresentados os respetivos casos de uso e é realizada a implementação das provas de conceito para se obter as características referidas.

Por fim, no último capítulo, são apresentadas as considerações finais, juntamente com sugestões para trabalho futuro.

Capítulo 2
Criptomoedas e CBDCs

Neste capítulo abordamos aspetos genéricos das criptomoedas, com particular destaque nas características e funcionamento da Bitcoin, da Diem (moeda estável) e das CBDCs (DCEP, Digital Euro e E-krona). Para além de apresentarmos a tecnologia de implementação das criptomoedas, especificamos as semelhanças e diferenças entre criptomoedas e CBDCs, particularmente no que respeita a aspetos concernentes a rastreabilidade e transparência e privacidade e confidencialidade.

Esta abordagem é fundamentada com a revisão bibliográfica realizada, que foi estruturada com recolha de informação através do método de revisão sistemática de literatura, que se aborda de imediato.

2.1 Metodologia

Como procedimento de recolha de informação utilizou-se o método de revisão sistemática de literatura, através das bases de dados *IEEEXplore*, *ACMDL* e *Science Direct*, devido à sua ampla cobertura de artigos e reconhecimento científico. Executaram-se alguns testes experimentais, para definir as palavras-chaves que deveriam ser incluídas e os campos de pesquisa a utilizar. Na base de dados *IEEEXplore* foi especificada uma restrição para serem apresentados unicamente jornais e conferências e na *Science Direct* as expressões foram centradas no título, resumo e nas palavras-chave.

Na Tabela I apresentamos os resultados obtidos da pesquisa realizada, em novembro de 2020, com as expressões indicadas, no que respeita ao número de artigos encontrados e analisados. Como se pode verificar, as pesquisas são todas posteriores a 2008 (data de publicação de Nakamoto), com alguns projetos a serem iniciados mais recentemente, como é o caso da E-krona (anunciada em 2017), do Digital Euro (divulgada em 2019) e da Diem (comunicada em 2019).

A informação obtida foi objeto de uma seleção, para eliminar os artigos duplicados e encontrar os mais pertinentes, cujos resumos foram analisados e classificados como (ir)relevantes. Os artigos relevantes (Apêndice A) foram analisados com maior acuidade. Adicionalmente foram utilizados materiais denominados de *grey literature*, como artigos, jornais e *whitepapers* publicados pelos Bancos Centrais, sendo este um tema muito atual. As secções seguintes são resultantes da análise destes artigos.

Tabela I - Expressões de pesquisa e base de dados

Expressão	Campos	Base de dados	#artigos encontrados	#artigos duplicados	#artigos analisados
CBDC OR "Central Bank Digital Currency"	resumo, palavras-chave, sem restrição de datas	IEEEXplore	14	-	4
		ACMDL	20	1	3
		Science Direct	30	-	-
"Bitcoin" AND Cryptocurrency AND blockchain	resumo, palavras-chave, sem necessidade de restrição de datas **(a)**	IEEEXplore (i) jornais e conferências	283	-	34
		ACMDL	85	-	10
		Science Direct (ii) título, resumo, palavras-chaves	96	-	10
("libra" AND "facebook") OR ("diem" AND "facebook")	resumo, palavras-chave, sem necessidade de restrição de datas **(b)**	IEEEXplore (iii) conferências	4	1	2
		ACMDL	1	-	1
		Science Direct	2	-	-
("DCEP" OR "Digital Currency Electronic Payment" OR "DC/EP" OR "yuan digital" OR china digital currency) AND CBDC	resumo, palavras-chave, sem necessidade de restrição de datas	IEEEXplore	-	-	-
		ACMDL	3	-	2
		Science Direct	-	-	-
"euro" AND CBDC	sem restrições	IEEEXplore	-	-	-
		ACMDL	4	4	-
		Science Direct	6	-	-
"e-krona"	sem restrições	IEEEXplore	-	-	-
		ACMDL	2	-	-
		Science Direct	10	-	-

a) Não foram encontrados artigos com data anterior a 2008.
b) Não foram encontrados artigos com data anterior a 2019

2.2 Breve resenha histórica

Em 3 de janeiro de 2009, alguém sob o pseudónimo de Satoshi Nakamoto minerou o primeiro bloco do que viria a ser a Bitcoin (Sebastião et al., 2020). Mais de dez anos depois, a invenção da primeira criptomoeda demonstrou ao mundo a utilidade da tecnologia de registo distribuído *blockchain.*

Apesar de se tornar o primeiro ativo digital criptográfico bem-sucedido na prática, a Bitcoin não foi a primeira tentativa de se criar uma moeda completamente digital, descentralizada e não copiável. Os primeiros trabalhos sobre moeda digital remontam ao início dos anos 80 do século XX, com o desenvolvimento de projetos com inovações cruciais para a conceção do que hoje se entende por criptomoedas: e-Cash, HashCash, B-money e o Bit-Gold.

A e-Cash foi a primeira tentativa de criação de uma moeda digital para a realização de transações, da autoria de David Chaum, em 1982 (Chaum, 1983). No final desta década, David Chaum fundou a DigiCash e iniciou os testes do e-Cash com os primeiros pagamentos bem-sucedidos, permitindo que os bancos pudessem adquirir uma licença da DigiCash para usar a tecnologia (Rocha, 2018a). No entanto, este modelo de criptomoeda menosprezava a importância da descentralização de uma moeda digital e necessitava de um intermediário financeiro para funcionar adequadamente. No início de 1996, o Deutsche Bank, o Banco Central da Alemanha, aderiu à iniciativa, seguindo-se outros bancos em diferentes países. Após três anos de testes e aproximadamente 5.000 clientes, a e-Cash foi dissolvida em 1998, após a compra do Mark Twain Bank pelo Mercantile Bank que, à época, tratava-se de um grande emissor de cartões de crédito e que entendia não obter ganhos tendo um produto concorrente no seu portefólio (Rocha, 2018a).

No início dos anos 90, os avanços no desenvolvimento da internet e a crescente popularidade do sistema de correspondência eletrónica (e-mail), trouxe alguns desafios, como a proliferação de mensagens de SPAM, tornando-se premente uma solução para mitigar este problema. Para o efeito, Cynthia Dwork e Moni Naor (Dwork & Naor, 1993) propuseram um sistema em que os remetentes anexariam alguns dados a qualquer e-mail enviado, que seriam a solução de um problema matemático exclusivo do e-mail em questão. Especificamente, Cynthia Dwork e Moni Naor propuseram três enigmas que poderiam ser usados para o propósito, todos baseados em esquemas de criptografia e assinatura de chave pública. O tipo de solução proposta pelos autores ficaria conhecido como um sistema de *Proof-of-Work* (PoW), ideia que não vingou para além de um círculo restrito de especialistas da área da computação (Rocha, 2018b).

Contudo, em 1997, Adam Back revê o conceito de Cynthia Dwork e Moni Naor e, com pequenas alterações, apresenta uma proposta para o mesmo problema sob a designação de um algoritmo HashCash. O *Hashing* consiste num problema criptográfico que utiliza todos os dados (seja uma única letra ou um livro inteiro) e transforma-os num número, aparentemente aleatório (Rocha, 2018b). Acresce que, o *hash* de qualquer uma das frases, seria completamente aleatório. A hipótese era que o HashCash se poderia transformar numa economia de rede, tornando o trabalho dos *spammers* pouco lucrativo, dado o alto-custo de enviar milhares de e-mails carimbados.

Apesar da designação, o HashCash não poderia ser considerada uma moeda propriamente dita, sendo a sua principal função, por meio do algoritmo PoW, criar e-mails infalsificáveis e facilmente validáveis. O HashCash não obteve o êxito comercial esperado, porque a morosidade do computador para validar um e-mail era considerável (Rocha, 2018b). Além disso, a máquina que realizava o PoW não era remunerada e tornava o modelo de negócios

pouco atrativo. Mais tarde, a Bitcoin utilizaria a engenharia de incentivos do HashCash, mas aprenderia com os seus erros ao remunerar o trabalho computacional. A prática ficaria conhecida como "mineração". Apesar das propostas de Cynthia Dwork e Moni Naor, assim como de Adam Back (de forma independente) não terem encontrado o sucesso desejado, elas introduziram algo novo, o conceito de prova de trabalho (Rocha, 2018b).

Ainda no final dos anos 90, Wei Dai propôs a B-money, um sistema de dinheiro eletrónico, distribuído e anónimo. Com uma ideia muito similar à futura Bitcoin, o projeto propunha ser um algoritmo para a realização de transações monetárias, sem a necessidade de uma terceira parte. A proposta de Wei Dai tinha muitas parecenças técnicas com a Bitcoin, tais como remunerar o esforço computacional despendido e a verificabilidade das transações num livro contábil coletivo (Campos, 2020). Além disso, Wei Dai sugeriu o uso de assinaturas digitais, ou chaves públicas, para autenticação de transações e cumprimento de contratos. No entanto, a B-money nunca foi lançada, chamando, no entanto, a atenção a Satoshi Nakamoto, o pseudónimo inventor da Bitcoin.

Posteriormente, em 2005, Nick Szabo propôs um sistema muito similar ao Bitcoin, a Bit-Gold, com uma arquitetura que já utilizava o algoritmo PoW e o registo de transações, análoga ao que se tornaria a *blockchain*. Uma característica da Bit-Gold residia no facto das transações só poderem ser realizadas de forma descentralizada, sem a intervenção de qualquer terceira parte, tal como ocorre com a Bitcoin, ao descentralizar e distribuir a confiança entre nós individuais que compõem a sua rede. Apesar do futuro promissor da ideia, Nick Szabo nunca conseguiu solucionar parte crucial do que viria a tornar-se a Bitcoin: uma moeda digital não copiável (Bit2Me Academy, n.d.; Satoshi Nakamoto Institute, n.d.).

O ano de 2009 viu o aparecimento da primeira moeda digital, sem o problema de *double-spending*, a Bitcoin, baseada no conceito de arquitetura de rede de computadores *peer to peer* (ponto a ponto), desenvolvido por um indivíduo ou grupo de indivíduos com o pseudónimo de Satoshi Nakamoto (Nakamoto, 2008), motivando o aparecimento tendencionalmente crescente de novas moedas digitais, impulsionadas pela crise do *subprime*, originada nos EUA. Entre 2007 e 2010, período em que as réplicas daquela crise alastraram ao mundo inteiro, a confiança nos bancos e terceiras entidades foi diminuindo, gerando um impulso e motivação essenciais para que a Bitcoin ganhasse mais atenção (Sebastião et al., 2020) e surgissem novas a*ltcoins* (criptomoedas independentes de entidades terceiras e alternativas ao Bitcoin), mas sem valor intrínseco associado e altamente voláteis, dependendo da confiança dos utilizadores, sendo consideradas um substituto imperfeito das moedas tradicionais (Bigmore, 2018). Embora não seja possível indicar, com exatidão, o número total de criptomoedas que existem atualmente, devido ao ritmo com que algumas surgem e outras vão desaparecendo, o volume de capital que movimentam é muito elevado (CoinLore, n.d.; CoinMarketCap, n.d.).

A perspetiva da indústria financeira tradicional sobre as criptomoedas foi marcada, durante algum tempo, por algum ceticismo sobre a possibilidade das moedas digitais mudarem o cenário monetário e financeiro existente. Para tal, eram invocadas questões fundamentalmente relacionadas com a volatilidade, descentralização e potencial para lavagem de dinheiro das moedas digitais. Contudo, após uma década de existência, é justo dizer que o conceito de criptomoeda vingou e apresenta uma tendência crescente de grande potencial.

Não podendo ignorar este novo paradigma das criptomoedas, os Bancos Centrais mostram-se, agora, interessados na criação das suas próprias moedas digitais (CBDC), cuja emissão é completamente controlada pelo Banco Central, e portanto, tal como as moedas fiduciárias,

têm uma volatilidade muito menor que as criptomoedas, funcionando como um substituto das moedas tradicionais.

As motivações económicas e institucionais para a emissão de CBDCs variam de país para país (Auer et al., 2020b), com alguns a considerarem a segurança e a eficiência dos pagamentos em criptomoedas, enquanto outros procuram encontrar soluções para responder ao decréscimo na utilização de dinheiro (Godinho et al., 2020). Adicionalmente a estas motivações, a atual situação da pandemia de Covid-19 e potencial transmissão do vírus através das trocas de dinheiro físico, pode também tornar-se num impulso para o desenvolvimento da CBDC (Auer et al., 2020b), apesar de alguns autores (Auer et al., 2020a) argumentarem que a pandemia pode retrair a emissão de CBDC, devido ao menor grau de transmissibilidade do vírus através de notas ser menos provável do que através de outros meios de pagamento com superfícies menos porosas, tais como cartões plastificados. Todavia, a moeda digital pode ser utilizada através de uma aplicação de telemóvel ou via o computador pessoal, tal como o demonstram os relatórios sobre o E-krona do Banco Central Sueco, que indicam serem aqueles os canais prioritários de utilização (Banco de Portugal, n.d.-a).

2.3 Características das criptomoedas e das CBDCs

Apesar das criptomoedas e CBDCs serem desmaterializadas, existem diferenças notáveis entre ambas.

De um modo geral, as criptomoedas são descritas como moedas digitais (sem forma física e intangíveis) sem valor intrínseco associado, altamente voláteis, com um comportamento de bolha e com movimentos extremos de curto prazo, com os seus valores a serem determinados pelo nível de confiança que os utilizadores têm nas mesmas. Algumas criptomoedas possuem características importantes, tais como anonimato (realização de transações sem a possibilidade de descobrir a pessoa/entidade responsável), escalabilidade (capacidade de lidar com uma grande quantidade de transações simultaneamente), acessibilidade (facilidade de utilização, de envio e receção de criptomoedas), velocidade de transação (tempo de realização da transação da criptomoeda), transparência (possibilidade das transações serem consultadas), integridade (preservação dos dados) e resiliência (capacidade de resistir a ataques), tornando-as bastante apelativas para serem utilizadas em atividades ilegais e como instrumento para o jogo de apostas de alto risco (Godinho et al., 2020).

A CBDC, apresentando-se como uma versão digital de uma moeda fiduciária (apoiada pelo Estado, sem ter valor intrínseco) emitida por um Banco Central, desempenhará as mesmas funções (meio de pagamento, unidade de medida e reserva de valor). Sendo uma moeda centralizada (emitida e administrada pelo Banco Central de um país), contrariamente às criptomoedas como a Bitcoin (emitida de forma distribuída), a CBDC será mais estável.

Para além da Bitcoin e outras moedas de 1ª geração e das CBDCs, as moedas estáveis (*stablecoins*) apresentam-se como um outro tipo de moeda digital, mas emitida pelo setor privado (p.e. uma empresa). Neste caso, a estabilidade das *stablecoins* é obtida através da sua ligação a uma reserva de bens reais e estáveis, que permite a minimização das flutuações de preços (Clifford Chance, 2020).

Na Tabela II apresentamos uma comparação entre as criptomoedas, CBDCs e *stablecoins*.

Tabela II – Comparação entre as diversas moedas digitais.

		Bitcoin	**CBDCs**	***Stablecoins***
Emissão	Entidade governamental	não	sim	não
	Entidade privada	sim	não	sim
Estabilidade		não	sim	sim
Suporte	Entidade governamental	não	sim	não
	Ativos estáveis	não	não	sim

A CBDC pode tornar-se num instrumento financeiro para acordo entre instituições financeiras, p.e. nas liquidações que utilizam depósitos de Bancos Centrais, ou passivos de Bancos Centrais, que tenham sido digitalizados. Este tipo de CBDC é disponibilizado apenas para bancos comerciais, para uso no mercado interbancário de grande escala (Bis Central bankers, 2019). O principal objetivo é aumentar a eficiência nos pagamentos interbancários nacionais ou internacionais, que hoje ainda são algo ineficientes, demorados e caros para os bancos. No entanto, a maioria dos testes com este tipo de CBDC foram realizados com foco no uso do utilizador final da moeda digital. Ao emitir esse tipo de moeda digital, os Bancos Centrais esperam obter maior eficiência nos pagamentos interbancários e na negociação e liquidação de títulos interbancários. Por outro lado, a CBDC pode servir o propósito de aumentar a inclusão financeira da sociedade, ou servir como uma alternativa estratégica à moeda fiduciária em economias onde esta está a perder força (p.e., Venezuela). Neste caso, a CBDC atua como substituta ou complemento da moeda fiduciária e uma alternativa aos depósitos junto dos bancos tradicionais (Auer et al., 2020b)(Bis Central bankers, 2019). Consoante o fim a que se destina, a CBDC pode caracterizar-se pelos tipos *wholesale* e *retail*. No primeiro caso, o objetivo é facilitar o pagamento entre bancos comerciais e o Banco Central ou outras entidades que têm uma conta no Banco Central. Por sua vez o *retail* CBDC é utilizada pelo público e/ou empresas, na realização de pagamentos e/ou criação de poupanças (Arslanian, 2020).

A acessibilidade da CBDC distingue-se entre *account-based* e *token-based* (taxonomia atualmente usada). Uma CBDC *account-based* necessita que o proprietário tenha uma conta no Banco Central, podendo ser considerada como uma conta bancária de acesso universal pelo seu proprietário para pagamentos e/ou depósitos de valores. A CBDC *token-based* tanto pode ser uma carteira de *software* (se for utilizada num telemóvel), como de *hardware (*se for usada de forma semelhante a um cartão pré-pago*)* e não requere uma conta bancária no Banco Central, permitindo que os seus proprietários tenham anonimidade.

A garantia de anonimidade na CBD *token-based* permite que possa ser considerada como um substituto do dinheiro físico, ao invés da CBDC *account-based*. Contudo, apesar da anonimidade ser uma característica apreciada pelos utilizadores, existem limitações rigorosas para este tipo de CBDC (Bofinger & Haas, 2020). Com efeito, é exigido às organizações financeiras tradicionais o cumprimento das normas KYC (*Know Your Costumer* ou *Know Your Client*) e AML (*Anti-Money Laundering*). Os procedimentos KYC requerem que as instituições financeiras autorizem e identifiquem o cliente para a criação das contas (Sebastião et al., 2020), enquanto a norma AML impõe às instituições financeiras a monitorização das transações efetuadas pelos clientes. Deste modo, estas normas pretendem

tornar mais difícil (evitando mesmo) a ocorrência de fraudes e o financiamento de atividades ilícitas.

2.4 Tecnologia das criptomoedas

Um aspeto crucial para a generalidade das transações com criptomoedas (podendo ou não englobar a CBDC), é a *distributed ledger technology* (DLT). Um *ledger* (livro-razão) distribuído é uma forma de banco de dados digital sobre as transações realizadas, descentralizado, gerido por vários participantes, não existindo uma autoridade central para transmitir os registos para todos os membros (R3, n.d.). Como todos os "nós" da rede (participantes) recebem e compartilham cada nova transação e mantém os dados registados, os "nós" precisam de ter acesso às listas de transações e passar por protocolos de validação para interagir com a rede. Geralmente, cada "nó" da rede tende a passar por um processo de acordo, para chegar a uma única conclusão, após o qual o registo distribuído é atualizado a todos os "nós" na rede e também de seu próprio registo.

Conforme referido, esta utiliza um *ledger* em que as transações são agrupadas em blocos da *blockchain*, pública e descentralizada (Sun et al., 2017), dado não existir uma entidade central, que é replicado entre os participantes da rede (nós), registando todas as transações que ocorrem e que podem ser consultadas (Rankhambe & Khanuja, 2019).

Após a realização de uma transação (Figura 6), é necessário proceder à sua verificação, ou seja, os "nós" têm de chegar a um acordo de que a transação efetivamente ocorreu, permitindo-a armazenar num bloco com todas as informações referentes à operação (hora, data, valor transacionada e assinatura digital).

As transações são criptografadas, gerando-se uma *string* alfanumérica – *hash* criptográfico – criando os blocos, posteriormente adicionadas ao *ledger*. Ou seja, cada bloco conterá um ID conhecido como *hash*, que ajuda à distinção entre todos os blocos de transações do registo. Como o *hash* criptográfico de um bloco é adicionado ao bloco seguinte, cria-se uma cadeia de blocos, que permite a rastreabilidade das transações.

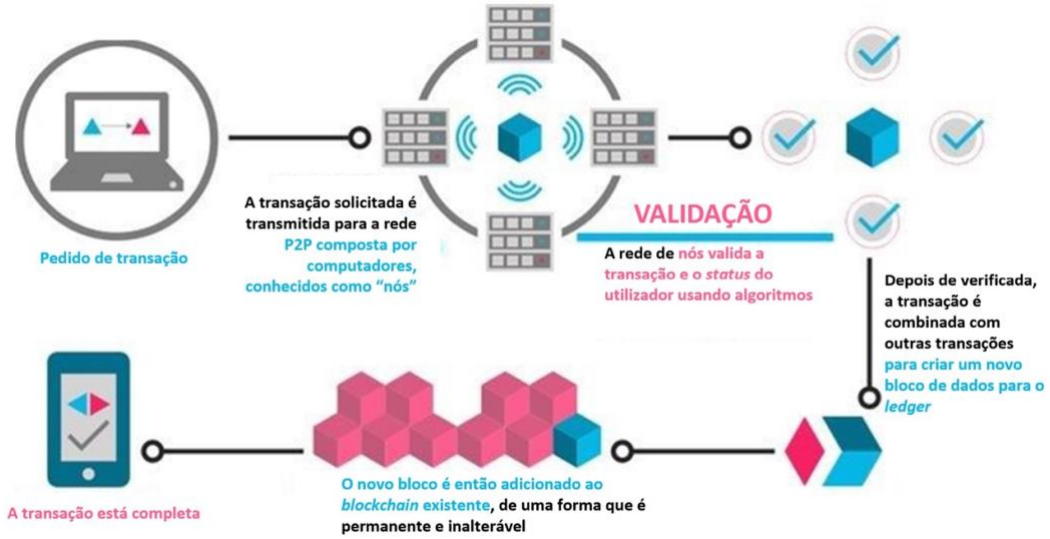


Figura 6 - Arquitetura simplificada da *blockchain* (adaptado de Lieure, 2018)

Nas Figuras 7 e 8 exemplifica-se uma *blockchain* constituída por três blocos, tendo cada um deles os registos do seu *hash* e do *hash* anterior, para ilustrar as diferenças entre uma *blockchain* sem e com alteração ilegítima.

No primeiro caso (Figura 7), como o primeiro bloco, denominado *Genesis*, não tem antecedente, o registo da *hash* do bloco anterior está a zero (Yaga et al., 2018). No entanto, nos blocos subsequentes as respetivas *hash* já estão preenchidas com os registos da *hash* do próprio bloco e do anterior.

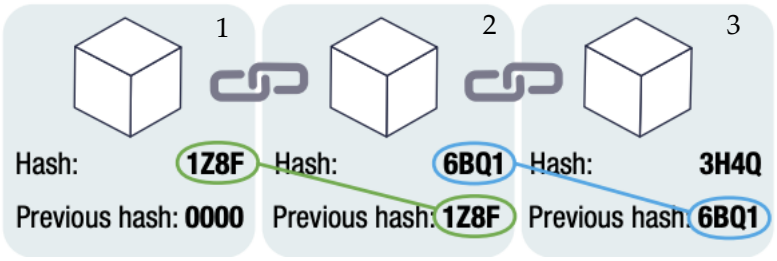


Figura 7 - *Blockchain* sem alteração ilegítima (adaptado de Aarvik, 2020)

Noutra situação (Figura 8), há uma tentativa de alteração ilegítima no bloco 2, cujo *hash* é modificado e, consequentemente, o bloco 3 não fica atualizado com o registo (falseado) do *hash* do bloco anterior. Na situação de apenas o conteúdo do bloco ser alterado, mantendo-se o valor do *hash*, resultará numa incoerência entre a informação do bloco e a informação contida no *hash*.

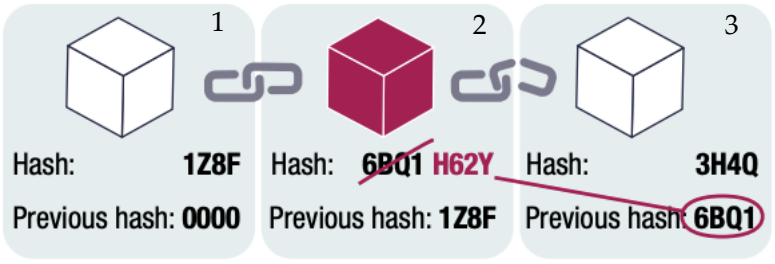


Figura 8 - *Blockchain* com alteração ilegítima (adaptado de Aarvik, 2020)

A alteração de qualquer dado num bloco requer que o respetivo *hash* seja alterado, afetando a *blockchain*. Se existirem poucos blocos na cadeia (por exemplo, apenas três), poderá ser exequível a alteração dos dados dos blocos e recalcular os *hash*, atualizando toda a *blockcahin*. Contudo, para uma cadeia longa de blocos é (praticamente) impossível alterar os *hashes* de todos os blocos, pela elevada capacidade de computação requerida, razão pela qual a *blockchain* é considerada imutável e confiável. Como o *hash* permite averiguar se os dados do bloco foram ou não adulterados, preservando a sua autenticidade e, como tal, a integridade de uma *blockchain* como um todo, nas situações de alteração ilegítima, todos os blocos posteriores serão invalidados, obrigando o atacante a calcular novos *hash* para os blocos alterados, acarretando um grande esforço computacional (Yaga et al., 2018).

Neste contexto, a utilização de criptografia garante a integridade do *ledger*, tornando-o inalterável (Sebastião et al., 2020). A utilização de um algoritmo de consenso permite chegar a acordo com o *hash* criptográfico, para garantir que o *ledger* é atualizado somente quando as transações são verificadas e validadas pelos participantes, evitando-se, assim, problemas como o *double-spending*. Este procedimento designa-se por mineração, com os nós que participam no processo de adicionar novos blocos ao *ledger* identificados por mineiros. Caso se verifique um *double-spending* é criado um *fork* (bifurcação) no *ledger* e, ao ser-lhe adicionado um novo bloco, é necessário que o mineiro resolva em qual das cadeias se faz essa adição, sendo válida a cadeia mais longa. Este processo é realizado continuamente, mas de complexidade decrescente, porque uma das cadeias será tendencionalmente maior que a outra. Os mineiros são incentivados financeiramente a adicionar o bloco à cadeia válida (Tomov, 2019).

O acesso a uma *blockchain* pode distinguir-se entre público e privado, segundo as autorizações concedidas aos participantes na rede (Yaga et al., 2018). Alguns autores, como (Zheng et al., 2018a), fazem ainda a distinção em *blockchain* de consorcio, sendo administrada por múltiplas organizações privadas.

A *blockchain* pública é descentralizada, aberta a qualquer participante e não requer permissão para leitura e escrita no *ledger*. Consequentemente, há a necessidade de utilizar um algoritmo de consenso com elevado poder computacional (por exemplo, PoW) exigido para evitar que utilizadores maliciosos publiquem blocos ilícitos, traduzindo-se por velocidades de transações mais lentas e baixa eficiência. Em contrapartida, a *blockchain* privada é parcialmente descentralizada, de acesso limitado à respetiva organização sendo necessário um convite para a participação na rede, restringindo a permissividade para publicar blocos no *ledger*, bem como o acesso de leitura dos blocos e emissão de transações. Deste modo, todos os participantes são conhecidos pela entidade responsável, sendo escolhido o algoritmo de consenso baseado na confiança mútua (por exemplo, *Proof-of-Authenticity* - PoA) devido à necessidade de permissão para participar na rede. A Tabela III sintetiza as principais diferenças entre os dois tipos de *blockchain*.

Tabela III - Comparação entre as diferentes *blockchain* (Ciaian, 2018; Samarakoon, 2019; Zheng et al., 2018b).

Blockchains	**Pública**	**Privada**
Permissionada	Não	Sim
Acessibilidade ao *ledger*	Sim	Apenas para as entidades autorizadas
Nível de privacidade	Nós anónimos	Nós conhecidos
Velocidade de transação	Lenta	Rápida

Nem sempre a ingerência numa *blockcahin* requer uma ação exterior podendo, em algumas situações, automatizar procedimentos através de *smart contracts* (linhas de código armazenadas na *blockchain*), que verificam o cumprimento de termos e condições predeterminados (Alharby & Van Moorsel, 2017; Campos, 2020).

Os benefícios dos *smart contracts* são mais evidentes na operacionalização de negócios, sendo normalmente usados para obrigar ao cumprimento de algum tipo de acordo, garantindo que todos os envolvidos possam ter a certeza do resultado, sem o envolvimento de um

intermediário (Mechkaroska et al., 2018). Como a natureza humana é propícia a erros, os *smart contracts* acrescentam uma componente de automatização e segurança à *blockchain*, permitindo executar termos de um acordo, ou iniciar relações de transação, sem a necessidade de intervenção humana, dado que todos os detalhes são explícitos e, caso não estejam reunidas todas as condições, a operação é abortada, pois não existe ambiguidade nem subjetividade nos termos e condições. De destacar, também, a autonomia, onde a natureza descentralizada da *blockchain* subjacente a estes *smart contracts*, bem como a própria natureza do contrato significa que nenhuma parte externa é necessária no processo. Por exemplo, a Ethereum permite o *touring* completo (é capaz de usar a sua base de código para realizar virtualmente qualquer tarefa) desde que tenha devidamente especificados as instruções corretas, o tempo suficiente e o poder de processamento (Binance Academy, n.d.).

Os *smart contracts* permitem, assim, economia de tempo e dinheiro, uma vez que a automatização de processos evita a utilização de intermediários, ficando mais económicos para quem os disponibiliza e usa (Gopie, 2018).

2.5 Moedas digitais

Nesta secção apresentamos alguns aspetos (características e funcionamento) da Bitcoin (criptomoeda), Diem (*stablecoin*) e DCEP, Digital Euro e E-krona (CBDC). A opção por estas moedas digitais deve-se ao facto da Bitcoin ser umas das maiores criptomoedas que utiliza a tecnologia *blockchain*, a Diem por ser emitida por uma empresa de grande reconhecimento impacto (Facebook) e as restantes por estarem numa fase adiantada em termos de pesquisa e desenvolvimento, estando a mesmo a DCEP já em fase piloto.

Bitcoin

Na rede Bitcoin os utilizadores são identificados por pseudónimos (carteiras não vinculadas a uma identidade), sendo conhecidos os números das suas contas, mas não existindo qualquer ligação que os identifique no mundo real (Sebastião et al., 2020). Na Figura 9 é ilustrada uma carteira com a sua respetiva identificação. Estas contas podem ser criadas sem a necessidade de exercer os procedimentos obrigatórios KYC exigidos às organizações financeiras, que têm a responsabilidade de verificar a identidade dos utilizadores. A utilização de pseudónimos foi uma escolha dos criadores da Bitcoin, no entanto, para sistemas que utilizam como base a *blockchain* não é obrigatório o uso dos mesmos (Sebastião et al., 2020). A Bitcoin utiliza a tecnologia *blockchain* pública, ou seja, quando novas transações são feitas, elas são comunicadas a todos os nós participantes na rede. Cada transação tem o *hash* assinado digitalmente da transação anterior e a chave pública do próximo proprietário (Vujičić et al., 2018).

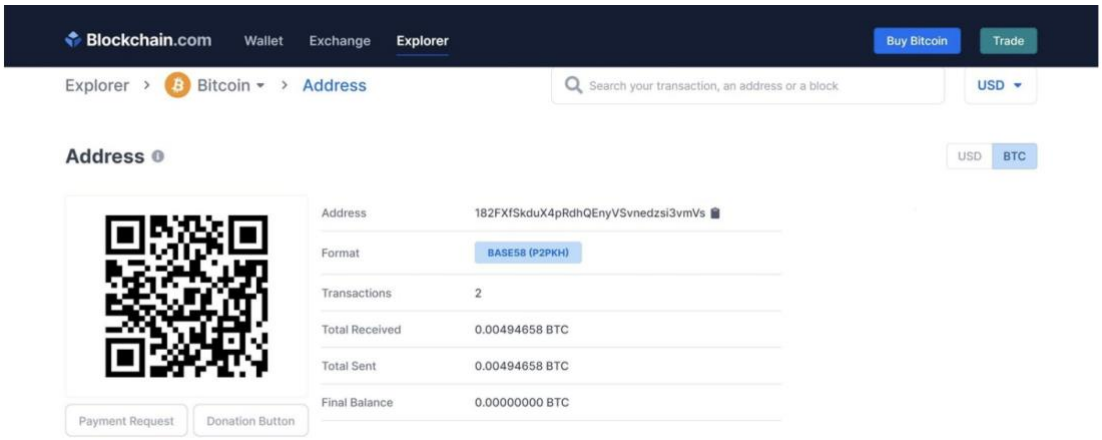


Figura 9 – Exemplo de uma carteira de Bitcoin com o endereço que a identifica (adaptado de Patrick, 2017).

O algoritmo de consenso utilizado é o PoW, consistindo na resolução de um puzzle (encontrar o *hash* criptográfico) e que requer um poder computacional elevado, porém de verificação fácil, o que desencoraja comportamentos fraudulentos (Rankhambe & Khanuja, 2019). O primeiro "nó" que conseguir resolver o puzzle adiciona-o ao *ledger*, sendo aceite pelos restantes sem que estes necessitam de atualizar as suas cópias do *ledger*. A complexidade do puzzle vai aumentando com o crescimento da rede (Hazari & Mahmoud, 2019).

Os "nós" que participam no processo de mineração são recompensados obtendo novos Bitcoins (Yaga et al., 2018). Ou seja, os Bitcoins são geradas através da mineração, que consiste na recompensa dada aos utilizadores pelos seus serviços. O protocolo Bitcoin foi projetado de uma forma que os novos Bitcoins são criadas numa proporção fixa sem outras entidades poderem controlar ou manipular o sistema para aumentar os lucros (Hayes Adam, 2020). A Bitcoin utiliza o algoritmo criptográfico SHA-2, que é um grupo de funções criptográficas para proteger os dados armazenados na *blockchain* (Rankhambe & Khanuja, 2019).

Devido ao elevado poder computacional necessário, a escalabilidade da Bitcoin pode ter dificuldade quando ocorre uma grande quantidade de transações simultaneamente, demorando mais a serem executadas. Esta pode caracterizar-se como escalabilidade de "nós" (mineiros) e escalabilidade de desempenho. Em relação à primeira, existe uma elevada escalabilidade sendo que, quanto mais "nós" a rede possuir, mais segura vai ser. Em contrapartida, a escalabilidade de desempenho é muito limitada, está dependente do algoritmo de consenso utilizado, que neste caso permite apenas cerca de sete transações por segundo (Rankhambe & Khanuja, 2019).

A Bitcoin apresenta alguns problemas relevantes: taxas de transações lentas, elevada volatilidade resultante da vulnerabilidade à especulação e elevada complexidade computacional no processo de mineração (conduzindo a um elevado consumo energia com fortes implicações ambientais) (Aarvik, 2020). Como a Bitcoin é criada numa taxa decrescente e previsível, o número total de Bitcoins criados a cada quatro anos é automaticamente reduzido pela metade, com o passar do tempo, até que a emissão seja completamente suspensa com um total de 21 milhões de Bitcoins (Hayes Adam, 2020).

Em suma, as principais características da Bitcoin são a descentralização, confiança e autenticação. É descentralizado porque utiliza a tecnologia *blockchain* pública, ou seja, não

existe uma entidade central. A confiança deve-se ao facto de os blocos serem certificados através de *hashs.* Por fim, a autenticação confirma a pseudoidentidade de um utilizador, utilizando assinaturas digitais nas transações entre utilizadores, permitindo integridade e não repúdio das mesmas (Mechkaroska et al., 2018).

Diem (ex Libra Facebook)

A Diem é uma proposta da rede social Facebook, controlada pela Libra Association, cujo conselho de administração é constituído por 27 empresas (Allen et al., 2020a). Será uma moeda estável apoiada pela Reserva Libra (mecanismo-chave para o alcance da preservação do valor) e lastreada por um conjunto de ativos líquidos e estáveis dando valor à Diem (Catalini et al., n.d.). Esta pode tornar-se uma moeda amplamente aceite, principalmente nos países em desenvolvimento em que "o Facebook é possivelmente mais respeitável do que os respetivos governos", estando a integridade da Diem dependente dos seus emissores (Li & Whinston, 2020).

A Diem poderá ter um maior nível de anonimidade, utilizando endereços pseudónimos sendo, contudo, provável, que seja possível conectar as carteiras dos utilizadores à conta do Facebook, que possui informações pessoais dos utilizadores, assemelhando-se um pouco à abertura tradicional de conta num banco (Li & Whinston, 2020). Até à data desconhece-se como é que a Diem planeia alcançar esta privacidade (Wang, 2020).

A Diem utiliza a Libra *Blockchain*, desenvolvida e operada pela Libra Association, que é *open-source*, permitindo aos programadores e utilizadores construir os seus próprios produtos e serviços na Libra *Blockchain* (Brühl, 2020). Na Figura 10 apresenta-se a arquitetura do ecossistema da Diem e como as componentes básicas interagem entre si.

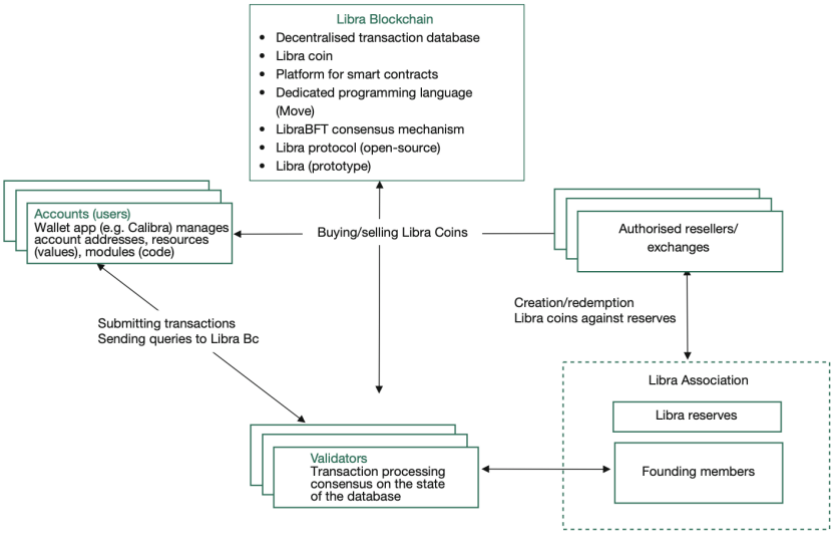


Figura 10 - Arquitetura do ecossistema Diem (retirado de Brühl, 2020).

Segundo a Libra Association Members (2020:1) a Libra *Blockchain* é uma "*decentralized, programmable database designed to support a low-volatility cryptocurrency that will have the ability to serve as an efficient medium of exchange for billions of people around the world.*" Tem por base a

tecnologia *blockchain*, presentemente com permissões de consorcio, sendo uma base de dados criptografada mantida pelo uso do protocolo Diem, assegurando que nenhuma moeda Diem será duplicada, perdida ou transferida sem autorização (Brühl, 2020). Este protocolo utiliza duas entidades: os agentes de validação (conjunto de super nós constituindo a Diem Association) (Abraham & Guegan, 2019) e os clientes. Os agentes de validação, tal como o nome indica, processam as transações efetuadas pelos clientes e são os únicos autorizados a alterar a base de dados (Abraham & Guegan, 2019). É utilizado um mecanismo de consenso distribuído para chegar a acordo sobre o resultado das transações efetuadas. Segundo Abraham e Guegan (2019) uma interação de um cliente, como a execução de uma transferência resume-se a quatro etapas: (i) o cliente contacta um agente de validação para submeter a transação denominado de líder para essa operação (a função de líder é alternada entre os agentes); (ii) o líder propõe a transação para os restantes agentes de validação; (iii) a rede de agentes de validação executa a transação e o mecanismo de consenso e (iv) este mecanismo tem como resultado uma assinatura digital provando que a transação foi realizada. A Libra *Blockchain* utiliza um algoritmo de consenso, LibraBFT (*Libra Byzantine Fault Tolerance*) (Libra Association Members, 2020). Este protocolo descreve a característica de um sistema informático distribuído, que continuará a funcionar corretamente mesmo que alguns componentes do sistema falhem, não se sabendo se um componente falhou (Libra Association Members, 2020) ou seja, continua sendo fiável mesmo na presença de comportamento malicioso ou erróneo por parte de uma minoria de validadores (um terço dos agentes validadores) (Li & Whinston, 2020). Quando um utilizador vê a confirmação de uma transação por parte dos agentes de validação, tem a certeza de que a transação já foi concluída (Libra Association Members, 2020).

Como o objetivo da *blockchain* é garantir um sistema de pagamento que satisfaça as necessidades financeiras diárias de um número grande de pessoas, o algoritmo de consenso necessita de ter a capacidade de ser escalável permitindo um elevado rendimento de transações, baixa latência e uma abordagem mais eficiente do ponto de vista energético do consenso comparativamente ao PoW (Libra Association Members, 2020).

Digital Currency Electronic Payment

A Digital Currency Electronic Payment (DCEP) é uma moeda digital que o Banco Central da China (*People's Bank of China* ou PBoC) está a desenvolver, conhecida como a versão digital do yuan (moeda física chinesa) apoiada com um rácio 1:1 da moeda yuan/renminbi (Xu & Prud'homme, 2020).

Segundo Xu e Prud'homme (2020) o sistema DCEP segue uma abordagem de "duas camadas": emissão e distribuição. Como é centralizada no PBoC, sendo um sistema digital soberano, é a única entidade emissora do DCEP e para a distribuição rápida da moeda ao público são selecionados bancos comerciais e instituições não financeiras (p.e. Alibaba, Tencent e Union Pay) na China, com fortes redes de pagamento móvel pré-existentes. Segundo (Auer et al., 2020b), espera-se que sejam usados diferentes níveis de identificação de utilizadores, através de um instrumento de pagamentos *token-based* (depósito do CBDC em aplicações de *smartphones* ou em cartões de circuito integrado e posterior transferência do valor para outros utilizadores quando se efetuam pagamentos) e/ou em contas (abertura de uma conta no Banco Central utilizada para fazer pagamentos e transferências entre contas).

Face ao interesse de "encontrar um equilíbrio" entre o anonimato e a necessidade de evitar crimes financeiros, o PBoC não exporá completamente a informação do utilizador aos bancos. Mas as identidades dos utilizadores serão, provavelmente, ligadas a carteiras individuais, dando às autoridades outras possibilidades de rastrear as transações (Bloomberg, 2020).

O DCEP permite a desvinculação a contas bancárias tradicionais para realizar transferências de valor, reduzindo significativamente a dependência de conta bancária para realizar transações. Assim, se os utilizadores e as empresas utilizarem apenas a DCEP para pequenos pagamentos diários, não há necessidade de ir a um banco comercial ou instituição comercial. Basta descarregar uma aplicação de carteira digital do Banco Central e completar o registo para utilizar o DCEP para transferências. Para além de retirar ou recarregar o DCEP na carteira digital, os utilizadores não precisam de vincular contas para transferências mútuas. Assim, os utilizadores poderão utilizar DCEP anonimamente em transações diárias (Shi & Zhou, 2020). Deste modo, será possível que os utilizadores sejam anónimos entre si, mas o PBoC terá informação suficiente para evitar o branqueamento de capitais e outras infrações criminosas e aliviar a carga de trabalho dos bancos comerciais (Auer et al., 2020b).

À semelhança das criptomoedas referidas anteriormente, será utilizada uma carteira digital, porém ainda não está confirmado se será necessário um registo formal para a utilização dessa carteira (Tran & Matthews, 2020). Estas podem ser baseadas em diversas formas de identificação, para além de informações pessoais, permitindo que os utilizadores decidam se querem ligar a carteira a uma conta bancária. Para permitir distintos níveis de anonimato, os procedimentos KYC teriam diferentes graus de força nos vários níveis, sendo que as transações de maiores montantes teriam requisitos mais elevados dos procedimentos KYC (Auer et al., 2020b). (Auer et al., 2020b). Assim, a DCEP pode não precisar de uma conta, mas pode necessitar dos procedimentos KYC (Perianne et al., n.d.), não oferecendo o mesmo anonimato que o dinheiro físico. Como, em geral, a utilização de dinheiro físico confere privacidade aos seus utilizadores (podendo eventualmente diferir de país para país), a aplicação dos procedimentos KYC pode conduzir a algum receio de exposição das vidas financeiras das pessoas às autoridades (Mukherjee, 2020).

O DCEP será construído num sistema de dois níveis distintos: (i) entre o Banco Central e os bancos comerciais e (ii) entre bancos comerciais, particulares e empresas (Perianne et al., n.d.). A arquitetura utilizada no projeto piloto é classificada como um modelo híbrido segundo (Auer et al., 2020b), sendo o DCEP um crédito direto sobre o PBoC, mas que utiliza operadores intermediários para pagamento em tempo real. O PBoC armazena periodicamente uma cópia das transações comerciais. O DCEP utilizará como tecnologia base um misto de base de dados convencional e a tecnologia *blockchain*, já que segundo a perspetiva de Auer et al. (2020) aquela tecnologia não está suficientemente madura para uma aplicação em larga escala, como no caso da China, que é necessário um elevado número de transações por segundo (TPS) para acomodar as necessidades do retalho.

Digital Euro

O Digital Euro pretende ser a CBDC do Banco Central Europeu (BCE), podendo apoiar a digitalização do euro, a economia e a independência estratégica da União Europeia devido ao declínio significativo no papel do numerário como meio de pagamento (European Central Bank, 2020). O Digital Euro está em fase de desenvolvimento, mas já foram exploradas

opções de implementação. Segundo o BCE (European Central Bank, 2020) a emissão desta CBDC deve permanecer sob o controlo do Eurosistema composto pelo BCE e os Bancos Centrais nacionais dos países que adotaram a moeda única (Banco de Portugal, n.d.-b). A tecnologia proposta pela Comissão Europeia para ser utilizada no Digital Euro é uma DLT (European Commission, 2020) sendo que podem ser consideradas duas estruturas de implementação ao nível do *back-end* da infraestrutura (European Central Bank, 2020): centralizada e descentralizada. Ou seja, os utilizadores podem aceder ao euro digital quer diretamente, quer através de intermediários supervisionados. Na abordagem centralizada, as transações digitais em euros são registadas no *ledger* do Eurosistema. Na segunda abordagem, o Eurosistema determina regras e requisitos para a liquidação de transações digitais em euros, que são registadas pelos utilizadores e/ou intermediários supervisionados. Nas duas abordagens referidas é possível a operação de agentes intermediários como elementos de liquidação ou como "controladores de acesso". Estes têm como funções básicas, à semelhança dos bancos comerciais, a autenticação dos utilizadores e lidar com os procedimentos KYC. Os agentes de liquidação têm, para além destas funções, a execução de transações digitais. Dois requisitos importantes a serem considerados num futuro Digital Euro são a privacidade e o seu uso offline. Podem ser resolvidos com um sistema em camadas para privacidade implementado em uma carteira bem como uso offline suportado por cartões inteligentes ou outras tecnologias (Bharathan, 2020).

E-Krona

A E-krona é a CBDC da Suécia (emitida pelo *RiskBank),* que se encontra em projeto piloto (Sveriges Riksbank, 2018). O *Riskbank* distingue dois tipos de E-krona: *account-based* e *token-based*. No primeiro caso a moeda é mantido numa conta no Banco Central (Hedqvist, 2018) apoiado na identificação do proprietário da mesma (Auer et al., 2020b). Pode ser descrita sob a forma de um saldo, que se encontra num registo central mantido pelo *Riksbank* (Sveriges Riksbank, 2018). No segundo caso, a forma mais semelhante à moeda fiduciária (Hedqvist, 2018), pode ser descrito como um valor pré-pago, que pode ser armazenado localmente (p.e. cartão ou telemóvel). É pressuposto que existe um registo implícito, sendo possível manter o registo das transações e garantindo quem é o legítimo proprietário da E-krona. Embora, regra geral, estas transações sejam rastreáveis, pode acontecer que no caso de um cartão pré-pago mudar de proprietário, não seja possível rastrear esta ação (Hedqvist, 2018). Os utilizadores permanecerão anónimos em relação ao *Riksbank*, mesmo com a E-krona *account-based*, uma vez que o Banco Central apenas recebe dos intermediários (responsáveis pelo cumprimento dos procedimentos KYC) informação sobre saldos e pagamentos de contas individuais e não sobre os titulares da conta (Auer et al., 2020b).

Na fase piloto, o *Riskbank* optou por uma utilizar a tecnologia R3 *Corda DLT* (Corda, n.d.), que difere da tecnologia usada na Bitcoin em diversos aspetos. A rede DLT da E-krona será privada e acessível apenas para os participantes aprovado pelo Banco Central (Nelson, 2020). A *Corda DLT*, comparativamente à *blockchain* com algoritmo de consenso PoW, consome menos energia e é mais escalável, já que apenas alguns "nós" e o "nó" notário (componente de suporte para evitar o *double-spending*), estão envolvidos em cada transação (Rolfe, 2020). A rede assegura que apenas as transações válidas são registadas e cada participante na rede *Corda DLT* executa um ou mais "nós" (armazena, recebe, valida e encaminha as transações) (Sveriges Riksbank, 2020).

Comparação

De forma sucinta, na Tabela IV comparamos a Bitcoin com as CBDC, anteriormente referidas, atendendo às seguintes características (Godinho et al., 2020):

- Nível de anonimidade: grau de confidencialidade associada aos utilizadores aquando das transações.
- Tecnologia: tipo de tecnologia usada.
- Nível de confidencialidade do *ledger*: quem é capaz de aceder ao *ledger* de forma a consultar as transações.
- Algoritmo de consenso: algoritmo de consenso utilizado.
- Escalabilidade: capacidade de lidar com uma grande quantidade de transações simultaneamente.
- Volatilidade: relacionado com o valor e estabilidade da criptomoeda/CBDC.
- Velocidade de transação: tempo necessário para a realização da transação.

Tabela IV – Comparação de algumas características entre Bitcoin, Diem e CBDC.

Características	Bitcoin	Diem	DCEP	Digital Euro	E-krona
Nível de confidencialidade do utilizador	Carteira com endereços pseudónimos	Carteira digital com possibilidade de a ligar a uma conta do Facebook ou carteiras anónimas (endereços pseudónimos)	Pagamentos *token-based* e *account-based*	*	Com carteiras *account-based* os utilizadores não vão ter anonimidade; Carteiras *token-based* têm anonimidade com valor relativamente pequeno
Nível de confidencialidade das transações do *ledger*	*Ledger* é público	Apenas as entidades permitidas têm acesso ao *ledger*	*Ledger* é privado e apenas o PBoC tem acesso	Apenas as entidades permitidas têm acesso ao *ledger*	Apenas as entidades permitidas têm acesso ao *ledger*
Tecnologia	Blockchain Pública	Blockchain de consórcio (Libra Blockchain)	*Blockchain* e bases de dados	DLT	R3 Corda (DLT Permissionada)
Algoritmo de consenso	PoW	LibraBFT	*	*	*
Volatilidade	Sim	Talvez (caso a credibilidade do Facebook seja abalada)	Não	Não	Não
Velocidade de transação (TPS) (Wang, 2020)	7	1.000	220.000	*	*

* Sem informação

Como podemos constatar pela Tabela IV, algumas diferenças relevantes entre a Bitcoin e as CBDC é que a primeira apresenta um maior nível de confidencialidade do utilizador relativamente às CBDC, uma vez que são utilizados endereços pseudónimos, qualquer que seja o montante transferido. Todavia, ao nível da confidencialidade das transações no *ledger*, a DCEP é a que apresenta mais confidencialidade, porque apenas o PBoC tem acesso às transações, a Diem, a Digital Euro e a E-krona apresentam menor confidencialidade, porque permite conceder acesso a pessoas, enquanto a Bitcoin não tem nenhuma confidencialidade, porque a consulta das transações é imediatamente acessível a qualquer pessoa. Por tal motivo, o algoritmo de consenso utilizado na Diem não necessita de tanto poder

computacional, comparativamente ao utilizado na Bitcoin, já que é utilizada uma *blockchain* privada. Igualmente relevante é a diferença respeitante à volatilidade das moedas: as CBDC têm menor volatilidade em relação à Bitcoin, por serem apoiadas por ativos líquidos e estáveis. Finalmente, merece realce a existência de um teto para a Bitcoin (21 milhões), o que garante uma deflação.

2.6 Rastreabilidade e transparência

A rastreabilidade (capacidade de verificar o histórico das transferências efetuadas de uma determina carteira) e transparência (apresentação de informação aberta, abrangente e compreensível) (Blocks99, n.d.) são dois conceitos muito importantes na moeda corrente. Ajudam a evitar ações fraudulentas, como a lavagem de dinheiro, já que os sistemas bancários têm a capacidade de, ao serem solicitadas com uma ordem do tribunal, apresentar todas as transações de uma determinada conta e saberem a que pessoa/entidade essa conta pertence. Ou seja, a transparência é essencial para a contabilidade e auditoria, contudo existe uma relação entre a privacidade e a transparência (Blocks99, n.d.), sendo que para haver mais transparência da informação menor será a privacidade dos utilizadores e vice-versa. Por outro lado, se for utilizado dinheiro em espécie (notas ou moedas) nas transações comerciais, tais conceitos já não se aplicam deixando uma abertura para ações fraudulentas.

Nas *blockchains* públicas (utilizadas na Bitcoin), onde as transações são armazenadas, o *ledger* é transparente (de modo a evitar manipulação de dados) já que todas as pessoas que aderirem à rede conseguem ver e analisar, a qualquer momento, as transações (Kritikos, 2018). A rastreabilidade permite que transações sejam investigadas e, caso existam atividades ilegais, estas moedas são consideradas ilegítimas e podem ser rejeitadas pelos prestadores de serviços (Werner et al., 2020).

A transparência, por sua vez, oferece a capacidade de verificar se os pagamentos e as despesas são divulgados de forma clara. Com a crescente adoção de criptomoedas, o histórico de transações de uma pessoa pode permitir tirar conclusões sobre o seu ambiente social e hábitos de compra (Werner et al., 2020).

Para o rastreamento de transações podem ser utilizados alguns *softwares*, como por exemplo:

- *Oxt*: mapa interativo da *blockchain* da Bitcoin, que permite a rastreabilidade de transações entre carteiras (Samourai Wallet, n.d.).
- *Ciphertrace*: ferramenta de remoção de anonimato para identificar e rastrear facilmente os criminosos (CipherTrace, n.d.).
- *Chainalysis*: permite conectar transações de criptomoedas a atividades do mundo real (Chainalysis, n.d.).
- *Graphsense*: plataforma de análise criptográfica, que permite investigações interativas e controlo completo de dados para execução de tarefas analíticas avançadas (Graphsense, n.d.).

2.7 Privacidade e confidencialidade

Privacidade e confidencialidade dos cidadãos são direitos e garantias legalmente instituídos numa sociedade democrática e de aplicação transversal aos vários setores de atividades da sociedade. Com características e abrangências distintas, a privacidade refere-se a pessoas, estando a confidencialidade restringidas à informação. À semelhança do dever de sigilo

bancário (abrangendo membros das instituições de crédito, respetivos colaboradores, mandatários, comissários e outras pessoas que lhes prestem serviços de forma permanente ou ocasional) a que se encontra obrigada a banca comercial, é fundamental que os direitos de privacidade e confidencialidade sejam viabilizados e respeitados nas CBDC, sem inviabilizar os processos regulamentares e de conformidade KYC/AML, que devem ser cumpridos (*The Digital Dollar Project*, 2020).

A conciliabilidade entre a garantia dos direitos de privacidade e confidencialidade e o cumprimento das normas KYC/AML é uma questão relevante para a viabilidade das CBDC. Por exemplo, a anonimidade total (em que existem privacidade e confidencialidade absoluta) permite que as CBDC sejam irrastreáveis, facilitando o comportamento ilegal e ilícito, não sendo desejável do ponto de vista da lei (*The Digital Dollar Project*, 2020). Em oposição, um sistema concebido para vigilância total e rastreabilidade, consegue atingir os objetivos de implementação legal, contudo, esta transparência reduziria a atratividade e inibiria a adoção das CBDC, com implicações na procura e no valor da moeda (*The Digital Dollar Project*, 2020).

No contextos das CBDC, a confidencialidade das transações realizadas pelos utilizadores significa a impossibilidade de conhecer os detalhes da transação) (Allen et al., 2020) enquanto a privacidade caracteriza-se por: (i) privacidade de identidade (incapacidade de ligar transações ou atividades ao remetente e/ou destinatário de uma determinada transação) (Allen et al., 2020); (ii) privacidade dos intervenientes (inviabilidade de conhecer as carteiras/contas utilizadas nas transações por parte dos utilizadores). Estas características são importantes tanto para os utilizadores finais, como para os Bancos Centrais já que estes pretendem a adoção das CBDC. Deste modo, a privacidade e a confidencialidade vão ser as características implementadas nas provas de conceito.

2.8 Sumário

O aparecimento da primeira moeda digital que resolvia o problema do *double-spending*, a Bitcoin, alterou o panorama monetário-financeiro mundial, impulsionando o rápido crescimento das *altcoins*. Apesar da renitência de alguns governos e instituições financeiras à aceitação das criptomoedas, particularmente devido à sua natureza descentralizada suportada por tecnologia *blockchain* (permitindo contornar qualquer instituição financeira centralizada), a moeda digital deixou de ser um assunto interdito no mundo das finanças, entrando na agenda dos bancos.

As tentativas governamentais para a criação de moedas digitais estão a ser implementadas por intermédio das CBDC. Alguns Bancos Centrais estão a lançar programas-piloto com o intuito de determinar a eficiência e/ou viabilidade do potencial das CBDC, como é o caso da China (DCEP), da Suécia (E-krona) e da comunidade europeia (Digital Euro). Também o setor privado tem manifestado interesse no lançamento de moeda digital própria, como é o caso da Diem (ex. Libra Facebook). Assim, a criação de uma CBDC é, por um lado, inspirada no sucesso das criptomoedas e na tecnologia subjacente ao seu desenvolvimento e, por outro lado, um sinal claro de que essas moedas digitais e a respetiva indústria não estatuída e descentralizada é uma ameaça à forma mais regulamentada e centralizada do sistema monetário estatal.

As questões relacionadas com a privacidade e a confidencialidade na utilização de moedas digitais são matéria de grande sensibilidade a levar em consideração na implementação das CBDC. A privacidade dos utilizadores e a confidencialidade das transações são características apelativas tanto para os utilizadores, cujos direitos devem ser

salvaguardados, como para os Bancos Centrais, como meio de incentivo à adoção das CBDC. Deste modo, o Banco Central poderá ter um registo da quantidade de dinheiro detida por cada entidade (pessoas e corporações), no entanto também assegurará a proteção de privacidade e segurança criptográfica apropriadas, numa tentativa de reunir a conveniência e segurança que são atribuídas às criptomoedas e à circulação monetária regulamentada e reservada do sistema bancário tradicional.

Consoante o fim a que se destina, as CBDC podem caracterizar-se pelos tipos *wholesale* (pagamento entre bancos comerciais e o Banco Central ou outras entidades que têm uma conta no Banco Central) e *retail* (utilizada pelo público e/ou empresas, na realização de pagamentos e/ou criação de poupanças). Quanto à acessibilidade das CBDC, podemos distingui-las entre *account-based* (necessita que o proprietário tenha uma conta no Banco Central) e *token-based* (carteira de hardware que não requere uma conta bancária no Banco Central, permitindo que os seus proprietários tenham anonimidade). A garantia de anonimidade nas CBD *token-based* permite que possam ser consideradas como um substituto do dinheiro físico, ao invés das CBDC *account-based*. Contudo, apesar da anonimidade ser uma característica apreciada pelos utilizadores, existem normativos KYC/AML para este tipo de CBDC.

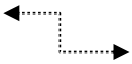
Capítulo 3
Cenários, casos de uso e provas de conceito

Neste capítulo abordamos alguns cenários e respetivos casos de uso e implementação de provas de conceito referentes à confidencialidade das transações realizadas pelos utilizadores e à sua privacidade (UCI Researchers, 2011). Conforme referido no capítulo anterior, a confidencialidade e a privacidade são direitos dos utilizadores, sendo fundamental que sejam garantidas nas CBDC, assegurando em simultâneo o cumprimento das normas KYC/AML. O acesso à identidade do utilizador e às transações por ele realizadas poderá ser efetuado pelo Banco Central, para o qual deverá ser requerido o levantamento da privacidade.

Para o estudo destes cenários distinguimos entre a utilização de carteiras (*token-based*) e de contas (*account-based*) assumindo-se, neste último caso, que será necessário a abertura de uma conta no Banco Central, à semelhança do que acontece atualmente na banca comercial. Para melhor interpretação dos cenários utilizaremos a simbologia e respetivo significado indicados na Tabela V.

A título ilustrativo, apresentamos os cenários base sem nenhum tipo de privacidade nem de confidencialidade, quer com carteiras (*token-based*), utilizados na Bitcoin e na CBDC, quer com contas (*account-based*), também utilizado na CBDC.

Tabela V – Simbologia utilizada no estudo dos cenários

Símbolo	Significado
Atores	
	Banco Central
	Utilizador (Alice ou entidade emissora e Bob ou entidade recetora)
	Carteira (*token-based*)
	Conta (account-based)
	Autoridades judiciais (Banco de Portugal, Comissão do Mercado de Valores Mobiliários, Fundo de Garantia de Depósito, Sistema de Indemnização aos Investidores, Administração Tributária, Sistema Judicial (Diário da República, 1992))
	Agente intermediário (bancos comerciais/retalho ou outros elementos do sistema financeiro)
	Terceiros
Inter-relações	
	Visibilidade
	Potencial visibilidade
	Transação
	Carteira pertencente a utilizador

Bitcoin (*token-based*)

A Bitcoin é o caso de referência inverso do exemplificado posteriormente. Neste cenário, apesar de Alice e Bob não se conhecerem, têm acesso a informações sobre as carteiras um do outro e à transação realizada. Por outro lado, qualquer pessoa e/ou autoridade judicial, pode ter acesso aos endereços pseudónimos das carteiras e respetivas transações não sendo, contudo, possível associá-las a quem pertencem (Figura 11). Nesta tipologia de cenário é

possível analisar as transações efetuadas entre carteiras, construir uma rede de rastreamento das transações e identificar padrões.

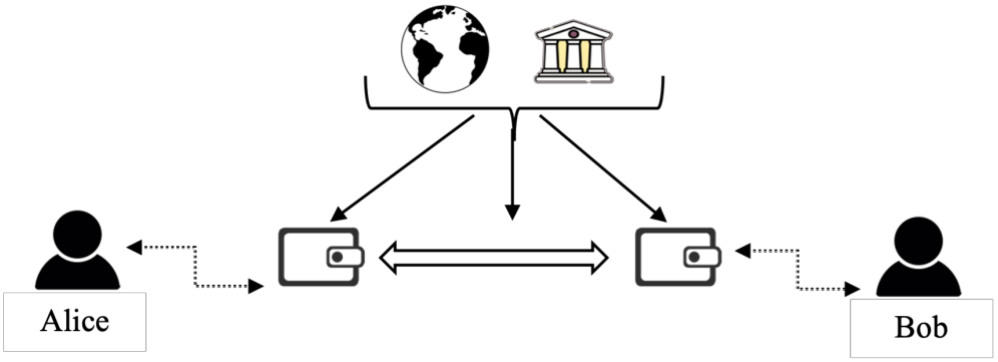


Figura 11 – Caso base da Bitcoin.

CBDC (*token-based*)

No contexto da CBDC *token-based* (com a utilização de carteiras virtuais) o banco tem acesso à identificação das carteiras, bem como aos respetivos proprietários e às transações realizadas por estes. Entidades terceiras não têm conhecimento sobre os utilizadores, nem das transações efetuadas por estes, nem das respetivas carteiras (Figura 12).

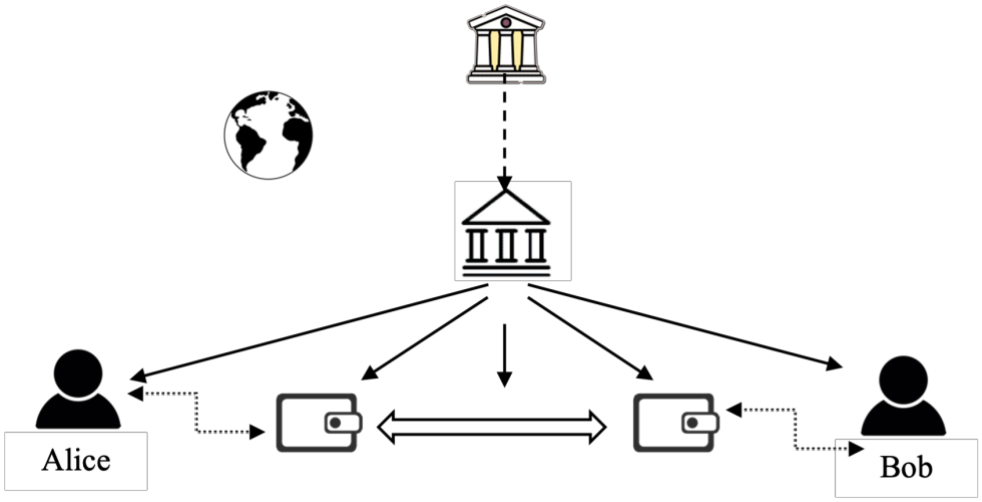


Figura 12 – Caso base CBDC *token-based*.

Neste caso não existe o fornecimento de privacidade aos utilizadores por parte do Banco Central, sendo o cenário mais básico. Seria possível, eventualmente, restringir o acesso do Banco Central aos utilizadores, carteiras e transações e garantir a privacidade com a utilização de tecnologias como os *smart contracts*.

CBDC (*account-based*)

No cenário da CBDC *account-based*, os Bancos Centrais têm acesso às contas e à informação dos respetivos titulares/proprietários, bem como às respetivas transações. De igual forma, autoridades fiscalizadoras, com ordens judiciais, têm permissão para consultar as informações necessárias. Semelhante ao descrito no cenário CBDC *token-based*, terceiras entidades não têm acesso aos utilizadores, às suas transações e às respetivas contas (Figura 13).

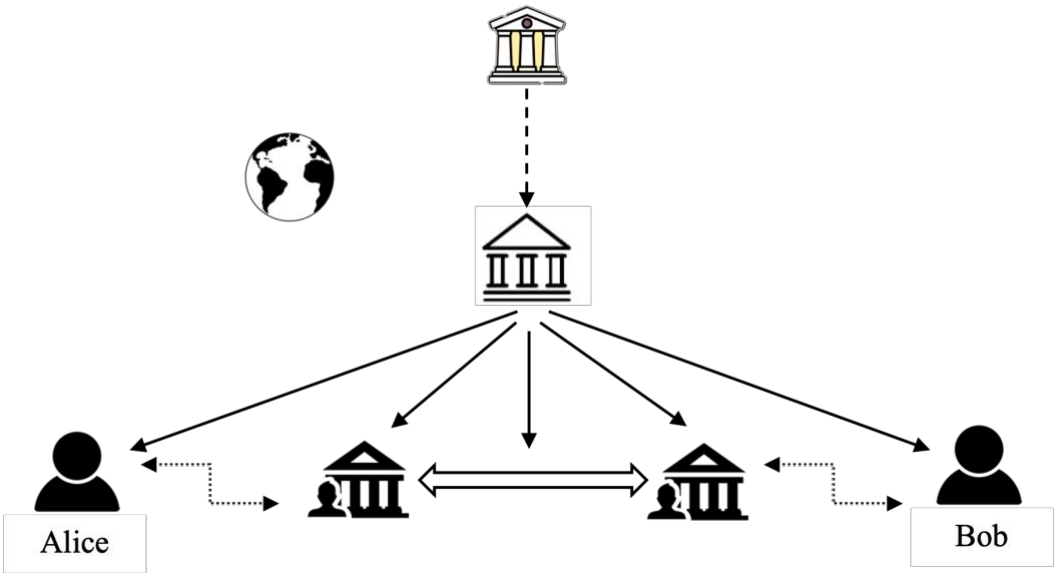


Figura 13 – Caso base CBDC *account-based*.

À semelhança do que acontece nos bancos comerciais, para o cumprimento das normas KYC/AML o Banco Central necessita de conhecer os utilizadores e respetivas contas, para evitar a ocorrência de fraudes. Contudo, é possível restringir o acesso a esta informações e assegurar a privacidade, com a utilização de tecnologias como os *smart contracts*, permitindo ao(s) Banco Central/autoridades judiciais terem acesso unicamente às transações com uma ordem judicial (por exemplo, se a transação ocorrida for superior a um valor definido) ou com a utilização de mecanismos automáticos que alertem o Banco Central (por exemplo, identificação de situações potencialmente suspeitas ao analisar as transações).

Como acabámos de ver, os cenários CBDC *token-based* e *account-based* são os casos base em que não são permitidas a privacidade de identidade nem a confidencialidade de transação. Os casos que passaremos a descrever de seguida, definem a credibilidade dos cenários que permitem a privacidade e/ou confidencialidade aos utilizadores.

Para facilitar a leitura, referenciação e identificação dos cenários, sub-cenários, casos de uso e implementações que vamos apresentar, utilizaremos a seguinte nomenclatura e respetivo significado:

- *Ci* : identificação do cenário *i*;
- *Ci.j* : referência ao cenário *i* e sub-cenário *j*;
- *Ci.jUk* : alusão ao cenário *i*, sub-cenário *j* e caso de uso *k;*
- *Ii* : menção à implementação do cenário *i*.

De realçar que, nos cenários em que Bob apenas conhece a transação, é essencial a utilização de uma terceira entidade, que conheceria ambas as partes envolvidas na transação, com o mínimo de informação possível, de modo a permitir a realização da mesma.

3.1 Cenários *account-based*

Os vários sub-cenários *account-based* que iremos considerar estão identificados e sintetizados na Tabela VI, identificando para cada situação se o Banco Central conhece ou desconhece o utilizador, conta e transações, que passaremos a caracterizar.

Tabela VI – Identificação dos cenários do Banco Central *account-based*

Cenário	Utilizador	Conta	Transação	Credível
C1	desconhece	irrelevante	irrelevante	não
C2	conhece	desconhece	irrelevante	
C3	conhece	conhece	desconhece	sim
C3.1	desconhece	conhece	conhece	
C3.2	desconhece	desconhece	conhece	
C3.3	conhece	conhece	conhece	
C4	conhece	conhece	conhece	sim
C4.1	desconhece	conhece	conhece	
C4.2	desconhece	desconhece	conhece	
C4.3	conhece	conhece	conhece	

C1: Banco Central desconhece utilizadores

Neste hipotético cenário, o Banco Central permite a privacidade de identidade, não conhecendo os utilizadores. Contudo, este cenário não é viável para implementação por contrariar o cumprimento das normas KYC/AML, que obrigam o Banco Central a conhecer as contas e respetiva titularidade.

C2: Banco Central conhece utilizadores, desconhece contas

Neste caso, o Banco Central tem conhecimento dos utilizadores, mas não da(s) respetiva(s) conta(s). Contudo, à semelhança do cenário *C1*, por imperativo de observância das normas KYC/AML, o Banco Central necessita de identificar a(s) conta(s) dos seus utilizadores, o que torna este cenário não credível para implementação.

C3: Banco Central conhece utilizadores e contas, desconhece transações

Nesta situação, o Banco Central tem visibilidade sobre as contas e os respetivos utilizadores. Ainda assim, é possível fornecer uma camada de privacidade aos utilizadores, porque o Banco Central não tem conhecimento direto sobre as operações efetuadas pelos utilizadores, permitindo a confidencialidade das transações. Contudo, o Banco Central pode conhecer os valores agregados (a totalidade das transações ou os valores por setor económico) calculados por *smart contracts*. De facto, a utilização de *smart contracts* (em *blockchain*) constitui uma implementação possível para este cenário, realizando análise de padrões das transações e permitindo a deteção de comportamentos fraudulentos. Existindo indícios de ilegalidades ou alguma solicitação pelas autoridades judiciais, as transações relevantes são desencriptadas para análise, sendo registado na *blockchain* as operações para as quais foi levantada a confidencialidade e os respetivos motivos.

Este cenário é credível para implementação por estar em conformidade com as normas KYC/AML. Para melhor o caracterizar apresentamos de imediato três respetivos sub-cenários.

C3.1: Bob desconhece Alice, conhece a conta desta e a transação

Na perspetiva do Banco Central, utilizadores e contas apresentam completa transparência. Por parte dos utilizadores, Bob não conhece Alice, mas tem acesso às transações que ela realiza com ele e ao identificador da conta da Alice, ou seja, ao endereço da conta (Figura 14).

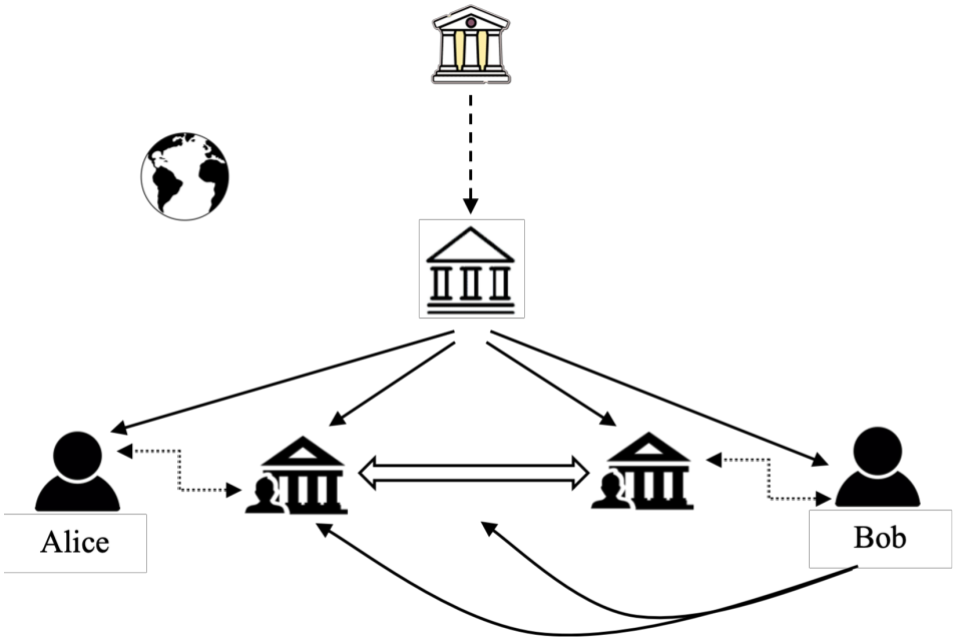


Figura 14 – *C3.1*: o Banco Central conhece os utilizadores e as contas; Bob conhece a conta de Alice e a transação realizada.

C3.2: Bob desconhece Alice e a sua conta e conhece a transação

Neste cenário, Bob apenas conhece a transação realizada, desconhecendo a conta de origem da transação e o respetivo proprietário (Alice). Para o Banco Central, utilizadores e contas garantem acesso total (Figura 15).

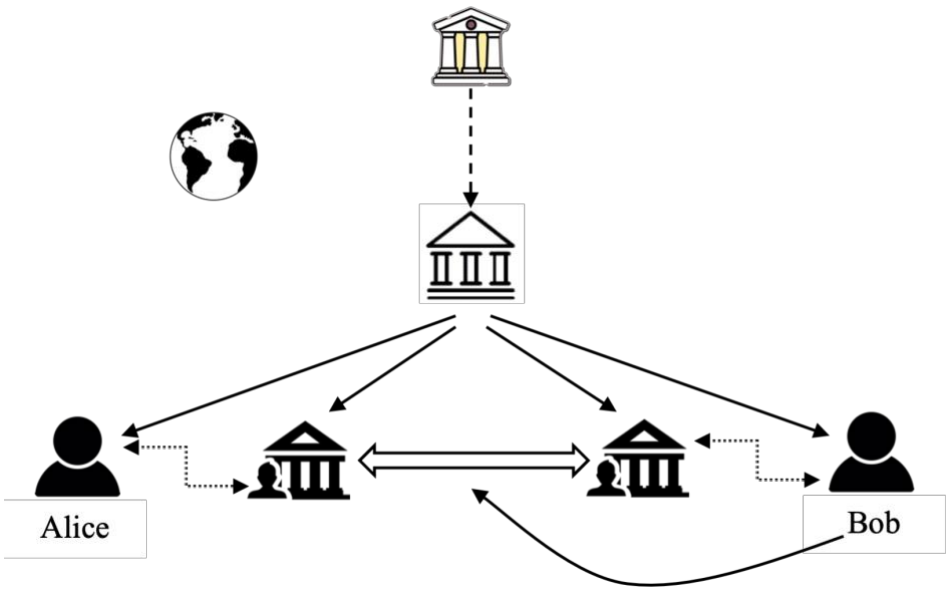


Figura 15 – *C3.2*: O Banco Central conhece os utilizadores e as contas; Bob apenas conhece a transação com Alice.

C3.3: Bob conhece Alice, a conta desta e a transação

Este cenário apresenta semelhanças com as transferências entre contas realizadas em bancos comerciais. Bob conhece a transação realizada, a sua proveniência (conta) e respetiva titularidade (Alice). O Banco Central apenas tem conhecimento de utilizadores e contas para cumprimento das normas KYC/AML que garantem a credibilidade de implementação do cenário (Figura 16).

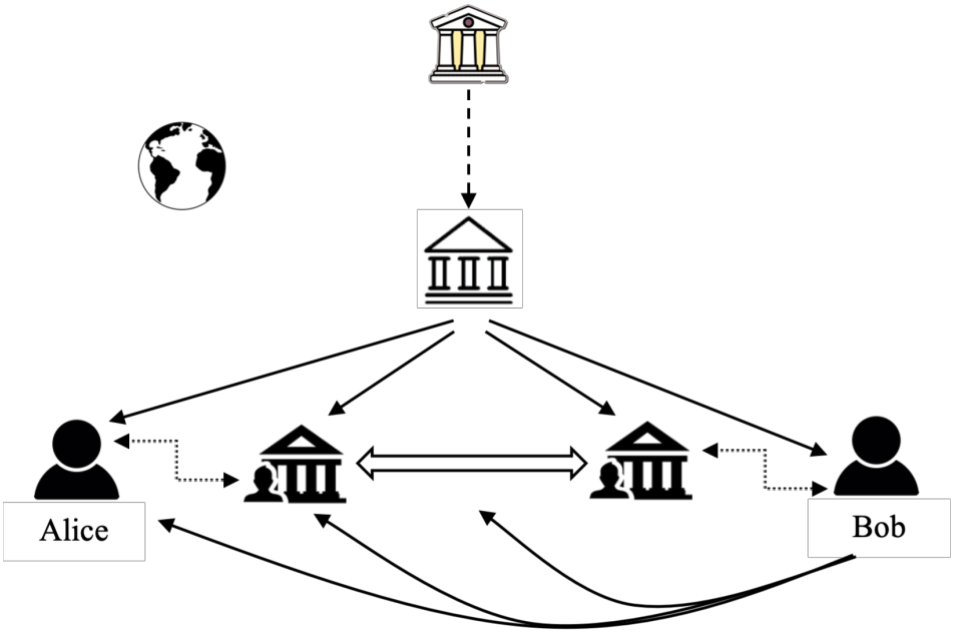


Figura 16 – *C3.3*: O Banco Central conhece os utilizadores e as contas: Bob tem conhecimento de Alice, da respetiva conta e da transação realizada.

C4: Banco Central conhece utilizadores, contas e transações

Este é o cenário com maior semelhança ao modo de operação dos bancos comerciais e que garante maior transparência ao Banco Central, permitindo-lhe o acesso a utilizadores, respetivas contas e transações efetuadas.

C4.1: Bob desconhece Alice, conhece a conta desta e a transação

A realização de operações entre utilizadores é realizada, neste contexto, apenas com conhecimento da transação realizada e da conta que lhe deu origem, mas com desconhecimento do respetivo proprietário (Alice) (Figura 17).

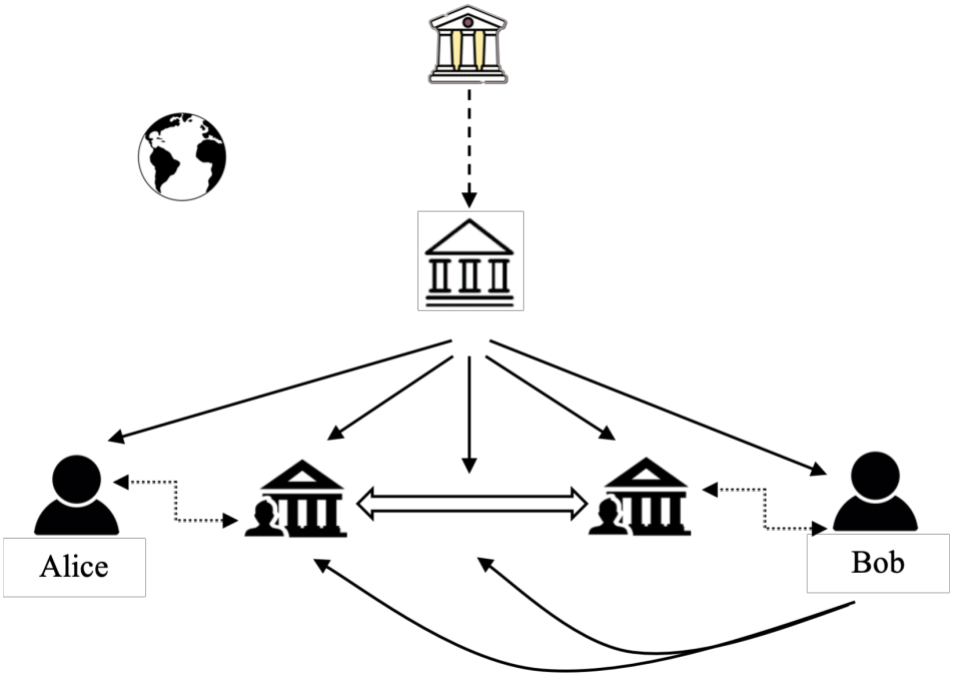


Figura 17 – *C4.1*: O Banco Central conhece utilizadores, contas e transações; Bob conhece a conta de Alice e a transação realizada.

C4.2: Bob desconhece Alice e a sua conta e conhece a transação

Este é o cenário mais limitativo para Bob, permitindo-lhe apenas o conhecimento da transação efetuada, com desconhecimento de Alice e da respetiva conta (Figura 18).

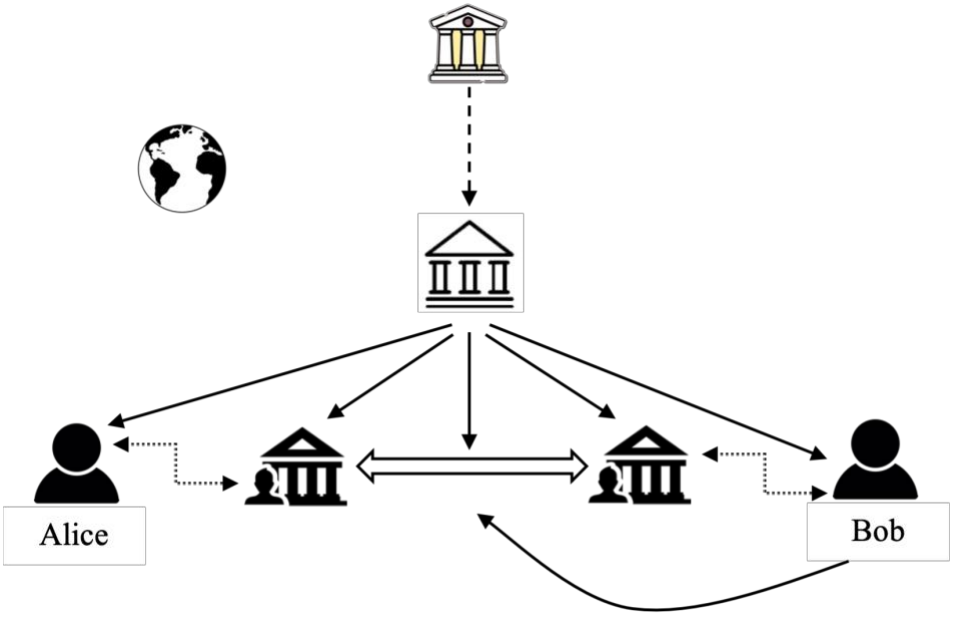


Figura 18 – *C4.2*: O Banco Central conhece utilizadores, contas e transações; Bob apenas conhece a transação efetuada.

C4.3: Bob conhece Alice, conhece a conta desta e a transação

Por oposição de ideias ao cenário *C4.2*, aqui Bob possui integral conhecimento das várias partes envolvidas (Alice, respetiva conta e transação) (Figura 19).

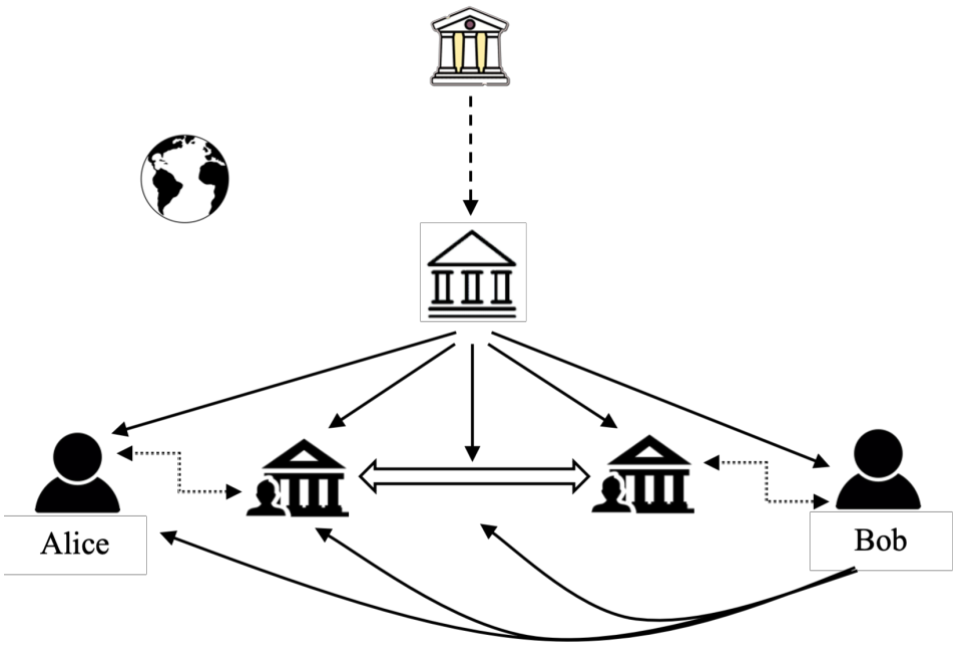


Figura 19 – *C4.3*: O Banco Central conhece utilizadores, contas e transações; Bob conhece Alice, a respetiva conta e a transação concretizada.

C5: Relação do Banco Central com utilizadores através de intermediários

A possibilidade de intermediar a relação do Banco Central com os utilizadores conferiria àquela instituição a figura de autoridade judicial, permitindo-lhe o acesso às informações pertinentes, nas situações que se justificassem (p.e. ordens judiciais). Trata-se de um cenário apenas credível para CBDC *account-based*, porque os agentes intermediários teriam acesso a toda a informação, não permitindo a confidencialidade das transações, nem a privacidade dos utilizadores, objetivo da implementação de CBDC *token-based*, que passaremos a abordar de seguida.

3.2 Cenários *token-based*

Os cenários *token-based* são baseados em carteiras, sendo as transações conhecidas momentaneamente pelos utilizadores, não ficando registadas à semelhança do que acontece atualmente com pagamentos em dinheiro. Para garantir algum controlo sobre os valores transacionados, o Banco Central pode impor um montante máximo que cada carteira pode possuir ou para cada transação.

Os vários sub-cenários *token-based* que iremos considerar estão identificados e sintetizados na Tabela VII que passaremos a caracterizar, identificando para cada situação se o Banco Central conhece ou desconhece o utilizador, conta e transações.

Tabela VII – Identificação dos cenários do Banco Central *token-based*

Cenário	Utilizador	Carteira	Transação	Credível
C6	desconhece	irrelevante	irrelevante	não
C7	conhece	desconhece	desconhece	
C7.1	desconhece	conhece	conhece	não
C7.2	desconhece	desconhece	conhece	
C7.3	conhece	conhece	conhece	
C8	conhece	conhece	desconhece	
C8.1	desconhece	conhece	conhece	sim
C8.2	desconhece	desconhece	conhece	
C8.3	conhece	conhece	conhece	não
C9	conhece	conhece	conhece	
C9.1	desconhece	conhece	conhece	não
C9.2	desconhece	desconhece	conhece	
C9.3	conhece	conhece	conhece	

C6: Banco Central desconhece utilizadores

À semelhança de *C1*, este cenário permite a privacidade de identidade aos utilizadores, mas não é credível para implementação pelo Banco Central, uma vez que, segundo as normas KYC/AML, os bancos necessitam de conhecer os seus clientes de modo a prevenir ações fraudulentas.

C7: Banco Central conhece utilizadores, desconhece carteira e transações

Nesta situação, o conhecimento do Banco Central restringe-se unicamente ao dos seus utilizadores, ficando impossibilitado de aceder a informações sobre as respetivas carteiras e às transações efetuadas, o que permite confidencialidade em relação às mesmas. Apesar do Banco Central não conseguir precisar o número de carteiras de cada utilizador, pode implementar mecanismos de controlo do número máximo de carteiras e dos respetivos montantes máximos, evitando a ocorrência de eventuais abusos. Todavia, a implementação deste cenário não é credível porque Banco Central necessita de emitir a carteira de cada utilizador e por seu próprio arbítrio esquece que carteira pertence a cada utilizador.

C7.1: Bob desconhece Alice, conhece a sua carteira e a transação

Neste cenário Bob tem acesso à transação realizada e à carteira da Alice (entidade emissora da transação), enquanto o Banco Central apenas conhece os intervenientes da transação (Bob e Alice), sem ter informação relativa às suas carteiras.

C7.2: Bob desconhece Alice e a sua carteira e conhece a transação

Neste caso Bob apenas conhece a transação efetuada por Alice, desconhecendo as informações referentes à sua proveniência (carteira) e à sua titularidade (Alice). Por sua vez, o Banco Central apenas tem conhecimento dos utilizadores.

C7.3: Bob conhece Alice, a sua carteira e a transação

Este cenário não é credível para implementação por não permitir nenhum tipo de privacidade à Alice, facilitando a Bob a sua identificação e associação à sua carteira. Deste modo, para o Banco Central, não decorrem daqui vantagens.

C8: Banco Central conhece utilizadores e carteiras, desconhece transações

Nos sub-cenários que iremos descrever existe confidencialidade em relação às transações por parte do Banco Central, mas não sobre as carteiras e respetivos utilizadores. As autoridades judiciais podem ter acesso à mesma informação que o Banco Central, contudo, tal está vedado a terceiras partes.

Neste contexto pode ser utilizada uma encriptação dos dados da transação (p.e. montante), ocultando os seus detalhes, ficando apenas acessível a verificação de identidade dos utilizadores. A implementação deste cenário pode ser realizada com recurso à utilização de protocolos *Secure Multiparty Comunication* (SMC) e/ou *Zero-Knowledge Proof* (ZKP). O SMC permite a privacidade entre os utilizadores sem necessidade de revelar os seus dados privados (Allen et al., 2020b). O ZKP permite o acesso a informação confidencial de um único utilizador, para verificação de autenticidade de uma transação, com um mínimo de informação (p.e. verificar que o emissor de uma transação não enviou mais dinheiro do que o que possui na sua carteira, sem revelar o seu montante). São exemplos de protocolos ZKP o *Sapling*, utilizado na *blockchain* Tezos e o protocolo *Nightfall*, que permite que *tokens* sejam transacionados na *blockchain* Ethereum com privacidade (solução experimental que ainda se encontra a ser desenvolvida).

C8.1: Bob desconhece Alice, conhece a sua carteira e a transação

Neste cenário Bob não sabe quem é a Alice, mas conhece a sua carteira bem como a respetiva transação efetuada (Figura 20).

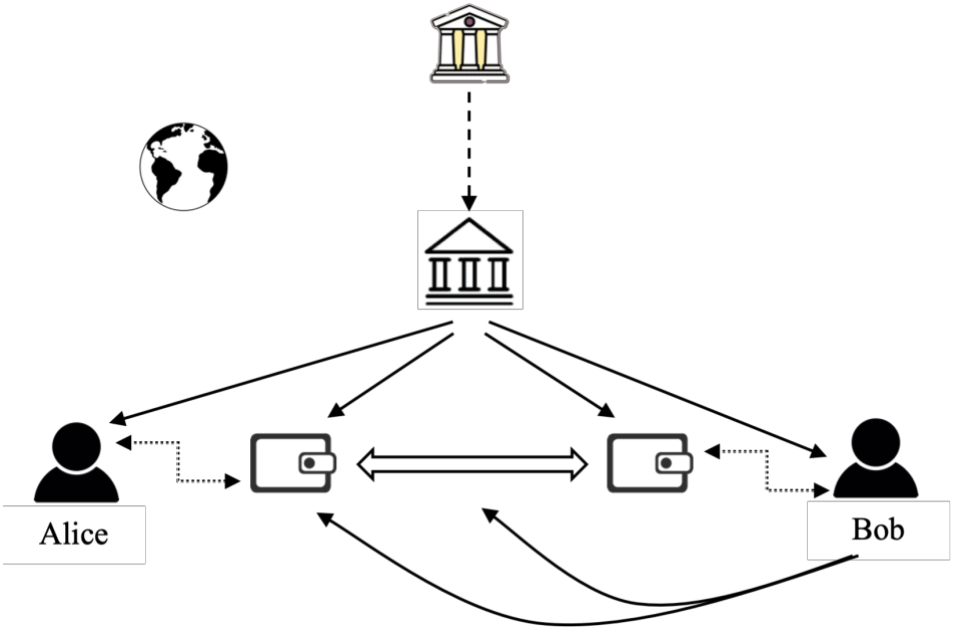


Figura 20 – *C8.1*: O Banco Central conhece os utilizadores e as suas carteiras; Bob conhece a carteira de Alice e a respetiva transação.

C8.2: Bob desconhece Alice e a sua carteira e conhece a transação

Neste cenário Bob apenas tem acesso à transação efetuada com Alice, desconhecendo a carteira que efetuou a transação e o respetivo proprietário (Figura 21).

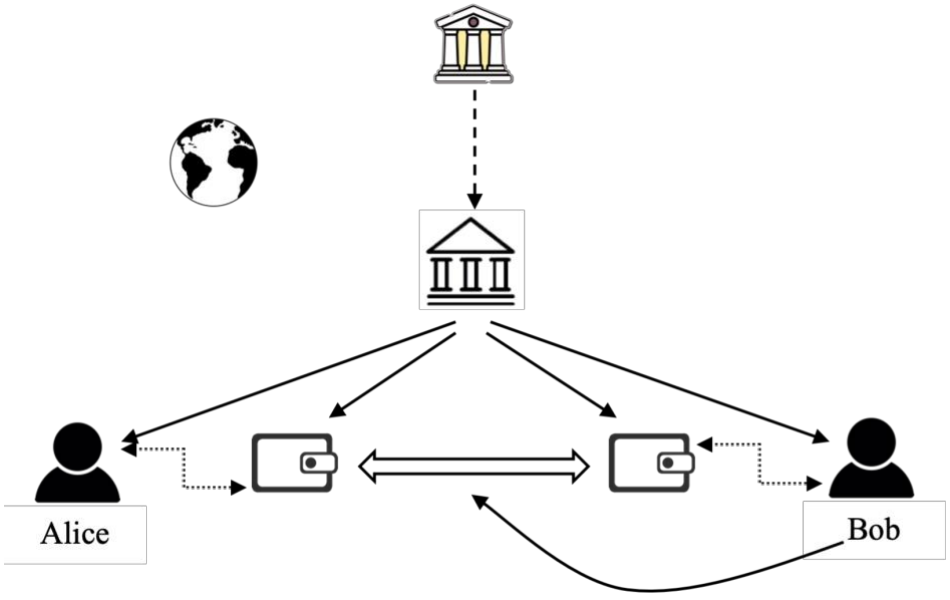


Figura 21 – *C8.2*: O Banco Central conhece os utilizadores e as respetivas carteiras; Bob apenas conhece a transação.

C8.3: Bob conhece Alice, a sua carteira e a transação

Este cenário não é exequível pela falta de privacidade relativamente à Alice. Bob, para além de ter acesso à carteira de Alice, conhece a sua identidade e tem acesso às transações com ela realizadas, não sendo credível para que o Banco Central o implemente nas CBDCs.

C9: Banco Central conhece utilizadores, carteiras e transações

Os cenários subjacentes a este contexto não cumprem com os requisitos de confidencialidade inerente à utilização de CBDC *token-based*, porque o Banco Central tem acesso tanto a informações sobre utilizadores, respetivas carteiras e transações realizadas. Trata-se de um cenário pouco apelativo para os utilizadores, pelo que é pouco provável que o Banco Central o venha a implementar.

C9.1: Bob desconhece Alice, conhece a sua carteira e a transação

Neste cenário Bob tem conhecimento da carteira da Alice e da respetiva transação, não a conseguindo identificar, o que permite privacidade em relação à sua identidade. Contudo, o cenário não é credível para implementação já que não existe privacidade por parte do Banco Central.

C9.2: Bob desconhece Alice e a sua carteira e conhece a transação

Neste caso Bob apenas teria conhecimento da transação efetuada, não conhecendo a Alice nem a sua respetiva carteira. Tal como no caso *C9.1*, o Banco Central não terá interesse em implementar este cenário devido à falta de privacidade em relação às identidades dos utilizadores, bem como às respetivas carteiras.

C9.3: Bob conhece Alice, a sua carteira e a transação

Este é o mais inverosímil dos cenários, pela absoluta transparência em relação aos intervenientes e às suas operações, tornando-o não credível de implementação pelo Banco Central.

3.3 Casos de uso dos cenários

Aqui destacaremos as possíveis utilizações dos cenários anteriormente descritos e as respetivas interações com um ou mais atores. Como alguns casos de uso são coincidentes em vários cenários, eles serão identificados no final deste capítulo, destacando-se apenas os casos de uso diferentes entre si.

C3.1U1: Transferência realizada por Alice (desconhecendo Bob)

É realizada uma transferência entre duas entidades singulares, de Alice para Bob, sendo que que Alice desconhece Bob, mas conhece o identificador da sua conta. Alice necessita de introduzir o identificador e o montante que pretende transferir na *interface*.

C3.1U2: Consulta de uma transação pelo respetivo utilizador

O utilizador (Alice ou Bob) que pretende consultar as informações de uma transação no qual é interveniente, necessita de conhecer o identificador da transação e a chave privada da sua conta e introduzir a informação na *interface*.

C3.1U3: Consulta das transações de uma conta pelo respetivo utilizador

É um caso de uso semelhante ao *C3.1U2* mas, em vez do identificador da transação, é necessário introduzir o identificador da conta do utilizador.

C3.1U4: Levantamento de confidencialidade de uma transação pelo Banco Central

Ao receber uma ordem judicial para consultar as informações de uma dada transação, o Banco Central, com a sua chave privada e o identificador da transação, consegue aceder às informações pretendidas (conta do emissor, conta do destinatário, objeto/serviço de compra, descrição, data e hora).

C3.1U5: Levantamento de confidencialidade das transações de uma conta pelo Banco Central

Este caso de uso é semelhante ao *C3.1U4,* diferenciado apenas no facto de a ordem judicial recebida pelo Banco Central permitir a consulta das informações das transações de uma conta (em vez de uma transação específica).

C3.2U1: Compra numa loja por Alice

Alice realiza um pagamento para Bob, entidade não singular (p.e. loja comercial) através de uma entidade intermediária de segurança (p.e. um prestador de serviços de pagamentos), que teria conhecimento das respetivas contas e, assim, efetuar a transação.

C3.3U1: Transferência realizada por Alice (conhecendo Bob)

É realizada uma transferência de Alice para Bob, sendo ambos entidades singulares que se conhecem, tendo Bob fornecido o identificador da sua conta a Alice. Deste modo, Alice consegue realizar a operação introduzindo na interface o identificador da conta de Bob e o montante que pretende transferir.

C4.1U1: Consulta de uma transação pelo Banco Central

O Banco Central apenas necessita de introduzir na *interface* o identificador da transação que pretende consultar.

C4.1U2: Consulta das transações de uma conta pelo Banco Central

É um caso de uso semelhante ao *C4.1U1*, com a diferença de que o Banco Central necessita de introduzir o identificador da conta, em vez do identificador da transação.

C8

Nos casos de uso relativos ao cenário *C8* a utilização de uma carteira de *hardware* é semelhante ao uso de um cartão pré-pago, sendo apenas necessário um dispositivo de leitura para o efeito.

C8.1U1: Consulta de montante da carteira

A carteira de *hardware* de Alice é lida num dispositivo e revela o valor que esta possui na conta.

C8.1U2: Transferência da Alice

Alice realiza uma transferência com a sua carteira de *hardware*, lida um dispositivo, e posteriormente introduz o identificador da carteira do Bob permitindo, assim, a realização da transferência.

C8.2U1: Pagamento de um serviço ou compra

Alice realiza um pagamento numa loja com a sua carteira de *hardware* lida por um dispositivo que permite a operação.

Conforme aludido no início deste capítulo, alguns casos de uso coincidem em vários cenários, conforme indicado na Tabela VIII. Como se verifica:

- Os cenários *C3.2* e *C3.3* têm casos de uso coincidentes com todos os *C3.1*, à exceção do *C3.1U1*;
- O cenário *C4.1* tem um caso de uso coincidente com o *C3.1U1*;
- O cenário *C4.2* tem casos de uso coincidentes com o *C3.1U2*, *C3.2U1* e todos os *C4.1*;
- O cenário *C4.3* tem casos de uso coincidentes com o *C3.1U2*, *C3.2U1*, *C3.3U1* e todos os *C4.1*;
- O cenário *C8.2* tem um caso de uso coincidente com o *C8.1U1*.

Tabela VIII – Casos de uso coincidentes

Casos de uso		**Cenários**					
		C3.2	***C3.3***	***C4.1***	***C4.2***	***C4.3***	***C8.2***
C3.1	***U1***			coincide			
	U2	coincide	coincide		coincide	coincide	
	U3	coincide	coincide				
	U4	coincide	coincide				
	U5	coincide	coincide				
C3.2	***U1***				coincide	coincide	
C3.3	***U1***				coincide	coincide	
C4.1	***U1***				coincide	coincide	
	U2				coincide	coincide	
C8.1	***U1***						coincide

3.4 Implementação das provas de conceito

Estas provas de conceito têm como objetivo verificar a viabilidade de utilização das características privacidade e confidencialidade nas CBDC. Deste modo, são exemplificados os modelos C4 que as provas de conceito (para os casos de uso credíveis) seguem, juntamente com a explicação do funcionamento da implementação efetuada. Nas demonstrações das provas de conceito é utilizada como unidade de valor ETH por ser usada na *blockchain* Ethereum. A nomenclatura usada é referente à implementação do cenário *i*, ou seja, *Ii*.

I3: Implementação relativa a *C3*

A abordagem da implementação do cenário 3 é sensível a vários aspetos. Não é possível realizar operações criptográficas "*in-chain*" (dependentes da *blockchain*) porque, assumindo que a *blockchain* de consórcio é pública (para quem a gere - uma vez que é preciso verificar e validar os *smart contract*), não é exequível ter chaves de encriptação confidenciais nos *smart contracts*. As operações criptográficas apenas são possíveis se a *blockchain* possuir características que assim o permitam, como s*ecret contracts*, que são um tipo de *smart contract* em que os dados originais são utilizados sem nunca serem revelados (Powers, 2020). Esta situação não abrange a *blockchain* da Ethereum, não sendo possível, de forma segura e confiável, realizar as operações de descodificação e codificação referidas, bem como a utilização de operações com números aleatórios gerados (chave simétrica). Deste modo, caso se utilize uma *blockchain* pública ou de consórcio, como a Ethereum, estes métodos teriam de ser substituídos por interações com uma entidade de confiança fora da *blockchain* ou com a utilização de computação verificada (Thiercelin et al., 2020). Contudo, na implementação realizada, foi seguida uma abordagem com métodos que têm a função de encriptação/desencriptação/geração de números aleatórios, em que o resultado é armazenado de forma legível, o que/como seria encriptado/desencriptado a informação por

uma questão de conveniência. Foi implementado um *smart contract* com vários métodos específicos para ações como encriptação dos dados, transação do montante e desencriptação dos dados.

Neste contexto, a prova de conceito *I3* segue o modelo *C4* em que Alice, Bob e Banco Central têm acesso ao sistema bancário (Figura 22).

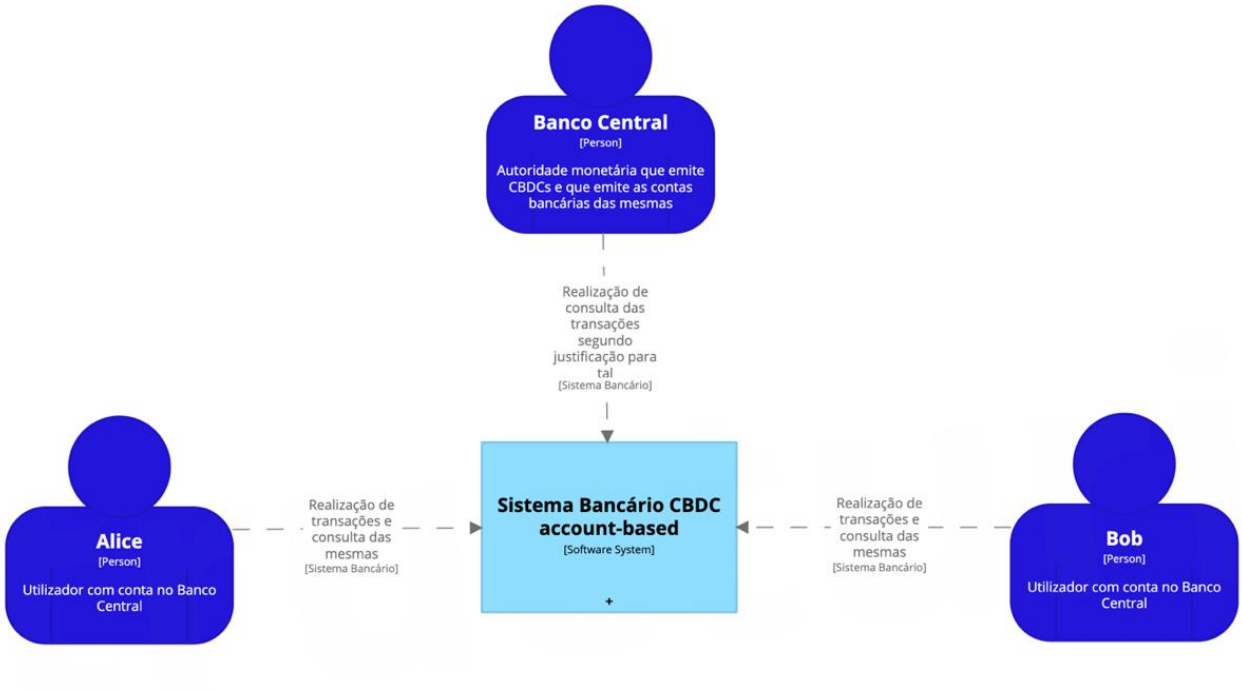


Figura 22 – Modelo C4 de contexto para implementação *I3*.

O sistema bancário, por sua, vez inclui o *Webservice*, que tem acesso ao *smart contract* enunciado no início, permitindo a utilização de métodos do mesmo, bem como ao *Ganache* (simulador de *blockchain* Ethereum), que permite o desenvolvimento de aplicações num ambiente seguro (Truffle Suite, n.d.) e que necessita do *software Metamask* para se conectar (Figura 23).

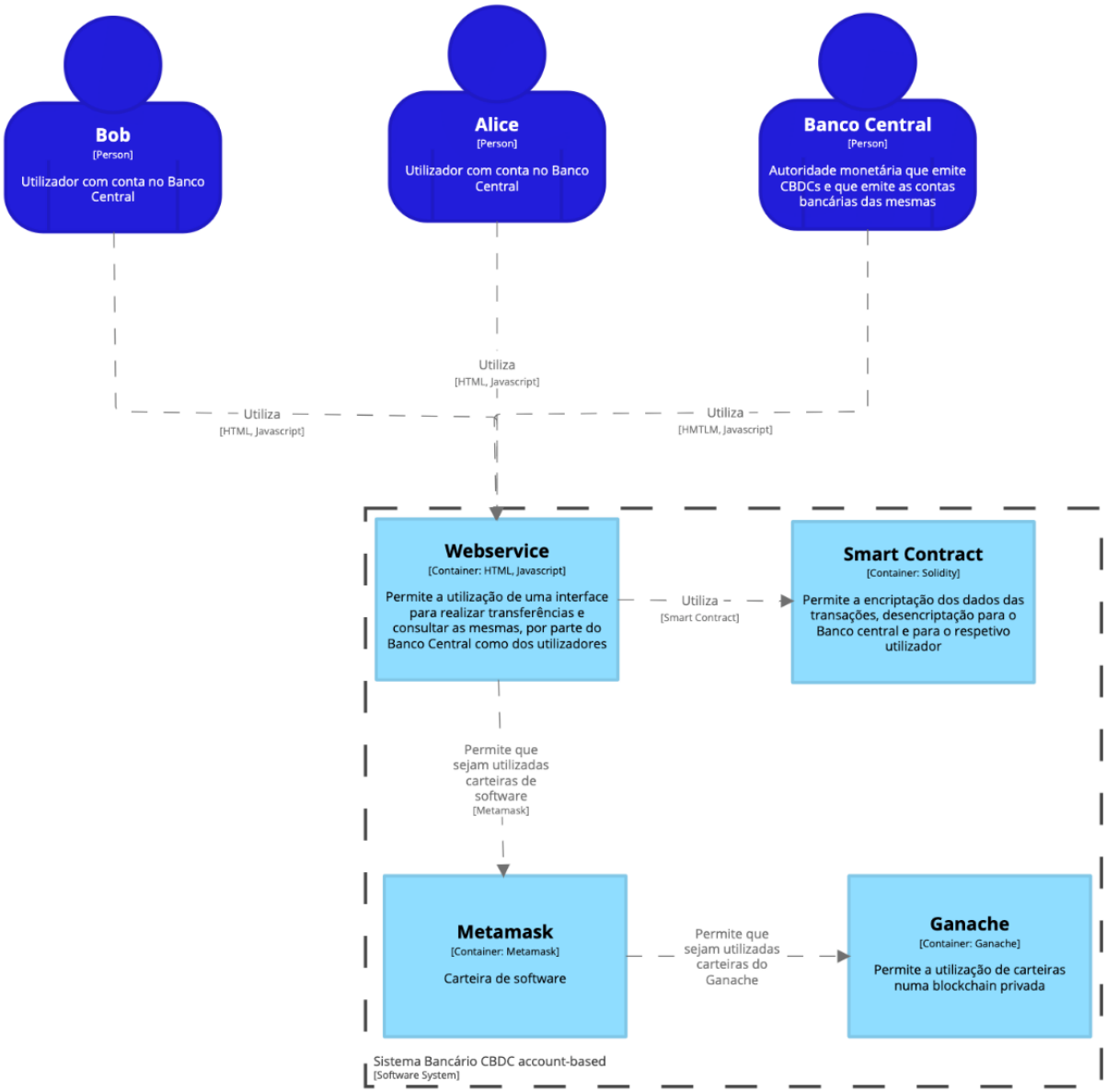


Figura 23 – Modelo C4 de contentores para implementação *I3*.

I3.1: Implementação dos casos de uso *C3.1U1* e *C3.3U1*

Para a realização de transações, é necessário preencher as informações exemplificadas na Figura 24, sendo "endereço de origem" o endereço da conta emissora, "endereço de destino" o endereço da conta recetora e "valor" o montante a ser transacionado entre as duas contas, indispensáveis para a realização da operação.

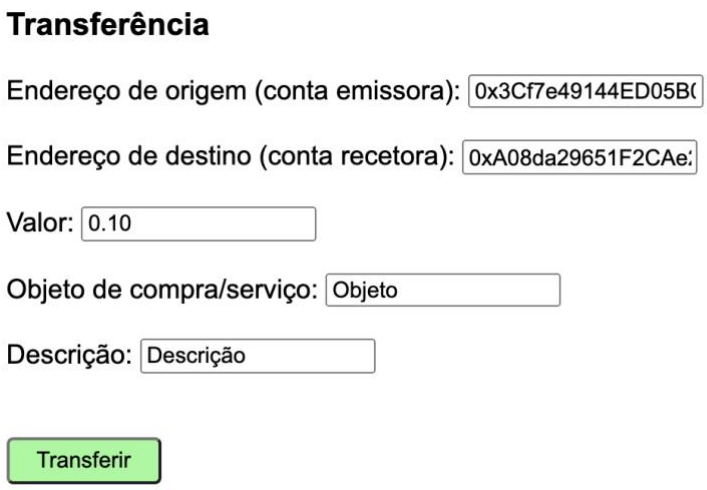
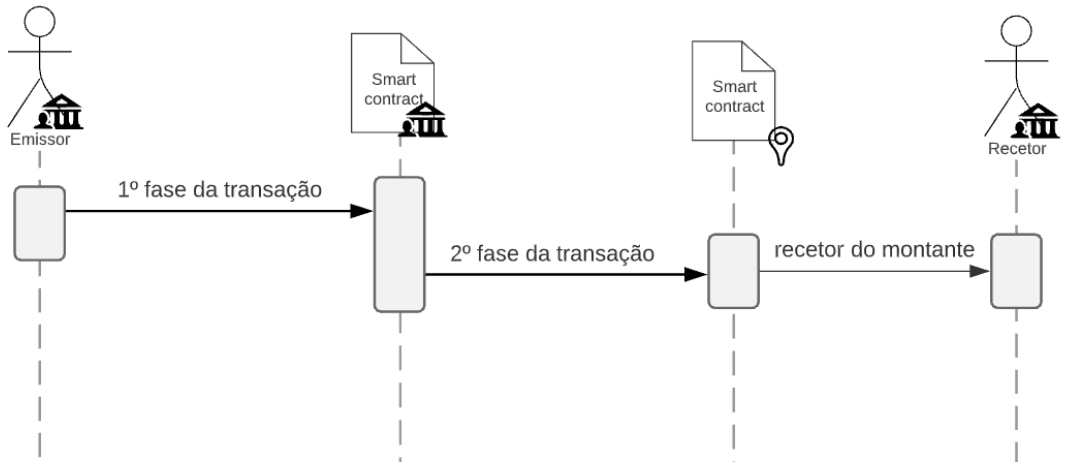


Figura 24 – Exemplificação de inputs para a transação do montante 0,10 ETH.

Para garantir o anonimato, é necessária a realização em duas etapas, conforme ilustrado na Figura 25, que apresenta o diagrama de sequência das transações, sendo utilizado o mesmo *smart contract*.



Legenda:

Conta do utilizador

Endereço da conta do *smart contract*

Endereço do *smart contract*

Figura 25 – Diagrama de sequência da transação e legenda dos ícones.

A primeira fase da transação é realizada no *webservice* (Apêndice B) e consiste na realização da transação conjuntamente com os respetivos detalhes (intervenientes, valor da transação, objeto/serviço de compra, descrição, data, hora), do montante da conta do emissor para a conta do *smart contract*. As informações são encriptadas através de uma chave simétrica (criada pelo *webservice* para cada transação), que encripta os dados enviados juntamente com a transação (Apêndice C). Por sua vez, a chave simétrica é encriptada com a chave pública da conta do validador do Banco Central (*KPvbc*) e também pela chave pública do emissor da transação (*KPut*), ficando registada na *blockchain*.

A encriptação é registada na *blockchain*, segundo a estrutura

enc[Ks](info)#enc[KPvbc](Ks)#enc[KPut](Ks)

em que *enc[Ks](info)* corresponde à encriptação de *info* com *Ks, enc[KPvbc](Ks)* corresponde à encriptação de *Ks* com *KPvbc* e assim respetivamente. Deste modo resulta:

Informação encriptada: enc[Ks(5383152094)](De: 0x3Cf7e49144ED05B0Ee3C9939362F838D6571EE7f

Para: 0xA08da29651F2CAe2dbda2b5C6a6079fFa8B6afCF Objeto/serviço de compra: Objeto Descrição da

compra:Descrição)#enc[KPvbc(976719550)(EndereçoCarteira(0xe0c208a921295e396ea831366f5a77d88308

dfe6)](5383152094)#enc[KPut(7353490771)(EnderecoCarteira(0x3Cf7e49144ED05B0Ee3C9939362F838

D6571EE7f)](5383152094)

Na *blockchain* (Figura 26) fica, então, registada a transação do montante de 0.10 ETH, da conta com endereço

0x3Cf7e49144ED05B0Ee3C9939362F838D6571EE7f

para a conta com o endereço

0xe0c208a921295E396EA831366F5A77d88308DFE6

(endereço da conta no *Ganache* do *smart contract*).

Figura 26 – Primeira fase transação na *blockchain*.

A segunda etapa, ilustrada no Apêndice D, contendo o excerto código do *smart contract*, consiste na transação do montante da conta do *smart contract* para a conta do destinatário final.

De forma análoga à efetuada na etapa anterior, os dados, enviados juntamente com a transação, são encriptados. Porém, em vez da chave simétrica ser encriptada com a chave pública da conta do emissor, é encriptada com a chave pública do recetor, resultando:

encriptacaoKsDados: "enc[Ks(611138867)](De: 0x3Cf7e49144ED05B0Ee3C9939362F838D6571EE7f

Para: 0xA08da29651F2CAe2dbda2b5C6a6079fFa8B6afCF Objeto/serviço de compra: Objeto Descrição da compra: Descrição)"

encriptacaoKsPto:
"enc[KPut(8006248613)(EnderecoCarteira(a08da29651f2cae2dbda2b5c6a6079ffa8b6afcf)](611138867)"

encriptacaoKsPvbc:
"enc[KPvbc(976719550)(EnderecoCarteira(e0c208a921295e396ea831366f5a77d88308dfe6)](611138867)"

Na segunda fase da operação na *blockchain* (Figura 27) é realizada, pelo *smart contract*, a transação para a conta do destinatário final, sendo efetuado o registo do montante de 0.10 ETH, da conta com endereço

0xe0c208a921295E396EA831366F5A77d88308DFE6

(endereço da conta do *smart contract*)

para a conta com o endereço

0x60E58Bdee7D4F0ADbdeAb31933a59a3eFEe906d2

(endereço do *smart contract* referido)

Figura 27 – Segunda fase transação na *blockchain*.

Na *blockchain* é possível confirmar a transação realizada do montante de 0.10 ETH, do endereço

0x3Cf7e49144ED05B0Ee3C9939362F838D6571EE7f

para o endereço

0xA08da29651F2CAe2dbda2b5C6a6079fFa8B6afCF

por sabermos que foram esses os endereços introduzidos na *interface* (Figura 28).

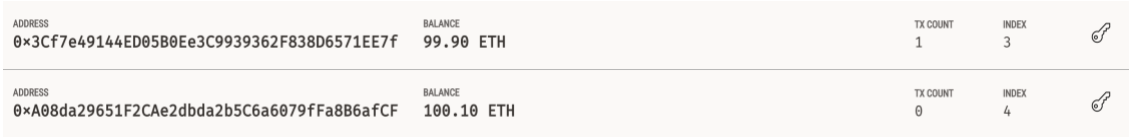


Figura 28 – *Output* da identificação da transação.

A realização sequencial das etapas anteriores permite, assim, assegurar a anonimidade, dado não ser possível consultar na *blockchain* o registo das informações da transação (conta do emissor, conta do destinatário, objeto/serviço de compra, descrição, data e hora), à exceção do montante das transações realizadas.

I3.2: Implementação dos casos de uso *C3.1U4* e *C3.3U5*

No que respeita ao acesso às informações das transações pelo Banco Central, é um procedimento realizado em duas fases, conforme ilustrado na Figura 29, que apresenta o diagrama de sequência para o levantamento de confidencialidade.

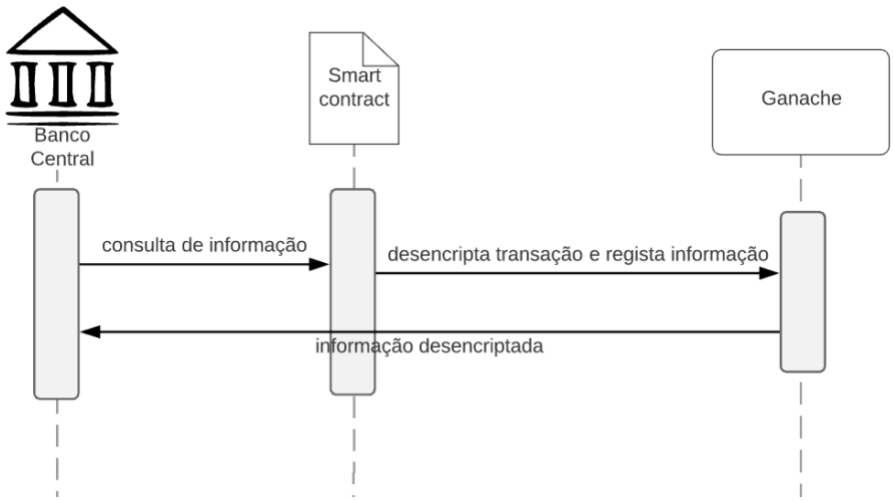


Figura 29 – Diagrama de sequência da consulta de informação pelo Banco Central.

A primeira fase consiste na desencriptação da transação e respetivo registo do levantamento da confidencialidade pelo Banco Central na *blockchain*, de acordo com a seguinte sequência: (i) a(s) transação(ões) são desencriptadas com a chave privada do validador do Banco Central; (ii) obtém-se a chave simétrica que encripta as informações da transação; (iii) a chave simétrica é encriptada com a chave pública do Banco Central, juntamente com a identificação da transação que se pretende aceder resultando

enc[KPbc(9732082143)](Ks(5383152094),_idTX(0x47bb6a91bb7c538dec4f7fe104c9f77efeb0fbd40448fbec9fb7622bae985197))

para que apenas o Banco Central possa ter acesso à consulta das informações; (iv) é feito o registo da fase (iii) descrito anteriormente na *blockchain* (Figura 30).

Figura 30 – Registo da transação encriptada com a chave pública do Banco Central na *blockchain*.

No Apêndice E é mostrado o código implementado no *smart contrat* para a desencriptação do registo da transação e encriptação com a chave pública do Banco Central.

A segunda fase consiste na desencriptação das informações da transação pelo Banco Central. Para tal, a chave privada (do Banco Central) permite obter a chave simétrica, desencriptando o que foi registado anteriormente na *blockchain* e, deste modo, desencriptar a(s)

transação(ões) original(ais) e aceder às respetivas informações. Na Figura 31 é exemplificado o acesso à informação apenas de uma transação, enquanto na Figura 32 é exemplificado o acesso a todas as transações de uma conta.

Figura 31 – *Output* com a informação de uma dada transação.

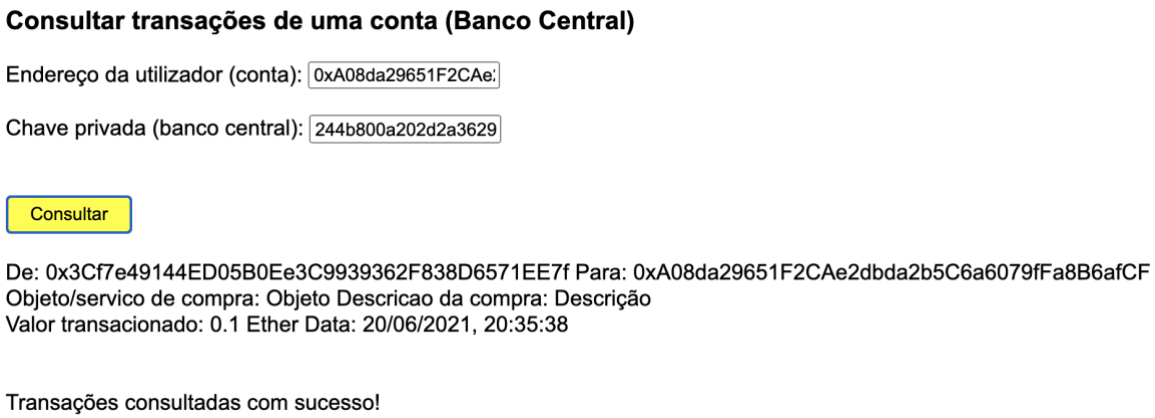


Figura 32 – *Outputs* com a informação das transações de uma conta.

Com estas duas etapas é garantida a confidencialidade das transações, face ao Banco Central, porque este somente pode consultar as informações se a transação for desencriptada unicamente pelo validador do Banco Central. Nesta situação é registado na *blockchain* que foi levantada a confidencialidade, como já explicado. Caso estas não sejam desencriptadas com a chave privada do validador do Banco Central, este não consegue aceder às informações das transações.

I3.3: Implementação dos casos de uso *C3.1U2* e *C3.3U3*

Por fim, abordamos a consulta dos movimentos da conta por parte dos utilizadores (Figura 33).

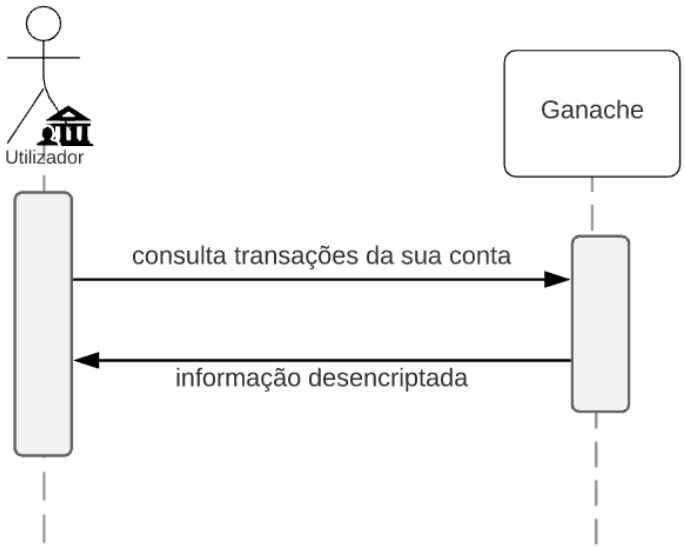


Figura 33 – Diagrama de sequência de consulta de informação pelo utilizador.

Como não existe aqui o problema de levantamento de confidencialidade, o utilizador (quer seja emissor ou recetor das transações) pode efetuar a consulta das suas transações. Para tal, são apenas necessários o seu endereço de conta e a chave privada (Figura 34) para que os dados

enc[KPut(8006248613)(EnderecoCarteira(a08da29651f2cae2dbda2b5c6a6079ffa8b6afcf)](611138867) com kput (4ff1f1d39588b26a06c710214c16c5d372891546147423a2dcecd40cb4f4d39a)

sejam desencriptados com a mesma, obtendo a chave simétrica da transação que é utilizada para a desencriptação da informação. Adicionalmente, é ainda possível especificar uma determinada transação (Figura 35).

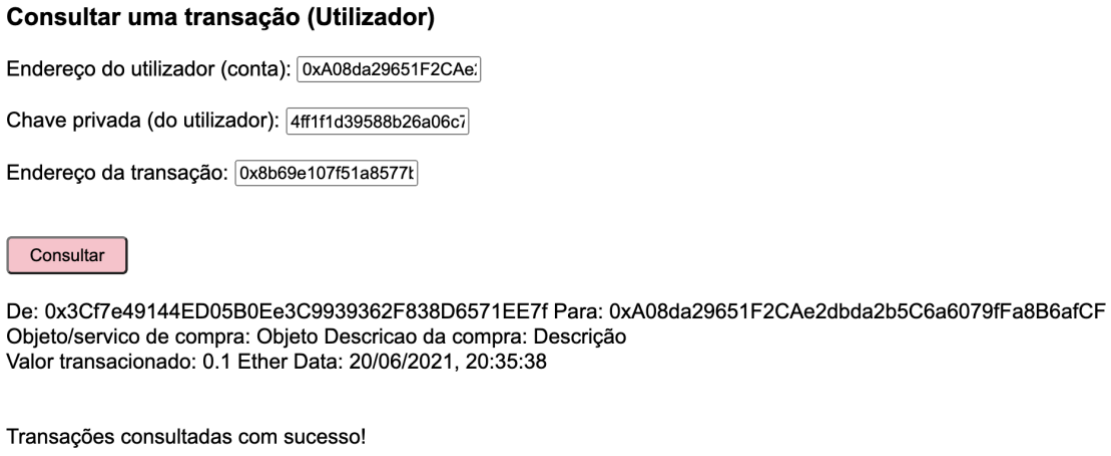


Figura 34 – Exemplificação dos *inputs* para a consulta de determinada transação.

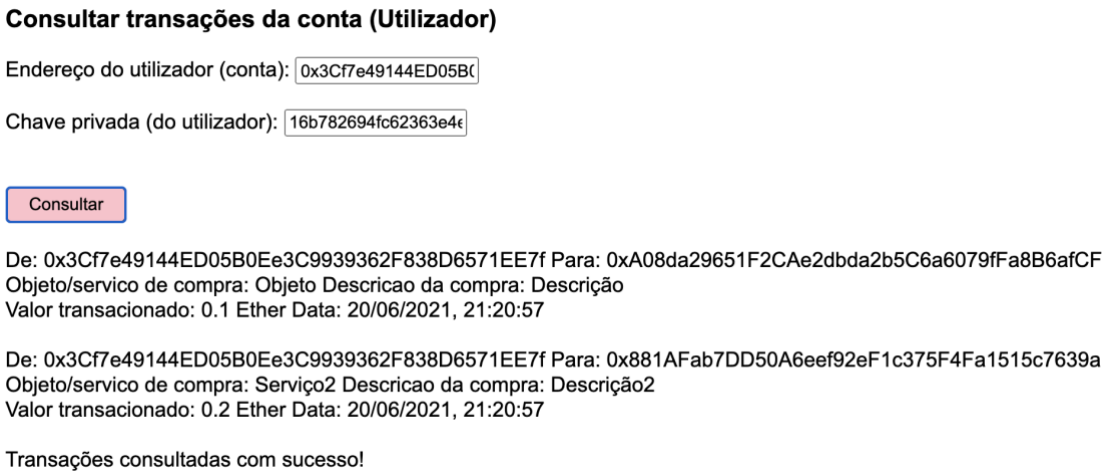


Figura 35 – Exemplificação dos *inputs* para a consulta de todas as transações de uma conta.

Resumidamente, foram implementados no *smart contract* dois métodos:

1. Registo da transação encriptada na *blockchain*;
2. Desencriptação da transação, a pedido do Banco Central, e registo na *blockchain* da transação encriptada com a chave pública do Banco Central;

I8: Implementação relativa a *C8*

Esta prova de conceito segue o modelo C4 de contexto em que os utilizadores usam o sistema CBDC *token-based* para acesso às respetivas carteiras (Figura 36).

Figura 36 – Modelo C4 de contexto para implementação *I8*.

Por sua vez, o sistema CBDC *token-based* inclui o *Webservice*, que apenas tem acesso ao Ganache, utilizando o *software Metamask* para se conectar (Figura 37).

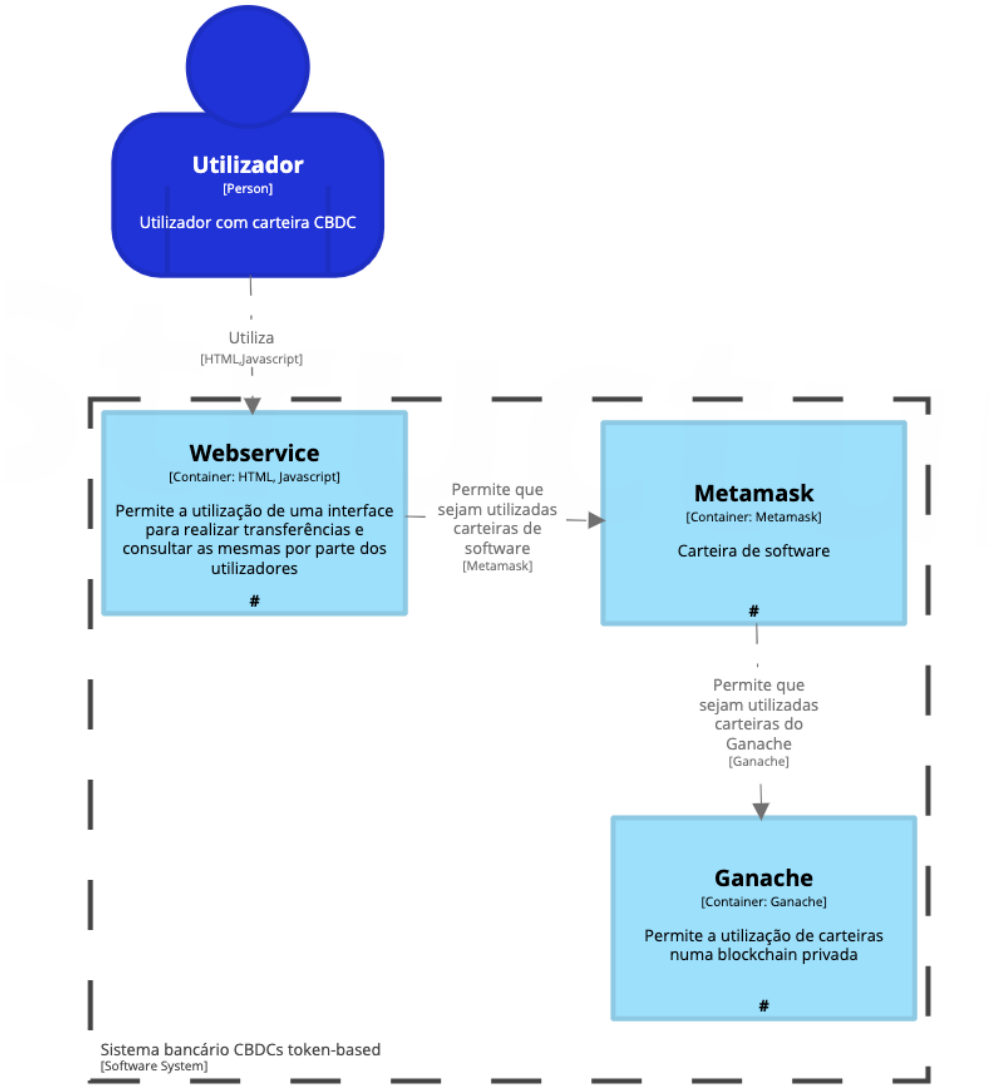


Figura 37 – Modelo C4 de contentores para implementação *I8*.

Para este cenário ser totalmente cumprido seria necessário a utilização de carteiras de *hardware* sem ligação à *blockchain*, uma vez que, apenas deste modo, as transações seriam realizadas sem o respetivo registo. A prova de conceito segue o modelo em que o utilizador apenas acede e realiza as transações sem precisar de aceder ao sistema bancário de CBDC, não sendo necessário registar o acesso na *blockchain*, nem a utilização do *smart contract*.

I8.1: Implementação do caso de uso *C8.1U1*

Neste cenário os utilizadores podem consultar o montante nas suas carteiras introduzindo o identificador da sua carteira na *interface* (Figura 38). O *webservice* apenas consulta o montante da carteira com o respetivo identificador.

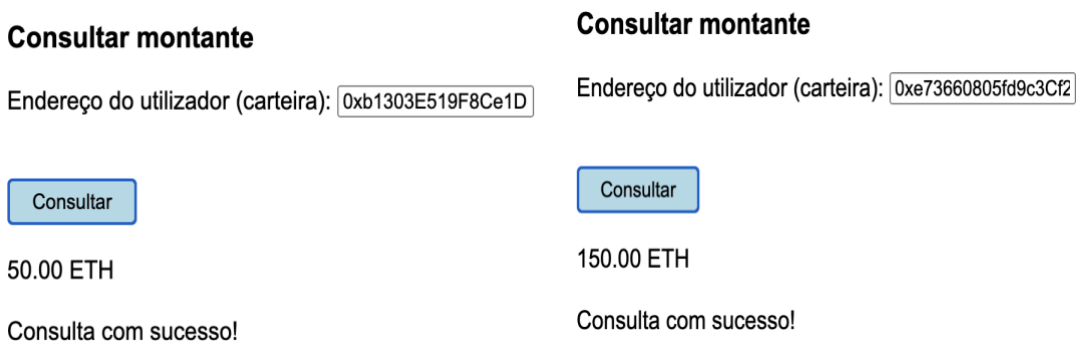


Figura 38 – Consulta de montante da carteira.

I8.2: Implementação do caso de uso *C8.1U2*

É possível a realização das transações entre as carteiras (que simula o pagamento de serviço/compras e as transferências), até a um limite máximo (neste caso 150 ETH), disponível em conta, sem que nada fique registado (Figura 39). Para tal, o *webservice* acede ao montante de ambas as contas, de forma a perceber se: (i) a carteira emissora da transação possui o valor que pretende transacionar; (ii) a carteira recetora, ao receber o montante, não excede o montante máximo permitido nas carteiras.

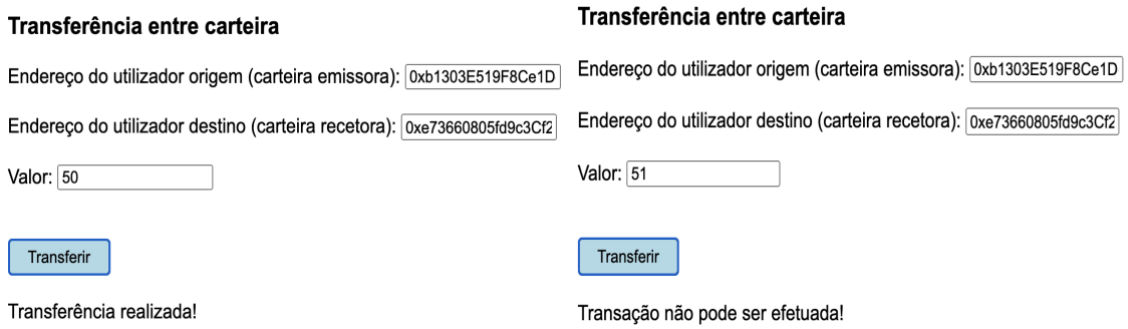


Figura 39 – Transação/tentativa de transação entre carteiras.

3.5 Sumário

Neste capítulo apresentaram-se todos os cenários e respetivos casos de uso e implementações das provas de conceito, que permitem verificar a viabilidade das CBDCs possuírem confidencialidade e, ao mesmo tempo, o cumprimento das normas KYC/AML (nos cenários *account-based*), uma vez que o levantamento da confidencialidade possibilita ao Banco Central consultar as informações das transações. Por outro lado, os cenários *token-based* permitem a privacidade e confidencialidade aos utilizadores, contudo é necessário que as carteiras possuam um montante máximo permitido, com o intuito de dificultar a eventual ocorrência de fraudes.

Capítulo 4
Considerações finais

Neste capítulo apresentamos as reflexões finais relativas ao trabalho, bem como as dificuldades encontradas e propostas para trabalho futuro.

4.1 Conclusões

O atual panorama das criptomoedas, desde algum tempo em forte ascensão, catalisou o interesse dos bancos centrais pelas CBDC. Contudo, a sua implementação deverá conciliar interesses dos utilizadores, similares ao manuseamento da moeda fiduciária, como a privacidade e a confidencialidade, com processos regulamentares e de conformidade, como as normas KYC/AML, para evitar situações de fraude. O objetivo principal deste trabalho consistiu, justamente, na implementação de provas de conceito com o objetivo de verificar se a privacidade e a confidencialidade são características exequíveis para as CBDC.

Para o efeito, foi necessário realizar previamente um estudo comparativo sobre a criptomoeda Bitcoin e respetiva tecnologia inerente (*blockchain*), sobre as CBDC DCEP, Digital Euro e E-krona e a *stablecoin* Diem, para compreender os seus funcionamentos e respetivos desenvolvimentos. Esta análise permitiu elaborar os possíveis cenários *token-based* e *account-based* que as CBDC poderiam adotar, quanto à privacidade e confidencialidade, tendo sido identificados e caracterizados os cenários credíveis para implementação como modo de exemplificação de utilização em cada modelo, ou seja, os casos de uso. Finalmente, foram implementadas as provas de conceito para os cenários credíveis, que exigiu um período de aprendizagem da linguagem *Solidity*, utilizada nos *smart contract* Ethereum, bem como a configuração do ambiente, que requereu pesquisa sobre como se poderia utilizar carteiras de teste com a *blockchain* Ethereum. A utilização de métodos criptográficos resultou numa dificuldade adicional, pelo facto do protocolo *Nightfall* ainda se encontrar em fase de desenvolvimento não podendo ser utilizado nas provas de conceito.

Como a privacidade e confidencialidade são requisitos não funcionais não foi possível a sua validação com recurso a testes. Assim, foi unicamente descrito e demonstrado o funcionamento das provas de conceito (implementação e arquitetura) para comprovar que os requisitos são atingidos.

4.2 Trabalho futuro

Embora as provas de conceito implementadas permitam verificar a viabilidade de utilização da privacidade e confidencialidade nas CBDC, seria benéfico a implementação:

- Das provas de conceito relativas aos cenários *account-based* com métodos criptográficos e com a utilização de *secret contracts*, para permitir a utilização de parâmetros confidenciais;

- Da prova de conceito *I8:* Implementação relativa a C8, relativa ao cenário *token-based*, com carteiras de *hardware* e com a utilização de uma entidade terceira nos sub-cenários em que tal é necessário, para compreender melhor como a privacidade e a confidencialidade poderiam ser alcançadas.

Referências

Aarvik, P. (2020). *Blockchain as an anti-corruption tool*. U4. https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption. Consultado em November 26, 2020

Abraham, L., & Guegan, D. (2019). The Other Side of the Coin: Risks of the Libra Blockchain. In *SSRN Electronic Journal*. arXiv. https://doi.org/10.2139/ssrn.3474237. Consultado em November 11, 2020

Alharby, M., & Van Moorsel, A. (2017). BLOCKCHAIN-BASED SMART CONTRACTS : A SYSTEMATIC MAPPING STUDY. In D. Nagamalai & et al. (Eds.), *3rd International Conference on Artificial Intelligence and Soft Computing* (pp. 125–140). Fatemeh soltani. https://doi.org/10.5121/csit.2017.71011

Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K., & Zhang, F. (2020a). Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. *National Bureau of Economic Research*. https://doi.org/10.3386/w27634. Consultado em December 19, 2020

Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K., & Zhang, F. (2020b). *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations*. https://doi.org/10.3386/w27634. Consultado em March 12, 2021

Arslanian, H. (2020, September 13). *CBDCs: What you need to know!* https://www.youtube.com/watch?v=6wPWQDFZF_c&ab_channel=HenriArslanian. Consultado em March 12, 2021

Auer, R., Cornelli, G., & Frost, J. (2020a). *Covid-19, cash, and the future of payments*. https://www.bis.org/publ/bisbull03.htm. Consultado em December 18, 2020

Auer, R., Cornelli, G., & Frost, J. (2020b). Rise of the central bank digital currencies: drivers, approaches and technologies. In *BIS Working Papers*. https://www.bis.org/publ/work880.pdf. Consultado em October 14, 2020

Banco de Portugal. (n.d.-a). *COVID-19. Pagar com notas e moedas é seguro*. https://www.bportugal.pt/page/covid-19-pagar-com-notas-e-moedas-e-seguro. Consultado em December 19, 2020

Banco de Portugal. (n.d.-b). *Eurosistema/SEBC*. Banco de Portugal. https://www.bportugal.pt/page/eurosistemasebc. Consultado em October 23, 2020

Barontini, C., & Holden, H. (2019). *Proceeding with caution - a survey on central bank digital currency*. https://www.bis.org/publ/bppdf/bispap101.htm. Consultado em December 29, 2020

Bharathan, V. (2020, October 7). *Digital Euro: A Report By The European Central Bank*. Forbes. https://www.forbes.com/sites/vipinbharathan/2020/10/07/digital-euro-a-report-by-the-european-central-bank/?sh=6162351c1860. Consultado em October 23, 2020

Bigmore, R. (2018, May 25). *A decade of cryptocurrency: from bitcoin to mining chips*. The Telegraph. https://www.telegraph.co.uk/technology/digital-money/the-history-of-cryptocurrency/. Consultado em December 19, 2020

Binance Academy. (n.d.). *Turing Complete*. https://academy.binance.com/en/glossary/turing-complete. Consultado em December 28, 2020

Bis Central bankers. (2019). *Should the Bank of Japan Issue a Digital Currency? Speech at a Reuters Newsmaker Event in Tokyo*. https://www.bis.org/review/r190712h.pdf. Consultado em December 26, 2020

Bit2Me Academy. (n.d.). *¿Quién es Nick Szabo?* https://academy.bit2me.com/quien-es-nick-szabo/. Consultado em December 29, 2020

Blocks99. (n.d.). *Crypto and the privacy-transparency tradeoff*. Blocks99. https://blocks99.com/features/crypto-and-the-privacy-transparency-tradeoff/. Consultado em December 19, 2020

Bloomberg. (2020, September 8). *How China Is Closing In on Its Own Digital Currency*. Bloomberg. https://www.bloomberg.com/news/articles/2020-09-08/how-china-is-closing-in-on-its-own-digital-currency-quicktake. Consultado em December 19, 2020

Bofinger, P., & Haas, T. (2020). *CBDC: A systemic perspective*. https://www.wiwi.uni-wuerzburg.de/fileadmin/wifak/Downloadpool/WEP/wep101.pdf. Consultado em March 12, 2021

Brühl, V. (2020). Libra — A Differentiated View on Facebook's Virtual Currency Project. *Intereconomics*, *55*(1), 54–61. https://doi.org/10.1007/s10272-020-0869-1. Consultado em October 20, 2020

Campos, M. (2020, April 15). *4 tentativas que falharam ao tentar criar o Bitcoin*. https://blocktrends.com.br/4-tentativas-que-falharam-ao-tentar-criar-o-bitcoin/. Consultado em December 29, 2020

Catalini, C., Gratry, O., Hou, J. M., Parasuraman, S., & Wernerfelt, N. (n.d.). *The Libra Reserve*. MIT Sloan. https://mitsloan.mit.edu/shared/ods/documents/?PublicationDocumentID=5860. Consultado em December 3, 2020

Chainalysis. (n.d.). *Chainalysis*. https://www.chainalysis.com/. Consultado em November 30, 2020

Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), *Advances in Cryptology* (pp. 199–203). Springer US. https://doi.org/10.1007/978-1-4757-0602-4. Consultado em December 28, 2020

Cheng, J., Lawson, A. N., & Wong, P. (2021). Preconditions for a general-purpose central bank digital currency. *FEDS Notes*, *2021*(2839). https://doi.org/10.17016/2380-7172.2839. Consultado em March 12, 2021

Ciaian, P. (2018). *Blockchain technology and market transparency*. Comissão Europeia. https://ec.europa.eu/info/sites/info/files/law/consultation/mt-workshop-blockchain-technology-and-mt_ciaian_en.pdf. Consultado em December 19, 2020

CipherTrace. (n.d.). *CipherTrace*. https://ciphertrace.com/. Consultado em November 30, 2020

Clifford Chance. (2020). *Central bank digital currencies and stablecoins*. https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-. Consultado em March 13, 2021

CoinLore. (n.d.). *CoinLore*. https://www.coinlore.com/. Consultado em December 28, 2020

CoinMarketCap. (n.d.). *CoinMarketCap*. https://coinmarketcap.com/. Consultado em December 28, 2020

Corda. (n.d.). *Corda*. Corda. https://www.corda.net/. Consultado em December 3, 2020

Diário da República. (1992, December 31). *Decreto-Lei n.º 298/92 - Regime Geral das Instituições de Crédito e Sociedades Financeiras*. https://dre.pt/web/guest/legislacao-consolidada/-/lc/117639376/201901181117/73650113/diploma/indice?p_p_state=maximized. Consultado

em March 25, 2021

Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In B. E.F. (Ed.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 740 LNCS* (pp. 139–147). Springer Verlag. https://doi.org/10.1007/3-540-48071-4_10. Consultado em December 28, 2020

European Central Bank. (2020, October). *Report on a digital euro*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf. Consultado em November 10, 2020

European Commission. (2020, September 24). *Questions and Answers: Digital Finance Strategy, legislative proposals on crypto-assets and digital operational resilience, Retail Payments Strategy*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1685. Consultado em December 28, 2020

Godinho, P., Rupino, P., Sebastião, H., Melo, P., & Sequeira, T. (2020). *DesCripto (comunicação particular)*.

Gopie, N. (2018, July 2). *What are smart contracts on blockchain?* https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/. Consultado em December 28, 2020

Graphsense. (n.d.). *Graphsense*. https://graphsense.info/. Consultado em November 30, 2020

Han, X., Yuan, Y., & Wang, F. Y. (2019). A Blockchain-based Framework for Central Bank Digital Currency. *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 263–268. https://doi.org/10.1109/SOLI48380.2019.8955032

Hayes Adam. (2020, December 17). *What Happens to Bitcoin After All 21 Million Are Mined?* Investopedia. https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/. Consultado em December 28, 2020

Hazari, S. S., & Mahmoud, Q. H. (2019). A parallel proof of work to improve transaction speed and scalability in blockchain systems. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 916–921. https://doi.org/10.1109/CCWC.2019.8666535. Consultado em December 13, 2020

Hedqvist, D. (2018, October 31). *This is the Swedish e-krona*. Bitcoin.Se. https://en.bitcoin.se/articles/this-is-the-swedish-e-krona. Consultado em December 19, 2020

Kritikos, M. (2018). *What if blockchain offered a way to reconcile privacy with transparency?* http://www.europarl.europa.eu/thinktank. Consultado em December 28, 2020

Li, X., & Whinston, A. B. (2020). Analyzing Cryptocurrencies. *Information Systems Frontiers*, *22*(1), 17–22. https://doi.org/10.1007/s10796-019-09966-2. Consultado em October 16, 2020

Libra Association Members. (2020, April). *White Paper v2.0*. Diem. https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf. Consultado em November 20, 2020

Lieure, A. (2018, May). *Herd behaviour and information uncertainty: insights from the cryptocurrency market*. https://www.researchgate.net/publication/330513654_HERD_BEHAVIOUR_AND_INFORMATION_UNCERTAINTY_INSIGHTS_FROM_THE_CRYPTOCURRENCY_MARKET. Consultado em January 2, 2021

Mechkaroska, D., Dimitrova, V., & Popovska-Mitrovikj, A. (2018). Analysis of the Possibilities for Improvement of BlockChain Technology. In D. Mechkaroska, V. Dimitrova, & A. Popovska-Mitrovikj (Eds.), *2018 26th Telecommunications Forum, TELFOR 2018 - Proceedings*. IEEE.

https://doi.org/10.1109/TELFOR.2018.8612034. Consultado em December 17, 2020

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.Org. www.bitcoin.org. Consultado em October 11, 2020

Nelson, D. (2020, February 21). *Sweden's Central Bank Finally Embraces DLT, but Only in Simulation Mode*. Coindesk. https://www.coindesk.com/swedens-central-bank-finally-embraces-dlt-but-only-in-simulation-mode. Consultado em October 27, 2020

Patrick. (2017, October 5). *Not seeing your transaction? Here's how to find your payment status....* Athena Bitcoin. https://www.athenabitcoin.com/news/2017/10/5/find-your-payment-status. Consultado em December 28, 2020

Perianne, B., Kaufman, M., & Law, R. (n.d.). *Blockchain: The Breakthrough Technology of the Decade and How China Is Leading the Way-An Industry White Paper*. Chamber of Digital Commerce. https://digitalchamber.s3.amazonaws.com/Blockchain-The-Breakthrough-Technology-of-the-Decade-and-How-china-is-Leading-the-Way.pdf. Consultado em November 10, 2020

Powers, B. (2020, September 2). *Secret Smart Contracts Move a Step Closer to Going Live*. https://www.coindesk.com/secret-network-privacy-smart-contracts-launch-date. Consultado em June 11, 2021

R3. (n.d.). *Blockchain/DLT 101* . https://www.r3.com/blockchain-101/. Consultado em December 28, 2020

Rankhambe, B. P., & Khanuja, H. K. (2019). A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum. *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 1–7. https://doi.org/10.1109/ICCUBEA47591.2019.9129332. Consultado em November 23, 2020

Rocha, L. (2018a, June 9). *eCash: como a criação de David Chaum deu início ao sonho cypherpunk*. https://www.criptofacil.com/ecash-como-a-criacao-de-david-chaum-deu-inicio-ao-sonho-cypherpunk/. Consultado em December 29, 2020

Rocha, L. (2018b, June 21). *Hashcash: como Adam Back projetou o motor do Bitcoin*. https://www.criptofacil.com/hashcash-como-adam-back-projetou-o-motor-do-bitcoin/. Consultado em December 29, 2020

Rolfe, A. (2020, February 26). *The Riksbank in Sweden launches e-krona pilot*. Payments Cards & Mobile. https://www.paymentscardsandmobile.com/the-riksbank-in-sweden-launches-e-krona-pilot/. Consultado em October 20, 2020

Samarakoon, G. (2019, January 26). *Public, Private and Consortium blockchains: What's the best flavour?* Medium. https://medium.com/blockchain-strategy-and-use-cases/public-private-and-consortium-blockchains-whats-the-best-flavour-7728834a4b1c. Consultado em December 19, 2020

Samourai Wallet. (n.d.). *OXT*. https://oxt.me/. Consultado em November 30, 2020

Satoshi Nakamoto Institute. (n.d.). *Bit Gold*. https://nakamotoinstitute.org/bit-gold/. Consultado em December 29, 2020

Sebastião, H., Cunha, P. R., & Godinho, P. (2020). *Cryptocurrencies and Blockchain . Overview and future perspectives*.

Shi, Y., & Zhou, S. (2020). *Central Bank Digital Currencies: Towards a Chinese Approach-Design Choices of Digital Currency Electronic Payment* [Jönköping University International Business School]. http://www.diva-portal.org/smash/get/diva2:1433870/FULLTEXT01.pdf. Consultado em October 20, 2020

Sun, H., Mao, H., Bai, X., Chen, Z., Hu, K., & Yu, W. (2017). Multi-blockchain model for central bank digital currency. *18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, *2017-Decem*, 360–367. https://doi.org/10.1109/PDCAT.2017.00066

Sveriges Riksbank. (2018, October). *The Riksbank's e-krona project*. Sveriges Riksbank. https://www.riksbank.se/globalassets/media/rapporter/e-krona/2018/the-riksbanks-e-krona-project-report-2.pdf. Consultado em November 21, 2020

Sveriges Riksbank. (2020, February 20). *Technical solution for the e-krona pilot*. Sveriges Riksbank. https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/. Consultado em November 21, 2020

The Digital Dollar Project. (2020). https://www.banking.senate.gov/imo/media/doc/Giancarlo Testimony Addendum 6-30-202.pdf. Consultado em March 12, 2021

Thiercelin, M., Cheng, C.-M., Miyaji, A., & Vaudenay, S. (2020). Smart contract with secret parameters. In *Symposium on Cryptography and Information Security 2020 (IRIS/SCIS)*. https://infoscience.epfl.ch/record/277810. Consultado em April 21, 2021

Tomov, Y. K. (2019, September 1). Bitcoin: Evolution of blockchain technology. *2019 28th International Scientific Conference Electronics, ET 2019 - Proceedings*. https://doi.org/10.1109/ET.2019.8878322

Tran, H., & Matthews, B. C. (2020, August 24). *China's Digital Currency Electronic Payment Project reveals the good and the bad of central bank digital currencies*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-digital-currency-electronic-payment-project-reveals-the-good-and-the-bad-of-central-bank-digital-currencies/. Consultado em December 19, 2020

Truffle Suite. (n.d.). *Ganache*. https://www.trufflesuite.com/ganache. Consultado em May 27, 2021

Vujičić, D., Jagodić, D., & Randić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *2018 17th International Symposium on INFOTEH-JAHORINA, INFOTEH 2018 - Proceedings*, *2018-January*, 1–6. https://doi.org/10.1109/INFOTEH.2018.8345547

Wang, A. (2020, August 19). *DCEP, Libra, Bitcoin and Cash compared*. Boxmining. https://boxmining.com/dcep-libra-bitcoin-cash/. Consultado em December 19, 2020

Werner, R., Lawrenz, S., & Rausch, A. (2020). Blockchain Analysis Tool of a Cryptocurrency. *ICBCT'20: Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, 80–84. https://doi.org/10.1145/3390566.3391671. Consultado em December 23, 2020

Xu, J., & Prud'homme, D. (2020). China's Digital Currency Revolution and Implications for International Business Strategy. *SSRN*. https://doi.org/10.2139/ssrn.3672240. Consultado em December 19, 2020

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018, October). *Blockchain Technology Overview*. NIST. https://doi.org/10.6028/NIST.IR.8202. Consultado em October 11, 2020

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018a). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647. Consultado em December 23, 2020

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018b). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647. Consultado em December 28, 2020

Apêndices

Apêndice A – Revisão sistemática de literatura

Neste apêndice apresenta-se os artigos (título e assunto) analisados, que sustentaram a revisão sistemática da literatura apresentada no Capítulo 2.

Os artigos encontram-se estruturados por expressão de pesquisa e base de dados.

Tabela IX – Artigos analisados e categorizados derivados da revisão sistemática de literatura

CBDC OR "Central Bank Digital Currency"

IEEEXplorer

Título	Tema
A Blockchain-based Framework for Central Bank Digital Currency	Requisitos de segurança do CBDC
Multi-Blockchain Model for Central Bank Digital Currency	Modelo MBDC baseado na tecnologia de *blockchain* de permissão
Blockchain Application for Central Banks: A Systematic Mapping Study	Casos de uso de Banco Central para adaptação de *blockchain*
A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures	CBDC baseadas em DLT com protótipos de prova de conceito

ACMDL

Título	Tema
Demystifying Stablecoins: Cryptography meets monetary policy	CBDC e obstáculos
Demystifying stablecoins	Funcionamento de *stablecoins*
Toward Emancipatory Currencies: A Critique of Facebook's Libra Cryptocurrency and Ideas for Alternatives	Cenários possíveis para a Libra e design de moedas digitais

"Bitcoin" AND Cryptocurrency AND blockchain

IEEEXplorer

Título	Tema
Comparative Analysis of Bitcoin, Ethereum, and Libra	Revisão e discussão da tecnologia *blockchain* analisando comparativa de Libra, Bitcoin e Ethereum
Bitcoin and Blockchain: Security and Privacy	Segurança e privacidade
A Comparative Analysis of Blockchain Platforms – Bitcoin and Ethereum	Visão geral de ambas as plataformas de tecnologia Bitcoin e Ethereum
A Refined Analysis of Zcash Anonymity	Análise do anonimato de Zcash
A Survey on Various Attacks in Bitcoin and Cryptocurrency	Funcionamento da *blockchain*
Comprehensive Overview of Selfish Mining and Double Spending Attack Countermeasures	Funcionamento da *blockchain* e analise de estudos
Consensus Algorithms in Blockchain Technology: A Survey	Algoritmos de consenso
Privacy-Preserving Solutions for Blockchain: Review and Challenges	Características da blockchain e preservação da privacidade
A Survey on Bitcoin Cryptocurrency and its Mining	Funcionamento da *blockchain*
Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities	Comparação algoritmos de consenso
Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing	Comparação algoritmos de consenso para os dois tipos de *blockchain*
Blockchain -the Technology of Crypto Currencies	Funcionamento *blockchain*
Blockchain and Cryptocurrencies: Model, Techniques, and Applications	Funcionamento da blockchain
A Survey on Security and Privacy Issues of Bitcoin	Bitcoin e tecnologias subjacentes
Blockchain technology, bitcoin, and Ethereum: A brief overview	Panorama da *blockchain* e *smart contracts*
Blockchain: Challenges and applications	Utilização de *blockchain* e desafios
A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems	Anonimidade e privacidade na Bitcoin
Blockchain: The perfect data protection tool	Privacidade na *blockchain*
Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies	Bitcoin e tecnologias subjacentes
Blockchain Technology and Cryptocurrenices	Bitcoin e funcionamento *blockchain*

Continua

Continuação da tabela anterior

Efficient approach towards bitcoin security algorithm	Bitcoin e vulnerabilidades
Bitcoin's Consistency Property	Propriedades Bitcoin
An Analysis of Blockchain-based Bitcoin Mining Difficulty: Techniques and Principles	Funcionamento *blockchain* e mineração da Bitcoin
A Survey of Distributed Consensus Protocols for Blockchain Networks	Comparação algoritmos de consenso
Solutions to Scalability of Blockchain: A Survey	Escalabilidade da *blockchain*
Blockchain Simulation and Development platforms: Survey, Issues and Challenges	Plataformas de simulação de *blockchain*
Blockchain: from Invention to Transformation	Funcionamento blockchain
Comparative study of permissioned blockchain solutions for enterprises	Comparação de *blockchains* permissionadas
Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis	Criptomoedas identificação e rastreio
On BlockChain Technology: Overview of Bitcoin and Future Insights	Bitcoin e funcionamento blockchain
A critical review of blockchain and its current applications	Análise *blockchain*
A Critical Review of Blockchain Consensus Model	Características de algoritmos de consenso
Potential of Blockchain Technology in Digital Currency: A Review	Análise tecnologia *blockchain*

ACMDL

Título	**Tema**
Towards a Model for Comprehending and Reasoning about PoW-based Blockchain Network Sustainabilit	Aspetos de segurança e eficiência na *blockchain*
Security and Privacy on Blockchain	Segurança e privacidade na *blockchain*
Making Smart Contracts Smarter	Segurança *smart contracts blockchain* pública
On the Security and Performance of Proof of Work Blockchains	Segurança algoritmo de consenso PoW.
Proof-of-stake at stake: predatory, destructive attack on PoS cryptocurrencies	Segurança *blockchain*

Continua

Continuação da tabela anterior

From Bitcoin to Bitcoin Cash: a network analysis	Comparação rede Bitcoin e Bitcoin Cash
Blockchain and Smart Contracts	Estruturas das tecnologias da Blockchain e Smart Contract
State of Public and Private Blockchains: Myths and Reality	Tipos de *blockchain* e funcionamento
Is Cryptocurrency Money?: Three Empirical Studies Analyzing Medium of Exchange, Store of Value and Unit of Account	Estudo características de moedas nas criptomoedas
Dandelion: Redesigning the Bitcoin Network for Anonymity	Anonimato e transparência

Science Direct

Título	**Tema**
Bitcoin's energy consumption is underestimated: A market dynamics approach	Avaliação consumo de energia da *Bitcoin*
Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects	Funcionamento *blockchain*
A systematic literature review of blockchain cyber security	*Blockchain* e segurança
Cryptocurrencies are (smart) contracts	Relação entre criptomoedas e *smart contracts*
Dissecting bitcoin blockchain: Empirical analysis of bitcoin network	Análise e funcionamento da *blockchain*
Blockchain and the built environment: Potentials and limitations	Fundamentos da *Blockchain*
Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash	Segurança e privacidade
Smart contract applications within blockchain technology: A systematic mapping study	Fundamentos da *Blockchain* e *smart contracts*
Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application	Compreenção e análise de transacções Ethereum com *blockchain* privada
Initial coin offerings and their initial returns	Estudo sobre *Initial Coin Offerings*

("libra" AND "facebook") OR ("diem" AND "facebook")

IEEEXplorer

Título	Tema
Performance Analysis of the Libra Blockchain: An Experimental Study	Estudo experimental na *blockchain* de Libra.
Comparative Analysis of Bitcoin, Ethereum, and Libra	Revisão e discussão da tecnologia *blockchain* analisando comparativa de Libra, Bitcoin e Ethereum

ACMDL

Título	Tema
Toward Emancipatory Currencies: A Critique of Facebook's Libra Cryptocurrency and Ideas for Alternatives	Cenários possíveis para a Libra e design de moedas digitais

("DCEP" OR "Digital Currency Electronic Payment" OR "DC/EP" OR "yuan digital" OR china digital currency) AND CBDC

IEEEXplorer

Título	Tema
Demystifying Stablecoins: Cryptography meets monetary policy	Funcionamento e características das *stablecoins*
Integrated DLT and non-DLT system design for central bank digital currency	*Wholesale* CBDC *design* com DLT

Apêndice B – Código do *webservice* para transação

Apresenta-se um excerto de código relativo à implementação no w*ebservice,* para a realização da primeira fase da transação.

```
function TransacaoConta(addrVBC, KPvbc, addressFrom_conta, KPfrom,
addressTo_conta, KPto, value, compra, descCompra) {
        var info = "De: " + addressFrom_conta  + " Para: "+ addressTo_conta + "
Objeto/servico de compra: " + compra + " Descricao da compra: " + descCompra;
        web3_ganache.eth.sendTransaction({//transacao do montante da carteira do
emissor para a conta do Banco Central
                from: addressFrom_conta,
                to: addrVBC,
                value: value,
                data: encrypt(addrVBC, KPvbc, addressFrom_conta, KPfrom, info),
        }, function(err, transactionHash) {
                if (err) {
                        console.log("erro na transacao");
                        console.log(err);
                        return;
                } else {
                console.log("id transação (FROM -> SC): "+ transactionHash);
                $("#hashTransacResult").html(transactionHash);
                $("#sendTransacResult").html("Transferência para a carteira do SC!");
                //transacao do montante da conta do Banco Central para a conta do
        destinatário final
                contract.Transaction(info, KPvbc, addrVBC, KPto, addressTo_conta ,
        {from: addrVBC, value:value, gas:3000000}).then(
                        function(result) {
                                //console.log(result);
                                console.log(result.logs[0].args);
                                console.log("id transação (SC -> TO): " +
                        result.receipt.transactionHash);
```

```
                $("#sendTransacResult").html("Transferência com
            sucesso!");
                return;
            })
        .catch(
            function(error) {
                console.log(error);
                console.log('Failed transaction');
                $("#sendTransacResult").html("Ocorreu um erro na
            transferência!");
                return ;
            })
        }
});
```

Apêndice C – Código de encriptação no *webservice*

Para a implementação da encriptação da primeira fase da transação no *webservice* foi utilizado o excerto de código seguinte:

```
function encriptar_assimetrico(KP, Ks, addr, vbc) {
        if(vbc == 1){
                var encriptacaoKs =
"enc[KPvbc("+KP+")(EndereçoCarteira("+addr+")]("+Ks+")";
        }
        else if(vbc == 0){
                var encriptacaoKs =
"enc[KPut("+KP+")(EnderecoCarteira("+addr+")]("+Ks+")";
        }
        return encriptacaoKs;
}

function encriptar_simetrico (Ks, info) {
        var encriptacaoKsDados = "enc[Ks("+Ks+")]("+info+")";
        return encriptacaoKsDados;
}

//Encripta os dados da transacao com a chave publica do validador do banco central do
sc e do
//emissor da transacao
function encrypt(addrVBC, KPvbc, addrUt, KPut, info) {
        //criada uma chave simetrica (entre 1000 e 10000000000) que encripta os dados
(info)
        var Ks = Math.floor(Math.random() * 10000000000) + 1000;
        var encriptacaoKsDados = encriptar_simetrico (Ks, info);
        var encriptacaoKsPvbc = encriptar_assimetrico(KPvbc, Ks, addrVBC,1);
        var encriptacaoKsPfrom = encriptar_assimetrico(KPut, Ks, addrUt,0);
```

```
        var dataEncrypt = encriptacaoKsDados.concat("#", encriptacaoKsPvbc, "#",
encriptacaoKsPfrom);
        console.log("Informação encriptada: " + dataEncrypt);
        var dados_encriptados = web3_ganache.toHex(dataEncrypt);
        return dados_encriptados;
}
```

Apêndice D - Código encriptação *smart contract*

Apresentação do fragmento de código alusivo à encriptação das informações das transações no *smart contract*.

```
function encriptar_assimetrico(uint _KP, uint _Ks, address addr, uint vbc) pure private
returns (string memory){
        string memory _encriptacaoKs;
                if(vbc == 1){
                        _encriptacaoKs = string(abi.encodePacked("enc[KPvbc(",
                uint2str(_KP),")(EnderecoCarteira(",toAsciiString(addr),")](",uint2str(_Ks
                ),")"));
                }
                else if(vbc == 0){
                        _encriptacaoKs = string(abi.encodePacked("enc[KPut(",
                uint2str(_KP),")(EnderecoCarteira(",toAsciiString(addr),")](",uint2str(_Ks
                ),")"));
                }
        return _encriptacaoKs;
 }

 function encriptar_simetrico(uint _Ks, string memory _info) pure private returns
(string memory){
         string memory _encriptacaoKsDados = string(abi.encodePacked("enc[Ks(",
uint2str(_Ks) ,")](",_info,")"));
        return _encriptacaoKsDados;
 }

 //esta funcao deve encriptar os dados com a chave publica do utilizador emissor da
transacao e com a chave publica do banco central
 function encriptTransaction(string memory _info, uint _KPvbc, address addrVBC, uint
_KPut, address addrUt) private returns (bool) {
         uint Ks = random();//chave simetrica criada em cada transacao
         string memory _encriptacaoKsDados = encriptar_simetrico(Ks, _info);
        string memory _encriptacaoKsPvbc = encriptar_assimetrico(_KPvbc, Ks,
addrVBC,1);
```

```
        string memory _encriptacaoKsPto = encriptar_assimetrico(_KPut, Ks, addrUt,0);
        emit checkEncript(_encriptacaoKsDados, _encriptacaoKsPvbc,
_encriptacaoKsPto, addrUt);
        return true;
 }

 function Transaction(string memory _info, uint _KPvbc, address addrVBC, uint _KPut,
address payable _addrTo) public payable {
        bool res = encriptTransaction(_info, _KPvbc, addrVBC , _KPut, _addrTo);
        if(res == true){
                (bool sent, ) = _addrTo.call{value: msg.value}("");
                require(sent, "Failed to send Ether");
        }
        return;
 }
```

Apêndice E – Código para desencriptação no *smart contract*

O excerto de código que se apresenta refere-se à implementação no *smart contrat* para a desencriptação do registo da transação e encriptação com a chave pública do Banco Central, para posterior acesso pelo mesmo.

```
  //desencripta o valor encriptado enc[KPvbc(EndereçoCarteira](KS) e retorna KS
  function desencriptar_simetrico(string memory _valorEncriptado, uint _ind) pure
private returns (string memory){
        //desencriptacao com Kpvbc
        string memory Ks = substring(_valorEncriptado, _ind,
bytes(_valorEncriptado).length-1);
        return Ks;
  }

  //encripta Ks e o id da transacao com a chave Publica do Banco Central
  function encriptar_assimetrico(string memory _Ks, uint _KPbc, string memory _idTX)
pure private returns (string memory){
        string memory _encriptPbc =
string(abi.encodePacked("enc[KPbc(",uint2str(_KPbc),")](Ks(",_Ks,"),_idTX(",_idTX,"))"));
        return _encriptPbc;
  }

  function decriptTransaction(string memory _idTX, string memory
_dataTransactionEncript, uint _KpVBC, uint _KPbc, uint _ind) private{
        string memory Ks = desencriptar_simetrico(_dataTransactionEncript, _ind);
        string memory _encriptPbc = encriptar_assimetrico(Ks, _KPbc, _idTX);//com
chave Publica do Banco Central
        emit checkDecript(_encriptPbc, uint2str(_KpVBC));
  }

  function consultaBC(string memory _idTX, string memory _dataTransactionEncript,
uint _KPbc, uint _ind) public {
        decriptTransaction(_idTX, _dataTransactionEncript, KpVBC, _KPbc, _ind);
  }
```