Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2781 (Cunningham) – As Amended April 5, 2022

**SUBJECT**: Office of Digital Innovation: blockchain technology study: employment claims

**SUMMARY**: This bill would require the Office of Digital Innovation (ODI) to study the feasibility and appropriateness of the Employment Development Department (EDD) utilizing blockchain technology for the purposes of identity verification and fraud prevention. Specifically, **this bill would**:

1) Require ODI to study the feasibility and appropriateness of the utilization of blockchain technology by EDD for the purposes of identity verification and fraud prevention, subject to the availability of funding in the bill or in the annual Budget Act.

2) Specify that the study pursuant to 1), above, shall include evaluation of potential inequities in the processing of claims and administration of benefits that could result from the use of blockchain technology by EDD for identity verification and fraud prevention.

3) Require ODI, by January 1, 2024, to report to the Legislature on the findings of the study conducted pursuant to 1), above, including the risks, benefits, and considerations for the potential use of blockchain technology by EDD for the purposes of identity verification and fraud prevention.

4) Define "blockchain," for the purposes of the bill, to mean a mathematically secured, chronological, and decentralized ledger or database.

5) Specify that the report submitted pursuant to 3), above, shall be submitted in compliance with existing laws pertaining to the submission of reports to the Legislature.

6) Provide that the provisions of the bill shall remain in effect only until January 1, 2026, and as of that date are repealed.

**EXISTING LAW**:

1) Establishes, within the Government Operations Agency (GovOps), ODI, with the mission of delivering better government services to the people of California through technology and design; and specifies that ODI will fulfill this mission by: collaborating with state entities to transform government services; investing in state capabilities to put users first, build iteratively, and let data drive decisions; rethinking and improving how the state buys digital services; and expanding the use of common platforms, services, and tools. (Gov. Code Sec. 12815.)

2) Declares, on behalf of the Legislature, that the public good and the general welfare of the citizens of the State require the compulsory setting aside of funds to be used for a system of unemployment insurance providing benefits for persons unemployed through no fault of their own, and to reduce involuntary unemployment and the suffering caused thereby to a minimum. (Unemp. Ins. Code Sec. 100.)

3) Establishes, within the Labor and Workforce Development Agency, EDD, to assume the duties, purposes, responsibilities, and jurisdiction of prior state agencies relating to job creation activities; and specifies that EDD shall be administered by a Director of Employment Development vested with the duties, purposes, responsibilities, and jurisdiction concerning: job creation activities; making manual computations and making or denying recomputations of the amount and duration of benefits; determination of contribution rates and the administration and collection of contributions, penalties, and interest; establishment, administration, and transfer of reserve accounts; making assessments and the administration of credits and refunds; and approving elections for coverage or for financing unemployment and disability insurance coverage. (Unemp. Ins. Code Sec. 301.)

4) Provides that it is a violation of law to willfully make a false statement or representation, to knowingly fail to disclose a material fact, or to use a false name, false social security number, or other false identification to obtain, increase, reduce, or defeat any benefit or payment, whether for the maker or for any other person. (Unemp. Ins. Code Sec. 2101(a).)

5) Specifies that, for the purposes of preventing payments on fraudulent claims for unemployment compensation benefits, the Director of Employment Development shall verify, with information provided by the Department of Corrections and Rehabilitation (CDCR), that the claimant is not an inmate currently incarcerated in state prisons; and requires EDD to complete necessary system programming or automation upgrades to allow electronic monitoring of CDCR inmate data to prevent payment on fraudulent claims for unemployment compensation benefits at the earliest possible date, but not later than September 1, 2023. (Unemp. Ins. Code Sec. 321.5.)

6) Requires EDD to provide a plan for assessing the effectiveness of its fraud prevention and detection tools by May 1, 2022, to the Senate Committee on Labor, Public Employment and Retirement, the Assembly Committee on Insurance, the Senate Committee on Budget and Fiscal Review, the Assembly Committee on Budget, and the Joint Legislative Audit Committee; further requires EDD to provide a report with an update on its progress on performing the assessment prescribed by that plan by July 1, 2022, to the same legislative committees; and further requires that, on or before January 1, 2023, and annually thereafter, EDD shall assess the effectiveness of its fraud prevention and detection tools and shall submit the analysis and assessment to the same legislative committees. (Unemp. Ins. Code Sec. 340.)

**FISCAL EFFECT**: Unknown

**COMMENTS**:

1) **Purpose of this bill**: In order to facilitate the extensive identity verification and fraud prevention efforts necessary for EDD to comply with its mandate, this bill seeks to ensure that the State gives due consideration to the relative merit of blockchain technology in supporting EDD's efforts to minimize the loss of state resources to fraudulent claims. This bill is author sponsored.

2) **Author's statement**: According to the author:

> EDD suffered (and continues to suffer) through missteps throughout the pandemic. This resulted in billions of dollars in fraudulent claims being paid out. It also resulted in individuals having their benefits frozen for weeks at a time, having to verify their identity

weekly, and an overall disjointed process that was riddled with errors and left thousands of people in distress.

In the report returned to the legislature by the Calderon Blockchain Group (*sic.*), several recommendations were made to implement digital identity and verifiable credentials. Specifically, the report suggests: "The state should consider using blockchain technology to create and verify tamper-resistant digital certificates of government-issued documents."

Relating to fraud prevention and security, the report also states: "The decentralized aspect of blockchain provides an additional layer of security, making hacking difficult because information cannot be gained or controlled from a single computer server. In addition to security, blockchain provides potential privacy benefits. In contrast to a traditional system in which a central authority verifies transactions, network users validate the transactions in a blockchain, replacing the need for a single third-party institution to provide trust."

3) **EDD, unemployment insurance (UI) fraud, and identity verification**: EDD is, among other things, tasked with administering the State's UI program, which provides partial wage replacement benefits to eligible Californians who have become unemployed. Beginning in March 2020, following the issuance of a statewide stay-at-home order at the start of the COVID-19 pandemic, EDD experienced a surge in the filing of unemployment claims which resulted in a significant increase in EDD's workload. During the same time period, Congress expanded federal UI benefits and relaxed the eligibility criteria for receiving those benefits through the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

In late November 2020, nine county district attorneys announced the discovery of widespread UI fraud involving tens of thousands of incarcerated individuals that took place during the first six months of the pandemic.[1] The extent of the fraud was uncovered after the U.S. Department of Labor crosschecked federal UI claims data against a list of state prison inmates that it had subpoenaed from the State and identified approximately 35,000 claims involving individuals incarcerated in the State's prisons. EDD estimated that it paid roughly $810 million in benefits between January 2020 and November 2020 to 45,000 claimants with information that matched incarcerated individuals.[2] Those figures include individuals incarcerated in county jails who were identified after EDD contracted with a private vendor that provided cross-reference inmate data "from prisons and jails in multiple states," including access to "real-time incarceration and arrest records." [3]

An audit of EDD's management of federal funds related to the COVID-19 pandemic published in January 2021 concluded that billions of dollars of benefit payments were

---

[1] Shawn Hubler, "Unemployment Scam Using Inmates' Names Costs California Hundreds of Millions," *New York Times*, Nov. 24, 2020, https://www.nytimes.com/2020/11/24/us/california-unemployment-fraud-inmates.html [as of April 16, 2022].
[2] Elaine M. Howle, "Employment Development Department: Significant Weaknesses in EDD's Approach to Fraud Prevention Have Led to Billions of Dollars in Improper Benefit Payments," *California State Auditor*, Report 2020-628.2, p. 27 http://www.auditor.ca.gov/reports/2020-628.2/index.html [as of April 16, 2022].
[3] *Id*. at pp. 29-30.

improperly paid due to significant weaknesses in EDD's approach to fraud prevention. Among the Auditor's key findings were the following:

- EDD failed to take fast enough action at the beginning of the pandemic to bolster its UI fraud detection efforts. As a result, from March through December 2020, out of $111 billion in UI benefits, EDD paid about $10.4 billion on claims that it later determined might be fraudulent.

- EDD paid $1 billion of the $10.4 billion in part due to a problematic decision to streamline its processes by removing a safeguard against paying individuals with unconfirmed identities. EDD issued payments to those claimants with unconfirmed identities before discovering it had inadvertently removed the safeguard for more than a four-month period.

- EDD faces an impending workload to assist the victims of identity theft whose personal information was used to file fraudulent claims. Given the high levels of potentially fraudulent claims and its processes for addressing them, EDD is underprepared to handle this work.

- In September 2020, EDD directed Bank of America to freeze 344,000 debit cards (accounts) because of concerns about UI fraud. Since then, EDD has not acknowledge its responsibility for this action, and it did not have a plan or take action to ensure that it could unfreeze those accounts belonging to legitimate claimants.

- EDD left itself especially vulnerable to UI fraud associated with incarcerated individuals […] because it has not had a system to regularly cross-match UI claims with information from state and local correctional facilities.

Clearly, inaccuracies and inefficiencies in identity verification and fraud prevention activities can be extremely costly to the state and impose significant hardship on legitimate UI recipients. In an effort to mitigate similar costs in the future, the Governor's 2022-23 budget proposal includes $29.8 million General Fund to fund six third-party contracts to prevent future fraud within the state's UI programs. These contracts, among other things, include identity verification and fraud detection tools that rely on opaque, artificial intelligence-based technology to flag claims of interest for further investigation. One such tool, a facial recognition-based service provided by ID.me, has come under recent scrutiny for potentially invasive practices. As the Legislative Analyst's Office's (LAO's) February 2022 report "Assessing Proposals to Address Unemployment Insurance Fraud" describes:

> The state hired ID.me to confirm workers' identities using so-called "one-to-one" face matching; that is, when a computer algorithm matches the photo or video submitted by the worker to the worker's identification card. Earlier this month, the company CEO admitted to misleading ID.me clients: although ID.me uses one-to-one matching to confirm identity, the company also made so-called "one-to-many" matches without their client's knowledge. One-to-many matches scan one person's face against large databases and therefore could help identify fraudulent actors who claim multiple benefits.

> However, privacy experts warn that these matching systems are prone to error, suffer from systematic racial bias, and have the potential to be misused.[4]

Another tool, the Thomson Reuters ID Risk Analytics framework, "combines a database of comprehensive public and proprietary records to verify identities. That data is then run through Pondera Solutions, which utilizes refined pattern-detection, program-specific models, and criminal network detection algorithms to identify more sophisticated schemes." In order to function, these tools rely on the accumulation of massive amounts of personal information (PI) from public and private sources, increasing the risk that sensitive data concerning California's most vulnerable residents may be compromised or inappropriately disclosed. Additionally, according to the LAO's report, while EDD identified 1.1 million claims as potentially fraudulent using these tools and stopped payment, more than half of those claims (600,000) were ultimately confirmed to be legitimate. The LAO report accordingly recommends investigating alternatives to these mechanisms:

> As the Legislature considers the ongoing use of facial recognition software for the state's UI system, we recommend that it direct the administration to follow through on the [Governor's strike team investigating the claims backlog and potential improvements at EDD] recommendation to assess the trade-offs and potential unintended consequences of anti-fraud measures, in this case for ID.me. The Legislature may also wish to task the administration with presenting alternatives to biometric scanning that achieve the same (or similar) level of automated security but that pose fewer potential privacy risks and equity concerns. […]
>
> We [also] recommend the Legislature reject the pandemic era anti-fraud contracts with Thomson Reuters for *automated batch review* and *identity risk analytics* because the state's use of these programs adversely impacted the experience of several hundred thousand unemployed workers with legitimate claims [].[5]

By initiating a study to explore the potential for blockchain technology to serve as a mechanism of EDD's identity verification and fraud detection architecture, this bill seems to operationalize the LAO's recommendation that the Legislature task the Administration with determining alternatives to the existing, idiosyncratic identity verification and fraud detection tools employed by EDD.

4) **Blockchain, generally**: The Massachusetts Institute of Technology (MIT) Technology Review describes blockchain as "a decentralized, online record-keeping system, or ledger, maintained by a network of computers that verify and record transactions using established cryptographic techniques."[6] Notably, the ledger of transactions can be added to, but never erased from, meaning the data that has been added to the ledger can never be changed. Blockchain realizes this though a mechanism for creating consensus between scattered or distributed parties that do not need to otherwise trust each other or a specific third-party, but rather need to trust the mechanism by which their consensus is established.

---

[4] Chas Alamo, "The 2022-23 Budget: Assessing Proposals to Address Unemployment Insurance Fraud," *Legislative Analyst's Office*, Feb. 2022.
[5] *Id.*
[6] Mike Orcutt, "Congress Takes Blockchain 101," *MIT Technology Review*, Mar. 15, 2017, https://www.technologyreview.com/2017/03/15/153241/congress-takes-blockchain-101/ [as of Apr. 15, 2022].

Blockchain initially gained notoriety for its applications in facilitating transactions using decentralized, digital currencies known as cryptocurrencies (e.g. Bitcoin, Ethereum). Recording financial transactions, however, is just one of blockchain's many applications. Blockchain technology "can maintain accurate chains of title to securities and other legal instruments in a reliable electronic form" and has been identified as having incredible value in its potential to record and secure an immense volume of trades and financial transactions on a perpetual basis.[7] According to a 2016 report by the Vermont Secretary of State, a valid blockchain can reliably confirm a party submitting a record to the blockchain, the time and date of the submission, and the contents of the record at the time of submission. This means blockchain holds significant utility for confirming authenticity of records, including validation that the record has not been doctored. As the Digital Currency Traders Alliance (DCTA), "a nonprofit coalition of retail investors, traders, businesses, and thought leaders in the Digital Currency space," explains in support of this bill:

> At its core, the blockchain is a growing sequence of "blocks" – units containing transaction data that are recorded to the network. Each new block is attached to the previous block and includes a record of all the previous blocks that preceded it. Records are typically considered unalterable in a blockchain system due to its design. Blocks cannot be altered retroactively without altering all other subsequent blocks or data – an act that requires an enormous amount of computing power. This makes blockchain technology uniquely promising for industries that regularly handle sensitive or personal data.
>
> Additionally, data recorded to the blockchain can be checked and verified – helping to eliminate opportunities for individuals to commit fraud. This can potentially have a huge impact on the effectiveness of government services here in California. The Employment Development Department provides an interesting case study on the potential benefits of implementing this technology.

Indeed, what makes blockchain so attractive for many uses is its security. Corruption or hacking of blockchain transactions is made incredibly unlikely, if not impossible given that the hacker would have to manipulate each block starting from the latest block added to the network in order to corrupt or hack any single transaction of a certain block.

This bill would require ODI to explore the possible utility of this technology for identity verification and fraud prevention by EDD.

5) **Blockchain Working Group (BWG)**: Recently, public and private entities alike have shown interest in blockchain as a possible mechanism for verifiable digital record keeping and identification. In 2018, Governor Brown signed into law two bills relating to blockchain technology, signaling the California state government's interest in exploring applications of blockchain. AB 2658 (Calderon, Ch. 875, Stats. 2018) in particular set the stage for future public and private adoption of blockchain technology by establishing a taskforce, the BWG, to evaluate the uses of blockchain in California's businesses and government. Consistent

---

[7] Riley T. Svikhart, "Blockchain's Big Hurdle," *Stanford Law Review*, Vol. 70, Nov. 2017, https://www.stanfordlawreview.org/online/blockchains-big-hurdle/ [as of Apr. 15, 2022].

with its mandate, the BWG reported its findings to the Legislature on July 1, 2020 in a report entitled "Blockchain in California: A Roadmap."[8]

The BWG's charge was threefold: to define the term blockchain; to evaluate blockchain uses, risks, benefits, legal implications, and best practices; and to recommend amendments to other statutes that may be affected by the deployment of blockchain. Toward the first objective, the BWG arrived at the following definition:

> "Blockchain" is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing trust relationship.
>
> Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. It may also include "smart contracts" that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore.[9]

Notably, this bill does not utilize the definition developed by the BWG, instead defining "blockchain," for the purposes of the bill, to mean "a mathematically secured, chronological, and decentralized ledger or database." Though this definition differs from that of the BWG, however, it does seem to include that definitions key features, and seems consistent with definitions of "blockchain" established in academic literature.

6) **Digital identity verification**: Of relevance to this bill, the potential uses of blockchain assessed by the BWG toward the second objective included "digital identity," i.e. the use of blockchain technology for ascertaining or verifying the identity of an individual. According to the report:

> The State of California is a major provider of identity verification for individuals. The most prominent service the state provides is driver's licenses and state identity cards. These are used daily by individuals for everything from age verification for alcohol purchases to identity verification for boarding airplanes. […]
>
> California is also a significant potential consumer of digital identity. Whenever individuals interact with the government, whether applying for a license, *obtaining benefits*, seeking redress, etc., they must verify their identity. Currently, this requires various paper documents, such as birth certificates, drivers licenses, passports, utility bills (to prove residence) and so on.[10]

Based on its assessment, toward the third objective, the BWG provided the following recommendation to the Legislature:

> The California Legislature should enact legislation that allows public entities to issue as authorized verifiable credentials the identification documents set forth in Section

---

[8] Blockchain Working Group, "Blockchain in California: A Roadmap," *California Government Operations Agency*, July 1, 2020.
[9] *Id.* at p. 18.
[10] *Id.* at p. 34; emphasis added.

> 1798.795(c) of the California Civil Code as verifiable credentials (*sic*.). Individuals would benefit from the ability to have these identification documents available in a secure and verifiable digital form under their control. Verifiable credentials would store no substantive personal information on the blockchain. Instead, decentralized identifiers (DIDs) would be stored verifying that the document was validly issued and shared with the individual's consent. [11]

The "verifiable credentials" referred to in the report are one promising application of blockchain technology that permits the certification of official documents by authorized issuers, in order to give the individual control over their own confidential information. The World Wide Web Consortium (W3C), in its "Verifiable Credentials Data Model 1.0," defines a verifiable credential as "a tamper-evident credential that has authorship that can be cryptographically verified." In essence, a verifiable credential is a set of claims issued about a subject for which the issuer of those claims can be independently verified, such as an assertion that an individual submitting a UI claim is, in fact, the individual specified in the UI claim.

In practice, this means a credential describing some information about an individual, e.g. the individual's age, is issued by an issuer, e.g. the DMV, who has been authorized to confer these credentials. The individual can then present that credential to another entity, e.g. a liquor store, who can cryptographically verify through a data registry that the issuer was authorized to provide that credential. In the examples provided, rather than presenting a physical driver's license in order to purchase alcohol, the liquor store could verify that the individual is over the legal drinking age by, with the consent of the individual, viewing the digital credential, and then verifying that it was issued by a legitimate, authorized entity, confirming the ID is not fake.

Verifiable credentials, like most forms of digital identification relying on blockchain technology, utilize DIDs, so-called "decentralized identifiers" that are unique cryptographic identifiers tied to an individual "wallet," which can in turn store several credentials. As joint report of the Center for Strategic and International Studies and Human Rights Initiative pertaining to "The Human Rights Risks and Opportunities in Blockchain" describes:

> [DIDs] could uniquely represent any person, organization, or object without needing to rely on any centralized registry, government authority, or private ID provider. […] DIDs can be thought of as a kind of URL that is uniquely associated with a single entity and which points to a digital document that contains instructions about how that DID can be used and how the owner can prove that the DID belongs to them. […]
>
> Importantly, at no point would it be necessary for a person to store personal data directly on the blockchain. Identifying information would only be stored by the user in their wallet application or off-chain by third parties according to the nature of that relationship. Blockchain's role in [self-sovereign identity] systems is not to store identity data itself but rather to act as a trusted public reference for DIDs and their associated public keys. The decentralized, immutable nature of blockchain is utilized here as a way of

[11] *Id*. at pp. 32-33

> establishing a common source of truth that lets any party verify who a given DID belongs to and evaluate the authenticity of digital credentials.[12]

In this way, verifiable credentials avoid the need for a centralized datastore that is vulnerable to breach or malfunction, and provide a mechanism by which individuals can verify their identity by certifying that the issuer of the credential (in this case, a document akin to a digital identification card) specifying that the DID corresponds to that individual is legitimate. Seeking to explore ways to capitalize on this potential utility, in 2020, this Legislature passed AB 2004 (Calderon, 2020), which would have created a working group within GovOps to explore the use of blockchain-based technology to provide verifiable credentials for communicating COVID-19 or other medical test results. AB 2004 was vetoed by Governor Newsom, whose veto message acknowledge the "innovative spirit" of the bill, but argued:

> [T]he COVID-19 Testing Task Force is already able to convene stakeholders and experts to discuss innovation in testing and reporting as needed. […]
>
> As an avenue to capitalize on California's innovation economy to meet government needs, last year I established the Request for Innovative Ideas (RFI2) process as a competitive procurement approach that seeks to engage innovators, entrepreneurs, scientists, vendors, and experts to collaborate on designing leading-educe solutions. […] At a time when California is facing fiscal constraints and unprecedented challenges, the millions of dollars this bill would cost would be better spent on timely solutions to meet our most pressing needs.

Nonetheless, as access to government services is increasing through digital media, the need for government agencies to accurately, efficiently, and securely confirm identity in order to avoid fraud is rapidly growing as well. This bill posits that blockchain technology may be a viable solution to meet this need, and recommends exploring its utility in serving those functions on behalf of EDD, which has demonstrated a particularly critical need for a reliable mechanism toward this end. As DCTA argues in support:

> Throughout the pandemic, the stress put on the EDD unemployment benefits system has revealed the deep flaws in the department's work protocols. As much as $31 billion was paid out in fraudulent or potentially fraudulent claims over the course of the last 2 years. This has been linked to data breaches, identity theft, and other misuses of personal data. The uptick in fraudulent claims has also led to legitimate filers having to jump through hoops, including certifying bi-weekly and submitting several different forms of identification while waiting weeks for their benefits.
>
> Fortunately, AB 2781 provides a solution to this longstanding problem. By directing [ODI] to study [EDD's] implementation of blockchain technology into their workflow, we can gain valuable insight into how this technology can be used to protect filers' personal information and streamline the filing process.

7) **Bill prudently contemplates potential equity implications**: While blockchain technology demonstrates significant promise for identity verification and fraud prevention functions,

---

[12] William Crumpler, "The Human Rights Risks and Opportunities in Blockchain," *Center for Strategic & International Studies*, Dec. 2021.

adoption of blockchain for a purpose as critical as the distribution of unemployment benefits without comprehensive study could have catastrophic results. As the BWG's report points out:

> Blockchain adoption is first and foremost a business decision, rather than a technical one. Good use cases must solve real problems for organizations. Great use cases solve real problems at a cost that is significantly lower than the benefits the adoption brings. Blockchain can be a precursor to, and in some cases require, the redefinition of associated processes. Thus, it should be analyzed holistically, rather than strictly through a technical lens.[13]

Over the past several years, blockchain technology has been studied in greater detail revealing a plethora of theoretical applications. But the practical realities of integrating blockchain technology into existing legacy IT systems that must continue to function even as they adapt are not as well studied. In general, one major obstacle to the modernization of legacy IT systems is that those systems are typically essential to fulfilling the day-to-day responsibilities of those agencies. Because state agencies routinely provide critical services to California residents, even temporary service outages can have profound effects on the well-being of the state's residents most in need. This is particularly true with a benefit as critical to the wellbeing of its recipients as UI. Furthermore, while several pilot projects to utilize blockchain technology in government services have been proposed or undertaken across the globe, few if any of these pilot systems have been adopted more widely. As a result, because this technology is so novel in these applications, it is difficult to predict possible long term pitfalls. That this bill requires a study to be undertaken, rather than providing an actual directive that EDD adopt this technology, seems to accommodate this reality, avoiding the hasty adoption of technology that may or may not adequately serve its intended function in practice.

Additionally, as the BWG report indicates, a key ethical consideration when determining whether blockchain technology is appropriate for a given function is whether its adoption will result in fair and equitable outcomes that do not discriminate or further alienate marginalized communities. The report contends:

> Blockchain technologists should implement processes to test for potential biases and seek to remediate their effects in the technology's design. Any type of bias, whether explicit or implicit, can lead to discrimination. It is incumbent upon blockchain proponents, including legislators, industry leaders, and academics, to ensure that we are creating an industry that is free from discriminatory actions and/or inadvertent discriminatory effects.[14] […]
>
> More Californians will ultimately be users of this technology rather than its designers or developers. It is therefore incumbent upon its creators to consider whether their designs are inclusive and advance equity among all California residents. […] Blockchain designers and developers should consider questions such as: how will this technology affect low-income populations, such as the unbanked? Will disabled or senior Californians be offered an equal opportunity to use this technology, particularly when it

---

[13] *Supra*, fn. 8, at p. 24.
[14] *Id.* at p. 28.

> comes to civic rights? Does this technology narrow or increase the gaps between rural and urban populations? Does this technology uniformly protect the privacy rights of all Californians?
>
> Identifying equity as a stated goal of blockchain legislation would be an important step toward cultivating an inclusive approach to this technology.[15]

Evidently acknowledging the essential role equity and fairness considerations must play in any adoption of new technology, including blockchain, the author has prudently specified in the bill that "[t]he study shall include evaluation of potential inequities in the processing of claims and administration of benefits that could result from the use of blockchain technology by [EDD] for identity verification and fraud prevention." This explicit directive to explore the possible social impacts of the technology's use in this space should ensure that the study will not neglect this critical consideration.

8) **ODI seems to be an appropriate entity to charge with performing the study required by this bill**: ODI was created within GovOps with the passage of the fiscal year 2019-2020 budget with a focus on identifying technological solutions to facilitating access to government services. According ODI's 2021 report on the office's activities submitted to the Joint Legislative Budget Committee, "ODI works with agencies, departments and the Governor's Office to rethink, rebuild and create services that better serve and engage Californians and enable new efficiencies. […] ODI applies technology, design, and research to deliver insights, strategy, websites, digital services, and data that respond to and anticipate Californians' biggest needs and challenges."[16] Documenting a sampling of projects ODI undertook during 2020, the report describes ODI's work to assist EDD with improving claimant and employer experiences, indicating that the office "[w]orked with EDD and other partners to simplify the instructions to apply for unemployment insurance, made it easier for employers to provide Work Share benefits, and quickly stood up a system to help claimants certify retroactively in the first months of the pandemic."

   Considering ODI's previous success streamlining processes within EDD and its dedication to applying innovative technology toward these ends, studying the feasibility and appropriateness of EDD utilizing blockchain technology to improve identity verification and fraud detection, as this bill proposes, appears to be an appropriate assignment. Though existing law explicitly provides EDD with the authority to independently conduct internal studies, publish results, and recommend actions, that authority is limited to specific objectives, consisting of: promoting the prevention of unemployment and the stabilization of employment; encouraging and assisting in the adoption of practical methods of vocational training, retraining and guidance; promoting the establishment and operation by government agencies of reserves for public work to be prosecuted in time of business depression and unemployment; promoting the reemployment of unemployed workers; reducing and preventing unemployment; and establishing the most effective methods of providing economic security through all forms of social insurance. (Unemp. Ins. Code Sec. 325.) A mechanism relating to the expedient and secure distribution of benefits does not seem to fall under any of those categories. Additionally, given EDD's considerable backlog of UI claims

---

[15] *Id.* at pp. 28-29.
[16] "Report to Senate Nancy Skinner, Chair of the Join Legislative Budget Committee," *Office of Digital Innovation,* Feb. 2021.

and apparently insufficient resources to faithful carry out its primary functions, diverting department resources toward this end would not seem prudent.

Rather, conducting the study externally, by way of an office specifically dedicated to investigating the role of innovative technology in facilitating government services, EDD can continue to expend all available resources on ensuring the economic security of the people of California as the value of this technology is contemplated.

**9) Related legislation**: AB 2689 (Cunningham) would authorize a public or private entity in this state to accept virtual currency as a method of payment for the provision of any good or service, including any governmental service.

SB 1275 (Kamlager) would authorize a state agency to accept cryptocurrency as a method of payment for the provision of government services.

**10) Prior legislation**: AB 110 (Petrie-Norris, Ch. 511, Stats. 2021) requires the Department of Corrections and Rehabilitation to provide the names and social security numbers of current inmates to EDD for the purpose of preventing payments on fraudulent claims for unemployment compensation benefits, and requires EDD to cross match that information before any payment of unemployment compensation benefits is provided.

AB 2004 (Calderon, 2020) *See* Comment 6.

AB 2568 (Calderon, Ch. 875, Stats. 2018) *See* Comment 5.

SB 838 (Hertzberg, Ch.889, Stats. 2018) authorized corporations and social purpose corporations, which do not otherwise have outstanding securities traded on one of the major U.S. stock exchanges, to adopt provisions within their articles of incorporation authorizing certain records administered by or on behalf of the corporation to be recorded and kept on or by means of blockchain technology, as specified.

**REGISTERED SUPPORT / OPPOSITION**:

**Support**

Digital Currency Traders Alliance

**Opposition**

None on file

**Analysis Prepared by**: Landon Klein / P. & C.P. / (916) 319-2200