TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS

TIMOTEO PIMENTA PIRES

TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO EM ENGENHARIA DE REDES DE COMUNICAÇÃO

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS

TIMOTEO PIMENTA PIRES

ORIENTADORA: Dra. EDNA DIAS CANEDO

TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO EM ENGENHARIA DE REDES DE COMUNICAÇÃO

PUBLICAÇÃO: PPGENE.TD – XX/2016

BRASÍLIA, DF: JUNHO / 2016.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS

TIMOTEO PIMENTA PIRES

TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO EM ENGENHARIA DE REDES DE COMUNICAÇÃO SUBMETIDO AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM ENGENHARIA DE REDES DE COMUNICAÇÃO.

APROVADO POR:

_____
EDNA DIAS CANEDO
DOUTORA, UNB/ENE (ORIENTADORA)

_____
LAERTE PEOTTA DE MELO
DOUTOR, BANCO DO BRASIL (EXAMINADOR EXTERNO)

_____
GEORGES DANIEL AMVAME NZE
DOUTOR, UNB/ENE (EXAMINADOR INTERNO)

BRASÍLIA, DF, 21 DE JUNHO DE 2016.

FICHA CATALOGRÁFICA

Pires, Timoteo Pimenta.

Tecnologia Blockchain e suas Aplicações para Provimento de Transparência em Transações Eletrônicas [Distrito Federal], 2016.

Xiii, 56p., 210 x 297mm (ENE/FT/UnB, Bacharel, Engenharia de Redes de Comunicação, 2016).

Graduação – Universidade de Brasília, Faculdade de Tecnologia.

1. Tecnologia Blockchain
2. Criptografia Assimétrica
3. Funcão de Hash
4. Redes P2P
5. Transparência Pública

I. ENE/FT/UnB
II. Título (série)

Departamento de Engenharia Elétrica.

REFERÊNCIA BIBLIOGRÁFICA

Pires, Timoteo Pimenta. (2016). Estudo da Tecnologia Blockchain e suas Aplicações para Provimento de Transparência em Transações Eletrônicas, Publicação PPGENE.TD-XXA/2016, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 56p.

CESSÃO DE DIREITOS

AUTOR: Timoteo Pimenta Pires

TITULO DA TESE Tecnologia Blockchain e suas Aplicações para Provimento de Transparência em Transações Eletrônicas.

GRAU / ANO: Bacharel / 2016

_____

Timoteo Pimenta Pires

SQN 312 Bloco B

CEP: 70.765-020 - Brasília – DF

AGRADECIMENTOS

Ao professor Peotta e à professora Edna, pelo incentivo e orientação sem os quais não teria chegado aqui.

Aos meus pais, pelo amor que jamais serei capaz de retribuir.

À minha noiva Brenda, com quem quero passar o resto da minha vida.

A Deus, criador de todas as coisas e de todo conhecimento que o homem possa ter, e que enviou seu filho para morrer pelo meu pecado.

RESUMO

TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS

Autor: Timoteo Pimenta Pires
Orientador: Professora Dra. Edna Dias Canedo
Programa de Graduação em Engenharia de Redes de Comunicação
Brasília, 21 de Junho de 2016.

O trabalho busca estudar o funcionamento do blockchain e mostrar como a tecnologia pode ser utilizada para aumentar o nível de confiabilidade e transparência nas ações governamentais. Por se tratar de uma tecnologia recente, há poucos trabalhos neste sentido e há uma grande necessidade de familiarização com a tecnologia nos meios acadêmico e legislativos. A metodologia utilizada foi a separação em fases de pesquisa, aplicação e proposta, buscando facilitar o entendimento do leitor. Ao final é mostrado porque o blockchain é uma tecnologia adequada para provimento de transparência na esfera pública e como isto pode ser alcançado.

ABSTRACT

BLOCKCHAIN TECHNOLOGY AND ITS APPLICATIONS FOR TRANSPARENCY IN ELETRONIC TRANSACTIONS

Author: Timoteo Pimenta Pires
Supervisor: Professor Dr. Edna Dias Canedo
Programa de Graduação em Engenharia Engenharia de Redes de Comunicação
Brasília, 21st June 2016

This paper aims to study the functioning of blockchain and how this technology can be used to increase the level of reliability and transparency in government actions. Because it is a new technology, there are not many studies in this regard and there is a great need to familiarize academic and legislative enviroments with the technology. The methodology used was split into phases of research, application and proposal, in order to facilitate the understanding. Finally, it is shown why the blockchain is a suitable technology for providing transparency in the public sphere and how this can be achieved.

SUMÁRIO

LISTA DE FIGURAS E TABELAS

LISTA DE ACRÔNIMOS

AML	*Anti Money Laundering*
CCE	Criptografia de Curvas Elípticas
CGU	Controladoria Geral da União
DCE	Diretório Central dos Estudantes
DOU	Diário Oficial da União
e-CPF	Cadastro de Pessoa Física eletrônico
ECDSA	*Elliptic Curve Digital Signature Algorithm*
FOIA	*Freedom of Information Act*
ICP	Infraestrutura de Chave Pública
IoT	*Internet of Things*
KYC	K*now Your Customer*
LAI	Lei de Acesso à Informação (Lei nº 12.527)
mBTC	milibitcoin
OGP	*Open Government Partnership*
PGP	*Pretty Good Privacy*
RFID	*Radio-Frequency IDentification*
RSA	Rivest, Shamir e Adleman
SHA	*Secure Hash Algorithm*
TCP	*Transmission Control Protocol*
TSE	Tribunal Superior Eleitoral

1. Introdução

Dois movimentos têm ganhado bastante força nos últimos anos e recebido especial atenção da sociedade e da comunidade acadêmica. O primeiro deles é uma demanda por maior transparência no modelo de administração pública em diversos países do mundo. O segundo é a expansão de uma tecnologia considerada por muitos a maior revolução tecnológica desde o surgimento da internet: o blockchain [Taylor, 2015]. Esses dois movimentos, aparentemente distantes um do outro, apontam para o surgimento de um novo modelo de gestão pública, capaz de prover muito mais transparência e confiabilidade.

A ideia de transparência na administração pública remonta à época do Iluminismo no século XVII, quando vários pensadores questionaram a validade dos 'Segredos de Estado', alegando o direito do povo às informações então restritas à elite social. Com os movimentos e revoluções que estabeleceram a formação geopolítica atual, várias constituições foram criadas estabelecendo-se os princípios da liberdade de acesso à informação pelo cidadão. Mas até as últimas décadas do séc. XX, movimentos relacionados à abertura de dados eram em sua maioria restritos às informações resultantes de trabalhos científicos.

A partir da última metade do séc. XX alguns fatos marcam de maneira significativa os avanços em direção a uma política de acesso à informação governamental. Em 1966, o então presidente dos Estados Unidos, Lyndon B. Johnson, assinou o Ato de Liberdade da Informação (FOIA) que estabelecia a abertura pública de uma série de dados restritos do governo. A ideia de que dados governamentais deveriam ser publicamente disponíveis ganhou força com o surgimento da internet e com o fortalecimento dos princípios de software livre. Em 2007, um grupo de trinta especialistas se reuniu na Califórnia para discutir e estabelecer princípios norteadores da política de dados abertos. O encontro marcou a criação dos oito princípios dos dados abertos governamentais, considerados até hoje os fundamentos do movimento de dados abertos. Em 2009, o presidente Barak Obama assinou o Memorando de Transparência e Governo Aberto, onde afirmava que informação mantida pelo governo federal é um patrimônio público e deve estar publicamente disponível de forma rápida e pronta para utilização, inaugurando o portal de dados abertos americanos *data.gov*.

Seguindo os avanços feitos pelo governo americano, Reino Unido, Nova Zelândia e outros países estabeleceram legislação específica para a abertura de dados governamentais. Em 2011 foi criado o OGP - *Open Government Partnership*, um acordo internacional no qual os países se comprometem com a implementação de uma série de medidas para

abertura de informações públicas.

No Brasil, o Diário Oficial da União (DOU) foi por muito tempo a única fonte oficial de dados abertos diretamente voltados ao cidadão, estendendo-se pela república e pelo governo militar. A partir do ano 2000 o governo desenvolveu mecanismos de fiscalização dos gastos federais como a Lei de Responsabilidade Fiscal e a Controladoria Geral da União (CGU), culminando na criação do Portal da Transparência em 2004.

Em 2009, entrou em vigor a Lei Complementar nº 131, determinando que a União, os Estados, o Distrito Federal e os Municípios disponibilizassem, em meio eletrônico e tempo real, informações pormenorizadas sobre sua execução orçamentária e financeira. Em novembro de 2011 foi aprovada a LAI - Lei de Acesso à Informação (Lei nº 12.527), que regulamentou o direito de acesso a informações públicas previsto na constituição brasileira bem como regras e procedimentos específicos para possibilitar o exercício desse direito pelos cidadãos. No final de 2011, o Brasil aderiu ao movimento internacional OGP - *Open Government Partnership*, comprometendo-se com a implementação de uma série de medidas para ampliação e melhora da publicação de dados da administração pública. Segundo informação no site da OGP, o país encontra-se atualmente em fase de implementação do segundo plano de ação, elaborado em agosto de 2013.

Outras iniciativas, em sua maioria de origem popular, tiveram importante papel no desenvolvimento da política de transparência pública no país. Entre elas destaca-se o movimento Transparência Hacker, composto na maior parte por desenvolvedores e ativistas com intuito de explorar dados abertos para criação de aplicativos que beneficiem a população. Outro movimento atuante nessa área é liderado pela ONG *Open Knowledge Foundation.* No Brasil, a ONG promove discussões e eventos que estimulam a criação de sistemas que façam uso de dados publicamente disponíveis.

Percebe-se, assim, a força deste primeiro movimento: a crescente demanda por maior transparência no modelo de administração pública, na execução de pagamentos, no cumprimento da previsão orçamentária e em diversas áreas de atuação do governo.

O segundo movimento, por sua vez, caracterizado pelo crescente interesse na tecnologia blockchain, considera-se estar ainda em seus primeiros estágios de maturidade. Apesar de existir desde 2008, a tecnologia blockchain ganhou a devida atenção apenas nos últimos anos. Até então, a atenção da mídia e do meio acadêmico era principalmente para o Bitcoin, a nova moeda digital que despontava como uma alternativa revolucionaria ao tradicional modelo de transação financeira existente. Recentemente, entretanto, o mundo despertou para o imenso potencial que a tecnologia por trás do Bitcoin oferece, algo que

vai muito além de uma simples aplicação de moeda criptográfica.

Em 2008, um artigo publicado em uma lista de e-mail, por um indivíduo identificado como Satoshi Nakamoto, cuja identidade nunca foi confirmada [Nakamoto, 2008], despertou um grande interesse mundial, especialmente entre a comunidade de programadores [Barber *et al*, 2012]. O artigo descrevia o funcionamento de uma moeda inteiramente digital, controlada por um protocolo da camada de aplicação e cuja a validação das transações financeiras era feita de maneira totalmente distribuída pelos nós de uma rede P2P. Dessa maneira, a moeda circularia sem a necessidade de uma instituição que regularizasse o seu funcionamento ou uma autoridade central que validasse as transações.

O sistema foi colocado em operação em 2009 em código aberto desenvolvido de maneira colaborativa e as primeiras transações começaram a acontecer, acertadas pelo fórum *bitcointalk*. Em 2010, ocorreu a primeira transação comercial conhecida com a tecnologia, duas pizzas *Papa Jonh's* foram compradas por 10.000 bitcoins, à época algo em torno de U$ 25,00, hoje algo em torno de U$ 4.500.000,00.

Com a popularização da tecnologia, diversas criptomoedas começaram a surgir, como o Litecoin, Dogecoin e Peercoin, denominadas de modo geral como altcoins. Recentemente, tecnologias que vão além da moeda digital começaram ser construídas sobre o blockchain. O Ethereum, uma plataforma de *smart contracts*, o Follow My Vote, para realização de votações e o BitHealth para acompanhamento de registros de pacientes são alguns exemplos. Existe uma grande quantidade de aplicações para diversos propósitos construídos com a tecnologia blockchain, também chamada ao redor do mundo *Distributed Ledger* - livro de registros distribuído.

Observando com mais atenção estes dois movimentos, a crescente demanda por maior transparência pública e o interesse global na tecnologia blockchain, não é difícil perceber que estamos diante de um cenário com grande potencial para o desenvolvimento de novas aplicações. Como seria se todos os repasses financeiros do governo, da esfera federal à municipal, fossem feitos por meio de moeda digital e registrados em um livro razão validado por diversos nós de uma rede P2P aberto a escrutínio público? Ou se a administração e execução de contratos e licitações fossem feitas com uso da tecnologia blockchain, passível de auditoria por todo cidadão digitalmente alfabetizado? Ou ainda, se as eleições fossem realizadas com o uso dessa tecnologia acompanhando ou substituindo a urna eletrônica, que inspira pouquíssima confiança no eleitor brasileiro, principalmente no meio acadêmico? [Aranha *et al*, 2013].

Enfim, existe um grande potencial a ser explorado a partir da integração de blockchain e gestão pública. São vários também os desafios que terão de ser enfrentados para que esta tecnologia alcance um nível de maturidade e efetividade no cenário global, tanto do ponto de vista técnico, quanto financeiro, quanto legal. Espera-se, entretanto, que governo, universidade e iniciativa privada trabalhem juntos para explorar todo o potencial que este cenário oferece.

1.1 Motivação

Apesar do grande interesse em novas aplicações da tecnologia de blockchain, pouco tem sido explorado quanto a sua aplicação para prover transparência na esfera governamental. A maior parte das pesquisas são para desenvolvimento de aplicações para uso comercial ou simplesmente para disseminar o conhecimento da tecnologia, ainda em seus primeiros passos de desenvolvimento.

Percebe-se ainda uma grande necessidade de familiarização com a tecnologia no meio acadêmico, visando, futuramente, maior segurança para criação de legislação nacional adequada ao tema. Boa parte do desenvolvimento tecnológico atual relacionado ao blockchain acontece em um ‘vácuo' legislativo. É necessário que as universidades do país estudem com profundidade o tema, familiarizem-se com a tecnologia, conheçam os riscos e oportunidades envolvidos a fim de que o poder legislativo do país tenha referências acadêmicas adequadas para criar o aparato legal em momento oportuno.

1.2 Objetivos

Os objetivos deste trabalho podem ser resumidos em:

a. Apresentar o funcionamento da tecnologia blockchain em sua estrutura fundamental como base para as mais diversas aplicações;
b. Avaliar casos de aplicação da tecnologia para provimento de transparência na gestão pública, principalmente, na esfera do Governo Federal;
c. Indicar possíveis implementações de aplicações que podem ser usadas no âmbito da administração pública para prover maior confiabilidade e transparência;
d. Simular a realização de um caso prático que demonstre a efetividade da tecnologia.

Assim, o principal objetivo deste trabalho, observando o estado da arte do blockchain, é

mostrar como esta tecnologia pode ser utilizada para se alcançar um modelo de governo com maior nível de transparência e confiabilidade;

1.3 Metodologia

A metodologia de pesquisa proposta foi dividida em fases 1, 2 e 3, para facilitar o entendimento do trabalho, conforme apresentado a seguir.

Fase 1 - Pesquisa teórica: permite a identificação, leitura e análise de publicações relevantes ao desenvolvimento do projeto e que fornecem a sustentação teórica para o estudo desenvolvido nas outras fases;

Fase 2 - Pesquisa por casos de sucessos na utilização da tecnologia: permite entender de maneira mais efetiva o resultado das aplicações que fazem uso da tecnologia estudada na fase anterior;

Fase 3 - Estudo de aplicações futuras: permite investigar novas soluções possíveis que fazem uso da tecnologia em questão para alcançar o objetivo proposto;

Fase 4 - Estudo de caso prático: permite reproduzir em menor escala os efeitos de uma aplicação da solução no cenário real.

1.4 Organização do Trabalho

O trabalho está dividido em outros três capítulos além desta introdução. O capítulo 2 oferece uma revisão dos principais conceitos teóricos abordados. Em seguida, todos esses conceitos são reunidos para descrever o funcionamento do blockchain, a execução de uma transação e o processo de mineração. Ao final do capítulo, são feitas várias considerações quanto às questões de segurança relacionadas ao tema e uma revisão de trabalhos correlatos.

No capítulo 3 são apresentadas diversas aplicações da tecnologia à esfera da administração pública. Questões como pagamento de servidores, execução de contratos, realização de eleições são analisadas cuidadosamente tendo em vista um novo cenário econômico e governamental, profundamente transformados pela tecnologia apresentada.

O Capítulo 4 apresenta uma simulação de votação com transações no blockchain do bitcoin e o capítulo 5 conclui trabalho com as considerações sobre o tema, indicações de trabalhos futuros e áreas promissoras para o desenvolvimento de pesquisa acadêmica.

2. Estado da Arte e Revisão Bibliográfica

Para abordar o tema de maneira clara e facilitar o entendimento, este capítulo foi dividido em três seções. A seção 2.1 apresenta os conceitos básicos relacionados à tecnologia como criptografia de chave pública, redes P2P e função de hash. A seção 2.2 integra os conceitos anteriores para explicar como acontece a inserção, espalhamento e validação de cada registro feito no blockchain, tendo como referência o modelo de registros utilizados pelo blockchain do bitcoin. Na seção 2.3 são abordados temas referentes à segurança do sistema como pontos de vulnerabilidade, confidencialidade e anonimato e na seção 2.4 trabalhos correlatos ao assunto.

2.1 Conceitos Elementares

Esta seção apresenta alguns conceitos teóricos essenciais ao entendimento do blockchain.

2.1.1 Criptografia de chave pública

A criptografia de chave pública, ou criptografia assimétrica, é o método criptográfico que faz uso de duas chaves diferentes, uma chave pública para criptografar e uma chave privada para descriptografar a mensagem. Este modelo contrapõe-se ao modelo de chave privada ou simétrica, onde a mesma chave é utilizada para criptografar e descriptografar a mensagem. A figura 2.1 ilustra o funcionamento de uma criptografia de chave pública e figura 2.2 de uma criptografia de chave privada no processo de encriptação da mensagem.

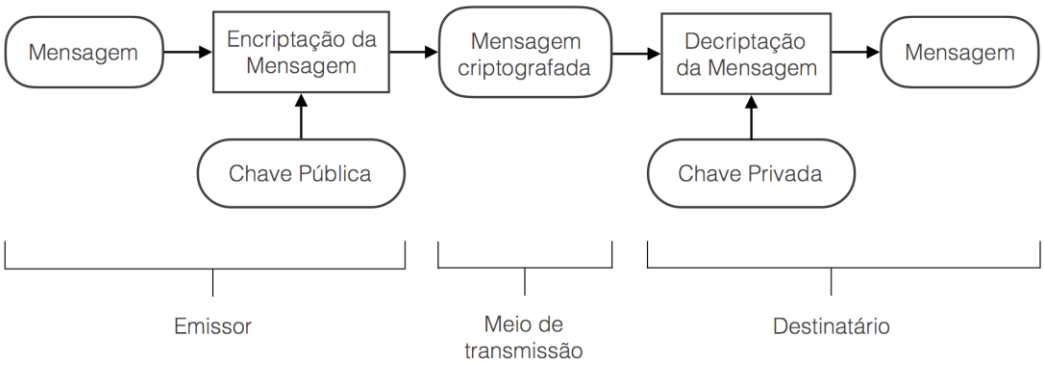

Figura 2.1 Criptografia de Chave Pública (Salomaa, 1996, *adaptado*)

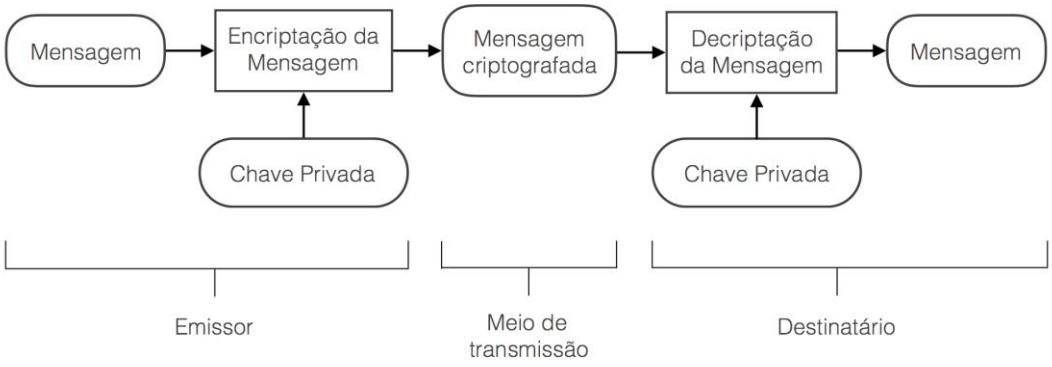

Figura 2.2 Criptografia de Chave Privada (Salomaa, 1996, *adaptado*)

Em um sistema de criptografia assimétrica, a chave pública é divulgada abertamente para todos que queiram enviar uma mensagem ao dono da chave ou verificar a autenticidade de uma mensagem por ele enviada. A chave privada, por sua vez, é mantida em segredo e qualquer pessoa com acesso a ela será capaz de decodificar a mensagem criptografada ou atestar a autenticidade da mensagem por meio de uma assinatura digital.

A segurança de um sistema criptográfico assimétrico está na diferença entre o caminho de ida e o caminho de volta da operação matemática em que a criptografia está fundamentada [Impagliazzo, 1989]. Quanto maior esta diferença, mais eficiente o algoritmo. Diffie-Hellman, um dos primeiros algoritmos a fazer uso de assimetria em criptografia, baseia-se na dificuldade de se reverter operações logarítmicas e é normalmente utilizado para acordo de uma chave privada. RSA, cujo nome remete às iniciais de seus inventores - Rivest, Shamir e Adleman - explora a dificuldade de se fatorar um número em fatores primos, comparado a facilidade de multiplicar dois primos para gerar um produto. Atualmente, a Criptografia de Curvas Elípticas - CCE - é considerada a mais eficiente, além de ser a mais utilizada para aplicações de blockchain.

A Criptografia CCE é baseada nas propriedades matemáticas das curvas elípticas, descritas pela seguinte equação:

$$y^2 = x^3 + ax + b$$

As chaves públicas e privadas do algoritmo são calculadas a partir de repetidas operações de adição de coordenadas polares, obtidas pela interseção da curva elíptica com diversas retas tangentes; uma explicação detalhada do funcionamento da CCE pode ser

encontrada em [Hankerson *et al*, 2006].

É importante ressaltar que uma chave criptográfica possui a propriedade de descriptografar a mensagem criptografada pela chave correspondente. Tanto a chave pública quanto a chave privada podem ser usadas para criptografar uma mensagem, dependendo da finalidade para a qual a criptografia é utilizada. De modo geral, a criptografia com a chave pública provê confidencialidade, enquanto a criptografia com a chave privada provê autenticidade. Esta ideia deve ficar mais clara na seção 2.1.3, onde é apresentado o conceito de assinatura digital.

2.1.2 Função Hash

Uma função hash é uma função matemática com as seguintes propriedades:

- A entrada pode ser qualquer sequencia de caracteres de qualquer tamanho;
- A saída é uma sequencia de caracteres de tamanho fixo;
- Sua eficiência é computável, ou seja, o tempo de execução da função para uma entrada de n caracteres deve ser O(n).

Na figura 2.3, (u, v, x, y, z) são entradas de tamanhos quaisquer para uma função de hash H(i). A saída dessa função é uma sequência de caracteres de tamanho fixo.

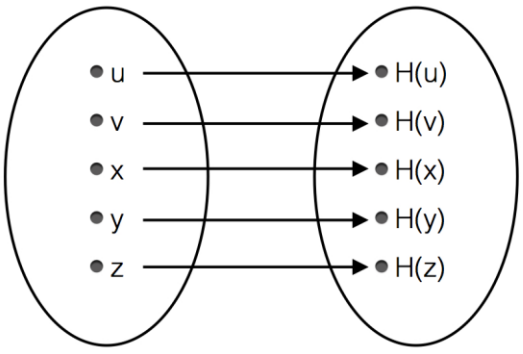

Figura 2.3 Entradas e saídas de uma função hash (Narayanan *et al*, 2016, *adaptado*)

As propriedades acima definem uma função hash de maneira geral, suficientes para construir uma tabela de hash. No entanto, há mais duas propriedades normalmente desejadas em uma função hash, ou propriedades que caracterizam uma função hash criptográfico [Narayanan *et al*, 2016]:

- Resistente a colisões;
- Anti-reversão;

Uma colisão acontece quando duas ou mais entradas diferentes produzem o mesmo hash de saída, como mostrado na figura 2.4:

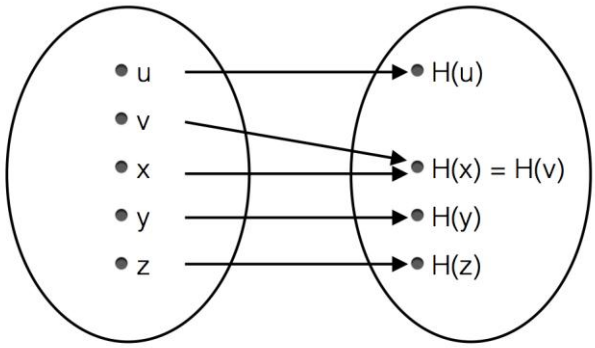

Figura 2.4 Colisão em uma função hash (Narayanan *et al*, 2016, *adaptado*)

Ser resistente a colisões significa que a probabilidade de duas entradas produzirem o mesmo hash deve ser pequena. Note que não se pode afirmar a impossibilidade da ocorrência de colisão, uma vez que o domínio dessa função é composto de todas as sequências de caracteres possíveis e a imagem pelo conjunto de sequencia de caracteres de um tamanho fixo. Se o domínio da função é um conjunto infinito e a imagem um conjunto finito, as colisões são inevitáveis. No entanto, boas funções de hash apresentam baixíssimas probabilidade de colisão. Na prática, é quase impossível a ocorrência de uma colisão natural. A resistência a colisão permite a utilização do hash como síntese de mensagem (do inglês *message digest*). Por exemplo, para verificar que um arquivo baixado de um servidor na nuvem corresponde ao arquivo desejado, basta fazer a comparação de seus hashes ao invés de comparar todo o arquivo [Narayanan *et al*, 2016].

Ser anti-reversão significa que não é possível obter a mensagem de entrada x a partir do hash h(x). Esta característica é alcançada fazendo com que a probabilidade dos hashes na saída da função obedeçam uma distribuição uniforme. Na prática, isto significa que não é possível correlacionar caracteres na entrada e na saída da função apenas observando a frequência com que eles aparecem [Narayanan *et al*, 2016].

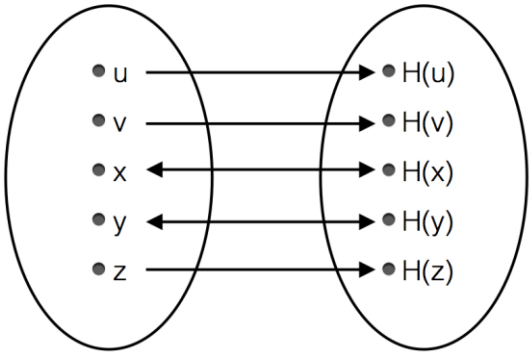

Figura 2.5 Reversão de uma função hash (Narayanan *et al*, 2016, *adaptado*)

A principal implementação de hash utilizada pelo blockchain é a SHA-256, projetada pela Agencia Nacional de Segurança dos EUA (NSA). O hash produzido nessa implementação tem um tamanho fixo de 256 bits. Uma análise mais detalhada do seu funcionamento pode ser encontrada em [FIPS, 2015].

Uma das principais utilizações de função hash na tecnologia blockchain é na construção de árvores de Merkle – árvores binárias de hash. A árvore é construída das folhas para a raiz, realizando o hash por pares. Quando há um numero impar de folhas, a última folha é duplicada e hasheada consigo mesma. Esta estrutura permite uma rápida verificação das entradas iniciais da função e reduz em um único hash a representação de todas as entradas (a raiz da Árvore de Merkle ou *Merkle Root*). A figura 2.6 ilustra a construção de uma árvore de Merkle [Okupski, 2014].

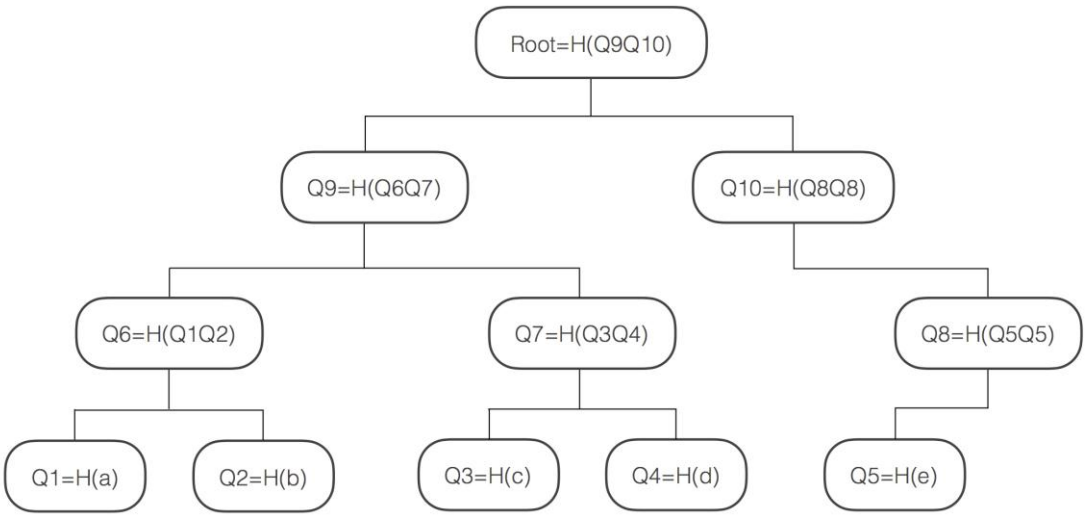

Figura 2.6 Ilustração de uma Árvore de Merkle (Okupski, 2014)

2.1.3 Assinatura Digital

Assinatura digital é uma aplicação criptográfica que aplica ao meio digital os princípios de uma assinatura convencional. Existem duas propriedades essenciais em uma assinatura convencional:

- **Autenticidade**: qualquer pessoa pode saber quem fez a assinatura, mas apenas o autor deve saber fazê-la;
- **Endosso**: a assinatura deve estar vinculada ao documento que se pretende endossar e a nenhum outro;

O que se espera com essas duas propriedades é que uma assinatura não possa ser forjada e não possa ser usada em um documento para o qual ela não foi feita. Quando se trata de assinatura digital esperamos o cumprimento dessas mesmas condições e a criptografia assimétrica pode ser usada para prover essas duas características ao processo.

Já vimos na seção 2.1 que um par de chaves criptográficas é composto por uma chave pública e uma chave privada; que apenas a chave privada pode descriptografar o que foi criptografado com a chave pública e que apenas a chave pública pode descriptografar o que foi criptografado com a chave privada. Logo a propriedades de autenticidade e endosso podem ser alcançadas aplicando-se a criptografia de maneira inversa à descrita no início da seção 2.1: a mensagem é criptografada (assinada) com a chave privada e descriptografada (verificada) com a chave pública. Perceba que neste modelo o objetivo é autenticidade e não confidencialidade da mensagem. A informação estará visível para qualquer pessoa que possuir a chave pública, e qualquer pessoa em posse desta chave poderá verificar que a mensagem foi emitida pelo proprietário da respectiva chave privada.

Existe ainda uma maneira de tornar a assinatura digital mais eficiente adicionando-se o conceito de função hash. Vimos na seção 2.2 que uma função hash é capaz de gerar uma palavra de saída única de tamanho fixo para uma entrada de tamanho qualquer (resistência à colisão). Logo, para criar uma assinatura digital podemos criptografar apenas o hash da mensagem com a chave privada. Para a realizar a verificação da assinatura, basta ao destinatário descriptografar a assinatura recebida e compará-la ao hash da mensagem recebida. A figura 2.7 representa este processo de assinatura e verificação.

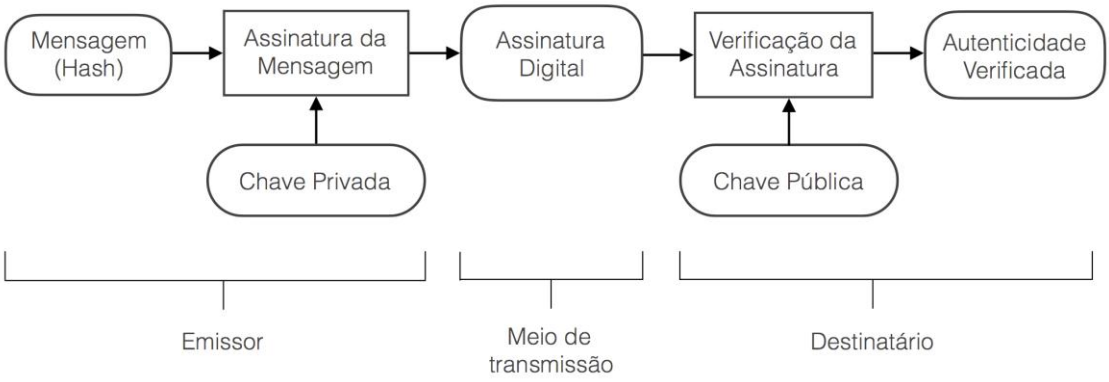

Figura 2.7 Assinatura e verificação com criptografia assimétrica (Narayanan *et al*, 2016)

Na tecnologia do blockchain, não há necessidade nem interesse de prover confidencialidade para as informações. Pelo contrário, a essência do blockchain é ser uma cadeia de registros públicos. Por outro lado, a autenticidade é essencial para o funcionamento do blockchain. É fundamental que cada registro no bloco seja feito apenas pelas pessoas autorizadas a fazê-lo. Por esse motivo, a criptografia no blockchain é normalmente aplicada como assinatura e não como encriptação de mensagem [Okupski, 2014]..

O algoritmo utilizado para gerar o par de chaves que assina e verifica a mensagem é o ECDSA (Elliptic Curve Digital Signature Algorithm) já mencionado na seção 2.1.1. O blockchain do bitcoin faz uso de uma curva elíptica específica, a "secp256k1", que prove segurança de 128 bits, ou seja, a dificuldade para se quebrar um par de chaves é aproximadamente a dificuldade de se realizar 2ˆ128 operações de criptografia simétrica, o que caracteriza um alto nível de segurança no cenário tecnológico atual. Informação detalhada do funcionamento do ECDSA pode ser encontrada em [Johnson *et al*, 2001].

2.1.4 Redes p2p

P2P é uma modelo de arquitetura de rede que se contrapõe ao tradicional modelo cliente-servidor. Redes p2p utilizam uma arquitetura descentralizada em que cada máquina, chamada de nó, executa ao mesmo tempo as funções de cliente e servidor, diferente da arquitetura cliente-servidor em que uma máquina cliente apenas envia solicitações e aguarda pela resposta do servidor. A figura 2.8 e 2.9 apresentam a estrutura dos dois modelos de arquitetura.

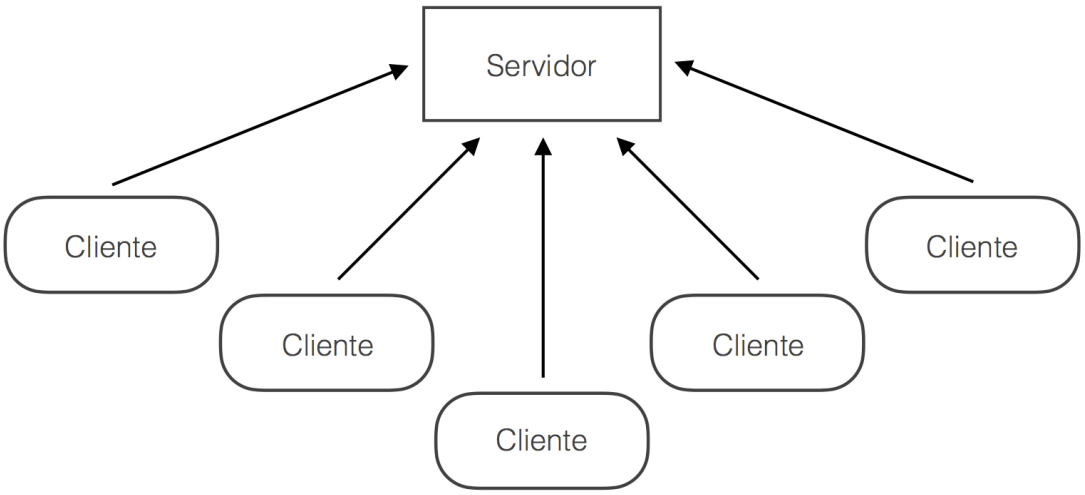

Figura 2.8 Arquitetura cliente-servidor (Wang, 2009, *adaptado*)

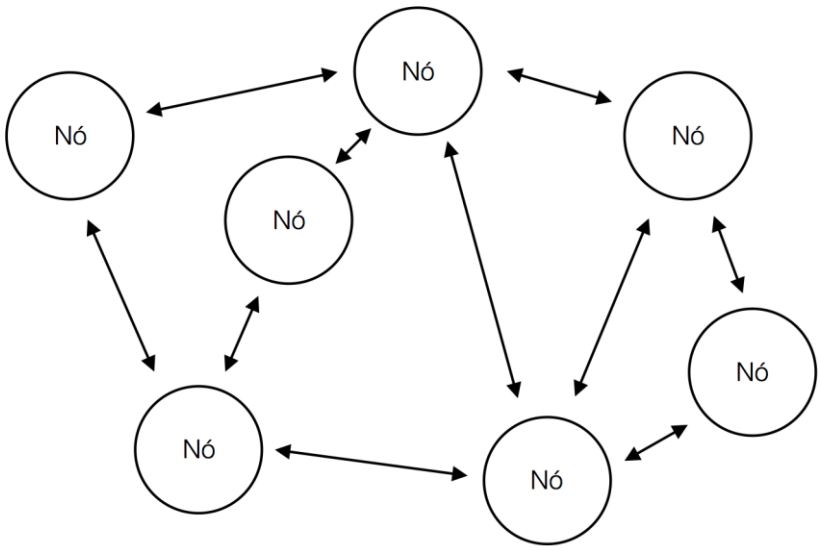

Figura 2.9 Arquitetura P2P (Wang, 2009, *adaptado*)

No modelo cliente-servidor o desempenho do servidor é deteriorado à medida que o numero de requisições dos clientes aumenta. Em redes p2p, o desempenho geral da rede aumenta à medida que cresce o numero de nós da rede. Normalmente, cada nó da rede pode realizar upload e download ao mesmo tempo e novos nós podem entrar na rede enquanto outros nós estão saindo, caracterizando um modelo de alta flexibilidade e ainda transparente ao usuário final.

Uma característica interessante de redes p2p é capacidade de tolerância a erros.

Quando um nó é desconectado da rede, a aplicação p2p pode continuar a operar utilizando outros nós que permanecem ativos. Na arquitetura cliente-servidor a conexão é interrompida se um servidor é desligado.

Outra característica importante das redes p2p, especialmente para a utilização com o blockchain, é o seu caráter descentralizado. Informações transmitidas por um nó da rede, podem rapidamente ser replicadas para máquinas em diversos lugares do mundo, tornando praticamente impossível apagar ou alterar registros espalhados em um número tão grande de nós.

No blockchain do bitcoin, quando um novo nó é adicionado à rede, ele envia uma mensagem a um ou mais nós específicos gravados no código do programa, chamados de nós sementes (do inglês *seed nodes*), requisitando outros nós da rede endereços de nós com os quais possa se conectar. Este processo se repete com os nós recém aprendidos até que o nó adicionado esteja conectado à vários outros nós da rede de maneira razoavelmente aleatória. Uma vez conectado à rede e com os registros do blockchain atualizados, o nó está apto a publicar novos registros através de um algoritmo de broadcasting (também chamado de algoritmo de *flooding* ou *gossip protocol*). De maneira simplificada, o nó envia o registro recém criado a todos os nós com o qual está conectado. Ao receber um novo registro, cada nó verifica se se trata de um registro novo ou se já o recebeu anteriormente. Caso seja um novo registro o nó adiciona o registro à sua lista e o replica para todos os nós a ele conectado. Caso o registro já tenha sido recebido anteriormente, ele simplesmente o ignora. Isto impede que mensagens fiquem trafegando indefinidamente pela rede. Existe ainda uma série de verificações feitas a cada inserção no blockchain, a seção 2.2 apresenta com mais detalhes como os registros do blockchain são criados, agrupados em blocos, validados por mineradores e espalhados pela rede.

2.2 Funcionamento do Blockchain

A seção anterior apresentou os principais conceitos teóricos essenciais ao entendimento do funcionamento do blockchain. Esta seção se propõe a utilizar os conceitos apresentados para explicar como o protocolo funciona, tendo como referencia o blockchain do bitcoin, a principal implementação de blockchain na atualidade.

O blockchain é uma cadeia de registros imutáveis, públicos e distribuídos. **Cadeia** porque os registros estão cuidadosamente encadeados uns aos outros por meio de chaves publicas, entradas e saídas. **Imutáveis** porque uma vez que o registro é inserido na cadeia, ele não pode mais ser alterado. **Públicos** porque a única condição necessária para que um cidadão possa ter acesso aos registros do blockchain é que ele tenha acesso à internet, e **distribuídos** porque esta cadeia de registro não está armazenada em um único servidor central, ao contrário, está replicada em milhões de máquinas distribuídas pelo mundo todo e nenhuma empresa ou indivíduo pode reivindicar a propriedade destes registros. Esta seção apresenta como é formada esta cadeia, observando ordenadamente o processo de formação dos registros, de formação dos blocos e a validação dessas informações, tendo como referência os textos de [Narayanan *et al*, 2016] e [Okupski, 2014].

2.2.1 A cadeia de blocos

O blockchain está estruturado na forma de blocos encadeados. Cada bloco possui uma área de transações e uma área de cabeçalho. A figura 2.5 apresenta uma visão do encadeamento dos blocos.

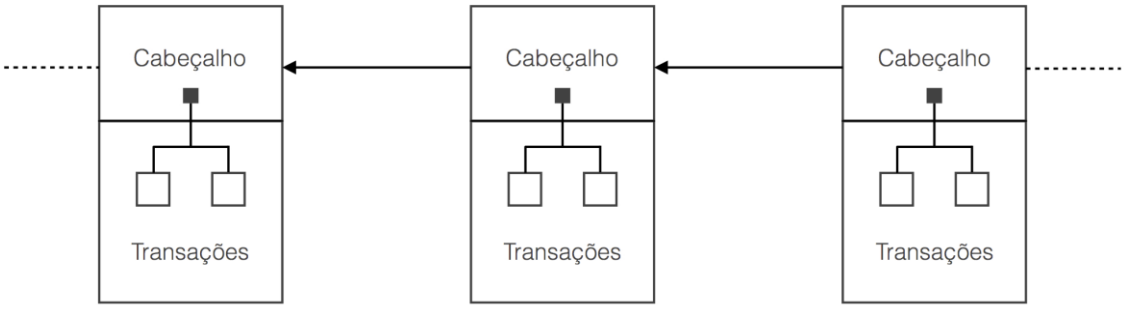

Figura 2.10 Cadeia de blocos do blockchain (Okupski, 2014, *adaptado*)

Na área de transações estão todas as transações coletadas por aquele bloco. Na área de cabeçalho se encontram o hash do cabeçalho do bloco anterior e a raiz da árvore de Merkle das transações presentes no campo de transações. Dessa forma, cada bloco está ligado ao

bloco anterior, formando uma cadeia de blocos e cada transação está representada no cabeçalho por meio da raiz da árvore de Merkle em que foi coletada [Narayanan *et al*, 2016].

É interessante notar que a propriedade de imutabilidade do blockchain e boa parte de sua segurança derivam-se da estrutura encadeada dos blocos. Como cada bloco contém em seu cabeçalho o hash do cabeçalho do bloco anterior, para se alterar um bloco da cadeia é necessário alterar todos os blocos posteriores, o que exige uma capacidade de processamento absurda, uma vez que novos blocos estão sendo constantemente adicionados por outros nós (a seção 2.2.3 explica por que é necessário alto grau de processamento para adicionar um bloco a cadeia).

A utilização da árvore de Merkle permite detectar qualquer alteração nas transações, uma vez qualquer alteração nas transações do bloco resulta em uma alteração na raiz da árvore de Merkle inserida no cabeçalho do bloco. Assim, a dificuldade para se alterar um registro do blockchain cresce a medida que novos nós são adicionados à rede [Okupski, 2014].

2.2.2 Transações (Registros)

Não apenas os blocos estão encadeados no blockchain, mas também as transações. A tabela 2.1 apresenta os campos que compõem uma transação e a figura 2.11 ilustra como as transações estão encadeadas por meio de suas entradas e saídas:

Tabela 2.1 Descrição dos campos de uma transação (Okupski, 2014)

Campo	Descrição
Metadados	Informações da transação como Id e tamanho.
Entradas	Vetor com informações de cada entrada da transação
Saídas	Vetor com informações de cada saída da transação

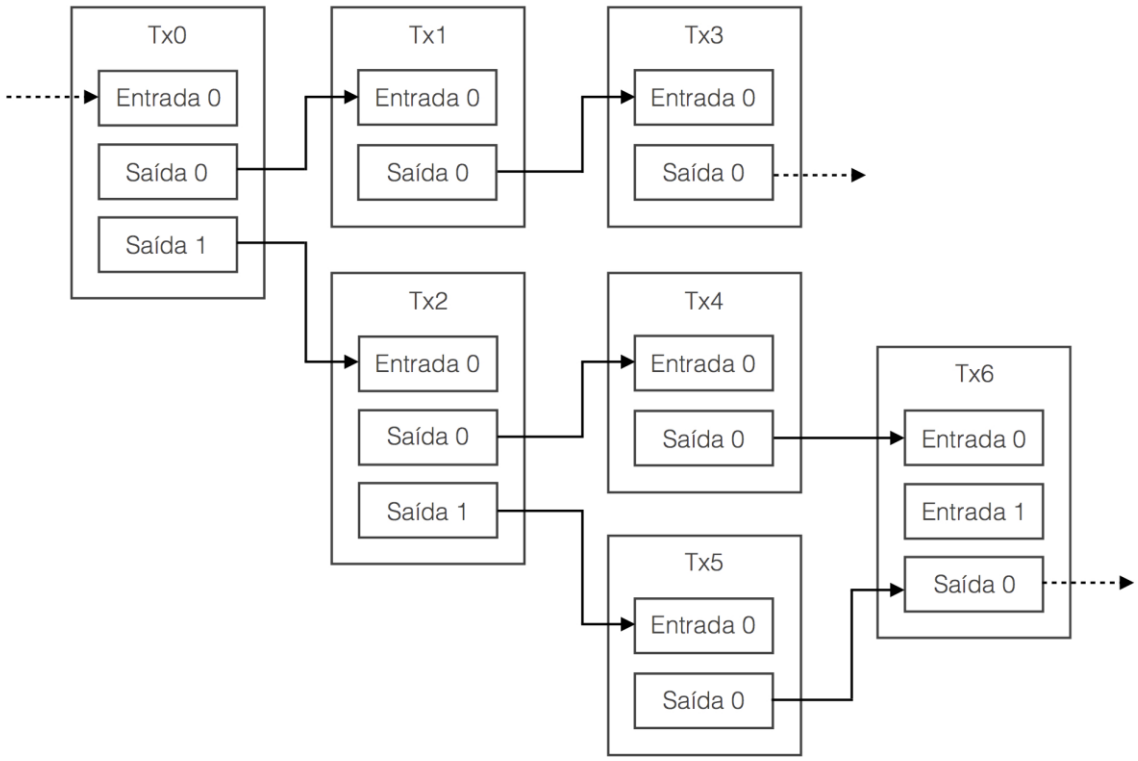

Figura 2.11 Encadeamento de transações no blockchain (Antonopoulos, 2014, *adaptado*)

O campo Metadados reúne informações gerais da transação como o tamanho da transação em bytes, quantidade de entradas e saídas, versão do protocolo e o id da transação, obtido a partir do cálculo de seu hash SHA256.

O campo Entradas apresenta uma lista numerada de entradas desta transação. Cada entrada de uma transação deve fazer referencia a saída de outra. Logo, neste campo há uma lista de id's de outros registros e o respectivo número da saída. Estas saídas devem ser computadas como entradas nesta transação. Ainda no campo entrada são adicionadas uma assinatura digital e uma chave pública responsáveis por confirmar que aquela transação está autorizada a utilizar as saídas indicadas no campo Entradas. O campo saída apresenta uma lista numerada de saídas que devem ser utilizadas como entradas de transações futuras. Este campo apresenta ainda um hash de chave pública que possui informações que condicionam a utilização dessas saídas por outra transação. A Figura 2.12 apresenta um exemplo de entradas e saídas de uma transação.

Figura 2.12 Exemplo de dados de transação (Narayanan *et al*, 2016)

Como mostrado na seção 2.1.3 a assinatura digital faz uso da chave privada para criptografar (assinar) uma mensagem e da chave pública para verificação da assinatura. Dessa maneira, ao inserir uma chave pública na saída da transação (ou um hash dela), apenas o portador da chave privada correspondente estará autorizado a utilizar aquela saída. No processo de validação da transação, a chave pública informada no campo Entrada é comparada com a chave pública previamente inserida na saída. Caso elas sejam diferentes, a transação é considerada inválida e não é propagada para os demais nós da rede. Caso elas sejam iguais, a assinatura informada no campo Entrada é verificada com a chave pública previamente confirmada. Se a assinatura for autêntica, ou seja, se a decriptação com a chave pública revelar o hash dos dados da transação, então a transação é validada, replicada para os demais nós da rede e coletada em bloco para mineração. Caso contrário, a transação é descartada. A figura 2.13 apresenta o processo de validação de transações com chaves publicas e privadas.

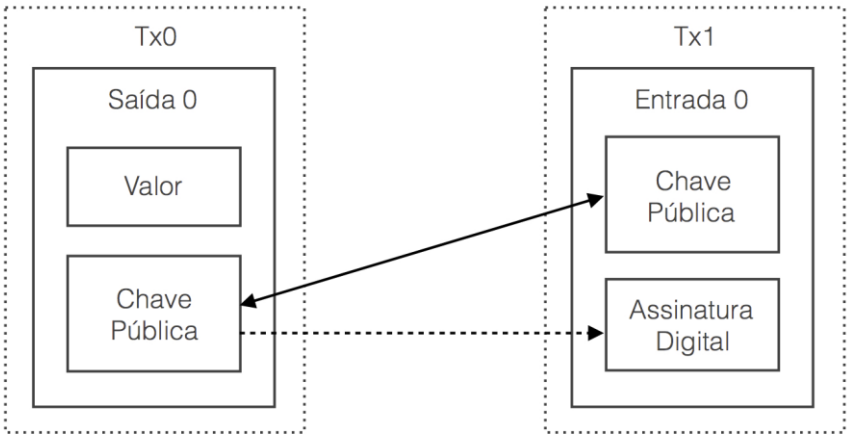

Figura 2.13 Processo de validação de transação com criptografia assimétrica (Okupski, 2014, *adaptado*)

2.2.3 Validação de blocos (Mineração)

Quando a transação é validada ela está pronta para ser coletada por um bloco e passar pelo processo de mineração. Um nó minerador da rede coleta as transações que deseja inserir no blockchain dentre todas as transações validadas recebidas, calcula a raiz da arvore de Merkle, como mostrado na seção 2.1.2, e passa a executar o algoritmo de prova de trabalho (do inglês *proof of work*).

Uma prova de trabalho é um desafio criptográfico utilizado para garantir que um nó realizou uma certa quantidade de trabalho. O bitcoin, em particular, utiliza uma prova de trabalho baseada no modelo de Adam Back [Nakamoto, 2008], outras aplicações do blockchain utilizam variações deste modelo, mas que tenham os mesmos dois princípios: a) garantir que o nó realizou uma quantidade predefinida de processamento e b) garantir que a prova entregue é objetivamente verificável. Tipicamente, uma prova de trabalho é um processo probabilístico e a probabilidade de sucesso depende da dificuldade estabelecida.

No bitcoin, por exemplo, a prova de trabalho é encontrar um valor chamado *nonce* cujo duplo hash SHA256 desse valor com a raiz de Merkle seja igual ou menor que um parâmetro T. A busca por esse valor é feita por tentativa e erro. Quanto menor o parâmetro T, menor a probabilidade de sucesso e mais difícil é conseguir realizar a prova de trabalho. Quanto maior o parâmetro T, maior a probabilidade e mais fácil encontrar um *nonce* válido. O protocolo do bitcoin ajusta o parâmetro T automaticamente a cada 2016 blocos para garantir que as provas de trabalho e, consequentemente, a mineração de um bloco aconteça, em média, a cada 10 minutos. Outros blockchains ajustam esse parâmetro para

que a mineração aconteça em intervalos menores, de alguns segundos por exemplo. Quando a prova de trabalho é vencida, o nó pode avisar toda rede que resolveu o desafio e inserir o bloco validado na cadeia de blocos. Ao realizar esta operação, o minerador recebe como recompensa uma quantia na unidade de valor utilizada pelo blockchain, além da diferença entre o valor de entrada e saída das transações, caso exista.

Quando um bloco é validado, ele é imediatamente publicado na rede para todos os nós adjacentes por meio de uma rede p2p (é utilizado TCP na camada de transporte). Cada um destes nós recebe o novo bloco, verifica se de fato se trata de um bloco ainda não recebido (cada bloco tem a sua numeração incremental, também chamada de altura do bloco) adiciona o bloco à sua cópia do blockchain e replica por sua vez aos nós adjacentes. O processo repete-se por toda a rede a fim de que haja consenso entre os nós da rede quanto ao estado da cadeia de blocos.

Caso aconteça de dois nós realizarem a prova de trabalho com uma diferença de tempo pequena, eles vão propagar blocos de mesma altura na rede gerando o que é chamado de Corrida de Blocos. O protocolo resolve essa questão da seguinte maneira: o maior segmento da cadeia de blocos é o segmento válido, isto é chamado de Regra da Maior Cadeia - *Longest Chain Rule*. Dessa forma, cada nó adiciona blocos recém criados à cadeia de maior altura até que uma bifurcação da cadeia se torne maior e a outra sequência de blocos seja abandonada, gerando os chamados blocos órfãos. No fim, existe apenas uma cadeia que liga o último bloco validado de volta até o primeiro bloco da cadeia. No caso do blockchain do bitcoin, este primeiro bloco é chamado de bloco gênesis (minerado em 1 de setembro de 2009).

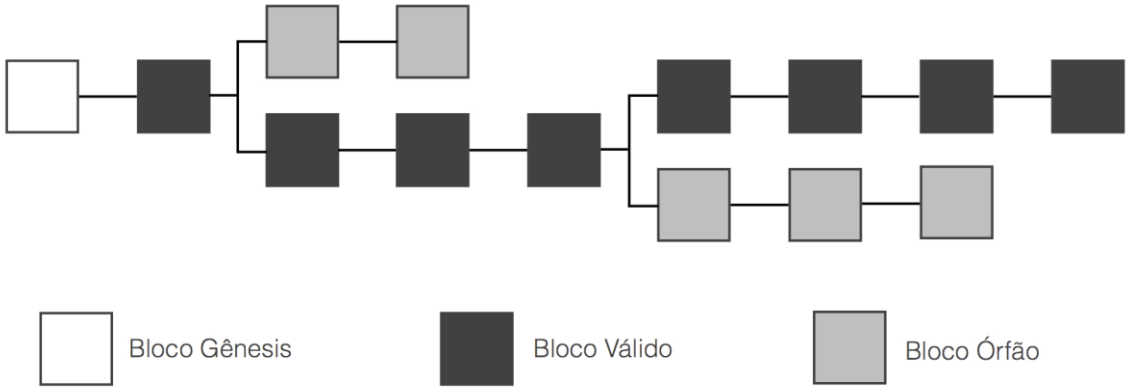

Figura 2.14 Regra da Maior Cadeia (Okupski, 2014)

Há muitos detalhes da implementação do blockchain que não foram apresentados

aqui. Tentou-se primar pelas propriedades comuns às várias implementações de blockchain existentes, tendo como referência o modelo de blockchain utilizado pelo bitcoin. Mais detalhes sobre implementações específicas de blockchain podem ser encontradas em [Okupski, 2014], [Wood, 2014] e [Narayanan *et al*, 2016].

2.3 Questões de segurança

Uma das melhores e mais simples definições de segurança pode ser encontrada em [Walport, 2016]: “Coisas que devem acontecer acontecem; e o coisas que não devem acontecer, não acontecem”. Com o blockchain não é diferente. A tecnologia tem sido alvo de várias pesquisas no âmbito da segurança. Muitos afirmam que não é possível alcançar um nível satisfatório de segurança na tecnologia, enquanto outros afirmam que poucas tecnologias no mundo oferecem a segurança provida pelo blockchain. Além disso, muito se discute sobre confidencialidade e anonimato de transações realizadas com a tecnologia. Esta seção analisa as principais vulnerabilidades relacionadas à tecnologia blockchain e apresenta algumas considerações sobre suas propriedades de confidencialidade e anonimato.

2.3.1 Ataque 51%

51% é o ataque em que um ou mais nós da rede alcançam capacidade de processamento total igual ou superior a 51% da capacidade de processamento de toda a rede. Deste modo, seria possível que transações feitas a partir de endereços não autorizados ou transações utilizando um valor já utilizado por outra transação (*dual spending*) fossem validadas pelos nós mal-intencionados. Como o atacante possui mais da metade da capacidade de processamento da rede, a bifurcação da cadeia (também chamado de *fork*) com os registros fraudados cresceria de maneira mais rápida que a bifurcação autêntica, validando transações que deveriam ser descartadas. Isto é chamado de ataque 51%. Existe algumas considerações importantes a respeito deste tipo de ataque:

- Não há registros de que este ataque tenha alguma vez alcançado sucesso desde a implementação do primeiro blockchain em 2009 [Eyal e Sirer, 2014];
- Caso um minerador possuísse 51% ou mais da capacidade de mineração da rede, seria mais vantajoso minerar as transações e receber as recompensas do protocolo do que efetuar um ataque à rede [Nakamoto, 2008];
- A possibilidade de se alcançar 51% da capacidade de processamento total da rede do blockchain do bitcoin é muito pequena;
- Outras tecnologias de blockchain, implementadas após o bitcoin, como o Litecoin, realizam um a prova de trabalho mais 'democrática' de modo que a simples capacidade de processamento não representa uma grande vantagem sobre os outros mineradores [Torres, 2013];

- Há propostas em alguns lugares do mundo, como no Reino Unido, para a regularização do processo de mineração de modo a impedir a existência de um minerador com tamanha capacidade de processamento [UK Gov, 2015]

Enfim, embora faça algum sentido do ponto de vista teórico, o ataque 51% não é uma ameaça na prática. Acredita-se que o maior risco relacionado ao ataque esteja na perda de confiança na tecnologia devido a existência de um super minerador e a consequente desvalorização da aplicação.

2.3.3 Chaves e Aleatoriedade

Para a utilização do Algoritmo de Assinatura Digital com Curvas Elípticas - ECDSA - uma boa fonte de aleatoriedade é essencial, pois há uma grande chance de vazamento da chave caso a fonte de aleatoriedade não seja eficiente [Narayanan *et al*, 2016]. Essa é uma vulnerabilidade do algoritmo de assinatura digital DSA todo e não apenas da sua implementação em curvas elípticas. Por isso, é comum em aplicações que fazem uso deste algoritmo, como o PGP, pedir que usuários movimentem o mouse e digitem textos aleatórios no teclado enquanto a chave é gerada [Poole, 2003]. Uma vez comprometida a chave privada na criptografia assimétrica a segurança está toda comprometida também, pois qualquer transação pode ser assinada indevidamente.

Na prática, porém, percebe-se que a maior vulnerabilidade do sistema não está nem na criptografia nem no protocolo, mas na parte humana do sistema. [Krombholz, 2015] cita que em uma pesquisa com cerca de 1000 usuários da moeda bitcoin, mais de 10% deles já havia perdido algum valor em virtude de falha humana, e conclui que o sistema apresenta baixa resiliência a este tipo de falha. A utilização do blockchain em seu modelo convencional não permite a recuperação de chaves perdidas, seja por esquecimento, morte ou qualquer outro motivo, o que resulta em uma grande quantidade de registros deixados para trás na cadeia de transação.

2.3.3 Confidencialidade e anonimato

Muito se discute sobre confidencialidade e anonimato no blockchain. Críticos alegam que a tecnologia apresenta propriedades facilitadoras para o comércio de produtos ilegais, como no caso SilkRoad [Walport, 2016] e atividades ligadas ao tráfico de drogas, terrorismo e lavagem de dinheiro [Taylor, 2015]. Neste ponto, um conceito precisa ficar bem claro: não existe confidencialidade na tecnologia blockchain. Pelo contrário, o

blockchain é uma cadeia de registros totalmente pública e todas as transações realizadas por ele estão disponíveis para qualquer cidadão com acesso à internet.

A confusão normalmente acontece por um motivo: o blockchain não trabalha com pessoas, trabalha com hashes de endereços públicos. Embora seja comum dizer que Alice transferiu uma quantia x para Bob utilizando alguma moeda digital, o que acontece na verdade é que a chave privada de Alice assinou um registro de transferência de valor para a chave pública de Bob. No entanto, os nomes de Bob e Alice nunca foram gravados no blockchain, apenas suas assinaturas e chaves públicas. Neste sentido, é correto dizer que o blockchain não exige identificação, mas não está correto dizer que ele prove confidencialidade.

A identificação do usuário que acessa o blockchain é realizada por aplicativos terceiros que adicionam as próprias regras de identificação ao protocolo da tecnologia, seguindo um conjunto de regras conhecidos como KYC (K*now Your Customer)*. O exemplo mais comum são as carteiras e sites de cambio e leilão de moedas digitais, que normalmente exigem uma identificação completa do usuário, inclusive com exigência de foto muitas vezes. Mas essas regras de identificação não fazem parte do protocolo do blockchain, são regras particulares de programas que utilizam o blockchain.

Em resumo, o blockchain prove um alto nível de transparência e rastreabilidade das transações. É possível rastrear qualquer valor até a sua transação *coinbase* por mais antiga que seja. A possibilidade de operar a tecnologia sem a necessidade de identificação é bastante atraente para operadores do comércio ilegal, mas de modo algum invalidam o uso da tecnologia de maneira adequada, apenas apontam para a necessidade de modernização dos instrumentos legislativos.

2.4 Trabalhos Correlatos

Esta seção apresenta trabalhos que estão de alguma forma relacionados ao tema de blockchain e transparência pública.

[Nakamoto, 2008] é um marco da criação da tecnologia e, provavelmente, a publicação mais importante sobre o tema. [Koshy, 2014] estuda a questão do anonimato no blockchain com especial atenção as propriedades de uma rede p2p; [Courtois, 2014] faz uma crítica à Regra de Maior Cadeia, utilizada para definir a cadeia válida em casos de *forks*, como mostrado na seção 2.2.3. [Eckenrode *et al*, 2015] e [Joshua *et al*, 2015] analisam a possibilidade e o impacto da criação de uma moeda virtual pelo governo e os riscos para a economia e a política desse país; [Scott, 2016] estuda a utilização do bitcoin

para fins de solidariedade e bem estar social; e, por fim, [UK Government, 2015] e [Walport, 2016] apresentam, respectivamente, o resultado de um pedido de informações sobre a tecnologia por parte do governo para a população, especialmente universidades e empresas, e um relatório do governo sobre a possibilidade de utilização do blockchain para criação de um modelo de administração pública mais confiável e transparente.

3 Aplicação da tecnologia à esfera pública

O capítulo 2 apresentou os principais conceitos teóricos relacionados ao blockchain e explicou o seu funcionamento de modo simplificado. Este capítulo busca encontrar aplicações do blockchain à esfera pública, com intuito de gerar maior legitimidade nas ações implementadas pelo governo, principalmente, no âmbito federal. [Walport, 2016] afirma em um relatório oficial do governo britânico sobre à tecnologia do blockchain:

> *Em suma, a tecnologia de Livro-razão Distribuído [do inglês Distributed Ledger Technology, outro termo para blockchain] provê a estrutura para que o governo reduza fraudes, corrupção, erros e custo… ela tem o potencial de redefinir o relacionamento entre governo e cidadão em termos de compartilhamento de dados, transparência e confiança.*

Outro trecho do relatório afirma:

> *A oportunidade é para o governo viabilizar um futuro onde a entrega de serviços públicos é mais pessoal, imediata e eficiente… A implementação da tecnologia de Livro-razão Distribuído com contratos inteligentes embutidos deve conduzir a uma evolução substancial em conformidade, eficiência e prestação de contas.*

Estas afirmações apontam para a importância da tecnologia no estabelecimento de uma relação de confiança entre governo e população. Esta seção apresenta algumas aplicações práticas do blockchain que possibilitam o aumento significativo do nível de transparência na administração pública.

3.1 Repasses de verbas em moeda digital

A primeira aplicação do blockchain é também a mais evidente e talvez a mais difícil de se implementar: a utilização de moedas digitais em repasses de verbas e pagamentos feitos pelo governo. Foi dito na introdução deste trabalho que a tecnologia do blockchain é "algo que vai muito além de uma simples aplicação de moeda criptográfica", e isso é verdade. No entanto, os benefícios da implementação da moeda digital não podem ser ignorados na busca por transparência governamental. As demais aplicações que serão apresentadas farão uso do blockchain de outras maneiras diferentes ou complementares a

utilização de moeda digital. Esta seção apresenta os benefícios, os desafios e algumas considerações do ponto de vista tecnológico da utilização de moedas digitais em repasses financeiros feitos pelo governo.

Existem pelo menos 4 tipos de repasses públicos que seriam muito beneficiados, em termos de transparência, pela utilização de moeda digital:

I. Repasse a empresas prestadoras de serviço;
II. Repasse de verbas às esferas estaduais e municipais;
III. Repasse de verbas para ONGs, instituições de caridade e ajuda humanitária;
IV. Repasse a partidos políticos e campanhas eleitorais;

Não é difícil imaginar os benefícios que a utilização de moedas digitais pode conferir a essas transações. Números da Folha de São Paulo indicam que em dezembro de 2015 havia cerca de 10.000 inquéritos abertos sobre desvio de verba pública apenas com a Polícia Federal, totalizando um valor de R$ 39,5 bilhões [Valente, 2015].

Uma vez que os repasses do governo são realizados em moeda digital, qualquer cidadão pode acessar e verificar os valores que foram repassados a cada entidade. Na verdade, esta era a expectativa do governo ao criar o Portal da Transparência em 2004, mas a experiência tem mostrado que registros podem ser muito diferentes da situação real e que 'pedaladas' podem fazer com que relatórios estejam bem distantes da realidade. Daí uma grande vantagem da moeda digital: não é possível separar registro de execução. O valor registrado no blockchain não é apenas um número a ser publicado, mas é o repasse financeiro em si, o que define a existência da moeda. Dessa maneira, é praticamente impossível, ou, pelo menos, muito mais difícil, apresentar a população um déficit nas contas públicas menor que o real ou um lucro maior que o atingido.

Além dos benefícios diretos de transparência providos pelo blockchain, existem ainda outros benefícios alcançados com a utilização de moeda digital [Walport, 2016]:

- **Ausência de limites geográficos:** o blockchain não está limitado a regiões geográficas. O território do blockchain é a internet e ele opera da mesma maneira em qualquer jurisdição no mundo. Essa característica é especialmente importante para repasses internacionais;

- **Conformidade com a finalidade do repasse:** o uso de moedas digitais previne

que um valor repassado para uma finalidade específica seja usado com outro propósito. Por exemplo, um repasse do governo para construção de um hospital não poderia ser utilizado para a construção de um estádio. Essa característica advém da capacidade que o blockchain oferece de rastrear qualquer transação;

- **Inclusão de pessoas não bancarizadas:** existem ainda, em regiões mais isoladas do país, pessoas sem qualquer acesso às instituições financeiras. O uso de moeda digital pode simplificar a tarefa de alcançar esse público, normalmente beneficiários de programas sociais.

Passamos agora a algumas considerações do ponto de vista tecnológico sobre a utilização de moeda digital por parte do governo. Os desafios para a implantação desta moeda são enormes, tanto do ponto de vista tecnológico, como econômico e legislativo, e é difícil imaginar a sua implementação num futuro breve no Brasil. Por isso, é importante observar o que está sendo feito em outros lugares do mundo, principalmente em lugares onde esta tecnologia tem se desenvolvido mais rapidamente, e considerar os desafios para sua implementação em nosso país.

[Eckenrode *et al*, 2015] apresenta um projeto de moeda digital patrocinada pelo estado, o *crypto-dollar*. O trabalho é desenvolvido no contexto da economia norte-americana, mas alguns princípios tecnológicos servem bem ao nosso cenário. Segundo o autor, o *crypto-dollar* apresentaria várias similaridades com o bitcoin, mas algumas modificações seriam necessárias. O autor defende que a atividade de validação (ou mineração) não deve ser feita por qualquer pessoa ou entidade, como acontece no bitcoin. Neste modelo, o governo deveria definir os mineradores da rede, anulando assim o risco de ataque 51 %, e as instituições financeiras seriam responsáveis pela guarda das chaves criptográficas do usuário, papel hoje desempenhado pelas carteiras digitais. Outra diferença citada é a inclusão de regras de conhecimento de clientes KYC e de prevenção à lavagem de dinheiro AML. Atualmente, os protocolos de moeda digital em geral não incluem qualquer tipo de regra de identificação de operadores. Como explicado na seção 2.3, a identificação é feita apenas por meio de chaves públicas e, atualmente, as agências de câmbio estão pouco preocupadas com a origem do dinheiro que compra seus bitcoins.

Uma recomendação interessante feita pelo autor é que a moeda digital patrocinada pelo estado não deve ser uma nova moeda ou uma moeda alternativa a moeda do país, e sim a versão digital da moeda que o pais já possui. No Brasil, isto se materializaria com a

criação do criptoreal ou do bitreal. Esta solução apresenta os benefícios de simplificar a implantação da moeda do ponto de vista econômico e legislativo, e de soar bem mais familiar aos ouvidos da população, diminuindo a resistência do cidadão à nova tecnologia. Por outro lado, elimina um dos grandes benefícios da moeda digital citado anteriormente, a ausência de limites geográficos, fazendo com que a moeda esteja submetida às mesmas restrições jurídicas e pagamento de impostos que a moeda tradicional.

Ao falarmos das limitações impostas ao blockchain por instituições públicas é interessante adicionar dois novos conceitos que ainda não foram apresentados: blockchain permissionado e não permissionado. [Walport, 2016] apresenta estes conceitos da seguinte maneira:

- **Blockchain não-permissionado** - são blockchains que não possuem proprietários, assim como o livro-razão do bitcoin. O objetivo de um blockchain não-permissionado é permitir que qualquer um possa inserir informações na cadeia de registros e que todos em posse dela tenham cópias idênticas. Isto gera uma resistência a qualquer tipo de censura, de modo que nenhum usuário da rede pode impedir uma transação de ser adicionada aos blocos. Os participantes mantêm a integridade da cadeia de blocos alcançando um consenso sobre o seu estado;

- **Blockchain permissionado** - são blockchains que possuem um ou mais proprietários. Quando um registro é adicionado, a integridade do livro-razão é verificada por um processo limitado de consenso. Este processo é realizado por operadores confiados - departamentos de governo ou instituições financeiras por exemplo - o que faz a manutenção da cadeia de registros muito mais simples que no caso de blockchains não-permissionados. A exigência de que diferentes departamentos do governo validem um registro no blockchain gera um nível elevado de confiança quando comparado, por exemplo, com o modelo convencional em que os diferentes departamentos compartilham as informações por meio de papel.

Percebe-se, por estas definições, uma clara tendência do governo britânico pela utilização de blockchains permissionados. De fato, é difícil imaginar a utilização de um sistema tão público, transparente e democrático quanto o blockchain do bitcoin puro na esfera governamental. Contudo, as restrições impostas à tecnologia, como a restrição de

mineradores apresentada nos conceitos acima, devem ser analisadas com muita parcimônia. O resultado de um blockchain restrito a validação de alguns poucos mineradores, escolhidos por interesses escusos, é uma cadeia de registros sem qualquer transparência e nenhuma confiabilidade. O poder do bitcoin de gerar transparência descende de seu caráter fortemente democrático. É preciso cuidado para que as restrições impostas a ele não anulem a própria razão de sua implementação.

Encerra-se esta seção com a citação de um caso de utilização de moeda digital por parte do governo local de uma cidade da Suíça, Zug. A partir de 1 de julho deste ano (2016), cidadãos da cidade de Zug poderão pagar seus impostos utilizando bitcoin. A medida será válida até o fim de 2016, quando o conselho da cidade se reunirá para definir quanto a sua permanência [Fortune, 2016]. A região onde fica a cidade é conhecida como *crypto-valley* devido a grande quantidade de startups ligados à tecnologia de moedas digitais instaladas no local. Trata-se de um projeto piloto em uma cidade de não mais que 100.000 habitantes, mas aponta para a possibilidade de uma nova realidade tecnológica e de inspiração para a adoção da tecnologia em outros lugares do mundo.

3.2 Contratos e licitações com tecnologia de contrato inteligente *(smart contract)*

A principal aplicação do blockchain depois da moeda digital são os contratos inteligentes (do inglês *smart contract*). Contratos inteligentes são linhas de código executadas a partir de transações realizadas no blockchain. São scripts em codificação de baixo nível executados independentemente em cada nó da rede P2P quando uma transação é feita para um endereço específico. Estas transações normalmente carregam informações que são utilizadas pelo script do contrato, que por sua vez, pode realizar um nova transação, consultar um banco de dados, emitir um alerta e etc.

Contratos Inteligentes estão intimamente relacionados com outra área de desenvolvimento tecnológico vista com grande expectativa para os próximos anos: a Internet das Coisas (IoT, do inglês *Internet of Things*), a ideia de ter objetos do dia a dia, como carros e refrigeradores, conectados à internet e comunicando-se de maneira digital. A combinação das duas tecnologias permitiria que a execução de um contrato inteligente ativasse um processo no mundo real, como o destrancamento de uma porta ou o apagamento de uma luz. Um contrato de compra de carro feito no blockchain, por exemplo, poderia automaticamente realizar a transferência do veículo para o novo dono e habilitar o sistema de ignição do carro. De modo simplificado, enquanto o blockchain de uma moeda digital provê uma plataforma para armazenamento descentralizado, o

blockchain de um contrato inteligente provê uma plataforma para computação descentralizada. Pensando em administração pública, algumas maneiras de se utilizar contratos inteligentes para prover transparência são:

- **Controle de percentual de arrecadação a ser designado para uma finalidade específica.** Na legislação brasileira é comum que um percentual da arrecadação de um determinado imposto seja destinado obrigatoriamente para saúde, educação, transporte e etc. A utilização de contratos inteligentes na arrecadação destes impostos permite que a distribuição destes percentuais saiam da gestão humana e seja gerenciada por linhas de códigos publicamente disponíveis;

- **Certificação de cumprimento de cláusulas de contrato.** Uma grande dificuldade na gestão dos recursos públicos é a garantia do cumprimento dos contratos de licitações feitas entre governo e empresas. A utilização de contratos inteligentes em conjunto com uma solução de Internet das Coisas permitiria que o pagamento por um determinado produto fosse feito a partir do resultado de sensores de estoque com tecnologia *Radio-Frequency Identification* (RFID) ou de uma balança digital.

- **Registro de ponto eletrônico de servidores públicos.** A tecnologia de contratos inteligentes pode ser utilizada para registrar e tornar público os horários de trabalho de deputados e demais servidores públicos. Além disso, o pagamento dos salários pode ser realizado automaticamente a partir dos registros de horas trabalhadas.

Existem várias outras aplicações possíveis de contratos inteligentes no âmbito do governo. As seções seguintes apresentam duas aplicações do blockchain que podem ser construídas com ferramentas de contratos inteligentes. Dissemos no começo do trabalho que a mídia e a comunidade acadêmica despertaram recentemente para o valor do blockchain. Muito deste despertamento se deve ao surgimento dos contratos inteligentes e de várias *startups* do ramo.

Dentre as principais plataformas para o desenvolvimento de aplicações de contratos inteligentes na atualidade estão o Ethereum, cujo projeto pode ser acessado pelo GitHub e cuja mineração das transações é feita de maneira pública, como o bitcoin, o Eris e o Clearmatics, que fazem uso de um blockchain permissionado, e o RSK, ainda em implementação, que tem por objetivo adicionar a tecnologia de contratos inteligentes às

transações do bitcoin.

3.3 Votações e leis de iniciativa popular

A tecnologia de blockchain pode ser utilizada para a implementação de eleições, leis de iniciativa popular e demais formas de manifestação do interesse da população.

Ao contrario do que é normalmente dito, as leis de iniciativa popular não são exatamente ‘populares'. Falta um instrumento operacional que autentique as milhares de assinaturas que pedem a criação de uma determinada lei. A lei da Ficha Limpa, tida popularmente como uma lei de iniciativa popular, foi na verdade proposta por um deputado na câmara que acolheu o projeto ao ver uma enorme quantidade de papel trazida à casa, com milhões de assinaturas que não tinham como ser verificadas, assim como aconteceu com a lei Daniella Perez de 1994 [Rais, 2014] e [Coletta, 2014]. Este fator ajuda explicar a pequena quantidade de Leis de Iniciativa Popular no Brasil.

O problema apresentado é um cenário próprio para a utilização do blockchain. Foi dito no inicio do capítulo 2 que o blockchain é uma cadeia de registros imutáveis, públicos e descentralizados. Se cada cidadão registrar seu apoio a um projeto de lei no blockchain, o poder legislativo do país tem condições de verificar e quantificar o apoio da sociedade ao projeto e votar pela sua aprovação. A tecnologia de contratos inteligentes, descrita no item anterior, pode ser usada para criação de uma aplicação que registre a assinatura de cada cidadão participante. O principal desafio à esta implementação está na distribuição de pares de chaves assimétricas aos cidadãos participantes. Como garantir que cada cidadão tenha um e apenas um par de chaves capaz de assinar seu registro no blockchain? Como garantir que estas chaves não serão vazadas e utilizadas de maneira fraudulenta? Em resposta a este desafio, um exemplo em outro lugar do mundo serve como prova de que é possível criar uma cultura de utilização de criptografia em escala nacional de maneira eficiente e segura.

Na Estônia, país com a ICP - Infraestrutura de Chaves Públicas - mais utilizada do mundo, os cidadãos são identificados com um cartão de identificação qual está vinculado seu par de chaves criptográficas, algo parecido com o e-CPF aqui no Brasil. Com esta identidade os cidadãos podem acessar contas bancárias, verificar as notas escolares dos filhos, gravar testamentos, encriptar documentos, assinar contratos e realizar mais uma série de atividades sobre o blockchain. Cidadãos da Estônia ainda podem usar sua identidade digital para acessar os serviços do bitnation.co, uma plataforma para o provimento de serviços de cartório em âmbito internacional, construídos sobre o

blockchain do bitcoin. Nessa plataforma é possível emitir certidão de nascimento e de casamento, contratos de negócio e realizar doações para projetos de ajuda humanitária [Walport, 2016] [Scott, 2016].

Outra possível aplicação da tecnologia no sentido de fortalecer a democracia é a sua utilização para registro dos votos em eleições. A cada eleição cresce a desconfiança da população e principalmente do meio acadêmico com respeito à confiabilidade das urnas eletrônicas. Este é um projeto extremamente difícil de se implementar dada a complexidade do processo eleitoral em um país como o Brasil, mas existem casos de sucesso em processos de votações mais simples na esfera pública em outros lugares do mundo, como na Dinamarca [Dotson, 2014]. Existem diferentes formas de se utilizar o blockchain em uma eleição, algumas consideram o blockchain um substituto à urna ou ao método de votação tradicional em cédulas de papel. Outros consideram o blockchain uma ferramenta complementar a ser usada em conjunto com o instrumento eleitoral principal. [Cometti, 2016] apresenta uma análise de 4 ferramentas de votação existentes ou em implementação ao redor do mundo com respeito à segurança, privacidade, custos e facilidade de adequação. A tabela 3.1 apresenta um resumo da análise:

Tabela 3.1 Comparativo de ferramentas de Votação com Blockchain (Cometti, 2016)

Ferramenta	Funcionamento	Pros	Contras
Blockchain Apparatus	Escaneamento de QRcode em urna off-line e posterior inserção no blockchain.	- Código Aberto; - Pode utilizar tanto o blockchain do bitcoin como o blockchain próprio chamado VoteUnit; - Fácil adaptação do eleitor;	- Não apresenta redução de custo comparado ao modelo tradicional; -Não permite o acompanhamento em tempo real
FollowMyVote	Programa instalado no computador pessoal do eleitor para inserção no blockchain.	- Código Aberto; - Baixo custo de implementação; - Voto pode ser alterado pelo eleitor durante o período da eleição;	- Usuários menos familiarizados com computação pessoal devem ter dificuldade;
V Iniciative	Utilização de Zerocash, variação do bitcoin com alterações de segurança.	- Segurança provida pelo sistema Zerocash; - Baixo custo	- Proposta de implementação não concluída.

		comparado ao modelo convencional;	
BitCongress	Eleitor recebe um token temporário para registrar voto em um blockchain de contrato inteligente do Ethereum.	- Utilização de tecnologias conhecidas como bitcoin e Ethereum; - Plataforma de legislação descentralizada além de realizar eleição	- Custo de transação por voto; - Usuários podem ter dificuldade de se adaptar;

O trabalho ressalta que a tecnologia de votos utilizando blockchain ainda é muito recente e que boa parte das ferramentas apresentadas ainda estão em fase de projeto, o que dificulta uma análise mais exata da eficiência das ferramentas. Fica claro, porém, o potencial que a tecnologia oferece no sentido de fortalecer e autenticar manifestações do interesse popular.

4. Proposta de Simulação de Votação

A simulação a seguir apresenta de maneira simples como a tecnologia do blockchain pode ser útil em um cenário de votação. Para simplificar a simulação e apresentar apenas os aspectos essenciais da tecnologia foi utilizado o próprio blockchain do bitcoin e os registros de voto computados a partir das transações.

Para contextualizar a votação, consideramos um cenário de eleição de representante de turma. A turma conta com 10 alunos votantes e 3 candidatos (incluídos no grupo dos 10 votantes): Bob, Alice e Charlie. A turma deve decidir de maneira democrática e utilizando o blockchain do bitcoin quem será o representante.

A descrição do processo de votação e os resultados podem ser visualizado nas etapas a seguir:

Etapa I - Identificação dos candidatos

Na primeira etapa, cada um dos candidatos recebe uma chave pública e uma representação em QR Code desta chave. Esta chave será utilizada pelos alunos da turma para realizar a votação. A chaves privadas correspondentes dos candidatos não serão utilizadas e devem ser descartadas.

Alice

1Gdnxs3GsdFzJUKiy6cJAs
nVU14RG8xfad

Bob

19XT9GYdU4L9dPjvMLVxNKU9T
MW4SH34qb

Charlie

1DzQA9g7BReCWRCtPfGP74
bJh7RAzQufdc

Etapa II - Identificação dos eleitores

Nesta etapa cada eleitor recebe um par de chaves pública e privada com o qual poderá realizar o seu voto. Serão gerados 10 pares de chaves, a chave pública caracteriza o aluno apto para a votação e a chave privada garante que o aluno assinou o voto enviado.

Para fazer a distribuição das chaves de votação é utilizado um sistema de impressão de chaves em papel, o BitcoinPaperWallet, que funcionará como uma cédula de votação. Nesta cédula está gravada a chave pública e privada do aluno e ele é responsável pela manutenção e privacidade destas informações. Além disso, cada cédula é previamente carregada com 1,1 mBTC para permitir o registro dos votos no blockchain. Uma cédula com o par de chaves é mostrada na Figura 4.1:

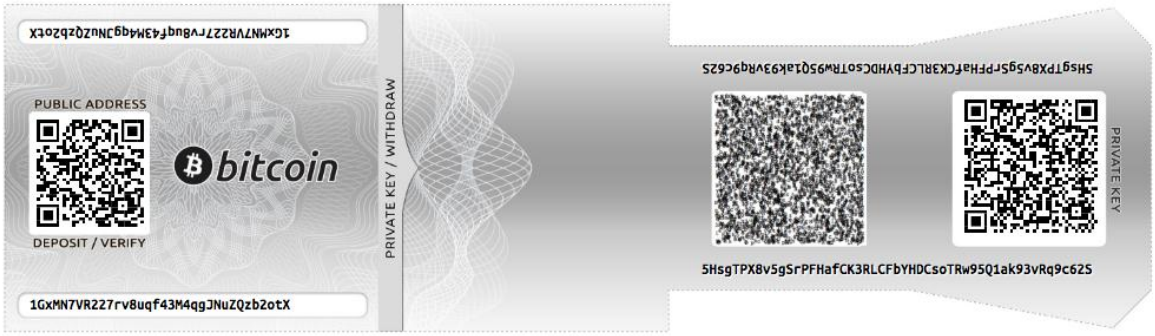

Figura 4.1 Cédula com chave pública e privada (criado com a ferramenta online *BitcoinPaperWallet*)

III. Votação

Após cada aluno receber a sua cédula de votação o processo segue para a etapa de votação. Cada aluno deve utilizar o seu par de chaves pública e privada para realizar uma transação com o candidato em que deseja votar. Nesta simulação, foi utilizada a ferramenta Blockchain Wallet para realizar as transações. A figura 4.2 apresenta informações da transação realizada com a cédula da Figura 4.1, a partir de consulta realizada na ferramenta online Blockchain Explorer.

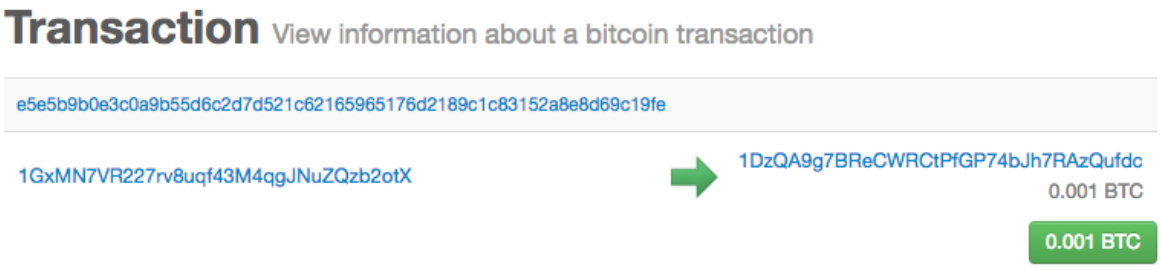

Figura 4.2 Informações da transação no Blockchain Explorer

Percebe-se que o endereço de origem da transação é a chave pública da Figura 4.1 e o endereço de destino da transação é a chave pública do candidato Charlie. O número na parte superior da imagem é o Id da transação obtido a partir do seu hash. Nesta simulação foi utilizado 1 mBTC como valor de referência.

Etapa IV - Resultado e Conferência

Após todos os alunos terminarem de votar, o resultado da votação pode ser obtido a partir de uma consulta ao Blockchain Explorer pelos endereços dos candidatos. A quantidade de transações e de bitcoins recebidos indicam a quantidade de votos de cada candidato. A figura 4.3 apresenta esta relação.

Summary		Transactions	
Address	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad	No. Transactions	4
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.004 BTC
		Final Balance	0.004 BTC

Summary		Transactions	
Address	19XT9GYdU4L9dPjvMLVxNKU9TMW4SH34qb	No. Transactions	1
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.001 BTC
		Final Balance	0.001 BTC

Summary		Transactions	
Address	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc	No. Transactions	5
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.005 BTC
		Final Balance	0.005 BTC

Figura 4.3 Quantidade de Transações e Bitcoins recebidos por cada candidato

O resultado aponta para uma vitória do candidato Charlie com 5 votos, enquanto Alice e Bob obtiveram 4 e 1 votos respectivamente. Uma consulta a todas as transações realizadas nesta simulação de eleição pode ser encontrada no apêndice A.

4.1 Observações

Faz-se agora algumas considerações a partir da observação dos resultados desta simulação.

O blockchain do bitcoin não foi projetado para votação. Trata-se de uma adaptação de um sistema de transação financeira para um sistema de voto. Mas há algumas propriedades desta tecnologia muito úteis em um processo de votação:

- A possibilidade de identificação de cada voto, sem necessariamente identificar o votante;
- A descentralização do processo de verificação dos votos;
- A auditabilidade do processo de contagem dos votos;
- A segurança na autenticidade do voto provida pela criptografia assimétrica;

Talvez, a maior dificuldade de implementação deste processo seja a manutenção e distribuição das chaves criptográficas aos eleitores. Alguns exemplos citados no capítulo 3 mostram que esta não é uma tarefa impossível, mas exige a estruturação de uma ICP eficiente e, em um cenário de eleição nacional, de um trabalho conjunto entre ICP-Brasil e TSE.

Destaca-se ainda que, conquanto o sistema seja bastante simples e necessitaria de grandes adaptações para uma eleição de médio e grande porte, algumas adaptações podem ser feitas para permitir a utilização da tecnologia em eleições menores como eleições de DCE, reitoria, conselhos administrativos e outras eleições realizadas em ambientes internos de organizações. Além disso, adaptações menores permitiriam a sua utilização para assinatura de Projeto de Lei de iniciativa popular pelos cidadãos.

4. Conclusão

A tecnologia do blockchain tem ganhado grande atenção nos últimos anos e, consequentemente, é crescente a quantidade de pesquisas que buscam entender e explorar o seu funcionamento. Existe uma grande expectativa quanto ao impacto que esta tecnologia irá causar nos próximos anos, mas ainda há muito a ser desenvolvido para que o blockchain se estabeleça como uma tecnologia segura e eficiente, tanto do ponto de vista tecnológico, quanto legal e econômico.

Este trabalho buscou explorar o blockchain do ponto de vista tecnológico, apresentando o contexto do seu surgimento, o seu funcionamento, a teoria de computação e redes de comunicação subjacente e as principais aplicações na esfera da administração pública.

A divisão do trabalho em etapas ajudou a alcançar os objetivos propostos permitindo uma abordagem equilibrada entre a teoria apresentada no capítulo 2 e as aplicações práticas do capítulo 3. Buscou-se entender primeiramente os fundamentos da tecnologia, como criptografia assimétrica, função de hash e assinatura digital, passando em seguida para o funcionamento da tecnologia e os aspectos de segurança e, por último, às aplicações do blockchain no contexto de transparência. A pesquisa bibliográfica demonstrou como a tecnologia ainda apresenta pontos controversos, como a regra de maior cadeia e a utilização de blockchains permissionados/não-permissionados. Outra conclusão feita a partir da revisão bibliográfica é que o desenvolvimento da tecnologia acontece de maneira muito globalizada, com várias frentes de pesquisa ao redor do mundo, mas pouca produção acadêmica em língua portuguesa.

As aplicações apresentadas mostram que a utilização da ferramenta para provimento de transparência e confiabilidade é um campo promissor, mas é preciso cautela, pois trata-se de uma tecnologia recém-nascida, carente de regulação específica e estudo acadêmico. Algumas restrições, como as regras de KYC e AML, são fundamentais para a utilização do blockchain de maneira institucionalizada pelo governo e apesar de todos os benefícios propostos com a utilização da tecnologia, o blockchain não pode resolver todos os problemas de transparência na administração pública.

Com todos os desafios, o blockchain permanece como uma ferramenta com grande potencial a ser explorado. Os dois movimentos citados no começo do trabalho, crescente demanda por maior transparência pública e o interesse global na tecnologia blockchain, não devem diminuir os passos tão cedo e o cenário é promissor para o desenvolvimento de aplicações que realizem essa integração.

4.1 Trabalhos Futuros

Alguns trabalhos futuros podem ser desenvolvidos a partir das ideias apresentadas neste trabalho.

Um estudo específico sobre segurança pode analisar questões como adaptação às regras de KYC e AML, vulnerabilidades relacionadas à pseudo-aleatoriedade na geração de chaves público/privada e ajustes no processo de mineração que reduzam o risco de ataques 51%.

Um trabalho que estude as vantagens e desvantagens em se utilizar blockchains permissionados e não-permissionados, explorando os riscos envolvidos em cada um dos casos, deve ser de grande utilidade para a adoção da tecnologia no meio público.

A utilização de moedas digitais é um tema bastante complexo. Uma análise da criação da versão digital do real, comparando com a criação de uma nova moeda oficial, ou até mesmo com o bitcoin, é de grande benefício para o desenvolvimento da tecnologia.

Existem várias ferramentas de desenvolvimento de aplicativos sobre o blockchain, principalmente com utilização de contratos inteligentes, e novas ferramentas estão surgindo a cada dia. Neste contexto, pode-se realizar um estudo de comparação destas ferramentas, explorando as vantagens e desvantagens de cada uma e em que áreas cada uma delas pode ser melhor aproveitada.

Por último, ressalta-se que o blockchain é uma tecnologia com grande relevância para às áreas de economia e direito. Um estudo feito de maneira colaborativa entre pesquisadores da área de tecnologia com pesquisadores destas duas áreas tem muito a contribuir para o desenvolvimento do blockchain.

REFERÊNCIAS BIBLIOGRÁFICAS

Antonopoulos; Antonopoulos, Andreas M. (2014). “Mastering Bitcoin - Unlocking Digital Cryptocurrencies”. Ed. O’Reilly Media. ISBN 978-1-449-37404-4. 15-28

Aranha *et al*; Aranha, Diego F., Karam, Marcelo M., Miranda, André de, Scarel, Felipe. (2013) "Vulnerabilidades no software da urna eletrônica brasileira”. Departamento de Ciência da Computação - Universidade de Brasília. Versão 1.0.2. 31 de março de 2013. 13-19.

Barber *et al*; Barber, Simon; Boyen, Xavier; Shi, Elaine; Uzun, Ersin. (2012) “Bitter to better—how to make bitcoin a better currency”. Palo Alto Research Center, University of California, Berkeley. 2-3

Coletta; Coletta, Ricardo Della. (2014) “Iniciativa Popular não pegou”. Reportagem do jornal Estadão em 15/09/2014. Disponível em: http://politica.estadao.com.br/noticias/eleicoes,iniciativa-popular-nao-pegou-imp-,1560343. Acessado em: Junho/2016.

Courtois; Courtois, Nicolas T. (2014) "On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies”. University College London, UK

Rais; Rais, Diogo. (2014). "Iniciativa popular à brasileira”. Texto publicado no site JusBrasil. Disponível em: http://diogorais.jusbrasil.com.br/artigos/121933824/iniciativa-popular-a-brasileira. Acessado em: Junho/2016.

Dotson; Dotson, Kyt. (2014) “First political party to use blockchain for e-voting is from Denmark”. Bitcoin Weekly 2014 May 7. The Rise of Digital Currency, Bitcoin’s niche in developing economies. In: SiliconANGLE.

Eckenrode *et al*; Eckenrode, Jim; Srinivas, Val; Rotatori, Denise. (2015) “State-Sponsored Cryptocurrency: Adapting the best of Bitcoin’s Innovation to the Payments Ecosystem”. Deloitte Development LLC.

Eyal e Sirer; Eyal, Ittay; Sirer, Emin G. (2014) “Majority is not enough: Bitcoin mining is vulnerable”. Department of Computer Science, Cornell University, Nova York, USA.

Handerson; Hankerson, Darrel; Menezes, Alfred; Vanstone, Scott. (2006). "Guide to elliptic curve cryptography. Springer. Nova York, USA. ISBN 0-387-95273-X.

Impagliazzo; Impagliazzo, Russell. (1989) “One-way functions are essential for complexity based cryptography”. Dept. of Math., California Univ., Berkeley, CA, USA. ISBN 0-8186-1982-1.

Johnson *et al*; Johnson, Don; Menezes, Alfred; Vanstone, Scott. (2001) “The elliptic curve digital signature algorithm (ECDSA)”. International Journal of Information Security. August 2001, Volume 1, Issue 1, 36-63.

Joshua *et al*; Baron, Joshua; O'Mahony, Angela; Manheim, David; Dion-Schwarz, Cynthia. (2015) "National Security Implications of Virtual Currency - Examining the Potential for Non-state Actor Deployment". Published by the RAND Corporation, Santa Monica, Calif. ISBN: 978-0-8330-9183-3

Koshi *et al*; Koshy, Philip; Koshy, Diana; McDaniel, Patrick. (2014) "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic". Pennsylvania State University, University Park, PA 16802, USA.

Krombholz *et al*; Krombholz, Katharina; Judmayer, Aljosha; Gusenbauer, Matthias; Weippl, Edgar. (2015) "The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy?". SBA Research, Vienna, Austria.

Nakamoto; Nakamoto, Satoshi. (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System".

Narayanan *et al*; Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven. (2016) "Bitcoin and Cryptocurrency Technologies". Princeton University Press - A priori. 23-40.

Cometti; Cometti, Natália P. V. (2016) "Um estudo sobre a tecnologia blockchain e sua aplicação em sistemas de votação." Universidade Federal de Pernambuco, 25-34.

NIST; National Institute of Standards and Technology. (2015). "FIPS PUB 180-4 Secure Hash Standard (SHS)". Federal Information Processing Standards Publication. August, 2015.

Torres; Torres, Osman X. J. (2013) "Tecnologias de suporte ao conceito de criptomoeda". Universidade Federal de Pernambuco. Centro de Informática. Recife, 2013. p. 13.

Poole; Poole, Bernard J. (2003) "Pretty Good Privacy - A Tutorial for Beginners to PGP". University of Pittsburgh at Johnstown, Johnstown, PA, USA.

Salomaa; Salomaa, Arto. (1996) "Public Key Cryptography". Ed. Springer 2a Ed. ISBN 978-3-642-08254-2. 55-71.

Scott; Scott, Brett. (2016) "How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?". "Prepared for the UNRISD Workshop Social and Solidarity Finance: Tensions, Opportunities and Transformative Potential" in collaboration with the Friedrich-Ebert Stiftung and the International Labour Office. UNRISD, Palais des Nations 1211 Geneva 10, Switzerland. 12-15

Taylor; Taylor, Simon. (2015) "Blockchain: understanding the potential". Item Ref: BM408383. July 2015. 2-4.

UK Gov; HM Treasury - UK Government. (2015) "Digital currencies: response to the call for information". ISBN 978-1-910337-91-2.

Valente; Valente, Luiz. (2015) "PF toca 9.400 inquéritos sobre desvios de verba pública". Reportagem do jornal Folha de São Paulo em 09/12/2015. Disponível em: http://www1.folha.uol.com.br/poder/2015/12/1717091-pf-toca-94-mil-inqueritos-sobre-desvios-de-verba-publica.shtml. Acessado em: Junho/2016.

Walport; Walport, Mark. (2016) “Distributed Ledger Technology: beyond block chain”. A report by the UK Government Chief Scientific Adviser. Information Policy Team, The National Archives, Kew, London TW9 4DU. 65-71.

Wang *et al*; Wang, Ping; Aslam, Baber; Zou, Cliff C. (2009) “Peer-to-Peer Botnets”. School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, Florida 32816.

Wood; Wood, Gavin. (2014) “Ethereum: a secure decentralized generalized transaction ledger”. Ethreum and Ethcore. Homestead Revision. 1-14.

APÊNDICES

APÊNDICE A – TRANSAÇÕES E ENDEREÇOS DE CHAVES PÚBLICAS UTILIZADOS NA SIMULAÇÃO DO CAPÍTULO 4

A tabela A1 apresenta os ID's, endereços de origem e destino de todas as transações realizadas na simulação de processo de votação. Os valores podem ser utilizados para consulta na ferramenta Blockchain Explorer, encontrada no endereço https://blockchain.info.

Tabela A1 - Id, Origem e Destino de transações da simulação

	Transação	Origem	Destino
1	c37a6f99a12f7e6d1551badb9e0b6a5a85e8497ebabc687275aa3fe0f1af6ef0	1JPsjF593orH5YTHRSY9JG4L5yh7W9EAAy	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad
2	b19a00e4d073d9d3343aacbf4ec6462c8beec6669935d27514d9177fcf540b9a	1FwUqTAqbqtkvwfDTdMZF2Sg78E2m1LLhd	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad
3	d3984469fd1ff8130d9f36fe8d5c1559e324bef79bfe94c87ad7a8f9193dcdad	16jRHpQdeRGDxQS7g5qQioYhHL7NQeEHeC	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad
4	140d7ea0012f99420dc6309efc219a6f953ea1e1b6faed7de4fcdc60d560475a	19MbGcn87m1Lk7qb9oGV6CaEo9bEoTyEXq	1Gdnxs3GsdFzJUKiy6cJAsnVU14RG8xfad
5	ccbaefc05f62a33c17c1ace18d9b0fa5100794226db7c208f354a258c79a318f	15F5skfGaDLNiQJqgz9x4PMuSwW1UAxiyZ	19XT9GYdU4L9dPjvMLVxNKU9TMW4SH34qb

6	356be81b5ebfb7948c9ed131494fe66528fdd8448cfdd57add769d20b123c4f3	1FvmV5a9mND7bUmmntBBDiVgQgjXYswRTZ	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc
7	4242d9219d8f4381c9990c4528d524fbe4504637f2ad9936fb5d126ff4968ed5	1NSiKSvuDrxej85ppkAaiZQJjxkiCCiezf	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc
8	964d3019b1aff0acf112501fe095f534ba16ca7175fc72ba114444001d93cb0f	18AHhziZjdNympfvy7PmirF1bgemi4XqiW	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc
9	d5f221286567cafe8c1724d69afeccbfed43c1f788413bf97bda406e09eba9e5	1Gt9ScKv89weHdzUWUG2xAi3DdTGmKfHXj	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc
10	e5e5b9b0e3c0a9b55d6c2d7d521c62165965176d2189c1c83152a8e8d69c19fe	1GxMN7VR227rv8uqf43M4qgJNuZQzb2otX	1DzQA9g7BReCWRCtPfGP74bJh7RAzQufdc