Date of Hearing: June 28, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
SB 786 (Hertzberg) – As Amended June 14, 2022

SENATE VOTE: 38-0

SUBJECT: Records: blockchain

SUMMARY: This bill would provide that, in addition to existing required methods, a county recorder may issue a certified copy of a birth, death, or marriage record by means of blockchain technology, as defined. Specifically, **this bill would**:

1) Provide that, in addition to the method required under existing law, a county recorder may issue a certified copy of a birth, death, or marriage record, as specified, by means of blockchain technology.

2) Define "blockchain technology" to mean a decentralized data system, in which the data stored is mathematically verifiable, that uses distributed ledgers or databases to store specialized data in the permanent order of transactions recorded.

EXISTING LAW:

1) Requires each live birth, fetal death, death, and marriage that occurs in this state to be registered as specified on the prescribed certificate forms; and specifies that all confidential information included in birth, fetal death, death, and marriage certificates and reports of dissolution of marriage, legal separation, or nullity that are required to be filed are exempt from disclosure pursuant to the California Public Records Act. (Health & Saf. Code Sec. 102100.)

2) Requires the State Registrar, local registrar, or county recorder to, upon request and payment of the required fee, supply to an applicant a certified copy of the record of a birth, fetal death, death, marriage, or marriage dissolution registered with the official; and specifies that when the original forms of certificates of live birth furnished by the State Registrar contain a printed section at the bottom containing medical and social data or labeled "Confidential Information for Public Health Use Only," that section shall not be reproduced in a certified copy of the record, except as specified. (Health & Saf. Code Sec. 103525(a).)

3) Provides that if a request for a certified copy of a birth, death, or marriage record is made electronically, the official may accept an electronic verification authenticating the identity of the applicant using a multilayered remote identity proofing process that complies with all of the following requirements:

- Meets or exceeds the National Institute of Standards and Technology (NIST) Special Publication 800-63A Digital Identity Guidelines, or its successor publication, on electronic authentication guidelines for multilayered remote identity proofing, as specified.

- Meets or exceeds the information security requirements of the Uniform Electronic Transactions Act and the Federal Information Security Management Act of 2002 and all other applciable state and federal laws and regulations to protect the personal information of the applicant and guard against identity theft.

- Retains for each electronic verification, as required by the NIST Special Publication 800-63A Digital Identity Guidelines, or its successor publication, a record of the applicant whose identity has been verified and the steps taken to verify the identity. Personal information and documents provided to the State Registrar, local registrar, or county recorder for the purpose of identity verification to acquire vital records shall not be used, shared, distributed, or accessed by any other state or municipal agency or third party for any other purpose. (Health & Saf. Code Sec. 103526(a)(3)(A).)

4) Requires that each certified copy of a birth, death, or marriage record issued pursuant to 2), above, to include the date issued, the name of the issuing officer, the signature of the issuing officer, whether that is the State Registrar, local registrar, county recorder, or county clerk, or an authorized facsimile thereof, and the seal of the issuing office. (Health & Saf. Code Sec. 103526.5(a).)

5) Requires all certified copies of birth, death, and marriage records issued pursuant to 2), above, to be printed on chemically sensitized security paper that measures 8.5 inches by 11 inches and that has the following features: intaglio print; latent image; fluorescent, consecutive numbering with matching barcode; microprint line; prismatic printing; watermark; void pantograph; fluorescent security threads; fluorescent fibers; and any other security features deemed necessary by the State Registrar. (Health & Saf. Code Sec. 103526.5(b).)

6) Requires the State Registrar, local registrars, county recorders, and county clerks to take precautions to ensure that uniform and consistent standards are used statewide to safeguard the security paper described in 5), above, including, but not limited to, the following measures: security paper shall be maintained under secure conditions so as not to be accessible to the public; a log shall be kept of all visitors allowed in the area where security paper is stored; and all spoilage shall be accounted for and subsequently destroyed by shredding on the premises. (Health & Saf. Code Sec. 103526.5(d).)

7) Prohibits the State Registrar, local registrar, or county recorder from providing certified copies of birth, death, or marriage records except in accordance with the above specifications. (Health & Saf. Code Sec. 103525(b).)

8) Requires the State Registrar to appoint a Vital Records Protection Advisory Committee to study and make recommendations to protect individual privacy, inhibit identity theft, and prevent fraud involving birth, death, and marriage certificates while providing needed access to birth, death, and marriage record information to those seeking it for legitimate purposes; and assigns that Committee the following duties:

- Reviewing and making recommendations as to the adequacy of procedures to safeguard individual privacy and prevent fraud, while ensuring appropriate access to brith, death, and marriage records.

- Making recommendations to the State Registrar as to items that should be redacted from informational certified copies of birth, death, and nonconfidential marriage certificates.

- Making recommendations to the State Registrar regarding fraud prevention measures concerning vital records. (Health & Saf. Code Sec. 103527(a).)

9) Provides that the Vital Records Protection Advisory Committee appointed pursuant to 8), above, shall include representatives from private and governmental entities that use vital records as identity or legal documents, consumers, law enforcement officials, genealogists, and organizations that research vital records for legal or social purposes; and specifies that the State Registrar shall make every effort to ensure that committee membership also represents the community at large. (Health & Saf. Code Sec. 103527(b).)

FISCAL EFFECT: None. This bill has been keyed non-fiscal by the Legislative Counsel. (*See* Comment #5.)

COMMENTS:

1) Purpose of this bill: This bill seeks to facilitate the secure, expedient electronic delivery of copies of vital records by permitting county recorders to provide certified copies of birth, death, and marriage certificates via blockchain technology. This bill is sponsored by the County Recorders Association of California.

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

> Individuals in immediate need of a certified copy of their vital records – such as birth, death, or marriage certificate[s] – must request it by visiting their local county recorder's office. However, since many individuals do not reside in their county of birth, most vital records are requested by mail, which takes seven to ten days for actual delivery of the document. This is a highly inconvenient process, as individuals usually need these documents to verify their identity when obtaining other essential documents – such as REAL ID, passport, or even to access their retirement benefits.
>
> One such solution is to authorize county recorders to use blockchain to expeditiously deliver an individual's vital records to them immediately. Blockchain is a decentralized, online record-keeping system – or ledger – maintained by a network of computers that verify and record transactions using established cryptographic techniques. Each "block" in the "chain" contains a number of transactions, and every time a new transaction occurs, a record of that transaction is added to every participant's ledger, thus making the data resistant to modification. In other words – blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. SB 786 permits county recorders to issue expedited certified copies of birth, death, [or] marriage certificates using blockchain technology. This effectively allows these vital records to be emailed and received within mere minutes – rather than ten days – and requires no special technology apart from the ability to view a PDF document. SB 786 also provide specific security measures to ensure the certificate's validity can be verified.

3) 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."[1] 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.

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.[2] 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:

> 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.

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, as it is currently in print, would authorize county recorders to issue certified copies of vital records via blockchain technology.

4) **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

[1] 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].
[2] 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."[3]

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.[4]

This bill does not utilize the definition developed by the BWG, instead defining "blockchain technology," for the purposes of the bill, to mean "a decentralized data system, in which the data stored is mathematically verifiable, that uses distributed ledgers or databases to store specialized data in the permanent order of transactions recorded." 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.

5) **Vital records**: "Vital records" generally refers to government records of significant life events, and includes birth certificates, death certificates, marriage certificates, as well as records of fetal death and marriage dissolution. In addition to facilitating the state's maintenance of statistics regarding its constituents, in many cases, these records can be used as identifying documents to obtain government-issued IDs or to access certain benefits. The State of California's website (www.ca.gov) identifies the following uses for birth, death, and marriage certificates, respectively:

> An authorized, certified California birth certificate can typically be used for travel, passport, proof of citizenship, social security, driver's license, school registration, personal identification and other legal purposes.[5]
>
> A certified copy of a death certificate can typically be used to obtain death benefits, claim insurance proceeds, notify social security and other legal purposes.[6]

[3] Blockchain Working Group, "Blockchain in California: A Roadmap," *California Government Operations Agency*, July 1, 2020.
[4] *Id.* at p. 18.
[5] "Apply for Birth Certificate," *California Department of Public Health*, 2022, https://www.ca.gov/service/?item=apply-for-birth-certificate [as of Jun. 25, 2022].
[6] "Apply for Death Certificate," *California Department of Public Health*, 2022, https://www.ca.gov/service/?item=apply-for-death-certificate [as of Jun. 25, 2022].

> A certified copy of a marriage certificate can typically be used as proof of marriage and other legal purposes.[7]

These uses confer particular sensitivity to vital records, especially with respect to birth and death certificates, as their utility in establishing identity and accessing benefits, among other things, means their compromise can create significant risk of fraud or identity theft. As a 2009 summary of a workshop conducted by the United States National Research Council's Committee on National Statistics explained:

> Birth certificates are breeder documents. In the United States, birth confers citizenship, and birth certificates constitute the proof. Thus, birth certificates are used by [the Social Security Administration] to generate Social Security numbers, by the U.S. Department of State as evidence for passports, and by state departments of motor vehicles to issue driver's licenses.
>
> Vital records offices always have had to protect against fraud. Alterations to birth certificates can be used to change identities or to steal them. Death certificates may be altered to commit fraud against insurance companies or to escape arrest warrants. […] [T]o protect against identity theft, it is important to match death with birth certificates and then mark the birth certificate "deceased."[8]

In California, the maintenance of vital records and the production of certified copies are subject to a strictly prescribed set of requirements in order to protect the privacy and security of the subject individuals, and often require coordination between state and local entities. As the BWG's final report explains:

> Vital records, or government-issued documents that catalog life events, are used to validate the identity of a person in order to provide access to a benefit or service such as applying for credit, obtaining a passport, receiving a driver's license, receiving benefits, enrolling a child in school, and more. The three most common types of vital records are birth certificates, marriage certificates and death certificates. […]
>
> In California, vital records are maintained by the local County Recorder's Office where the birth, marriage or death took place and then shared with the California Department of Public Health – Vital Records (CDPH-VR), which maintains birth, death, fetal death/stillbirth, marriage, and divorce records for the state. Local county recorder's offices are responsible for the intake and recording of information: the registration. During this process, birth, death, and fetal death certificate information is submitted to CDPH-VR electronically for state review, processing, and issuing certified copies. Marriage certificates are transmitted to CDPH-VR as paper documents and are subsequently reviewed and indexed to be stored as digital images for issuing certified copies. Services provided by CDPH-VR include issuing certified copies of California vital records, registering and amending records. Currently marriage records are the only type submitted by counties that are not already digitized as part of the registration

[7] "Apply for Marriage Certificate," *California Department of Public Health*, 2022, https://www.ca.gov/service/?item=apply-for-marriage-certificate [as of Jun. 25, 2022].

[8] Steven Schwartz, "The U.S. Vital Statistics System: The Role of State and Local Health Departments," Vital Statistics: Summary of a Workshop, *National Research Council Committee on National Statistics*, https://www.ncbi.nlm.nih.gov/books/NBK219870/ [as of Jun. 25, 2022].

> process. When a paper marriage record is received by CDPH, a staff member scans the document into the vital records database and conducts a key data entry exercise to make that scanned image searchable for issuance. This process is called "indexing."
>
> Because of the range of uses, the validation of vital records is conducted by a multitude of federal, state and local entities that rely on certified copies. Certified copies of vital records are typically marked with a government seal that might be raised or embossed, and/or multicolored. In addition to an official seal, the certificate could include the signature of the state, county or city registrar.[9]

The BWG identifies vital records as one of many possible uses for blockchain technology by this state. In particular, the BWG identifies blockchain's functionality with respect to access and authentication as well suited for the provision of vital records:

> By using the distributed ledger function of blockchain and storing the hash of a digital file (which can correspond to any record), it is possible to assure third parties of the authenticity of the file without revealing the actual content of the record itself. Ensuring that individuals have immediate access to their information and the ability to confirm its authenticity can more quickly connect them to needed services. This allows for more efficient and secure interactions with government, which requires the proper forms of identification for verification.[10]

According to the County Recorders' Association of California, who are the sponsors of this bill, such utility has already been realized elsewhere in the United States:

> Washoe County in Nevada has successful [*sic.*] distributed over 4,500 digital marriage certificates to customers since implementing blockchain technology in 2018. Certificates are delivered within minutes – not just in the United States, but to destinations such as Spain, Canada, and Asian countries. Agencies that have accepted the electronically certified marriage record from Washoe County include the Social Security Administration, the Department of Motor Vehicles, cruise lines, veteran's benefits offices, and other offices that need proof of marriage. Additional Nevada counties have begun using blockchain technology to increase services to their customers.

In 2019, prior to publication of the BWG's report, the author of this bill proposed SB 373 (Hertzberg, 2019), which initially would have permitted a county recorder to issue a certified copy of a birth, death, or marriage record by means of blockchain technology. The Senate Health Committee's analysis of that bill suggested that significant limitation of the bill's provisions due to the sensitivity of vital records may be appropriate. The author subsequently amended that bill to limit the furnishing of certified copies via blockchain technology to marriage records, which are generally the least sensitive of these vital records, and to sunset the authority provided in the bill two years following its effective date. The limitation to marriage records corresponds to the precedent of Washoe County, which was

[9] California Blockchain Working Group, "Blockchain in California: A Roadmap," *California Government Operations Agency*, Jul. 1, 2020, pp. 59-60.
[10] *Id.* at p.62.

subject to similar limitations. SB 373 did not receive a hearing in the Assembly Privacy & Consumer Protection Committee.

In 2021, the author of this bill introduced SB 689 (Hertzberg, 2021), which would have provided that "a certified copy of a birth, death, or marriage record [] may be issued by means of blockchain technology." In contrast to this bill and to SB 373, that bill did not limit the authority to issue vital records via blockchain technology to county recorders. As a result, the role of state agencies in facilitating the process of providing blockchain vital records was unclear, leading to significant estimated costs. According to the Senate Appropriations Committee with respect to SB 689, "[t]he California Department of Public Health's (CDPH) Information Technology Services Division (ITSD) estimates a one-time cost of $158,086,664 and an annual ongoing/maintenance and operations cost of $29,150,000. HSSF and GF []." The Senate Appropriations Committee analysis of that bill explained:

> Due to the nature of vital records (e.g. privacy, statutory requirements, and ongoing requests from the public and counties), the build of blockchain would need to happen in a phased approach. The phased approach assumes that the proposed bill language focused on blockchain technology use for access to obtaining birth, death, fetal death, and marriage certificates. This would impact the Electronic Birth Registration System (EBRS), FileNet, and the Vital Records Image Redaction and Statewide Access (VRIRSA) first. There would also need to be local assistance fund [*sic.*] provided to the local health jurisdictions (e.g. county registrars, county recorders, and local health departments) so that they could utilize, accommodate, and maintain blockchain technology.

Consequent to these estimated costs, SB 689 died on the Suspense File in the Senate Appropriations Committee.

This bill would limit authority to provide vital records via blockchain technology to county recorders, and thus, like SB 373, has been keyed non-fiscal by the Legislative Counsel. That said, it is unclear whether, as indicated with respect to SB 689, local assistance funds would be necessary to assist the establishment of this technology by county recorders.

6) **Bill in print lacks implementation standards, and could consequently jeopardize security of sensitive vital documents**: This bill, as it is currently in print, would authorize a county recorder, in addition to the required existing physical method, to issue a certified copy of a birth, death, or marriage record by means of blockchain technology. The sponsors of this bill argue:

> According to the Pew Research Center report published in 2008, only 37 percent of people live in their hometown. This leaves a large population who may need to obtain their personal vital records housed in the county in which they were born or married. Implementing blockchain technology would allow citizens to request their records be sent to them electronically, without having to travel long distances to obtain the certificate personally, or wait the 7 to 10 days to receive it in the mail.
>
> Having the ability to use blockchain technology would increase productivity in the Recorder's office as well as increase service delivery to the customer in a secure manner. It is more secure than the traditional current method of paper certification which can

> theoretically be forged, due [to] the nature of a decentralized computer network working together to protect the authenticity of the transaction.

However, with respect to the use of blockchain technology for vital records, the BWG report identifies several concerns that are critical to consider in implementing blockchain. Among them are material concerns pertaining to privacy and governance:

> Under the U.S. Constitution, every citizen is protected from unlawful search and seizure. Arguably, this means that even if a government entity is an administrator of information held on a blockchain, that entity may not have unfettered access to personal information of citizens without reasonable controls. This concern is at the heart of many fears surrounding blockchain. Given the general hesitation to publish private information on a distributed ledger, it is recommended that private personal [*sic.*] identifiable information be kept to a minimum. Although vital data may be stored on the blockchain, what generally is stored is a hash of the data, not the data itself.
>
> To preserve privacy, institutions should not store personal information on a blockchain, encrypted or not. They should also be cautious with hashes of private data because hashing functions are deterministic, and if the input is known, the hash can be verified. If a small amount of information is hashed, such as names or emails, an attacker could run through a list of likely inputs and compare the generated hashes. Protection against such an attack is typically achieved by adding arbitrary data (known as salt) to the data that will be hashed.
>
> Additionally, if illegal, incorrect or otherwise objectionable data is entered onto a blockchain ledger, it cannot be removed. The permanence and persistence of this information could potentially affect the privacy of individuals. Strong governance models and controls regarding data security and privacy must be examined carefully to regulate information added to the blockchain.
>
> Finally, to the extent the State retains responsibility for vital records, it will need to establish a mechanism for public oversight of the governance of blockchains used to store and access them.[11]

Because this bill specifies that certified copies may be "issued" via blockchain technology rather than "accessed" via blockchain technology, it is unclear whether the bill makes accommodations for the critical recommendation that the records themselves be stored off of the blockchain, with hashes sufficient for authorized persons to access those documents stored on the blockchain itself.

Additionally, while the BWG report provides this general guidance regarding some key considerations for implementation of blockchain technology in the domain of vital records, it does not provide comprehensive standards or best practices sufficient to direct implementation. Though blockchain technology, if properly implemented, can be extremely secure and efficient, substandard implementation, or implementation not ideally suited for the particular use case, can introduce significant risks.

[11] *Id.* at pp.63-64.

Presently, there is no singular authoritative document on best practices for implementing blockchain technology for this particular use. The World Wide Web Consortium (W3C) maintains a relevant living document of recommendations with respect to the issuing of verifiable documents via blockchain technology, but this document also stresses the case-specificity of implementation. The W3C Recommendation on "verifiable credentials," published March 3, 2022, cautions that there may be some privacy vulnerabilities inherent to the technology, and that careful and specifically tailored approaches to different use cases are necessary to avoid compromising confidential information. W3C writes:

> The persistence of digital information, and the ease with which disparate sources of digital data can be collected and correlated, comprise a privacy concern that the use of verifiable and easily machine-readable credentials threatens to make worse.[12]

The Recommendation identifies 16 different potential privacy vulnerabilities and eight potential security vulnerabilities, suggesting certain best practices in response to each of them, depending on the demands of the use case.

Despite the importance of carefully tailored implementation approaches to the privacy and security of blockchain technology and the sensitivity of the records in question, the bill in print provides no specific guidance on the implementation of blockchain technology for this purpose. In contrast to physical copies of vital records, which are subject to numerous provisions of law that specifically define, e.g., features of the paper on which certified copies must be printed and recordkeeping regarding that paper, this bill would provide no such protections for certified copies issued via blockchain technology. Notably, county governments vary in technical sophistication, and, as such, their capacity to ensure that due care is assigned to this technically complex process may similarly vary. By assigning this authority in perpetuity to all county recorders, the bill would likely result in varied approaches to implementation, which could hinder efficient transaction of records, and may increase the likelihood that vital records are compromised due to implementation that is not consistent with best practices. Should this bill pass out of this Committee, as the bill moves through the legislative process, the author may wish to consider following the precedent of Washoe County and limiting the provision of vital records via blockchain to marriage records, which have less utility in perpetrating identity theft and fraudulently accessing benefits.

7) **Author's amendments**: To clarify that a certified copy of a birth, death, or marriage record shall only be furnished via blockchain technology if it is so requested (#1), and to provide that if such a copy is issued, it must be subject to sufficient technical safeguards to prevent fraud and to protect the privacy of the individual (#2), the author has offered the following amendments:

Author's amendment #1:

On page 4, at the beginning of line 15, insert: "***upon request,***".

[12] W3C Recommendation, "Verifiable Credentials Data Model v1.1," Mar. 3, 2022, https://www.w3.org/TR/vc-data-model/ [as of Jun. 25, 2022].

Author's amendment #2:

> On page 4, after line 17, insert: "***(2) A county recorder that issues a certified copy of a birth, death, or marriage record pursuant to paragraph (1) shall ensure that the release of the copy is subject to technical safeguards sufficient to prevent fraud, and to protect the document and its contents from unauthorized or illegal access, destruction, use, modification, and disclosure.***"
>
> On page 4, line 18, strike "(2)" and insert: "***(3)***".

8) **Related legislation**: AB 2176 (Wood) would require each live birth to be registered with the local registrar of births and deaths for the district in which the birth occurred within 21 days, rather than 10 days, following the date of the event.

AB 2436 (Bauer-Kahan) would revise the information required on a death certificate to include the full names, including all legal names, and birthplaces of both parents, without reference to the parents' gender.

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

AB 2781 (Cunningham) would require the Office of Digital Innovation to study the feasibility and appropriateness of the Employment Development Department utilizing blockchain technology for the purposes of identity verification and fraud prevention.

SB 689 (Hertzberg) *See* Comment #5.

SB 1190 (Hertzberg) would create the California Trust Framework to provide industry standards and best practices for the issuance of credentials used to verify information about a person or a legal entity.

9) **Prior legislation**: AB 751 (Irwin, Ch. 623, Stats. 2021) deletes the January 1, 2022 sunset date for authorizing an official to accept an electronic request for a certified copy of a birth, death, or marriage certificate from an authorized person if the request is accompanied by an electronic verification of identity and an electronic statement sworn under penalty of perjury.

AB 2004 (Calderon, 2020) would have required the Government Operations Agency to appoint a working group to explore methods of using verifiable health credentials for the communication of COVID-19 test results or other medical test results in this state, and would have tasked the Department of Consumer Affairs with establishing procedures for authorizing health care providers to issue verifiable health credentials and with developing and maintaining a verifiable issuer registry. This bill was vetoed by the Governor, who indicated that a competitive procurement approach to investigate these types of solutions already exists via the Request for Innovative Ideas process, and stated "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."

SB 373 (Hertzberg, 2019) *See* Comment #5.

SB 838 (Hertzberg, Ch. 889, Stats. 2018) permits corporations to include a provision in their articles of incorporation authorizing the use of blockchain technology to record and track the issuance and transfer of stock certificates.

AB 2658 (Calderon, Ch. 875, Stats. 2018) *See* Comment #4.

10) **Double referral**: This bill was double-referred to the Assembly Health Committee, where it was heard on June 21, 2022 and passed out 15-0.

REGISTERED SUPPORT / OPPOSITION:

Support

County Recorders Association of California (sponsor)

Opposition

None on file

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