PERCEPÇÕES DE COLABORADORES DE CERTIFICAÇÃO DIGITAL ACERCA DAS INFLUÊNCIAS DA CRIAÇÃO DE UMA IDENTIDADE DIGITAL BASEADA EM BLOCKCHAIN NO COMÉRCIO DE CERTIFICADOS DIGITAIS

João Marcos Ramos[1]*

Prof. Esp. Rafael Hungaro Cabral[2]*

RESUMO

O intuito da presente pesquisa é analisar a criação de uma identidade digital baseada em *blockchain,* e como pode afetar o comércio de certificados digitais. Com esta análise, se determina que a implementação do ID em *blockchain,* feita da maneira correta, pode ser mais segura, e gerar um custo menor para o cliente final, descentralizando o esquema hierárquico criado pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). A pesquisa foi feita no intuito de observar como é vista a implementação de uma ID digital baseada em *blockchain* pelos funcionários/empreendedores e usuários de certificados digitais, e qual sua perspectiva de como isso afeta o comércio da certificação digital. Em um questionário embasado em questões de comércio e segurança diante das duas tecnologias, certificação digital e *blockchain*, sendo feita na cidade de Formiga, em Minas Gerais. Os resultados foram satisfatórios, foi possível observar alguns detalhes a mais sobre a certificação digital, a necessidade de inovação em métodos e novas tecnologias e com a implementação do *blockchain* como identidade digital afeta diretamente o comércio da certificação digital, fazendo com que ela tenha que se reinventar para acompanhar a tecnologia do *blockchain*.

Palavras-chave: Certificado Digital. *Blockchain*. Identidade Digital. Comércio.

1 INTRODUÇÃO

A cada passo que a Tecnologia da Informação e Comunicação (TIC) evolui, surge uma real necessidade de estar mais conectado virtualmente e consequentemente gerando mais

[1]* Graduando em Sistemas de Informação pelo Centro Universitário do Sul de Minas - Unis - MG, jmramos625@gmail.com.

[2]* Graduado em Ciência da Computação. Especialista em Engenharia de Sistemas pelo CEFET-MG. Docente no Centro Universitário do Sul de Minas.

dados nessa rede mundial. Com o aumento da globalização e esse avanço tecnológico, se torna necessário as empresas buscarem o melhor dessa tecnologia, para buscar os seus resultados positivos e consequentemente vantagens sobre a concorrência(SOUZA; RIGUETTO; SOUZA; DAHI, 2017).

Todos esses dados que armazenamos nesta rede acabam gerando mais informações sobre os cidadãos. Torna-se então necessária a segurança dos dados que podem ser acessados a qualquer momento de qualquer dispositivo, desde que tenha um usuário e senha já cadastrados em um banco de dados de algum serviço qualquer na internet.

Nesse momento é necessário pensar em novas soluções de como proteger os dados, mas também poder continuar a usufruir de todos os benefícios da internet. Para aumentar a proteção, atualmente o modo de identificação digital mais utilizado é o Certificado Digital, que é utilizado em escala exponencial. Dados do ITI demonstram que no ano de 2017 entre janeiro e setembro foram emitidos 2.693.298 certificados de CPF e CNPJ(ITI, 2017), que podem ser utilizados em forma de arquivo (A1) ou em *tokens*/cartões (A3) (SOUZA; NETO, 2017).

O uso crescente de certificados digitais atrai pessoas mal intencionadas, aumentando cada vez mais o ataque de *hackers*. Por mais que os Certificados Digitais usem de criptografia, utilizando chaves privadas e públicas e um sistema também centralizado que tem como base o ICP-Brasil que é a AC (Autoridade Certificadora) Raiz. No ramo as suas conseguintes, que são as AC de 1º nível, AC de 2º nível e a AR (Autoridade de Registro), podem ter uma maior taxa de ataques, principalmente de engenharia social.

Com o método *Blockchain*, é possível colocar essas informações de forma totalmente descentralizada, gerando uma maior segurança das informações do cidadão, sobretudo quando não se armazena os dados dos documentos em si, como CPF, RG, mas informações como serviço, hábitos. Quanto maior a cadeia e mais tempo o dado se encontra na cadeia do *blockchain*, maior a segurança da sua informação (NAKAMOTO, 2008). O *Blockchain* já vem sendo implementado em vários serviços privados e como identificação de cidadãos por governos ao redor do mundo, como as empresas *OriginalMy*, *OpenBadge* e Kryptus.

Buscar o entendimento sobre como uma identidade baseada em *blockchain* pode afetar de forma direta o comércio de certificados digitais, trazendo uma nova forma de trabalho, implementação dessa identidade inovadora, aumento exponencial da segurança da identidade digital. Pelo fato de ser totalmente descentralizada, trazer consigo preços mais acessíveis, logo

pode se tornar uma identificação usada em qualquer local, apenas com um dispositivo. Assim, a presente pesquisa pretendeu analisar como os funcionários de empresas de Certificados Digitais entendem essa chegada da identidade baseada em *blockchain* e como isso afetaria seu dia a dia e qual o seu conhecimento sobre *blockchain*, buscando no final ver quais são as vantagens e desvantagens dos certificados digitais e como a identidade em *blockchain* entraria nesse cenário.

2 IMPLEMENTAÇÃO DA IDENTIDADE DIGITAL

Com a evolução da tecnologia da informação, e como ela se integra no ambiente social e empresarial, a identificação dos usuários nessas plataformas vira algo crucial, desde simples aplicativos de redes sociais e jogos, até cadastro de empresas em sites governamentais. Partindo desse ponto é necessário algo que identifique os indivíduos e empresas em todos os âmbitos e aplicações atuais, nisso foram criadas novas rotinas e consequentemente novas exigências do governo para a utilização de identidades digitais por exemplo (ALMEIDA FILHO, 2015).

Com a possibilidade de tanto uma empresa precisar se conectar a uma rede social simples até um cidadão comum fazer seu cadastro como pessoa em sites do governo, o método como é feito esse cadastro é muitas das vezes inseguro e até criminoso. Qualquer pessoa, de posse de dados pessoais de alguém, pode abrir uma conta em qualquer tipo de site com apenas alguns cliques.

Nesse pensamento de segurança da informação do cidadão e/ou sua empresa, foram implementados novos métodos de identificação digital. O principal nos dias de hoje é conhecido como Certificado Digital, por meio do qual é criada uma assinatura digital implementada em um arquivo, token ou cartão para que o usuário possa utilizar como acesso, assinatura e outras formas de identificação.

2.2 CERTIFICAÇÃO DIGITAL

No ano de 1996 foi implementado o ramo de Certificação Digital no Brasil, com origem na empresa Certisign (CERTISIGN, 2017), foi também designada uma das três

plataformas de Infraestruturas de Chaves Públicas (ICP). Posteriormente em 2001, com a criação da ICP-Brasil (art. 1º, da MP 2.200/01), a empresa que gerencia as chaves públicas, criou uma hierarquia para que as empresas disponibilizassem essas certificações digitais, permitindo sua validação.

Segundo o Comitê Gestor da Internet no Brasil (CGI, 2017), com o aumento exponencial de vários meios de comunicação digital e o acréscimo dos dados gerados nessas plataformas geraram uma grande mudança que afetou diretamente o Brasil e se fez necessária a apresentação das estratégias de melhoria.

De acordo com a Medida Provisória 2.200-2, de 24 de agosto de 2001, se inicia no Comitê Gestor de autoridade máxima que fiscaliza e aprova as normas determinadas pela Autoridade Certificadora (AC) Raiz, que é o Instituto Nacional de Tecnologia da Informação (ITI). No grau inferior vem as AC's de primeiro nível, que se responsabilizam por autenticar, emitir, revogar e gerenciar os Certificados digitais de AC's de segundo nível. Em seguida vem as AC's de segundo nível, basicamente fazem o mesmo que a AC de primeiro nível, porém já do certificado do usuário final. Por fim se encontra a Autoridade de Registro (AR) que tem a responsabilidade de identificação direta do usuário final, como documentos, fotos, digitais e outros, com isso fazendo a solicitação e emissão de certificados digitais.

Para que seja seguro, é necessário que o certificado possua uma criptografia que proteja todos os dados presentes nele, pois como dito anteriormente é feita a coleta de fotos, digitais, documentação e afins. Seguindo essa linha de raciocínio é feita diretamente pela ICP-Brasil um tipo de criptografia determinada como assimétrica, que consiste em uma chave pública e privada(MONTEIRO; MIGNONI, 2007).

Por esse fato que se chama Infraestrutura de Chaves Públicas, pois é a própria ICP que faz a liberação dessas chaves para que possam ser feitos os certificados digitais (MONTEIRO; FAORO; ABREU; SILVA, 2018).

A criptografia assimétrica funciona com duas chaves: uma pública e outra privada, com isso uma é feita para ler os dados que a outra gera. A chave pública é gerada para todos aqueles que querem mandar algum tipo de documento para assinar, ou algum tipo de local para acesso com certificado digital. Quando o portador da chave privada, a qual fica apenas com o usuário, recebe algum tipo de solicitação com a chave pública relacionada a sua chave privada, ele poderá descriptografar usando-a. Se observa que nesse método apenas o portador

da chave privada específica da chave pública disponibilizada, poderá descriptografar tal mensagem (HARTMANN JUNIOR, 2009).

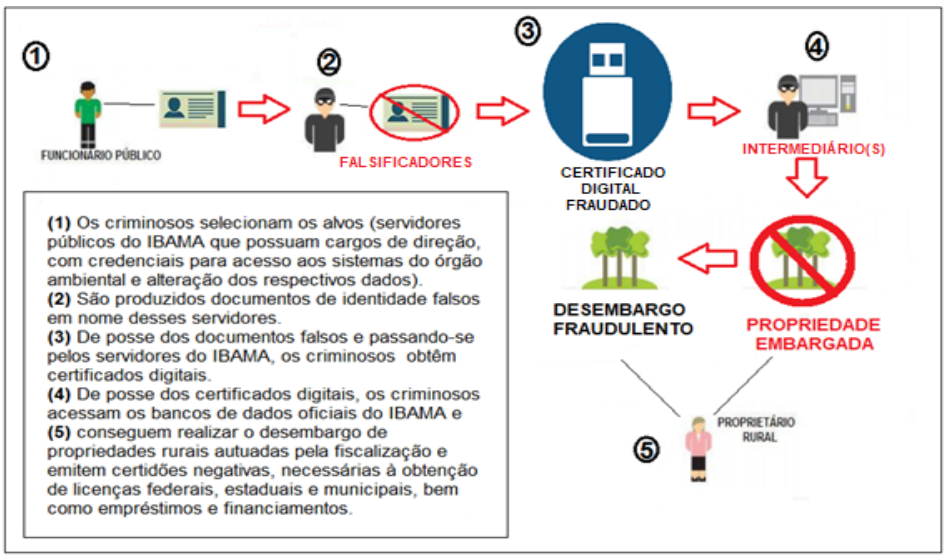
Porém, esses certificados são classificados de quatro maneiras: A1, A2, A3, A4, sendo os mais comuns e comercializados os modelos do tipo A1 e A3, que “A” determina a classe o número determinada a segurança (HARTMANN JUNIOR, 2009). O modelo de A1 é do tipo arquivo, onde é criado um arquivo de extensão “.pfx” que é a extensão do certificado, que é instalado com uma senha diretamente na máquina do cliente, ficando armazenado nos certificados da máquina. O tipo de certificado A1 pode ser usado simultaneamente em várias máquinas, desde que se tenha a senha criada para a instalação do certificado.

Conforme Hartmann Junior (2009) o certificado do tipo A3 é feito em um hardware, pode ser um cartão, que é necessário um leitor na máquina para seu funcionamento, ou do tipo token, no qual se assemelha a um pendrive, quando se insere na máquina é necessário a instalação de um driver específico para o reconhecimento do certificado digital. Ainda existe outro método do tipo A3 que é o certificado em nuvem, no qual se usa uma plataforma que gera um código de autenticação rotativo para que seja usado no seu acesso ou assinatura digital.

Apesar de a criptografia apresentada na Certificação Digital ser uma das melhores e bem robustas, ainda se pode ver falhas em seu andamento, desde a parte da emissão dos certificados, até a parte de usabilidade. Quando se vai emitir um certificado, todos os dados apresentados pelo cliente são vistoriados e conferidos por uma Central de Verificação, que é um grupo de pessoas treinadas que verificam a veracidade de todas as informações. Mesmo que com muito treinamento, algumas informações, tanto por descuido, quanto por complexidade de documentação apresentada, podem passar despercebidas(ZATARIN; SILVA; PIACENTE, 2020).

Como dado no exemplo da imagem abaixo, certos fraudadores usaram de dados de servidores públicos para acesso de informações sigilosas do banco de dados do IBAMA, com o intuito de beneficiar certos proprietários rurais, gerando um prejuízo de cerca de R$150 milhões (GOV.BR, 2020).

Figura 1 - Sistema de Fraude com Certificação Digital



Fonte: Gov.br (2020)

Quando se cria um certificado do tipo A1, no qual precisa apenas da senha para instalá-lo em sua máquina, é um arquivo pequeno que se pode passar por e-mail, aplicativos de conversas e até por pendrive. Considerando essa facilidade, caso esse arquivo seja capturado e possua senha, ele poderá ser instalado em qualquer computador até que vença o prazo de validade ou seja revogado.

Caso um certificado chegue para uma pessoa que está buscando fraudar o sistema, ela pode causar vários problemas para o titular dos documentos. Com um certificado digital, pode-se abrir e fechar empresas, empregar e demitir funcionários, assinar contratos, assinar procurações e dentre outros piores tipos de fraudes que o mesmo pode fazer (GOV.BR, 2020).

Outro caso é apontado pelo Tribunal Federal Federal da 3ª Região, em que dois indivíduos usaram de meios tecnológicos para *hackear os* dados de cidadãos que tinham acesso ao sistema Processo Judicial Eletrônico (PJe). O PJe é bastante acessado por advogados e outros trabalhadores do ramo, que possuem acesso a informações críticas, com esses certificados os *hackers* acessaram vários documentos e fizeram várias alterações para vantagem pessoal (TRF3, 2021).

Sendo o *blockchain* uma tecnologia que gera muita segurança em seus dados, e como também é usado em várias outras aplicações além de moedas digitais, como sistemas de pagamentos, contratos inteligentes, educação, supply chain e saúde. Podendo assim o *blockchain* trabalhar em várias vertentes, ele foi implementado na identificação digital, como

por exemplo na empresa *OrignalMy*, onde é feito o cadastro podendo ser físico ou jurídico, de forma totalmente gratuita onde se paga apenas pelo uso da assinatura (IBM, 2021).

2.3 BLOCKCHAIN

O *Blockchain* foi criado em conjunto com o Bitcoin, que é um moeda que visa a transferência de dinheiro entre duas partes de forma online, sem a necessidade de um terceiro para intermediar e garantir a segurança da informação, gerando praticidade e segurança. Com isso era necessário um sistema de pagamento que fosse baseado em criptografia, no lugar da confiança de um terceiro, podendo as duas partes se comunicarem diretamente sem nenhuma interferência (NAKAMOTO, 2008).

É criado, assim, o *blockchain*, o sistema que é feito por meios computacionais onde todos os dados neles inseridos se tornam imutáveis conferindo assim uma maior veracidade de seus dados e poder posteriormente conferir essas informações baseados em um carimbo de data e hora que é feito pelos processadores e gerando assim a ordem cronológica de cada uma das transações feitas (NAKAMOTO, 2008).

Baseado em um banco de dados, o *blockchain* se caracteriza pelo fato de não ser possível alterar os dados nele inseridos, configurando assim a melhor veracidade possível, onde o que se encontra nele se torna verdade, feito pela validação de cada bloco. Como forma de recurso de segurança, o *blockchain* é feito de forma descentralizada, sem um controle central, pois não há nenhum órgão que regulamenta, tirando assim também taxas sobre o usuário (BATISTA, 2018 apud NAKAMOTO, 2008).

O funcionamento do *blockchain* baseado no bitcoin é feito de forma simples. Primeiramente, ele cria o registro da transação feita de uma pessoa para a outra, determinando destinatário, remetente e quantia, assim sempre preservando a identidade dos envolvidos. Na sequência é colocado em incógnito o dono da carteira, mas não o endereço dela, ambos os usuários participantes da transação, criando assim a primeira criptografia, gerando assim a chave privada deles (FRAJHOF, 2019). Depois é necessário que seja feito uma análise da transação e a dê validade, é feita agora pela parte dos mineradores, que são as máquinas que resolvem os problemas matemáticos complexos para que seja feita a validação das transações. A validação é feita de 10 em 10 minutos, podendo ter uma variação de acordo com o tamanho da rede. Assim é criado a identificação da transação, que é totalmente criptografada.

Para que os blocos criados a cada cadeia de blocos, que é gerado a cerca de 10 minutos, podendo variar, não sejam alterados por qualquer um com acesso a esses dados, é necessário que seja criado uma criptografia desse conjunto de blocos, criando uma criptografia final juntando a do bloco atual com a do anterior (MIRANDA, 2018). Assim, para que se possa fazer alterações no *blockchain*, podem ser utilizados o *SoftFork* ou o *HardFork*, que são utilizados para se fazer modificações simples ou até mesmo grande alterações que podem mudar o rumo do *blockchain*.

O *SoftFork* cria uma bifurcação nos blocos criando algumas pequenas atualizações para que se otimize a segurança, já o *HardFork* é utilizado para grandes alterações no protocolo do *blockchain*, onde muita das vezes cria uma nova cadeia de blocos como uma nova regra derivada da anterior.

Baseado nisso, percebe-se que quanto maior a cadeia de blocos gerados no *blockchain*, menor a probabilidade de alterações em seus dados, pois seria necessário a descriptografia final criada com o bloco anterior, a do bloco atual e a do anterior a esse, sendo assim uma segurança praticamente exponencial.

Serviços já existentes atualmente como os da empresa OriginalMy, já utilizam da tecnologia *blockchain* para assinaturas de contratos e documentos até provas de autenticidade de conteúdos digitais como músicas, e-books, games, códigos fonte, segredos comerciais e dentre outros. A criação de uma certificação em *blockchain* é totalmente gratuita, desde a apresentação dos seus dados como RG, CPF, comprovante de endereço e outros, até a criação da chave de acesso da sua identificação.

Como temos a criação de uma identificação totalmente gratuita, a partir do momento onde as empresas começarem a aceitar o login utilizando essa certificação, poderemos ter um acesso bem mais seguro e eficaz e com certificados totalmente criptografados. Os gastos com certificação em *blockchain* vem com as assinaturas e serviços prestados usando essa identificação.

Na OriginalMy, os pagamentos são feitos por cada assinatura usada, sendo assim, além de não ter uma validade onde na certificação digital é necessário a renovação após o fim da validade, você paga apenas pelo uso efetivo da assinatura digital em *blockchain*. Os planos de assinatura em novembro de 2021 na OriginalMy, são de R$13,50, para a assinatura somente, R$14,80 para uma assinatura e pode ser usada também para um PACDigital (Prova de Autenticidade de Conteúdo Digital) (ORIGINALMY, 2021).

Além de poder ser usada por cada assinatura, ela oferece também outros serviços, nos quais estão incluídos PACDigital e o PACWeb, que são programas de autenticidade de conteúdo, no caso do Web, ele autentica posts em sites e mensagens em chats privados como Whatsapp, Telegram e outros. Essa identidade em *blockchain* também possui serviços como OMyPass e KYC, sendo o OMyPass um tipo de autenticação para acesso de sites e lugares sem a necessidade de cadastro, documentos ou login e senha e o KYC um tipo de averiguação de antecedentes de clientes e organizações.

3 MATERIAIS E MÉTODOS

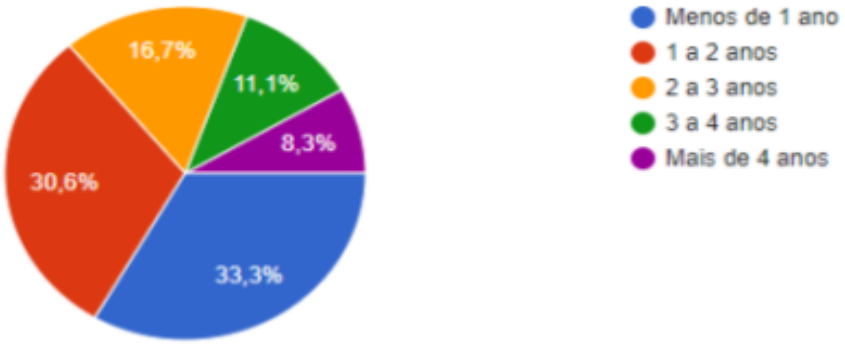
Para se obter um olhar mais profissional e voltado para os trabalhadores da área de certificação digital, acerca de tecnologia usada em certificação digital e seu conhecimento sobre *blockchain*, foi aplicado um questionário (APÊNDICE A), no qual teve uma abordagem técnica, visando o olhar para dentro da empresa e seus funcionários.

Esse questionário foi direcionado para pessoas que já trabalham no ramo da certificação digital, essas tendo um maior entendimento sobre o assunto, onde foi observado quais são as maiores dificuldades e importâncias para o meio de assinatura digital atual, e qual sua opinião sobre o surgimento do ID *Blockchain*, verificando qual terá maior predominância no futuro.

4 RESULTADO E DISCUSSÃO

A pesquisa foi realizada na cidade de Formiga, Minas Gerais, com 36 entrevistados. Todos que responderam ao questionário foram ou são colaboradores de empresas de Certificados Digitais. Percebe-se que a maioria dos entrevistados trabalham até no máximo 2 anos no ramo, o que indica como a certificação digital na região ainda é nova.

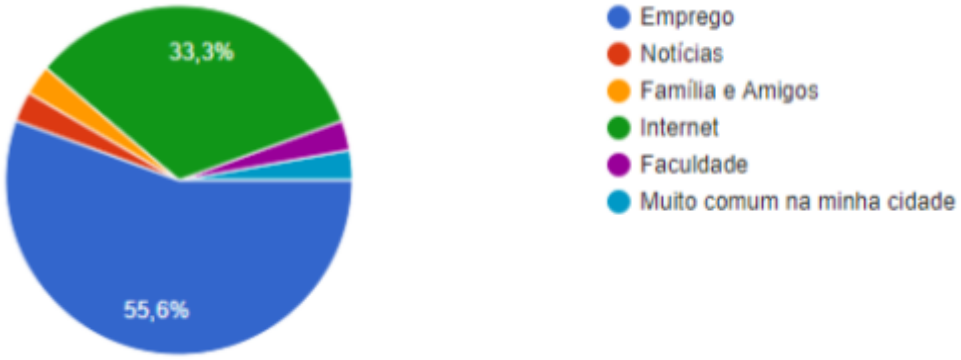
Gráfico 1 - Tempo de trabalho com certificado digital.



Fonte: elaborado pelo autor

Baseando-se em colaboradores, também é possível observar que a maioria deles tiveram o conhecimento de certificação digital através de seus empregos, o que mostra que por maior que seja sua força com identidades digitais, além de ser nova na região, ela possivelmente possui uma divulgação ainda baixa.

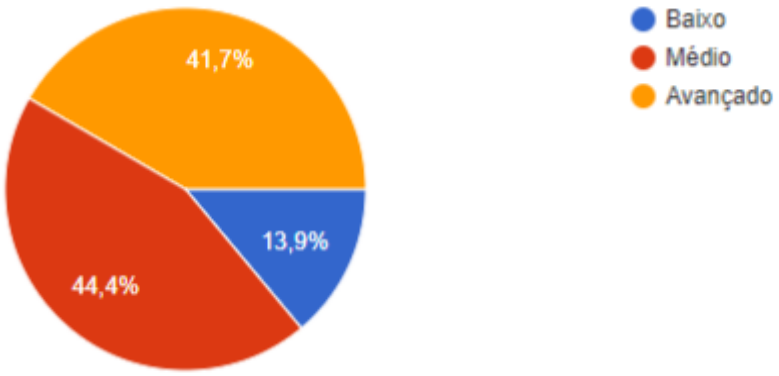
Gráfico 2 - Como conheceu o certificado digital.



Fonte: elaborado pelo autor

Para ingressar em uma empresa de certificação digital, os colaboradores passam por um treinamento sobre todo o processo da certificação. Esse treinamento é exclusivo para eles e alguns até específicos para suas funções, começando com o funcionamento do certificado, a criptografia assimétrica, o entendimento da hierarquia da ICP-Brasil, indo desde a AC-Raiz, passando pelas AC's até chegar na AR. Ainda é apresentada toda a parte de emissão do certificado, documentação, fotos e biometria e colocar a assinatura digital e suas cadeias dentro do certificado, caso do tipo A3.

Gráfico 3 - Nível de conhecimento em certificados digitais.

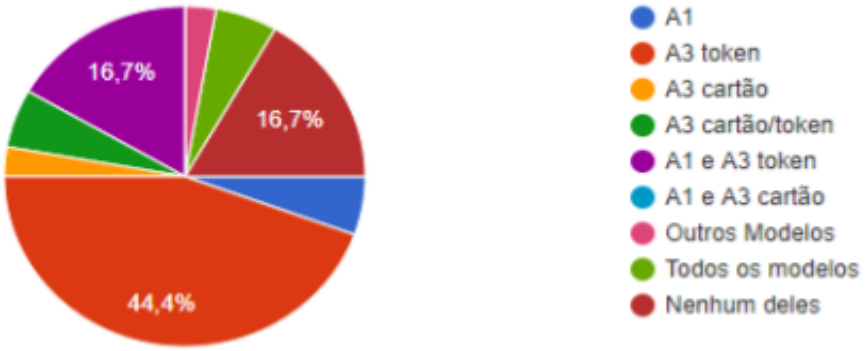


Fonte: elaborado pelo autor

Apesar do treinamento obrigatório na empresa, ainda se percebe que menos da metade dos entrevistados têm pleno conhecimento sobre a certificação, o que traz um pouco da complexidade em algum dos seus processos até a emissão para o cliente. Os treinamentos são iguais para todos os colaboradores, o que pode trazer a ideia da dificuldade para se trabalhar com certificação digital, se observar que 58,3% dos funcionários não têm conhecimento avançado.

Podemos encontrar vários tipos de certificados, desde os mais comuns como A1 e A3, podendo o A3 ser em token ou cartão, e atualmente os certificados em nuvem, mas pode-se ver que o modelo mais utilizado é o A3 em token. Além da maior compatibilidade com os sistemas que usam certificados digitais, o A3 é o mais seguro e prático entre os demais. Nem todos os colaboradores precisam de um certificado digital, com isso pode ser que nem todos, dependendo de sua função, podem ter uma certificação digital.

Gráfico 4 - Tipos de certificados mais usados pelos colaboradores

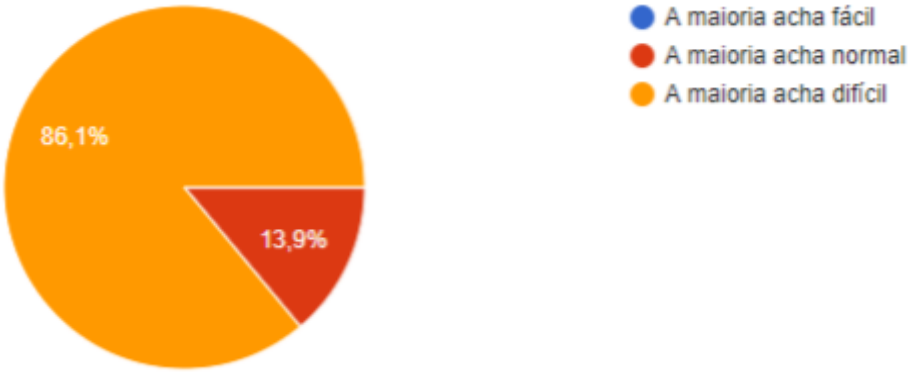


Fonte: elaborado pelo autor

O token não é nada mais que um pendrive que tem uma configuração totalmente destinada para certificados, sendo assim mais prático e móvel que os demais, no qual se usa em qualquer máquina, necessitando apenas da instalação de seu driver em específico. Traz consigo também a segurança, pois funciona apenas se o token estiver plugado na máquina.

Outro aspecto que podemos observar é a utilização dos certificados digitais, no quesito de dificuldade. Dentre os entrevistados que lidam com os clientes, 86,1% dizem que acham difícil quando são certificados do modelo A3:

Gráfico 5 - Dificuldade dos cliente com certificados do tipo A3.

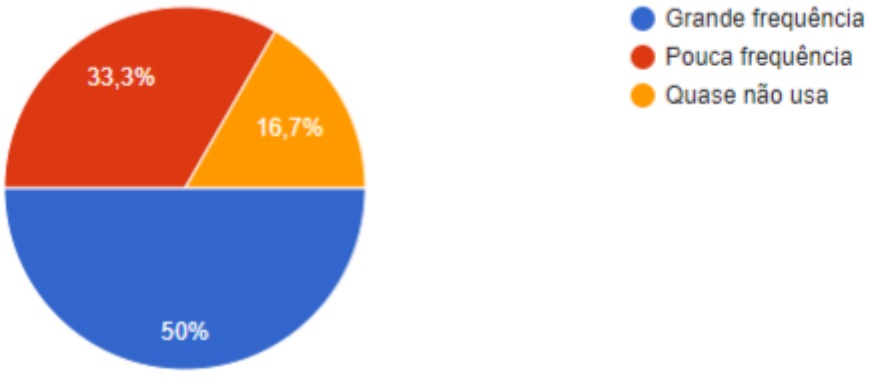


Fonte: elaborado pelo autor

Um dos motivos para este resultado pode ser a instalação e usabilidade em determinados sites, como sites do governo ou de bancos que dão essa possibilidade de acesso com certificados digitais.

Dentre os colaboradores e clientes, apenas a metade usa com grande frequência os seus certificados, o que acaba gerando questionamentos sobre o seu preço. A outra metade usa a sua assinatura digital apenas algumas vezes no tempo de validade do certificado. Tendo isso em vista, seria interessante haver uma maior gama de tipos de certificados e validades para eles.

Gráfico 6 - Uso dos certificados digitais.



Fonte: elaborado pelo autor

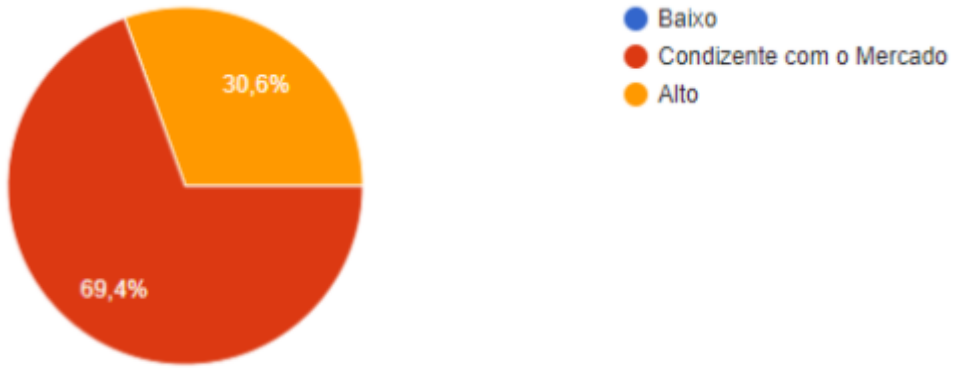
Cada empresa de certificação digital possui sua tabela de certificados e preços, com isso quanto maior a tecnologia, gadgets usados e tempo de validade, maior o seu preço. Os

certificados mais baratos são do tipo A1, que são apenas arquivos instalados na máquina para utilização do certificado, mas temos certificados bem mais complexos.

Os certificados do tipo A3, por exemplo, se forem do tipo de cartão, eles têm a necessidade de um leitor de cartão plugado na máquina para seu funcionamento e também caso se compre com a validade máxima de 3 anos, sendo esses os mais caros. No caso de perda do cartão ou inutilização do cartão, é necessário a emissão de um novo certificado, mesmo que sua validade ainda esteja vigente, sendo assim necessário pedir a revogação do certificado.

Falando do quesito de preço dos certificados, 69,4% dos entrevistados disseram que os preços são condizentes com o mercado. Os preços de uma AR seguem as diretrizes e escalas de preços determinadas pela AC. Ainda muito relevante é que 30,6% ainda acha o preço alto e nenhum considera o preço de certificados baixo, o que nos leva a pensar que ainda não é um tipo de tecnologia acessível para qualquer pessoa interessada.

Gráfico 7 - Percepção sobre preços dos certificados.



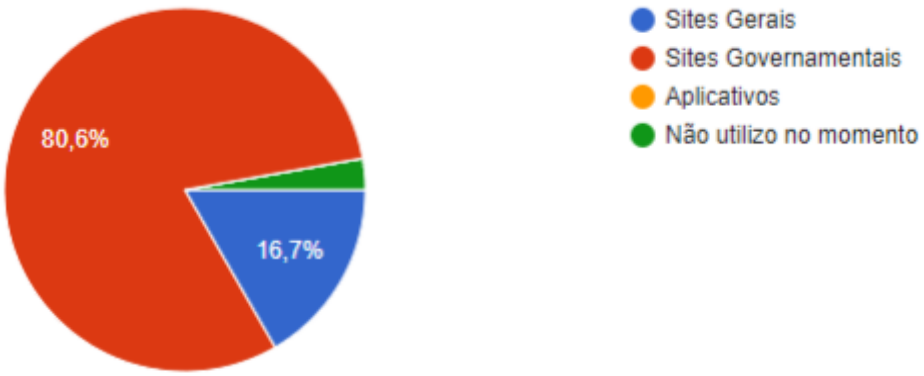
Fonte: elaborado pelo autor

Em novembro de 2021, baseados em certificadoras como Valid, CertiSign e CertificaMinas, os valores dos certificados estão na média de um A1 por R$152,00, do tipo A3 em token por R$355,00 e A3 no cartão sem o leitor por R$239,00, todos com validade de 1 ano. Com isso é notável que, a depender do porte da empresa, não é acessível manter um certificado com tal anuidade.

Os certificados digitais têm grande foco em empresas e empresários, assim como visto pelos colaboradores das empresas entrevistadas, porém, a maior demanda de uso do

certificado é decorrente de sites do governo. Esse uso é feito frequentemente para fins contábeis da empresa, grande parte é feita nos sites governamentais. Outra observação é que, por grande parte dos clientes serem contabilidades e contadores em geral, acaba gerando uma maior demanda de certificados e com isso atraindo possíveis clientes.

Gráfico 8 - Locais onde mais se utiliza o certificado digital.

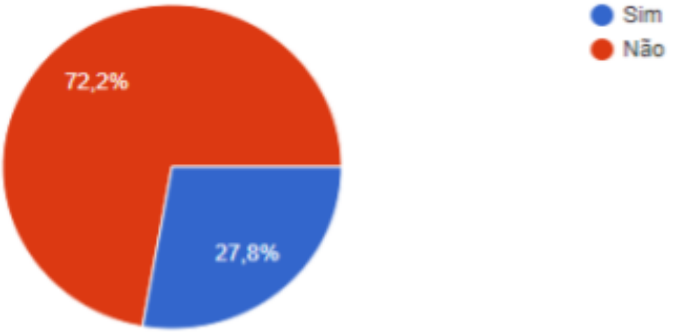


Fonte: elaborado pelo autor

Apesar de muitas empresas utilizarem os certificados, sendo em função de obrigatoriedade ou outras funções gerais da empresa, nem sempre é feito um uso em grande frequência. E algumas das vezes é feito apenas para abertura ou fechamento da empresa e em outros casos também para o acerto de contas de algum de seus colaboradores. Nesse sentido, torna ainda mais caro o valor do certificado, ainda mais pela validade. Algumas empresas já implementaram certificados com menor validade, mas nem sempre são compensadores.

Com a apresentação do *Blockchain* no questionário e mostrando onde é utilizado, seu funcionamento e o que agregou para o mundo da moeda digital, muitos ainda não conheciam a tecnologia. Apesar de alguns terem o conhecimento do Bitcoin, se observa que a maioria não sabia o seu funcionamento e segurança.

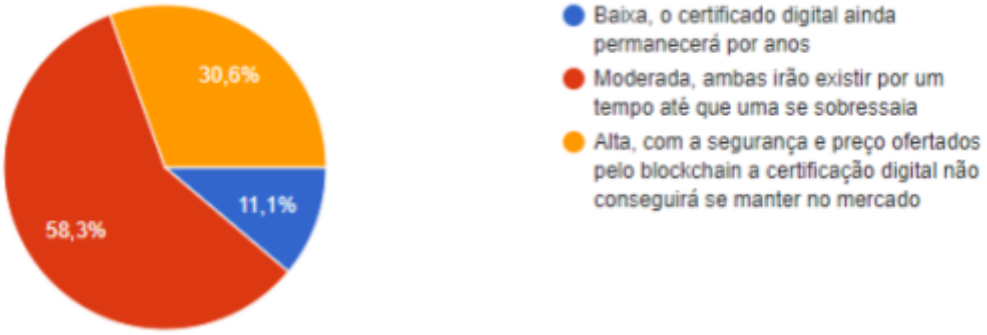
Gráfico 9 - Conhecimento sobre a tecnologia blockchain



Fonte: elaborado pelo autor

Agora com o conhecimento do *blockchain*, sua estrutura básica e como ela funciona em uma identidade digital, foi questionado aos entrevistados quais seriam as chances dessa identidade digital baseada em *blockchain* tomar o lugar da certificação digital. A maioria ainda se ateve ao moderado, acreditando que as duas ficariam por muito tempo subsistindo até que uma sai na frente da concorrência.

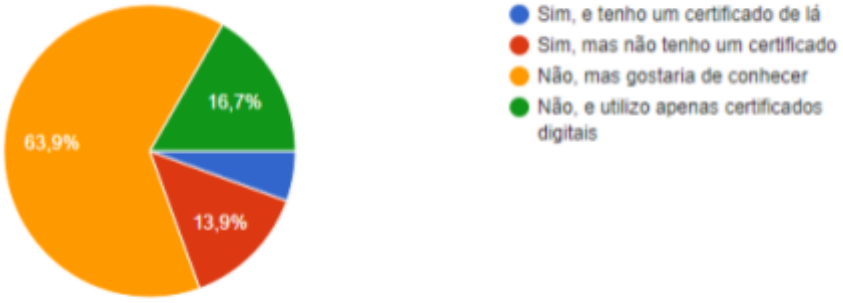
Gráfico 10 - Chances do blockchain ID tomar o lugar da certificação digital.



Fonte: elaborado pelo autor

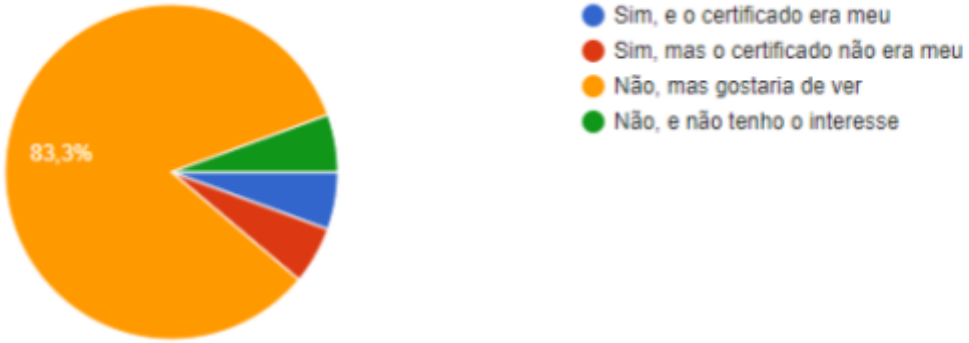
Mesmo a tecnologia não estando totalmente difundida atualmente, podemos observar que 58,3% acreditam que as duas tecnologias irão coexistir por um tempo, trazendo uma ideia ainda conservadora sobre a implementação da nova tecnologia.

Gráfico 11 - Interesse em conhecer sobre Identidades Digitais baseadas em blockchains.



Fonte: elaborado pelo autor

Gráfico 12 - Interesse em conhecer sobre funcionamento de ID's digitais baseados em blockchain.



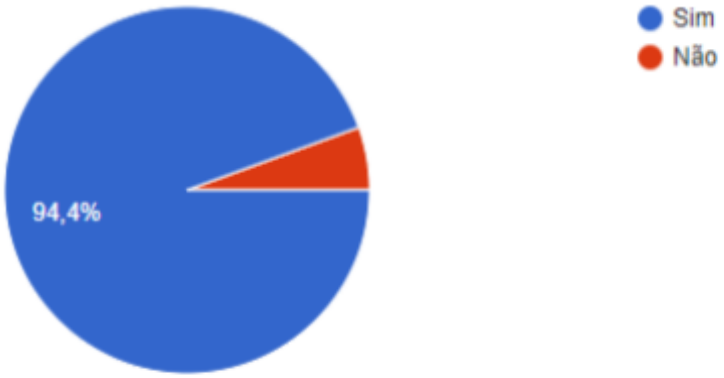
Fonte: elaborado pelo autor

Nos gráficos 11 e 12, o primeiro em questão sobre o certificado em si, sua aparência tipos e o segundo em seu funcionamento como locais que podem ser usado e aplicações, reparamos ainda que, apesar de ainda pouco conhecida, a tecnologia de *blockchain*, após a sua apresentação, despertou interesse entre os entrevistados. Temos que 63,9% deles gostariam de conhecer as identidades digitais baseadas em *blockchain*, ainda 16,7% se sintam relutantes sobre o *blockchain*, e também 83,3% gostariam de ver o funcionamento. O fato da descentralização, facilidade de emissão e preços, podem ser os fatores mais predominantes na implementação, como podemos ver no gráfico 13.

Apesar de algumas pessoas ainda não demonstrarem interesse pelo *blockchain*, a maior porcentagem dos entrevistados vê a inovação que é esse tipo de tecnologia e como ela chegaria revolucionando o mercado de certificação.

Considerando os preços ditos anteriormente e agora ponderando que, no momento em que não houver uma entidade no centro que faça a regularização de preço de emissão de certificados, os preços irão cair exponencialmente. Perguntados a respeito do custo X benefício do *blockchain* sobre o certificado digital, se seria o fator determinante para a sua ascensão no ramo de identidade digital, 94,4% disseram que isso será o ponto alto na mudança.

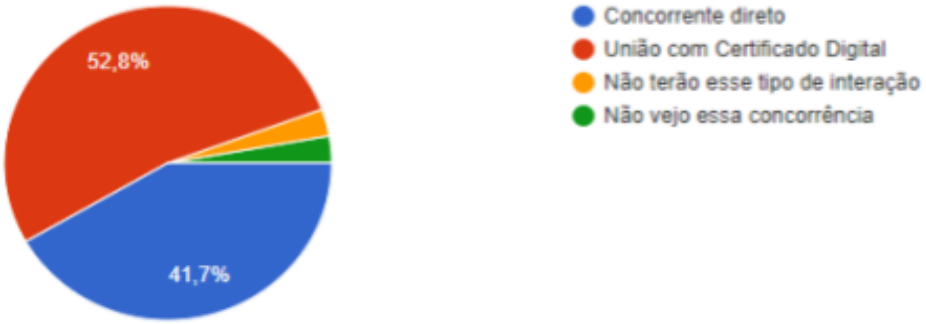
Gráfico 13 - Custo X benefício do blockchain sobre o certificado digital é ponto crucial para mudança de assinatura digital?



Fonte: elaborado pelo autor

Neste caso, 94,4% dos entrevistados acreditam que se uma identidade digital baseada em *blockchain*, se implementada da maneira correta e se estabelecer em todos os outros serviços que usam certificados digitais, se acredita que pode ser a nova certificação digital.

Gráfico 14 - Possíveis situações da duas tecnologias pelos próximos anos.



Fonte: elaborado pelo autor

Quando olhamos para o que realmente importa, sobre quem prevalecerá como assinatura digital recorrente, ainda temos uma porcentagem bem conservadora, com 52,8% que acredita que terá a união entre as duas tecnologias. Apesar de termos uma maioria conservadora, vemos ainda (em laranja) que apenas 2,8% acreditam que essa interação não ocorrerá de maneira alguma e que outros 2,8% (em verde) não veem que o blockchain seja alguma concorrência para o certificado digital.

No gráfico 15, foi questionado se caso o ID digital baseado em *blockchain* fosse implementado, quais seriam as alterações necessárias para que o certificado digital se mantenha no mercado. Verifica-se que 36,1% acreditam que a tecnologia da certificação deve

Gráfico 15 - Alterações do certificado digital após implementação do ID baseado em blockchain.

Fonte: elaborado pelo autor

ter uma mudança, como novas tecnologias em cima da segurança e emissão, criação de gadgets para utilização, onde se conseguiria manter o preço.

Notamos que há alguns que veem uma necessidade de inovação para o certificado digital. Observando essa chegada do ID em *blockchain*, é possível que essa tecnologia venha para tomar o lugar do certificado digital ou mudar totalmente o comércio de certificados, com mudanças de preços, novas tecnologias ou até mesmo novos certificados.

5 CONCLUSÃO

Resgatando a nossa questão principal, sobre como a criação de uma ID digital baseada em blockchain afetaria o comércio de certificados digitais, temos que uma tecnologia tão robusta e revolucionária como o blockchain vem sendo implementada para assinatura digital. Além de dar palco para a maior moeda digital que é o Bitcoin, o blockchain vem forte para a implementação em identidade digital, entendendo todas suas nuances e vantagens, pode substituir o certificado digital.

Com os resultados da abordagem realizada com os colaboradores das empresas de certificação digital, observou-se que ainda pode ser necessário um maior treinamento e entendimento de assinaturas digitais em geral aos colaboradores de tais empresas, visando sua funcionalidade e empregabilidade. Em uma visão retrospectiva sobre os certificados digitais, desde 2001 quando implementado pelo governo a ICP-Brasil e os certificados, pouco se mudou em questões de tipos de certificados e validades.

A dificuldade de instalação e utilização de certificados digitais por clientes, como expresso na pesquisa, mostra com maior clareza que ainda podem ser feitas modificações no processo da certificação, desde a sua emissão até a sua utilização final. Como a maioria dos certificados utilizados, de acordo com pesquisa, são do tipo A3, podemos observar que apesar da dificuldade em cada um de seus passos é o mais utilizado por trazer maior segurança.

Quando entendida a tecnologia de *blockchain* e seu funcionamento como assinatura digital, podemos observar que houve um certo interesse por parte dos colaboradores, por demonstrar um novo método de segurança e emissão de certificados. Quando observado pela pesquisa que o preço de um certificado baseado em blockchain pode ser bem mais barato, a maioria acredita que esse seja o ponto chave que o fará se tornar uma grande concorrência.

A forma descentralizada do blockchain traz consigo uma maior segurança e também o fato de ter um baixo custo, por não ser necessária uma entidade centralizada para comercialização e regularização dessa identidade digital. Com esse ponto determinante o ID

digital baseado em blockchain sai em grande vantagem contra seu concorrente, pois como observamos anteriormente o valor e validade dos certificados digitais são os pontos mais negativos.

Este artigo pode ser enriquecido pela implementação de novas identidades baseadas em blockchain e as novas que irão surgir, para que possa ser determinado o quão acessível virá essa tecnologia e como ela será empregada na sociedade. Como será feita essa implementação em sites do governo, a aceitação de bancos com ID’s baseadas em blockchain, e como isso pode ser usado para autenticação em servidores ainda é um caso muito importante a ser observado.

INFLUENCES OF CREATING A BLOCKCHAIN-BASED DIGITAL IDENTITY IN THE DIGITAL CERTIFICATE TRADE

ABSTRACT

In order to analyze the creation of a blockchain-based digital identity, and how it can affect the commerce of digital certificates. With this analysis, the implementation of the blockchain ID in the correct way, being more secure, and generating a low cost for the end customer is determined, decentralizing the hierarchical scheme created by the Brazilian Public Key Infrastructure (ICP-Brasil). The research was done in order to observe how the implementation of a blockchain-based digital ID is seen by employees/entrepreneurs and users of digital certificates, and what their perspective on how this affects the digital certification commerce is. In a questionnaire based on trade and security issues regarding the two technologies, digital certification and blockchain, being carried out in the city of Formiga, in Minas Gerais. The results were satisfactory, it was possible to observe some more details about digital certification, the need for innovation in methods and new technologies and with the implementation of the blockchain as a digital identity directly affects the digital certification commerce, causing it to be reinvent to keep pace with blockchain technology.

Keywords: Digital Certificate. Blockchain. Digital Identity. Business.

REFERÊNCIAS

AARÃO, Maria Teresa. **Entrevista sobre *Blockchain* e Chttps://docs.google.com/document/d/16tdTIYDmOiftVQ6aW7isstAKselx4FMCpNWqlxwRkGU/edit#ertificado Digital. Blog Certisign**, 2019. Disponível em: https://blog.certisign.com.br/blockchain-e-certificado-digital-perguntas-e-respostas-de-como-uma-tecnologia-pode-trabalhar-com-a-outra/. Acessado em: 25 set. 2021.

ASSUNÇÃO, Lucas Carvalho. **A Segurança da Certificação Digital.** 2017. Curso de Engenharia de Computação na Universidade de Uberaba.

BATISTA, Alex Oliveira Abreu. et al. **Identificação digital baseada em *blockchain*: Um conceito disruptivo no ciberespaço**. 2018. V simpósio internacional de inovação em mídias interativas. Goiânia: Media Lab / UFG.

BRASIL. Medida Provisória nº 2.200-2, de 24 de Agosto de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências**. Brasília, DF, D.O.U de 27/08/2001, pág. nº 65.

CERTISIGN. **21 anos de Certificação Digital no Brasil. Blog Certisign**, 2017. Disponível em: https://blog.certisign.com.br/21-anos-de-certificacao-digital-no-brasil/. Acessado em: 19 set. 2021.

CGI.BR. **Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro**. CGI.BR, 2017. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/TIC_eGOV_2017_livro_eletronico.pdf. Acessado em : 19 set. 2021.

FRAJHOF, Isabella Z. **Os desafios da tecnologia blockchain: resenha à obra "Entender Blockchain: Uma introducción a la tecnologia de registro distribuído", de Manuel González-Meneses**. Civilistica.com. Rio de Janeiro, a. 8, n. 2, 2019. Disponível em: http://civilistica.com/os-desafios-da-tecnologia-blockchain/. Acessado em: 21 nov. 2021.

GAMA, Vitor Sad Cortat Xavier da. et al. **Certificado Digital: Um estudo sobre os efeitos da implantação do sistema de certificação digital nas empresas de contabilidade da região.** 2017. II Jornada de Iniciação Científica, III Seminário Científico da FACIG.

GOV.BR. **PF deflagra operação TOKENS que investiga fraudes em certificados digitais de fiscais e gestores do IBAMA**. GOV.BR, 2020. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2020/09-Noticias-de-setembro-de-2020/pf-deflagra-operacao-tokens-que-investiga-fraudes-em-certificados-digitais-de-fiscais-e-gestores-do-ibama. Acessado em: 19 set. 2021.

IBM. **O que é a tecnologia blockchain?** 2021. Disponível em: https://www.ibm.com/br-pt/topics/what-is-blockchain. Acessado em: 11 nov. 2021.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Apresenta informações sobre: ICP-Brasil e sua estrutura, certificação digital e dados relacionados à emissão de certificados.** Disponível em: <http://www.iti.gov.br/>. Acesso em 11 nov. 2021.

HARTMANN JUNIOR, Joel. **Certificado Digital**. 2009. Curso de Especialização em Redes e Segurança de Sistemas. Pontifícia Universidade Católica do Paraná.

LEE, Jong-Hyouk. **BIDaaS: *Blockchain* Bases ID as Service**. 2017. Department of Software, Sangmyung University, Cheonan 31066, South Korea.

LIN, Qun. et al. **An ID-Based Linearly Homomorphic Signature Scheme and Its Application in *Blockchain***. 2018. Institute of Mathematics and Statistics, Hanshan Normal University, Chaozhou 521041, China.

MIRANDA, Júlio César de. et al. **TECNOLOGIA BLOCKCHAIN:a disrupção na indústria financeira**. 2018. DOI: 10.31510/infa.v15i2.376. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/376/333. Acessado em 21 nov. 2021.

MONTEIRO, E. S.& MIGNONI, E. M. **Certificação Digital: Conceitos e Práticas**. Rio de Janeiro: Brasport, 2007

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Bitcoin, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acessado em: 11 ago. 2021.

ORIGINALMY. **Safe and low-cost growth.** 2021. Disponível em: https://originalmy.com/pricing. Acessado em: 23 nov. 2021.

SOUZA, Alice. et al. **Estoque Beer Zone Ferramenta de administração de estoque com estudo de caso na Cervejaria Cruzeiro MC.** 2017. Etec Prof. Carmine Biagio Tundisi Atibaia, Centro Paula Souza, Governo do Estado de São Paulo.

SOUZA, Isabella Pegorete Mandetta de. et al. **Certificação Digital: Conceitos e aplicações.** 2017. Faculdade de Tecnologia de Taquaritinga (FATEC) – Taquaritinga – SP – Brasil.

TAPSCOTT, D.;TAPSCOTT, A. **Blockchain Revolution: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo**. São Paulo: SENAI –SP Editora, 2016. 392 p.

TRF3. **JUSTIÇA FEDERAL DETERMINA PRISÃO DE SUSPEITOS DE FRAUDE DE IDENTIDADE PARA USO EM SISTEMA PROCESSUAL ELETRÔNICO**. Tribunal Regional Federal da 3ª Região, 2021**.** Disponível em: http://web.trf3.jus.br/noticias/Noticias/Noticia/ExibirNoticia/407878-justica-federal-determina-prisao-de-suspeitos-de-fraude. Acessado em: 19 set. 2021.

ZATARIN, Jonathan Kelsson. et al. **Análise da padronização do trabalho na área de certificação digital: um estudo de caso.** 2020. Research, Society and Development, v. 9, n.

10, e309108394, 2020 (CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v9i10.8394.

APÊNDICE A - QUESTIONÁRIO PARA OS PROFISSIONAIS DA ÁREA DE CERTIFICAÇÃO DIGITAL

QUESTIONÁRIO - APÊNDICE A

1 - Há quanto tempo trabalha ou trabalhou com certificação digital?

a - menos de 1 ano

b - 1 ano

c - 2 anos

d - 3 anos

e - mais de 4 anos

2 - Como lhe foi apresentada a certificação digital?

a - Emprego

b - Notícias

c - Família e Amigos

d - Internet

e - Outros

3 - Como considera seu nível de conhecimento em certificação digital?

a - Baixo

b - Médio

c - Avançado

4 - Por mais que não seja obrigatoriedade para se trabalhar na área, você possui certificado digital? Se sim, em qual modelo?

a - A1

b - A3 token

c - A3 cartão

d - A3 cartão/token

e - A1 e A3 token

f - A1 e A3 cartão

g - Outros Modelos

h - Todos os modelos

i - Nenhum deles

5 - Se possui um certificado digital, com que frequência costuma utilizá-lo?

a - Grande frequência

b - Pouca frequência

c - Quase não usa

6 - Quanto a certificados do tipo A3 que são necessários drivers para a utilização dos mesmos, na sua perspectiva qual a dificuldade sobre a instalação e utilização deles?

a - Eu acho fácil

b - Eu acho normal

c - Eu acho difícil

7 - Quanto a certificados do tipo A3, são necessários drivers para a utilização dos mesmos, na sua perspectiva qual a dificuldade que o usuário vê sobre a instalação e utilização deles?

a - A maioria acha fácil

b - A maioria acha normal

c - A maioria acha difícil

8 - O que acha do preço dos certificados digitais?

a - Baixo

b - Condizente com o Mercado

c - Alto

9 - Se fosse possível fazer alguma alteração no funcionamento do certificado digital, qual seria? (Opcional)

10 - Qual o local onde mais utiliza o certificado digital?

a - Sites Gerais

b - Sites Governamentais

c - Aplicativos

d - Outros

11- Qual a maior qualidade do certificado digital que você pode identificar trabalhando com o mesmo?(Uma palavra)

12 - Qual o maior defeito do certificado digital que você pode identificar trabalhando com o mesmo?(Uma palavra)

13 - Conhece a tecnologia de Blockchain?

a - Sim

b - Não

14 - De acordo com as informações acima, dê um breve parecer sobre o que achou sobre.(Opcional)

15 - Quais as chances do blockchain como ID digital tomar o lugar da certificação digital?

a - Baixa, o certificado digital ainda permanecerá por anos

b - Moderada, ambas irão existir por um tempo até que uma se sobressaia

c - Alta, com a segurança e preço ofertados pelo blockchain a certificação digital não conseguirá se manter no mercado

16 - Conhece alguma empresa que já fornece identificação digital baseada em blockchain?

a - Sim, e tenho um certificado de lá

b - Sim, mas não tenho um certificado

c - Não, mas gostaria de conhecer

d - Não, e utilizo apenas certificados digitais

17 - Já teve a oportunidade de ver o funcionamento de uma identificação digital baseada em blockchain?

a - Sim, e o certificado era meu

b - Sim, mas o certificado não era meu

c - Não, mas gostaria de ver

d - Não, e não tenho o interesse

18 - Considerando uma ID digital com um preço muito baixo, podendo acessar praticamente todos os sites, aplicativos e serviços do certificado digital, e posteriormente em sites governamentais, você acha que o custo benefício possa vir a ser o ponto crucial para a implementação do ID em blockchain?

a - Sim

b - Não

19 - No quesito segurança, o Blockchain é de fato o concorrente direto da Certificação Digital, ou pode-se unir a ele criando uma nova perspectiva de certificação?

a - Concorrente direto

b - União com Certificado Digital

c - Outro (Se tiver como colocar justificativa)

20 - Com uma futura implementação de ID em Blockchain, na sua opinião o que irá acontecer com os valores da certificação digital?

a - Diminuir drasticamente para se adequar ao mercado

b - Implementar novas tecnologias, gadgets para poder manter o preço

c - Subir o preço para poder manter o nome forte de certificação digital

d - Criar novos métodos, como o de prazo de validade, modos de certificação e novos token/cartões para se equiparar aos preços do ID em Blockchain.

e - Outro