Autenticação segura de pessoas com carteira digital: um estudo no CPQD

Fabiani de Souza[1], **José Reynaldo Formigoni Filho**[1], **Fernando Cezar Herédia Marino**[1], **Andressa Souza Sampaio**[1]

[1]CPQD, CEP 13086-902 – Campinas – SP – Brasil

{fabiani, reynaldo, fmarino, asampaio}@cpqd.com.br

Abstract. *This paper describes a study carried out at CPQD using a digital wallet for secure authentication of people by reading a QR Code. The study involved the institution's employees in three phases: 1) research on habits and perceptions about digital authentication, 2) usability evaluation, and 3) testing in a real environment of use. The paper also discusses lessons learned from the study and future work.*

Resumo. *Este artigo descreve um estudo realizado no CPQD utilizando uma carteira digital para autenticação segura de pessoas a partir da leitura de QR Code. O estudo envolveu os funcionários da instituição em três etapas: 1) pesquisa a respeito de hábitos e percepções sobre autenticação digital, 2) avaliação de usabilidade e 3) teste em ambiente real de uso. O artigo também discute as lições aprendidas a partir do estudo e os trabalhos futuros.*

1. Introdução

Um dos grandes desafios para impulsionar a transformação digital em diferentes setores da economia é a existência de soluções de identidade digital seguras e fáceis de usar. Na visão do Fórum Econômico Mundial, "à medida que avançamos para a Quarta Revolução Industrial e mais transações são realizadas digitalmente, a representação digital da identidade de uma pessoa se torna cada vez mais importante; isso se aplica a humanos, dispositivos, entidades legais e além" [WEF 2021]. Atualmente, os modelos centralizados de identidade digital, associados ao par usuário/senha, enfrentam desafios não só pela dificuldade do usuário em memorizar, normalmente, dezenas de senhas, mas também devido à dificuldade das soluções de atenderem às leis gerais de proteção dados, levando à violações de dados, fraude de identidade e perda econômica e de privacidade para os envolvidos. Esses eventos recorrentes destacam a falta de segurança, controle e gerenciamento que os usuários experimentam com suas identidades digitais hoje.

Em resposta a esses desafios, os aplicativos de carteira digital baseados em identidade autossoberana, ou *Self-Sovereign Identity* (SSI) – uma nova geração de sistemas de identidade digital – permitem ao usuário controlar e gerenciar sua identidade digital de forma segura em seu dispositivo móvel, sem a necessidade de memorizar inúmeras senhas. Embora o foco das pesquisas atuais em SSI seja os aspectos técnicos, de segurança e de privacidade, uma alternativa madura para o uso do par usuário/senha exige a implantação em grande escala para fins de autenticação real e testes com usuários [Bonneau et al. 2012], dado que a experiência do usuário é um dos principais fatores para a adoção de novas formas de identificação digital.

Com o objetivo de desenvolver uma carteira digital que atenda as necessidades dos usuários, o estudo descrito neste artigo foi realizado no CPQD e envolveu os funcionários da instituição em três etapas: 1) pesquisa a respeito de hábitos e percepções sobre autenticação digital; 2) avaliação de usabilidade; e 3) teste em ambiente real. Para facilitar a compreensão deste artigo, a Seção 2 apresenta alguns conceitos e o contexto relacionados ao estudo. A Seção 3 descreve a abordagem utilizada. A Seção 4 apresenta os resultados e na Seção 5 eles são discutidos. A Seção 6 conclui este artigo.

2. Conceitos e contexto

O conceito de SSI baseia-se nos princípios de identidade descentralizada que aproveitam as tecnologias de livro de registro distribuído (uma classe mais ampla de tecnologia "inspirada em *blockchain*") [Zachariadis et al. 2019] e credenciais que podem ser verificadas criptograficamente [W3C 2021][W3C 2022] para fornecer a identidade digital dos usuários de forma descentralizada, sem depender de intermediários [Naik and Jenkins 2020]. Adicionalmente, o paradigma da SSI possui atributos que garantem a soberania dos usuários sobre sua identidade, bem como o controle do armazenamento dos dados confidenciais associados à sua identidade [Naik and Jenkins 2020].

Desde 2019, o CPQD vem desenvolvendo componentes, protótipos e pilotos de identidade digital para diferentes setores da economia, como agronegócio, saúde, educação, governo e financeiro. Em 2021, como parte de uma plataforma de SSI que provê infraestrutura para soluções de identidade digital, o CPQD iniciou o desenvolvimento da carteira digital CPQD iD. Carteiras digitais são *softwares* que permitem ao usuário gerar, armazenar, gerenciar e proteger chaves criptográficas, credenciais verificáveis e outros dados privados e confidenciais [Preukschat and Reed 2021]. Uma credencial verificável é a representação digital de credenciais físicas, como a Carteira Nacional de Habilitação (CNH) e o Registro Geral de Identidade (RG). Para efeito do estudo, a versão da carteira digital descrita neste artigo contava com apenas uma credencial de identificação e uma funcionalidade: autenticação digital por meio de *QR Code*.

3. O estudo no CPQD

O estudo ocorreu em três etapas, entre outubro de 2021 e março de 2022. A participação no estudo era opcional e todas as etapas possuíam um termo de ciência e concordância esclarecendo sobre o uso dos dados e ideias dos participantes, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD) [Brasil 2018].

3.1. Hábitos e percepções sobre autenticação digital

Na primeira etapa do estudo, os funcionários do CPQD foram convidados a participar de uma pesquisa sobre seus hábitos e percepções em relação à autenticação digital. A pesquisa utilizou a ferramenta Google Forms e foi compartilhada em diversos grupos de *chat* da instituição durante um período de dois dias. O formulário contava com perguntas sobre a opinião dos participantes em relação à segurança da autenticação única com Facebook/Google e formas utilizadas para gerenciamento de senhas. A pesquisa teve como objetivo identificar potenciais usuários da carteira digital e interessados em participar da segunda etapa do estudo. As respostas foram avaliadas a partir de duas hipóteses:

- H1: Os funcionários do CPQD consideram inseguro se autenticar em sites e aplicativos utilizando a autenticação única com Facebook/Google; e
- H2: Os funcionários do CPQD têm dificuldades para memorizar suas senhas.

3.2. Avaliação de usabilidade

A segunda etapa do estudo utilizou a primeira versão da carteira digital: um aplicativo Android para emissão de uma credencial de identificação para autenticação (Figura 1). A emissão da credencial passava pelo cadastro de dados biográficos (nome e CPF) a partir da foto de um documento (RG ou CNH) utilizando a tecnologia de reconhecimento ótico de caracteres (OCR); comparação entre os dados biométricos da foto do usuário no documento e a foto do rosto feita pelo aplicativo; e cadastro de e-mail. Também era necessário criar uma senha para proteger o acesso ao aplicativo. Com a credencial emitida era possível usar o aplicativo para ler um *QR Code* e se autenticar em um site fictício.

Figura 1. Telas da primeira versão da carteira digital CPQD iD.

Para avaliar a usabilidade do aplicativo antes de testá-lo em ambiente real, foram convidadas sete pessoas que manifestaram interesse em continuar participando do estudo na pesquisa citada na Seção 3.1. Os sete participantes foram considerados potenciais usuários da solução, dado que validaram as duas hipóteses da pesquisa. Os testes foram pré-agendados e feitos por chamada de vídeo usando a ferramenta Google Meet. Os participantes instalaram o aplicativo no próprio *smartphone* e compartilharam a tela para que fosse possível acompanhar a interação com o aplicativo.

Para registro e análise das respostas afetivas dos participantes em relação à interação com o aplicativo, um conjunto de artefatos foi utilizado: com base nos três níveis para o *design* emocional de Norman [Norman 2004] – visceral, comportamental e reflexivo – a metodologia adaptada de [Hayashi et al. 2009] e apresentada na Figura 2 foi aplicada. Para as respostas viscerais, foram observados os comentários espontâneos dos participantes durante a interação com o aplicativo. Para as respostas comportamentais, foram considerados os toques na tela. Tanto os comentários quanto os toques foram capturados pela chamada de vídeo. As respostas em nível reflexivo foram coletadas após a interação com o aplicativo por meio do *emoti*-SAM [Hayashi et al. 2016], um questionário pictográfico que capta três dimensões de uma resposta emocional – satisfação, motivação e sentimento de domínio/controle –, utilizando a ferramenta Google Forms.

3.3. Teste em ambiente real

O teste em ambiente real foi realizado durante um mês. A divulgação foi feita via e-mail corporativo e convidava todas as pessoas que possuíam documento com CPF – RG ou

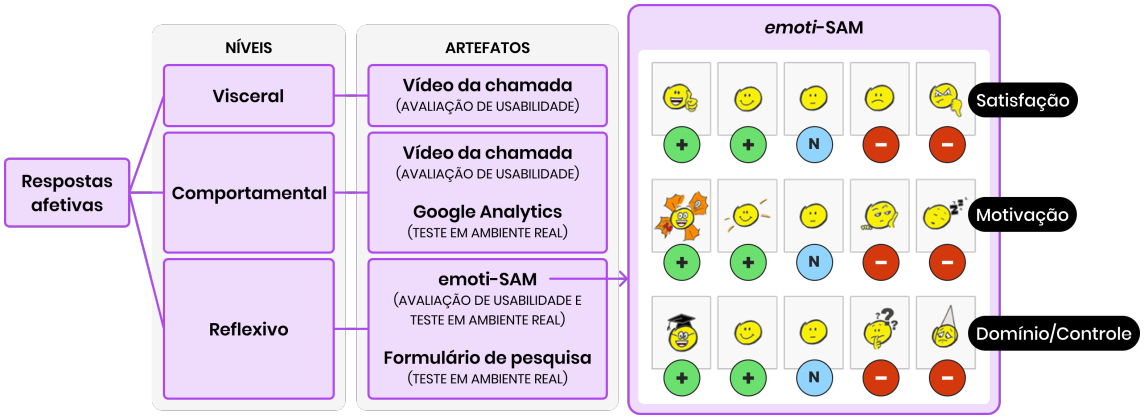

Figura 2. Modelo para avaliação das respostas afetivas e *emoti*-SAM.

CNH – e *smartphone* Android a fazer parte do teste. Os participantes deveriam instalar a carteira digital no seu *smartphone* e passar pelo mesmo processo de emissão de credencial citado na Seção 3.2 – com extração de dados do documento por OCR, validação biométrica e cadastro de e-mail e senha. Uma vez emitida a credencial, o aplicativo poderia ser utilizado para autenticação no Jira[1] (sistema de uso diário na instituição), sem a necessidade de informar usuário/senha. O objetivo era avaliar a viabilidade do uso da carteira digital como alternativa para autenticação nos sistemas do CPQD e de seus clientes.

Durante o teste, as respostas dos usuários em nível comportamental foram coletadas a partir de métricas pré-definidas usando a ferramenta Google Analytics: quantidade de aplicativos instalados, quantidade de credenciais emitidas e quantidade de autenticações no sistema Jira utilizando a carteira digital. Duas semanas após o início do teste, foi divulgada por e-mail uma pesquisa para coletar as respostas em nível reflexivo. A pesquisa utilizou a ferramenta Google Forms e continha perguntas para que os participantes classificassem, de 1 (muito difícil) a 5 (muito fácil), a dificuldade percebida durante o cadastro no aplicativo e a autenticação no Jira, além de coletar percepções sobre a experiência de uso geral do aplicativo, por meio de perguntas abertas e questionário *emoti*-SAM. Após responder o formulário, os participantes podiam optar por conversar com a equipe responsável pelo estudo para dar mais detalhes ou sugestões.

4. Resultados

4.1. Hábitos e percepções sobre autenticação digital

A pesquisa a respeito dos hábitos e percepções sobre autenticação digital obteve 208 respostas. Em relação à segurança de se utilizar o Facebook para autenticação, 45,2% disseram ser inseguro; 30,8% seguro; e 24% sem opinião formada. Sobre a autenticação com Google, 50,5% disseram ser seguro; 28,8% inseguro; e 20,7% sem opinião formada. Ainda que a porcentagem de pessoas que disseram ser seguro seja menor que 50% para a autenticação com o Facebook e maior que 50% para o Google, a diferença é muito pequena para fazer afirmações sobre hipótese H1 sem uma análise estatística destes dados. Em relação a memorização de senhas, 63,5% disseram utilizar métodos variados para contornar o esquecimento de suas senhas, fornecendo indícios sobre a validade da hipótese

[1]https://www.atlassian.com/software/jira

H2: 22,6% anotam as senhas em algum lugar; 12,5% usam o gerenciador do navegador; 11,1% usam um gerenciador de senhas específico; 7,7% quase sempre usam a opção "esqueci minha senha"; e 9,6% adotam outros métodos, como anotação de parte das senhas, anotação em papel usando taquigrafia, arquivos criptografados e uma senha por arquivo. Os demais, 36,5%, disseram não utilizar métodos para gerenciamento: 29,8% sempre lembram as senhas e 6,7% quase sempre usam a autenticação do Facebook/Google.

4.2. Avaliação de usabilidade

Os resultados em **nível visceral** foram analisados a partir dos comentários espontâneos coletados durante a interação com o aplicativo. Comentários geralmente relacionados a dúvidas ou insatisfação foram manifestados durante a foto do próprio rosto, que ocorria de forma automática quando o usuário piscava: *"Ah, quando vai tirar selfie eu não aperto nada, vai automático?"*; e *"Opa, travou. Ah não, acho que toquei na foto sem querer e a foto saiu"*. Por outro lado, comentários que podem ser considerados positivos forneceram indícios a respeito da satisfação dos participantes: *"Ele tirou a foto? Tirou automático, que bonito!"*; e *"Que legal!"* (sobre a autenticação com *QR Code*).

Para avaliar as respostas afetivas em **nível comportamental**, a métrica definida em [de Souza et al. 2021] foi utilizada para classificar a completude das etapas da avaliação: verde, conseguiu finalizar; amarelo, finalizou com obstáculos ou ajuda; e vermelho, não conseguiu finalizar. No total, cinco participantes concluíram todas as etapas. Dois dos participantes não finalizaram o processo de cadastro para emissão da credencial por questões técnicas não identificadas nos testes de *software* anteriores à avaliação de usabilidade. Em um dos casos, o resultado da avaliação biométrica indicou que a pessoa da foto no momento do cadastro não era a mesma da foto no documento; no outro caso, o aplicativo parou de responder após o cadastro da senha. As etapas de fotos do documento e do rosto tiveram as menores taxas de sucesso, como exibe o gráfico na Figura 3.

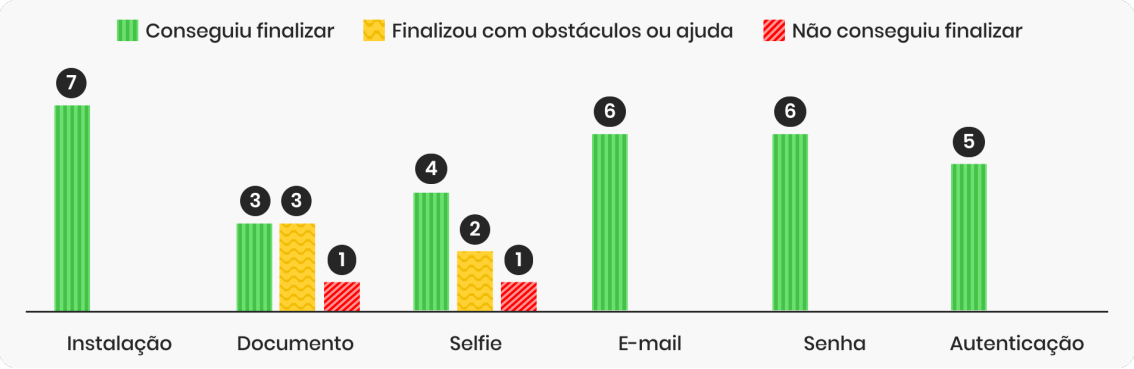

Figura 3. Completude de cada etapa na avaliação de usabilidade.

Para analisar as respostas afetivas em **nível reflexivo**, a frequência de respostas para cada dimensão do *emoti*-SAM foi calculada e agrupada em respostas positivas, neutras e negativas. Os resultados estão exibidos na Tabela 1.

4.3. Teste em ambiente real

No **nível comportamental**, o teste obteve 172 instalações do aplicativo, 65 credenciais criadas e 131 autenticações no Jira. Este resultado indica que muitos dos participantes instalaram o aplicativo, mas não completaram o cadastro para emissão da credencial.

Tabela 1. Frequência de respostas em nível reflexivo na avaliação de usabilidade.

Dimensão	Positiva	Neutra	Negativa
Satisfação	6	0	1
Motivação	5	2	0
Domínio/Controle	2	3	2

A pesquisa em **nível reflexivo** obteve 24 respostas. Para a dificuldade percebida, foi calculada a frequência de respostas para cada valor da escala, de acordo com a etapa de uso do aplicativo. Os resultados na Tabela 2 indicam maior dificuldade para completar as etapas de fotos, tanto do documento quanto do rosto. O cadastro de senha obteve uma resposta neutra, mas foi considerado como fácil pela maioria. Já as etapas de cadastro de e-mail e a autenticação no Jira, foram classificadas como fáceis por todos os participantes. Sobre a experiência de uso geral da carteira digital, as respostas do *emoti*-SAM na Tabela 3 indicam resultados melhores que os obtidos na avaliação de usabilidade, com a maioria positiva para todas as dimensões. Os comentários nas respostas às perguntas abertas da pesquisa indicaram percepções a respeito do uso de fotos no cadastro e da autenticação por meio da leitura do *QR Code*. Cada tema citado nos comentários teve sua frequência calculada a partir da quantidade de participantes que o mencionaram e sua valência classificada em positiva, neutra ou negativa. A Tabela 4 reúne as percepções mais frequentes extraídas dos comentários e a valência de cada uma delas.

Tabela 2. Dificuldade percebida no cadastro e na autenticação.

Etapa	1 (muito difícil)	2	3	4	5 (muito fácil)
Foto do documento	1	1	5	2	15
Foto do rosto	1	1	1	2	18
E-mail	0	0	0	1	22
Senha	0	0	1	2	19
Autenticação no Jira	0	0	0	3	20

Tabela 3. Frequência de respostas do *emoti*-SAM no teste em ambiente real.

Dimensão	Positiva	Neutra	Negativa
Satisfação	21	2	1
Motivação	20	3	1
Domínio/Controle	20	3	1

5. Discussão

A análise das respostas afetivas ajuda a formar uma visão global da experiência dos participantes durante a interação com a carteira digital. Na avaliação de usabilidade, pode-se afirmar que o aplicativo se comportou de forma inesperada durante a foto do rosto. Esta afirmação tem como base o resultado do *emoti*-SAM (domínio/controle), confirmado pelos comentários dos participantes expressando dúvidas e incertezas. As respostas negativas e neutras no *emoti*-SAM também corroboram a análise da completude das etapas, já que alguns participantes tiveram dificuldade ou não conseguiram completar o cadastro. A

Tabela 4. Percepções mais frequentes sobre a experiência de uso do aplicativo.

Etapa	Freq.	Percepção	Valência
Foto do documento	9	Fácil; uma boa ideia; inovador.	Positiva
	4	Invasivo; preocupação com a privacidade.	Negativa
	3	Importante passar segurança no processo.	Neutra
Foto do rosto	8	Simples; fácil; uma boa ideia.	Positiva
	4	Chato; preocupação com a privacidade.	Negativa
	3	Gostaria de repetir a foto, mas não pôde.	Negativa
Autenticação no Jira	9	Simples; prático.	Positiva
	5	Mais difícil que usar usuário/senha.	Negativa
	3	Trabalhoso.	Negativa

partir destes resultados, algumas modificações foram feitas no aplicativo: na tela de foto do documento, foi adicionada uma moldura com o modelo do documento para orientar o usuário, melhorando a qualidade da foto e consequentemente a extração de dados do documento; na foto do rosto, foram adicionadas informações sobre a captura automática.

A frequência de respostas positivas foi superior às respostas negativas em todos os aspectos analisados no teste em ambiente real. As respostas para a dimensão domínio/controle no *emoti*-SAM fornecem indícios de que as alterações após a avaliação de usabilidade melhoraram a experiência de uso do aplicativo. Pode-se afirmar, também, que as respostas negativas e neutras no *emoti*-SAM reforçam a dificuldade percebida pelos participantes no uso do aplicativo. Por meio das perguntas abertas, nota-se que os participantes que precisaram repetir as fotos várias vezes foram os mesmos que classificaram a dificuldade destes passos como 2 (difícil) ou 3 (média). Da mesma forma, o participante que não concluiu as etapas de fotos classificou a dificuldade como 5 (muito difícil) e expressou a sua insatisfação com respostas negativas no *emoti*-SAM.

A obrigatoriedade das fotos do documento e do rosto pode ser uma das causas para o abandono durante o processo de cadastro, constatado pela diferença entre o número de instalações e de credenciais emitidas. Em conversa com a equipe do estudo, um dos participantes disse ter instalado o aplicativo, mas desistido ao notar a exigência das fotos. Alguns participantes também mencionaram que as fotos são chatas, invasivas, e um risco à privacidade (Tabela 4). Na prática, o uso das fotos não era necessário no contexto deste estudo, dado que a identidade dos participantes foi registrada no momento da contratação pelo CPQD e poderia ser verificada pelo e-mail corporativo. Embora estas etapas tenham sido mantidas para simular o comportamento de uma carteira digital para o público geral, o cenário deste estudo é comum em várias instituições e evidencia a necessidade de tornar o processo de emissão da credencial mais flexível para atender contextos diversos.

O entendimento de que a adoção de carteiras digitais exige uma mudança de comportamento dos usuários foi reforçado pela percepção de que o seu uso é mais difícil e trabalhoso que a autenticação com usuário/senha. Uma das dificuldades citadas foi o uso de senha para acessar o aplicativo. Embora a senha seja necessária para proteger as credenciais, o acesso pode ser facilitado pela utilização do método de desbloqueio do próprio dispositivo. A comodidade de manter usuário e senha salvos no navegador, porém, além de ser um risco à segurança, não é algo que as carteiras digitais se propõem a oferecer.

6. Conclusão

O equilíbrio entre segurança e usabilidade é um grande desafio para *designers* e profissionais de segurança da informação. Além de reforçar este fato, o estudo descrito neste artigo coloca em evidência a necessidade de envolver os usuários no processo de desenvolvimento de novos produtos. Com os resultados obtidos, espera-se inspirar as comunidades empresariais e acadêmicas a buscar alternativas para os métodos atuais de autenticação, propensos à fraude e perda de privacidade. Uma das limitações deste estudo é o perfil dos participantes, relativamente homogêneo em relação ao uso de tecnologias no dia-a-dia. Após modificar a carteira digital para tornar o uso das credenciais mais flexível, pretende-se dar continuidade ao estudo no CPQD e coletar métricas de uso fora da instituição, por meio de clientes do CPQD.

Referências

Bonneau, J., Herley, C., Oorschot, P. C. v., and Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567.

Brasil (2018). Lei geral de proteção de dados pessoais. Lei nº 13.709.

de Souza, F., Vechini, G., and Bonadia, G. (2021). Making design of experiments (doe) accessible for everyone: Prototype design and evaluation. In *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, pages 1–7.

Hayashi, E., Neris, V., Baranauskas, C., Martins, M. C., Piccolo, L., and Costa, R. (2009). Avaliando a qualidade afetiva de sistemas computacionais interativos no cenário brasileiro. *Usabilidade, Acessibilidade e Inteligibilidade Aplicadas em Interfaces para Analfabetos, Idosos e Pessoas com Deficiência*, 55.

Hayashi, E., Posada, J. G., Maike, V., and Baranauskas, M. C. C. (2016). Exploring new formats of the self-assessment manikin in the design with children. In *Proceedings of the 15th Brazilian Symposium on Human Factors in Computing Systems*.

Naik, N. and Jenkins, P. (2020). Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*. IEEE.

Norman, D. A. (2004). *Emotional Design: why we love (or hate) everyday things*. Basic Books, New York.

Preukschat, A. and Reed, D. (2021). *Self-sovereign identity: Decentralized Digital Identity and Verifiable Credential*. Manning Publications.

W3C (2021). Decentralized identifiers (dids) v1.0. `https://www.w3.org/TR/did-core/#introduction`. Accessed: 2022-06-25.

W3C (2022). Verifiable credentials data model v1.1. `https://www.w3.org/TR/vc-data-model/`. Accessed: 2022-06-25.

WEF (2021). Digital identity on the threshold of a digital identity revolution. Technical report, World Economic Forum.

Zachariadis, M., Hileman, G., and Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, 29(2):105–117.