ISSN 3085-5624

Eixo Temático 2 – Informação, Comunicação e Processos Tecnológicos

HEALTHWALLET: uma carteira digital para privacidade de dados de saúde

HEALTHWALLET: a digital wallet for health data privacy

Charles Alencar – Universidade Federal de Alagoas (UFAL) – *caoa1@ic.ufal.br* – Orcid: https://orcid.org/0009-0001-7245-3020

Leonardo Pedrosa Leite – Universidade Federal de Alagoas (UFAL) – *leo.leite@ic.ufal.br* – Orcid: https://orcid.org/0009-0009-1742-0144

Pedro Henrique Barbosa da Cunha – Universidade Estadual de Ciências da Saúde de Alagoas (UNCISAL) – *pedro.cunha@academico.uncisal.edu.br* – Orcid: https://orcid.org/0009-0005-4271-8138

Lucas Barros de Souza – Universidade Estadual de Ciências da Saúde de Alagoas (UNCISAL) – *lucas.barros@academico.uncisal.edu.br* – Orcid: https://orcid.org/0009-0004-6921-6309

Modalidade: Trabalho Completo

Resumo: Diante do cenário tecnológico atual, cada vez mais presente no dia a dia da população, os dados pessoais tornam-se ativos de suma importância para as instituições. A utilização da identidade digital, torna-se necessária para reduzir processos burocráticos e aumentar a confiabilidade nas relações digitais. Este trabalho aborda um mecanismo sugerido pela World Wide Web Consortium, principal organização de padronização da Web, sintetizado em uma carteira de dados, utilizando credenciais verificáveis e identificadores descentralizados, para garantir segurança, privacidade e autenticidade nos moldes das regulamentações globais para o sistema de saúde pública.

Palavras-chave: credenciais verificáveis; blockchain; identidade auto soberana; healthtech; LGPD.

***Abstract**: Given the current technological scenario, increasingly present in the population's daily lives, personal data has become an extremely important asset for institutions. The use of digital identity is necessary to reduce bureaucratic processes and increase reliability in digital relationships. This work addresses a mechanism suggested by World Wide Web Consortium, the main Web standardization organization, synthesized in a data wallet, using verifiable credentials and decentralized identifiers to guarantee security, privacy and authenticity along the lines of global regulations for the public health system.*

***Keywords**: verifiable credentials; blockchain; self-sovereign Identity; healthcare; LGPD.*

1 INTRODUÇÃO

A transformação digital vem modificando os processos realizados dentro das instituições, além de receber cada vez mais atenção na utilização de processos críticos para reduzir o número de fraudes e garantir um melhor tempo de resposta nas operações de forma confiável.

Diante das novas legislações e normativas mundiais, e com base na General Data Protection Regulation (GDPR), iniciada na Europa no ano de 2012 e aprovada em 2016, servindo de norte para Lei Geral de Proteção de dados pessoais (LGPD) no Brasil, se impõe a necessidade de manter o controle e privacidade nas operações que correspondem ao processamento de dados pessoais em relações comerciais, no meio fisico ou digital, mantendo a preservação da dignidade humana e não discriminação.

Para atingir a maturidade no tratamento de dados pessoais, várias iniciativas vêm sendo debatidas pela indústria de software e academia (Yaqoob, 2021). Dentre essas iniciativas, surge a necessidade de aplicar de uma forma confiável e privada, às informações de identidade de um indivíduo no meio digital (Jørgensen; Beck, 2022). Esse campo de pesquisa visa criar soluções computacionais que possibilitem autenticar documentos ou comprovar a veracidade e origem de uma informação, pautada na criação de normas internacionais e legislações específicas de cada país, no intuito de garantir o acompanhamento e a responsabilização das partes envolvidas no tratamento de dados pessoais.

As carteiras de saúde possibilitam que os indivíduos mantenham controle sobre seus dados pessoais de saúde, assegurando privacidade e segurança.

2 REFERENCIAIS TEÓRICOS

Blockchain, uma tecnologia revolucionária, está preparada para remodelar vários setores e transformar a forma como as transações são conduzidas (Swan, 2018). O seu potencial vai muito além da criptomoeda, à medida que indústrias como a bancária, saúde, arte e educação estão a explorar as suas capacidades (Duy et al., 2018). A ascensão da

tecnologia blockchain atraiu a atenção de vários setores, pois tem o potencial de revolucionar os sistemas e processos tradicionais (Zhou, 2020). A Blockchain consiste em uma rede descentralizada e criptografada que certifica e guarda todas as informações transacionais entre as partes envolvidas de forma imutável (Nakamoto, 2009).

2.1 Ledger

Ledger é referido como um livro-razão distribuído, é um registro digital onde as transações feitas dentro do blockchain são registradas cronologicamente e publicamente. Este conceito é o que permite a existência de um registro transparente e imutável de todas as transações.

2.2 Credenciais Verificáveis (VCs)

Credenciais físicas são constantemente usada pela sociedade, normalmente designadas para comprovar dados de quem a possui e relações entre a pessoa na qual foi designada e a entidadeemissora, são constituída por informações, às vezes sensíveis, sobre o proprietário e o emissor, o assunto no qual a credencial se refere, como atributos e propriedades específicas que a autoridade emissora declara, restrições que possa ser atribuída sobre o documento e informações de como ela foi declarada.

Contudo na web essas credenciais tem seu uso indefinido, o que dificulta a comprovação de certos dados nesse ambiente e o benefício que essas credenciais físicas trazem acaba se perdendo. Então pra expressar esses tipos de credenciais de forma criptograficamente segura, respeitando a privacidade e verificável por máquina as credenciais verificáveis (VCs) foram elaboradas, representando todas as mesmas informações fornecidas por uma credencial física com aadição de tecnologias para torná-las mais invioláveis e mais confiáveis. E aumentando ainda mais a segurança que as VCs podem trazer, a sua integração com a rede blockchain traz a transparência nasoperações, de forma persistente, se mantendo aderente às normas e leis vigentes.

2.3 Identificadores Descentralizados (DIDs)

Atualmente qualquer organização ou indivíduo utiliza identificadores exclusivos globalmente em vários contextos e geralmente são esses identificadores que torna as credenciais físicas únicas, contudo a grande maioria desses identificadores não estão sobre controle dos seus referidos, além de serem facilmente falsificados e reivindicados por outras pessoas. Os mesmo tem um contexto muito individual, sendo aceito em certas organizações específicas e podem revelar informações pessoais de forma desnecessária.

Com isso um novo tipo de identificador que permite uma identidade digital verificável e descentralizada. Os DIDs foram criados para serem independentes de registros centralizados, provedores de identidade e autoridades certificadoras. Fornecendo que as entidades comprovem suaveracidade por meio de uma autenticação criptografada, além de ter controle sobre os dados sensíveis que serão mostrados. Trazendo assim, segurança e confiança nas interações web.

A interconexão entre DIDs e VCs é fundamental e complementar. Os DIDs estabelecem uma infraestrutura para identificação autônoma, enquanto as VCs proporcionam um método para a confirmação de declarações de forma imediata e verificável. A emissão de uma VC associada a um DID resulta em uma comprovação descentralizada e robusta da autenticidade da credencial. Tal associação habilita o controlador do DID a engajar-se em transações digitais com elevado grau de confiabilidade. Conjuntamente, DIDs e VCs constituem os alicerces de um novo modelo de administração de identidade e autenticação no ambiente digital, promovendo uma transformação na interação segura e privada na web.

2.4 Minimização de dados

A minimização de dados, permite que um usuário solicite uma credencial de um emissor, registrada por meio de um blockchain DApp. Quando uma credencial é compartilhada, o usuário pode definir as partes da credencial divulgadas para minimizar o compartilhamento de dadosprivados, mantendo a validade da credencial sem exposição de

dados pessoais adicionais. Além de poder optar por gerar restrição de tempo de acesso para cada instância de compartilhamento, limitando o período de acesso do verificador.

2.5 Minimização de dados por prova de conhecimento zero

A prova de conhecimento zero é um método pelo qual uma parte (o provador) pode provar à outra parte (o verificador) que uma determinada afirmação é verdadeira, sem transmitir qualquer informação. A essência das provas de conhecimento zero é que é trivial provar que alguém possui conhecimento de certas informações simplesmente retornando verdadeiro ou falso. O desafio é provar tal posse sem revelar a própria informação ou qualquer informação adicional.

3 METODOLOGIA DA PESQUISA

A etapa seguinte consiste na aplicação de critérios de inclusão e exclusão, que busca filtrar os resultados, trazendo resultados mais específicos e alinhados com o presente trabalho. Os critérios adotados e os respectivos resultados de trabalhos são apresentados na Tabela 1.

Tabela 1 – Total de trabalhos encontrados por repositório

REPOSITÓRIO	QUANTIDADE
Springer	267
IEEE	94
Total	361

Fonte: Dados da pesquisa (2024).

Critérios: Publicações a partir de 2017 até 2022; Trabalhos acima de cinco páginas; e Proximidade com a temática abordada.

Tabela 2 – Total de trabalhos encontrados por repositório

REPOSITÓRIO	QUANTIDADE
Springer	7
IEEE	4
Total	11

Fonte: Dados da pesquisa (2024).

Após a filtragem com base nos critérios citados anteriormente, a quantidade final de trabalhos reduziu conforme demonstrado na Tabela 2. Nessa etapa, os trabalhos relevantes foram lidos e interpretados integralmente, com o objetivo de compreender completamente as respectivas publicações e trazer seus resultados buscando a aderência a pesquisa e sendo classificado por aproximação ao interesse da pesquisa, chegando a quantidade conforme demonstrado na Tabela 3.

Tabela 3 – Total de trabalhos encontrados por repositório

REPOSITÓRIO	QUANTIDADE
Springer	7
IEEE	2
Total	9

Fonte: Dados da pesquisa (2024).

A próxima etapa do processo consiste em uma pesquisa aplicada, na qual se utiliza como metodologia de trabalho a revisão de literatura e a pesquisa exploratória. Nessa etapa, os trabalhos relevantes foram lidos e interpretados integralmente, com o objetivo de compreender completamente as respectivas publicações e trazer seus resultados para enriquecer a base de conhecimento, bem como debater os mesmos. Dessa forma, os trabalhos serão descritos a seguir.

4 ANÁLISE DO ESTADO DA ARTE

Saidi et al. (2022), propõem o sistema descentralizado DSMAC, baseado em blockchain e Self-Sovereign Identity (SSI), para dados médicos, permitindo que pacientes mantenham o controle sobre suas informações e concedam direitos de acesso a terceiros.

Kaur et al. (2018) destaca a importância dos prontuários médicos e a necessidade de garantir sua segurança e privacidade. Propõe o uso de blockchain para transações confiáveis e auditáveis em dados de saúde, apresentando uma arquitetura baseada nessa tecnologia e sugerindo pesquisas futuras sobre o armazenamento de dados corporativos.

Yaqoob et al. (2021) discute a integração do blockchain em sistemas de saúde, destacando sua capacidade de proporcionar gestão descentralizada, rastreável e segura. Aponta desafios como imaturidade tecnológica, escalabilidade e interoperabilidade, mas

conclui que o blockchain tem potencial para transformar o setor de saúde.

Jørgensen e Beck (2022) propõe uma taxonomia para carteiras universais e enfatiza a necessidade de pesquisa em identidades digitais e gerenciamento de identidade auto-soberano. Discute desafios de desempenho, segurança e governança, além das implicações sociais das carteiras digitais.

Rouhani et al. (2021) propõe o uso de blockchains autorizados, como Hyperledger Fabric, em sistemas de controle de acesso para auditorias confiáveis. Valida o sistema com um caso de uso em bibliotecas digitais, destacando sua audibilidade e escalabilidade. Sugere a criação de uma estrutura independente de plataforma para controle de acesso distribuído.

Hesse e Teubner (2020) introduz a reputação portátil no gerenciamento de identidade digital, apresentando um modelo conceitual e destacando a necessidade de orientação regulatória clara. Propõe o uso de PIMS e blockchain para estabelecer a portabilidade da reputação, abordando desafios sociotécnicos e sugerindo cenários futuros.

Abubakar et al. (2021) descreve uma solução baseada em blockchain para vacinação digital e certificados de teste, usando Ethereum e contratos inteligentes. Avalia a segurança, desempenho e custos de transação, apontando o custo das transações e gerenciamento de chaves como desafios.

Purohit et al. (2021) apresenta o HonestChain, um sistema que facilita decisões rápidas no processamento de solicitações de dados protegidos, beneficiando a pesquisa clínica. Avaliações mostram que o HonestChain é prático, escalável e aumenta a reputação dos provedores, sugerindo melhorias futuras para cargas de trabalho maiores.

Ahene et al. (2022) propõe um esquema de criptografia de assinatura heterogênea com recriptografia de proxy, usando blockchain para projetar um sistema EHR seguro e auditável. O esquema é robusto contra ataques e aplicável a diferentes ambientes criptográficos.

5 SISTEMA PROPOSTO PARA COMPARTILHAMENTO DE DADOS PESSOAIS COM USO DE VC E DID

O ecossistema que compõem esse sistema é elaborado por um emissor(Issuer), no

qual reivindica um novo identificador e cria uma VC para que seja enviado para o detentor/usuário(Holder) dono de uma ou mais VCs no qual contem os seus dados. O Holder tem o poder de gerar uma Apresentação Verificável para ser mostrada ao o verificador(Verifier), que desempenha o papel de verificar a informação para realizar o processamento do dado recebido de forma confiável e segura.

Princípios da identidade descentralizada:

1. Controle do usuário sobre a sua identidade;

2. Acesso disponível a todo tempo;

3. Transparência onde o usuário sabe como os dados são utilizados e por quem;

4. Persistência onde a credencial continua existindo independente de fornecedores;

5. Portabilidade entre vários sistemas e serviços;

6. Interoperabilidade garantindo que os dados possam ser interpretados por outros serviços;

7. Consentimento para que o usuário permita ou não o compartilhamento de dados;

8. Minimização mantendo somente os dados necessários na verificação da identidade;

9. Proteção de dados;

10. Recursos mapeados para implementação;

11. Receituário digital;

12. Mapeamento das áreas demandadas na pesquisa sobre credenciais verificáveis;

13. Atestado médico digital;

14. Acompanhamento na administração de medicamento para o usuário;

15. Acompanhamento dos cuidados básicos de saúde;

16. Divulgação dos pontos de coleta baseado em estoque de medicamento que está disponívelpara o usuário;

6 ARQUITETURA DA SOLUÇÃO PROPOSTA

Nesta sessão, será proposta a utilização de credenciais verificáveis para criação de uma carteira de dados de saúde visando alcançar informações sobre o acompanhamento de

exames periódicos da população.

Com a tecnologia, pode-se ter um controle no gerenciamento de dados pessoais, fornecidos através de uma organização, compartilhando dados escolhidos e reduzindo o compartilhamento aos dados mínimos para a validação da transação. Podendo o usuário decidir os dados que serão transmitidos no momento da solicitação dos dados, com o controle individual por requisição.

A blockchain neste cenário traz benefícios importantes, como imutabilidade, transparência e segurança, para o gerenciamento das transações realizadas, sem que haja a necessidade de armazenamento de dados pessoais na rede blockchain, os avanços da pesquisa apontam a preferência do uso da Hyperledger na implementação de identidades digitais.

6.1 Hyperledger

Hyperledger Foundation é a principal comunidade de desenvolvedores de software que criam código aberto de nível empresarial, na forma de plataformas, bibliotecas, ferramentas e soluções, para sistemas multipartidários usando blockchain, livro-razão distribuído e tecnologias relacionadas; A infraestrutura técnica é hospedada na Linux Foundation, estabelecendo um lar neutro para a infraestrutura da comunidade, reuniões, eventos e discussões colaborativas; impulsionando a ampla adoção da tecnologia construindo um ecossistema substancial e diversificado de provedores de soluções, fornecendo soluções e redes de produção e organizando osusuários finais do setor;

6.1.1 Hyperledger Indy

O Hyperledger Indy é um projeto de código aberto e faz parte do ecossistema Hyperledger. Ele é comumente associado à Fundação Sovrin, que fornece uma estrutura de governança e confiança para identidades digitais baseadas no código do Indy-Node. O projeto chamado de Hyperledger Indy é uma plataforma de contabilidade distribuída projetada especificamente para identidades descentralizadas. Fornecendo ferramentas,

bibliotecas e componentes reutilizáveis baseadas em blockchains ou outros livros distribuídos para que sejam interoperáveis entre domínios administrativos, aplicativos e qualquer outro silo.

6.1.2 Indy-Node

O Indy-Node é o ponto inicial para o desenvolvimento de um projeto com foco em identidades digitais, que é utilizado para criar uma infraestrutura na qual os participantes possam criar e gerenciar identidades digitais auto-soberanas, com ele é possível operar os nós (validadores ou observadores) que compõem a rede de contabilidade distribuída do Hyperledger Indy. Esses nós são a base do blockchain e são responsáveis por processar transações e manter o estado da rede, garantindo a integridade e a confiabilidade dos dados de identidade.

O Indy-Node foi projetado com um forte foco em privacidade e segurança, utilizando técnicas como Provas de Conhecimento Zero (ZKP) para permitir a verificação de credenciais sem expor informações sensíveis. Ele implementa um protocolo de consenso chamado RBFT (Redundant Byzantine Fault Tolerance), que é uma variação do algoritmo de consenso Byzantine Fault Tolerance (BFT).

O Indy-Node suporta o conceito de Identidades Descentralizadas (DIDs) sendo ele o DID:Indy, que está em conformidade com a especificação Decentralized Identifier (DID) publicada pelo World Wide Web Consortium (W3C). O DID:Indy permite a interoperabilidade entre diferentes redes Hyperledger Indy, como Indicio, Sovrin, IdUnion, entre outras.

6.1.3 Indy-CLI

O Hyperledger Indy também fornece o Indy-CLI a sua própria interface de linha de comando, com ele é possível interagir com a rede criada e seus nós, além da criação e gestão de DIDs (Identificadores Descentralizados), a emissão e verificação de credenciais verificáveis, e a administração geral da rede Indy. Ele oferece um meio eficiente para executar comandos relacionados ao ledger, como enviar transações, ler e escrever dados, e

configurar nós na rede. O mesmo suporta dois modos de execução: interativo e em lote. No modo interativo, os comandos são inseridos um a um na linha de comando, enquanto no modo em lote, os comandos podem ser executados em série a partir de um arquivo de texto ou pipe. Isso facilita a automação de tarefas e a integração com outras ferramentas e sistemas.

Foi criado para ter uma flexibilidade podendo ser conectado a qualquer número de ledgers Indy e permitindo que os usuários interajam com diferentes redes de acordo com suas necessidades.

6.1.4 Indy-VDR (Verifiable Data Registry)

O Indy-VDR (Verifiable Data Registry) é uma biblioteca e servidor proxy desenvolvidos para interagir com instâncias do ledger do Indy Node. Ele é escrito em Rust e inclui uma interface de programação de aplicativos (API) para Python e um servidor proxy independente. Podendo se conectar a um ou mais pools de ledgers do Indy Node, dados conjuntos de transações de gênese. Ele fornece métodos para construir solicitações de ledger e enviá-las aos validadores, coletando os resultados e garantindo que haja consenso entre os nós.

6.1.5 Hyperledger Aries

O Hyperledger Aries também é um projeto de código aberto e faz parte do ecossistema Hyperledger. Ele não é um blockchain nem uma aplicação, mas sim um kit de ferramentas compartilhado, reutilizável e interoperável projetado para iniciativas e soluções focadas na criação, transmissão e armazenamento de credenciais digitais verificáveis. É uma infraestrutura para interações peer-to-peer baseadas em blockchain. Este projeto consome o suporte criptográfico fornecido pelo Hyperledger Ursa, para fornecer gerenciamento seguro de segredos e funcionalidade descentralizada de gerenciamento de chaves.

6.1.6 Aries Cloud Agent - Python (ACA-Py)

O ACA-Py é um agente Aries que roda em servidores, incluindo ambientes de nuvem, corporativos e dispositivos IoT, e não é projetado para dispositivos móveis. Ele é construído sobre os conceitos e funcionalidades do Aries Interop Profile (AIP) 2.0, suportando protocolos Aries essenciais para a emissão, verificação e posse de VCs. Ele funciona criando um controlador de lógica de negócios que “conversa” com uma instância do ACA-Py, enviando solicitações HTTP e recebendo notificações via webhook. O ACA-Py lida com os protocolos Aries e DIDComm e funcionalidades relacionadas, enquanto o controlador pode ser construído em qualquer linguagem que suporte HTTP, sem a necessidade de conhecimento em Python. Isso permite que os desenvolvedores se concentrem em construir soluções de VC usando tecnologias de desenvolvimento web familiares.

Com isso o objetivo de gerência de dados médicos é construído fornecendo transparência, segurança, descentralização, rastreabilidade e imutabilidade aos dados escritos no ledger da rede blockchain, diminuindo a necessidade de confirmação de veracidade por terceiros em cada documento gerado. Fornecendo também uma facilidade no controle e no fornecimento dos dados decada usuário.

7 CONCLUSÃO

Neste artigo, mostramos uma alternativa para criação do registro eletrônico verificável e identidade digital descentralizada, para compartilhamento de dados baseado em blockchain usando DID e VC, fundamentada na recomendação da W3C. O sistema proposto permite que os usuários gerenciem seus dados pessoais por meio do armazenamento fornecido por diversos sistemas. Podendo autenticar a identidade e provar a propriedade dos dados sem a necessidade de nenhum sistema centralizado e interação humana.

REFERÊNCIAS

ABUBAKAR, M.; McCARRON, P.; JAROUCHEH, Z.; AL DUBAI, A.; BUCHANAN, B. Blockchain-based platform for secure sharing and validation of vaccination certificates. In:

INTERNATIONAL CONFERENCE ON SECURITY OF INFORMATION AND NETWORKS (SIN), 14., 2021. **Proceedings** [...]. [S. l.]: IEEE, 2021. v. 1, p. 1–8.

AHENE, E.; WALKER, J.; GYENING, R.-M. O. M.; ABDUL-SALAAM, G.; HAYFRON-ACQUAH, J. B. Heterogeneous signcryption with proxy re-encryption and its application in EHR systems. **Telecommunication Systems**, [S. l.], v. 80, n. 1, p. 59–75, 2022.

DUY, P. T.; HIEN, D. T. T.; HIEN, D. H.; PHAM, V. H. A survey on opportunities and challenges of blockchain technology adoption for revolutionary innovation. In: INTERNATIONAL SYMPOSIUM ON INFORMATION AND COMMUNICATION TECHNOLOGY, 9., 2018. **Proceedings** [...]. [S. l.]: ACM, 2018. p. 200–207.

HESSE, M.; TEUBNER, T. Reputation portability quo vadis? **Electronic Markets**, [S. l.], v. 30, n. 2, p. 331–349, 2020.

JØRGENSEN, K. P.; BECK, R. Universal wallets. **Business & Information Systems Engineering**, [S. l.], p. 1–11, 2022.

KAUR, H.; ALAM, M. A.; JAMEEL, R.; MOURYA, A. K.; CHANG, V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. **Journal of Medical Systems**, [S. l.], v. 42, p. 1–11, 2018.

NAKAMOTO, S. Bitcoin open source implementation of P2P currency. **P2P**, [S. l.], v. 11, 2009. Disponível em: https://bitcoin.org. Acesso em: 8 dez. 2024.

PUROHIT, S.; CALYAM, P.; ALARCON, M. L.; BHAMIDIPATI, N. R.; MOSA, A.; SALAH, K. Honestchain: Consortium blockchain for protected data sharing in health information systems. **Peer-to-Peer Networking and Applications**, [S. l.], v. 14, n. 5, p. 3012–3028, 2021.

ROUHANI, S.; BELCHIOR, R.; CRUZ, R. S.; DETERS, R. Distributed attribute-based access control system using permissioned blockchain. **World Wide Web**, [S. l.], p. 1–28, 2021.

SAIDI, H.; LABRAOUI, N.; ARI, A. A. A.; MAGLARAS, L. A.; EMATI, J. H. M. DSMAC: Privacy-aware decentralized self-management of data access control based on blockchain for health data. **IEEE Access**, [S. l.], v. 10, p. 101011–101028, 2022.

SWAN, M. Blockchain for business: Next-generation enterprise artificial intelligence systems. In: ZELKOWITZ, M. V. **Advances in computers.** [S. l.]: Elsevier, 2018. v. 111, p. 121–162.

YAQOOB, I.; SALAH, K.; JAYARAMAN, R.; AL-HAMMADI, Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. **Neural Computing and Applications**, [S. l.], p. 1–16, 2021.

ZHOU, L.; LU, R.; WANG, J. Development status, trends and challenges in the field of “blockchain and education”. **Journal of Physics,** [S. l.], v. 1621, p. 012112, 2020.