CA Blockchain Working Group

Cybersecurity & Risk Management Report – Arshad Noor

March 21, 2020

1. Describe the California context for the given subject.

As the fifth largest economy in the world, the State of California has an extraordinary influence on almost every aspect of commerce. As a progressive state and the home of Silicon Valley, it leads the world on technology, including matters of data security and privacy. California was the first jurisdiction in the world to pass a law in 2002, mandating the disclosure of a data breach affecting Californians[1]. It was also the first state in the US to pass a privacy law in 2018, protecting the personal information of Californians[2]. It would be an understatement to say that any legislation on blockchain will have an out sized effect on the Californian economy, and quite possibly, the world.

While Silicon Valley companies may have created some of the most useful computing technology to serve people, they have also been responsible for some of the largest data breaches in the world[3]. These breaches affected not just Californians, but people globally. While California might have a responsibility to only serve its residents, given the dark history of some Silicon Valley companies' inventions, it behooves the State to consider the impact of any technology related legislation when it might affect the lives of people around the world. At a time when the world is burdened with decades-long wars, xenophobia and an unprecedented divide between the "haves" and "have nots", any technology related legislation involving blockchain becomes a moral imperative.

In light of this, it is important that the State consider the risks of blockchain technology going awry carefully, and design in fail-safe controls to ensure Californians – and possibly, the world – have mechanisms to reset blockchain transactions before blockchain transactions are deemed secure enough to replace current practices.

2. Review any current literature or pilot projects relevant to the given use case. Describe any existing best practices.

Blockchain is an extraordinarily young technology. As such, it hasn't matured sufficiently to have identified best practices that can be applied to projects across the board. However, given that blockchain technology falls into the intersection of databases, network protocols and security, there are voluminous books and papers on efficient designs and best practices for a variety of use-cases. Without a detailed understanding of each business application, its data model and the impact its

[1] SB-1386 Personal Information: privacy (2001-2002), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386

[2] AB-375 Privacy: personal information: businesses. (2017-2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[3] Jordan Valinsky, CNN Business, July 30, 2019, https://www.cnn.com/2019/07/30/tech/biggest-hacks-in-history/index.html

business transactions are likely to have on networks, it is difficult to make generalized recommendations in these areas.

Notwithstanding this, California's data breach disclosure law provides an extensive record of all publicly disclosed breaches[4] since 2004. While this chronology does not provide guidance on how to prevent these breaches, it does provide a documented record of the types of problems government and private sector companies have not prevented.

Based on 20+ years of active and continuous practice in the field of cybersecurity, and having helped some of the worlds largest companies and government organizations in highly sensitive and mission-critical environments, this author has summarized six best practices[5] for any modern application operating within complex networked systems. The State is strongly encouraged to incorporate as many, if not all, of these best practices for blockchain applications the State will implement. Ignoring these defenses creates vulnerability gaps which will almost certainly be exploited by attackers.

3. What agencies, companies or organizations might benefit most from improvements to data collection, storage, workflow? Which are responsible for managing confidential records, providing benefits, etc.?

Every agency, company and organization can benefit from improvements to data collection, storage and workflow. Technology evolves rapidly; yet business processes are falling behind in leveraging advanced technology to improve services, productivity and security. While the underlying fundamentals of the security best practices (mentioned in the previous answer) are nearly three decades old, nonetheless, they represent the state-of-the-art for protecting information.

4. What is the scale of stakeholders, constituents or beneficiaries affected? (E.g. number of people, size of market, $$ transacted, etc.)

Not applicable, since a specific use-case is not being discussed in this report.

5. How mature is the current IT infrastructure?

Not applicable, since a specific use-case is not being discussed in this report.

6. What are the parameters for consideration regarding security and privacy? (E.g. HIPAA requirements for medical records, other requirements for confidentiality, etc.)

Regardless of the agency involved, with the new privacy law in California and in other jurisdictions, sensitive information has to be protected. Indeed, even if there were no personally identifiable information within a use-case, in order to carry out its mission, the State has to depend on the authenticity and integrity of information it uses in its daily business activities. The security best

[4] Data Breaches, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches

[5] Disruptive Defenses Are The Key To Preventing Data Breaches, Arshad Noor, https://www.forbes.com/sites/forbestechcouncil/2020/03/06/disruptive-defenses-are-the-key-to-preventing-data-breaches/

practices referenced earlier ensure that that information can be protected, and relied upon, with a high degree of confidence.

7. How might blockchain provide value in this context?

While it has always been possible to securely share business transactions with other interested parties within any ecosystem, blockchain technology simplifies many aspects of this process and reduces the friction typically encountered in distributed database designs.

One strong benefit is in enabling transparency by making government data available to the public with little effort on the part of the agency. While this data-sharing must be subject to privacy regulations, it would be the equivalent of a permanent "freedom of information act" record available on the internet. Its benefits to preserving democratic norms and holding the government accountable to its constituents cannot be overstated.

While blockchain has its benefits, it does not eliminate all problems:

- If multiple companies and government agencies must collaborate on transactions to complete business processes, they must all agree on transaction protocols and the rules that regulate those transactions. This can be a simple or burdensome activity depending on the use-case;
- Implementers must handle physical technology problems independent of the blockchain: hardware failures, network outages, security vulnerabilities, etc. It will be argued that multiple copies of the blockchain make data always available. This is true even of traditional databases. However, there is a cost to both that must be taken into account when designing blockchain applications;
- Unless open-source blockchain software implementations are used, licensing costs will be a factor;
- Given the newness of this technology, there is a tendency to equate all blockchain implementations with that of the "Bitcoin" blockchain. However, this is a misconception. There are a variety of ways in which blockchain applications may be implemented. Without a thorough understanding of the use-case and the technical ramifications the implementation, state agencies might not make the optimal decision.

8. What trade-offs should be considered before deciding whether to adopt a block-chain based system? What are the potential risks and benefits?

Blockchain is a technology that solves certain problems in a different way. As with any new technology: mobile, web, cloud, etc., its benefits and risks must be evaluated on a case-by-case basis until a body of knowledge is achieved that promotes the most efficient designs to the forefront. Every application will have differences that may require making trade-offs; to assume that every blockchain application must/will be deployed in a similar manner is misguided.

That said, the requirements for security and risk-management are universal. Even when blockchain is not used, the best practices provided earlier are worth implementing to mitigate California's cybersecurity risks.

9. Who else should be consulted before making a recommendation on this use case?

Not applicable, since a specific use-case is not being discussed in this report.

10. Please include any preliminary recommendations.

Government regulation in some aspects of blockchain development has the potential to address the security problem. While there is no guarantee that regulation will be successful in stanching security breaches, it is certain that in the absence of any regulation, there will continue to be systemic breaches, which on systems operating blockchain applications, will exacerbate losses to consumers.

The following recommendations are made when considering laws related to blockchain. It must be emphasized that these recommendations pertain only to applications implemented and/or used by California government agencies to conduct government business. Private companies may choose to do whatever they wish with blockchain applications to the extent they comply with regulations that govern their businesses.

Certification of Blockchain Application Developers

A fundamental problem with current applications is that, not only are they extraordinarily complex, but they operate within an infrastructure of significant complexity. An inherent lack of understanding of this complexity leads to software developers building software without recognizing the risks to the users of the software. While technological complexity is unlikely to decrease, the only antidote to this problem is to study and understand it.

It is recommended that the State of CA regulate practices followed in other areas of professional endeavor: accounting, law, medicine, engineering including information technology, to minimize risk to the community they serve: specifically, the practice of certifying and/or licensing blockchain application developers who develop for or supply blockchain applications to the State of CA. This can be accomplished through a course of study, an examination, experience and certification much as the networking industry certifies network specialists[6] or the security industry certifies security professionals[7].

While such a "Certified Blockchain Application Developer" (CBAD) course of study or certification exam does not yet exist and cannot guarantee that certified developers may not create faulty or vulnerable software, this is likely to establish a baseline level of knowledge, expertise and experience that mitigates the risk of catastrophic security failures. The State's educational systems – California State University and/or the University of California – should convene a panel of application

[6] CompTIA Network+, https://www.comptia.org/certifications/network

[7] CISSP – The World's Premier Cybersecurity Certification, (ISC)^2, https://www.isc2.org/Certifications/CISSP

development experts from academia and industry to define the curriculum and criteria for becoming a CBAD.

There are many arguments that have been raised against such a proposal; the arguments and their counters are summarized below:

Arguments Against CBAD	Responses
It will stifle innovation and move blockchain investment out of California	California has been a leader in many regulations that have benefited its residents, America and the world; this has only propelled it to become the fifth largest economy in the world. California will, once again, show leadership by ensuring that blockchain applications are built by software developers who are certified to build secure applications that operate in secure environments.
It will be too expensive for some software developers to pay for the certification examination even if they have the knowledge and experience	Community colleges, the CSU and/or UC systems can be encouraged to structure certification exams that can be paid for in a variety of ways: scholarships, internships, apprenticeships, student loans, etc. It is anticipated that the examination itself will not be expensive and will represent an insignificant portion of the CBAD's annual salary – perhaps, less than 1%. The cost of instituting a process for ensuring the security of California's blockchain applications should not be left to chance.
It will be perceived as being discriminatory to people without privilege: a college degree, experience, etc.	A college degree should not be a requirement to be a CBAD. However, possession of relevant knowledge and a demonstration of capability is essential. Both can be achieved through an examination and internships and/or apprenticeships prior to being certified.
It will be perceived as being discriminatory to minorities who are disproportionately under-represented in the technology sector	Community colleges, the CSU and/or UC systems can be encouraged to offer need-based free classes to help people get certified. Such programs can enable them to find internships and apprenticeships that will enable them to qualify to become CBADs.
It will be perceived as the "industry" blocking out individuals from certification	Much as anyone may be certified to become an electrician, a lawyer, a nurse, etc., the State can make it possible for anyone with the appropriate knowledge and experience to become a CBAD. While the details will need to be defined

	separately, any regulation can ensure that the system is fair and open to anyone who chooses to become a CBAD.

Disruptive Defenses

NOTE: These recommendations pertain only to blockchain applications implemented and/or used by California government agencies to conduct government business. Private companies are free to do what they want, but are encouraged to follow similar guidelines.

It is recommended that California make these defenses mandatory for government blockchain applications. While this might seem draconian, the evidence leads to mandatory controls as a logical solution to the problems[8] that continue to persist within the industry. Unless the state disrupts the current paradigm of how applications mitigate the risk of a data-breach, it is conceivable that these problems will persist with blockchain applications.

The vast majority of data-breaches are caused by failures to protect data from known vulnerabilities; very few attacks are caused by "zero-day vulnerabilities" - vulnerabilities that were never known until the attack and its methods were discovered.

Based on more than two decades of cybersecurity practice, it is this author's professional opinion that most vulnerabilities in an application – any application – can be addressed with stronger defenses. These defenses are not unproven new technologies, but are based on current industry standards that raise application security to much higher levels.

While one cannot guarantee that the use of these defenses will prevent an application from being compromised (since not all threats can be mitigated, or the cost of mitigating all threats will make it prohibitively expensive to implement the application), one can reasonably expect a high probability of a compromise if one or more of these defenses are not incorporated within the application.

These defenses are:

1. **Eliminate *weak authentication technology***: Invented in the 1960's, the *username/password* technology is the progenitor of a class of *authentication* schemes, including *One-Time Passcodes (OTP), Short Message Service (SMS) Codes, Knowledge Based Authentication (KBA), etc.*, that are compromised on a regular basis. They present applications on the internet as targets of "scalable attacks" where a compromise of the authentication scheme compromises everybody's credential.

[8] Beware – This Open Database on Google Cloud 'Exposes 200 Million Americans', Forbes, https://www.forbes.com/sites/zakdoffman/2020/03/20/stunning-new-google-cloud-breach-hits-200-million-us-citizens-check-here-if-youre-now-at-risk/#52d6a0398587

a. **Recommendation**: The use of *public-key cryptography* authentication will eliminate authentication secrets in applications, thus eliminating the attack vector on target systems. Combining this with cryptographic hardware to protect cryptographic keys will prevent compromises of the user's credential. Invented three decades ago, public-key cryptography is used to protect the most sensitive systems around the world. Expensive and complex in the past, industry standard protocols from the FIDO Alliance and the World Wide Web Consortium[9], reduce this cost and complexity dramatically. NIST rates FIDO standards at Authenticator Assurance Level 3[10], its highest assurance level for authentication, which provide "*very high confidence that the claimant controls authenticator(s) bound to the subscriber's account*".

    i. **Objections**: The use of public-key cryptography with cryptographic hardware will be expensive and not provide the level of desired security due to advances in Quantum Computing (which have the potential to "brute-force" compromise public-key cryptography).

    ii. **Response**: The FIDO2 protocol has been standardized at this time of writing across operating system platforms (Windows, Android, iOS, OS-X[11]) and all modern browsers (except Internet Explorer). Additionally, cryptographic hardware which support the FIDO2 protocol are now standard components in modern business desktops, laptops and mobile devices. As such, the burden of Californians adopting this authentication technology is reduced to web-applications supporting the use of FIDO2 to authenticate users. Login.gov is a US Federal website that supports this authentication protocol, and aims to become the gateway to all Federal applications for consumers.
    NIST and its contemporaries are aware of the threat to public-key cryptography by Quantum Computing. However, NIST has been conducting a program to standardize "post-quantum safe" cryptographic algorithms[12]. It is this author's professional opinion that the next 3-5 years will see post-quantum safe cryptographic algorithms incorporated into FIDO/W3C protocols for strong-authentication.

2. **Ensure the *provenance* of a transaction before it enters the blockchain**: Applications almost, universally, assume that data received within a server is the same data input at the user. This cannot be taken for granted due to inherent vulnerabilities. This is true even when

[9] Web Authentication, W3C Recommendation, https://www.w3.org/TR/webauthn/

[10] Digital Identity Guidelines, US NIST Special Publication 800-63B, Pages 3 and 8, https://doi.org/10.6028/NIST.SP.800-63b

[11] At the time of writing this report, Apple, Inc. has only provided partial support for FIDO protocols, but its joining the FIDO Alliance is a statement of commitment to this capability. https://www.forbes.com/sites/kateoflahertyuk/2020/02/12/apple-just-made-a-striking-new-security-move-that-could-impact-all-users/#6369c07331a7

[12] NIST Computer Security Resource Center, Post-Quantum Cryptography, https://csrc.nist.gov/projects/post-quantum-cryptography

the application uses the Transport Layer Security (TLS) protocol to secure data-transmission . There are two vulnerabilities that TLS cannot protect from: i) the theft of a stolen user credential, such as their username/password; and ii) the compromise of data within the user's computer after it is submitted by the legitimate user and before it enters the TLS channel - this is possible if the computer system on which the user is executing the transaction has been compromised[13].

   a. **Recommendation**: A *digitally signed* blockchain transaction before it is submitted by the user will mitigate this risk. However, it is essential to protect the cryptographic key performing the digital signature. This is typically accomplished using cryptographic hardware to secure the *signing key*. With a digitally signed transaction, i) the attacker will not be able to submit a spurious transaction because he will not have possession of the user's *signing key*; and ii) any modifications of the signed transaction, by the attacker, will alert the application through a failed verification of the user's signature. It is noteworthy to mention that the FIDO2 protocol which can strongly authenticate users, also includes specifications for *Transaction Confirmation* that delivers this capability.

      i. Not having heard any objections to this recommendation, there is no counter response.

3. **Preserve the confidentiality of sensitive information within and outside the blockchain**: This is no longer an option; the California Consumer Privacy Act (CCPA) requires this as do many laws around the world. Encryption is the industry standard mechanism for preserving the confidentiality of sensitive information.

   a. **Recommendation**: Only applications that have a need to see/use sensitive data must be responsible for encrypting and decrypting sensitive data. Applications must use dedicated cryptographic modules to perform this function and not take it upon themselves to perform these operations. Adhering to NIST guidelines and in keeping with industry best-practices, the cryptographic modules must be FIPS 140-2 or FIPS 140-3 certified[14]. The cryptographic operation (encryption/decryption) must not be delegated to general-purpose elements of the blockchain application, including the blockchain itself. It is imperative that sensitive data be encrypted before it gets on the blockchain so its confidentiality is not compromised.

      i. Not having heard any objections to this recommendation, there is no counter response.

4. **Preserve the integrity of transaction data even when outside the blockchain**: While a user-submitted digitally signed transaction provides assurances about the *provenance* of the

[13] Man-in-the-middle (MITM) Attack, Wikipedia, https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[14] NIST Computer Security Resource Center, Security Requirements for Cryptographic Modules, https://csrc.nist.gov/publications/detail/fips/140/2/final

transaction, it cannot guarantee the integrity of transactions as that data morph over its lifetime

   a. **Recommendation**: A digital signature must be applied on the transaction by the application each time the transaction undergoes a change; this ensures that the integrity of the transaction can be verified through its lifetime. It is imperative that the transaction be signed before it gets on the blockchain so its integrity is preserved within and outside the blockchain. As with the recommendations on confidentiality, it is recommended to adhere to NIST FIPS 140-2 or FIPS 140-3 cryptographic modules to protect the signing keys of the application.

      i. Not having heard any objections to this recommendation, there is no counter response.

5. **Use cryptographic hardware wherever cryptographic keys are used**: Cryptography is complex; application developers not used to working with cryptography underestimate the task and skimp on security controls around key-management – the discipline of managing the life-cycle of cryptographic keys. Even billion dollar companies have been compromised because of this[15].

   a. **Recommendation**: Blockchain applications using cryptographic keys for encryption and signing must use FIPS 140-2 or FIPS 140-3 certified cryptographic hardware solutions to secure cryptographic keys, in adherence to NIST guidelines and in keeping with best-practices of the industry

      i. **Objections**: The use of cryptographic hardware modules will be expensive and not provide the level of desired security based on recent discoveries of hardware vulnerabilities[16].

      i. **Response**: Specialized cryptographic hardware solutions were expensive – and continue to remain expensive for ill-informed buyers. However, the industry innovated by delivering industry-standard security hardware at very reasonable prices[17]. Currently, every business-class laptop, desktop, server and mobile device come embedded with *secure elements* that are cryptographic hardware elements capable of sophisticated key-management functions when designed appropriately. Intel's vulnerabilities were due to the optimization of the central processing unit (CPU) for faster operations, without taking account potential vulnerabilities. A

[15] The Marriott Data Breach, Federal Trade Commission, https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

[16] Meltdown and Spectre: "worst ever" CPU bugs affect virtually all computers, The Guardian, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw

[17] Trusted Platform Module, Wikipedia, https://en.wikipedia.org/wiki/Trusted_Platform_Module

purpose-built cryptographic element is significantly less complex with fewer opportunities for compromise.

6. **Ensure application access to cryptographic services remains within a *secure zone***: Cloud computing presents many opportunities for alternative deployment strategies for IT systems, yet challenges traditional notions of data security. Companies have made the mistake of taking "on-premises" applications to the public cloud on the assumption that cloud service providers (CSP) have better security controls to protect data. Sadly, evidence suggests the opposite[18].

   a. **Recommendation**: Blockchain applications that use the public cloud must leverage an application architecture[19] that defines a *secure zone* – distinct from the cloud's *public zone* – where the application has access to cryptographic services.

      i. Not having heard any objections to this recommendation, there is no counter response.

Agency specific Blockchain Advisory Groups

Given the paradigm shift that blockchain based systems are expected to have on current systems, California agencies must establish Blockchain Advisory Groups with the following types of representatives/stakeholders to oversee the creation and modification of public-sector blockchain based systems that have an impact on consumers:

- Business representatives;
- Government representatives of existing systems-of-record (where public records are involved);
- Independent legal and privacy advisers;
- Experienced regulators from other sectors such as construction, finance, utilities, etc.;
- Experts proficient in systems, application and cryptographic security – not network security;
- Representatives of the public who will be affected by the blockchain based system;

Until such time it is demonstrated that the industry and government have reasonable control over cybersecurity risk – where no harm befalls the consumer from moving to/using the blockchain based system – such a group must be used to help guide public institutions in these implementations.

[18] Uber Reveals Data Breach and Cover-Up, Leading to Two Firings, The Wall Street Journal, https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453
Capital One Data Breach Compromises Data of Over 100 Million, The New York Times, https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

[19] Build a Regulatory Compliant Web Application, Arshad Noor, https://www.ibm.com/developerworks/cloud/library/cl-regcloud/

Online Academic/Industry Security Advisory Group

It is recommended that the state establish a public online forum, and invite security and cryptography experts from academia and the industry to join this forum to review security designs for blockchain appliances, and provide feedback to the state. The proposed forum might work along the following lines, with details to be finalized by the state:

1. California state announces forum publicly, and invites security experts from academia and the industry to join the forum to provide voluntary feedback on proposed blockchain application security designs. The state defines the rules of engagement for the forum, and has final decision on who is accepted to this forum; general public may have read-only access to the forum;
2. California agencies proposing to build or implement blockchain applications post the security architecture – which must include a *threat model* of proposed application on the forum – and publish a *Request for Comments (RFC)*;
3. Academic experts accepted to the forum should have the first opportunity to debate among themselves to arrive at a consensus among themselves (if feasible);
4. Industry experts accepted to the forum may provide their comments before the closing date of the specific RFC;
5. The agency's Blockchain Advisory Group reviews comments and makes a recommendation on the security design/architecture.
6. Final security design/architecture is published on the forum for general public.

While this process is clearly likely to slow the implementation of an agency's blockchain application, it benefits from having the threat-model and security design reviewed by dozens of professional security experts. This process is similar to the process used by Internet Engineering Task Force (IETF) to define standards for the internet through its request for comments.

Publishing Forensic Report of Data Breaches

When California passed its data breach disclosure law in 2002, it did something bold. However, it did not go far enough that could have prevented the 11,000 publicly disclosed breaches that followed the law going into effect: it did not mandate that the company or government agency publish a standardized forensic report that documents the breach and the mechanics of how it occurred.

When a data breach occurs today, most cybersecurity professionals who do not have access to the evidence, have to deduce (at best), or guess (at worst) how the data breach occurred and what might have prevented it. The industry that creates technology products and universities that educate/train new generations of technology professionals have no knowledge of how to prevent these problems within their applications and infrastructure unless the US Cybersecurity and Infrastructure Security Agency (CISA)[20] publishes an advisory of a vulnerability through a US-CERT alert.

Much as the US Department of Transportation researches automobile accidents and publishes advisories through the National Highway Traffic Safety Administration, and the Federal Aviation Administration investigates airplane crashes to learn how to prevent future crashes, it is strongly recommended that the California Legislature modify its existing breach disclosure law to require companies and government agencies that are breached to produce and publish a "Data Breach Forensic Report" (DBFR). The DBFR should be standardized[21] to carry sufficient information regarding technology components, version numbers, design methods, application and system configuration details with an explanation on how the data breach occurred. The team providing the forensic report should also provide recommendations on how the data breach might have been prevented.

The DBFR should be accessible publicly so academia and the technology industry may learn from them and improve their designs and technology implementations.

Private, Permissioned Blockchains

It is recommended that different blockchains be used for different application contexts to manage financial and operational risk.

While a home and an automobile are assets, typically purchased by consumers and registered with the State of California, given the different ecosystems these asset classes operate in, two separate blockchain based systems to track these assets is logical. The same analogy applies to humans who participate in different ecosystems: healthcare, education, finance, government, employment, commerce, etc. Each ecosystem may be deserving of its own blockchain to support California agency transactions pertaining to that ecosystem.

Just as a traditional relational database management system (RDBMS) is designed to solve a specific business problem, so must a blockchain based application system; to use a single or a few blockchains for all government related transactions is analogous to using one or a few RDBMS to track all government transactions – it is simply a bad and unwieldy design.

For instance, the registration of an automobile to a specific individual or business, whose address is listed within the registration is essential as a matter of public record to satisfy claims of ownership of the asset. But, is it essential that anyone with access to the internet and an "automobile blockchain" be able to determine the name and address of someone they see in a vehicle with a specific registration number? Not necessarily. However, within the context of the life-cycle of the

[20] Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/about-cisa

[21] Much as the state convened the California Blockchain Working Group, it should convene a similar California DBFR Working Group to draft a policy, procedures and standardized report formats to support the creation, collection and distribution of such reports. While it would be logical for the US Federal government to establish a department to perform these functions (similar to the NHTSA and the FAA who do so for their respective industries), it is recommended that California not wait for the Federal government to initiate this effort.

automobile, authorized individuals and organizations must be able to ascertain these facts. This authorization must be defined in policy to ensure that the privacy of the asset owner and the public good is served. Systems must be designed with appropriate security controls to implement such policies.

Privacy is a desirable feature of information that is not – nor must it be positioned as – a contradiction to the immutability of blockchains. The State must take into consideration that neither a blanket privacy law nor a headlong rush to blockchain is the optimal answer for society. Where transparency of information serves a public good, government must make considered decisions to find the right balance.

Experimental Period

The speculative nature of crypto-currencies and the dramatic events surrounding public blockchains – the collapse of Mt. Gox[22] and the "hard fork" of the Ethereum blockchain[23] - suggests that the State of California might consider defining an *experimental* period of perhaps 5-7 years, where State implementations of blockchain based applications are restricted to only private and/or permissioned blockchains, under the State's control, for use-cases that reflect public data. This does not imply that the State may not implement blockchain based applications – merely that in the early phases of adoption, the State avoids the use of public, permission-less blockchains such as the Bitcoin blockchain, Ethereum or similar public blockchains where anyone may participate in introducing transactions and/or processing data without permission.

Initial applications might be in experimenting with a blockchain simulating the Registry of Births, Deaths and Marriages, or the registration of Business Entities, where information is public by law. This will enable the State to enter the field cautiously and learn from its experience before taking bolder steps. However, until such time computer security and the blockchain ecosystem can prove it can protect the average consumer (so no additional harm befalls them that they might not be exposed to under current systems), State agencies must run parallel systems to ensure that in the event of a conflict, existing systems-of-record will prevail over blockchain based systems.

[22] Mt. Gox, Wikipedia, https://en.wikipedia.org/wiki/Mt._Gox

[23] The DAO (organization), Wikipedia, https://en.wikipedia.org/wiki/The_DAO_(organization))

Appendix A

A Brief Background on Information Security

In an age where almost everyone in the developed world – and increasingly, people in the developing world – are connected to the internet, businesses are rapidly transforming themselves to transform how they manufacture products for, and how they deliver services to their customers. Every sector of the economy is affected by the new ways of conducting business over the internet. However, what is little recognized is that important elements of trust engendered over centuries of handwritten ledgers and record-keeping, are being eroded through this transition.

If we assume that consumers and markets had implicit trust in business transactions in the middle of the 20th century, when almost all record-keeping was manual and based on handwritten records, the introduction of mainframe computers did not erode this trust. Checks and balances, implemented during the days of manual record-keeping continued to verify that mainframes recorded and delivered the same results as manual ledgers. Additionally, given the cost of transitioning to computerized record-keeping was very high, enormous care was taken to ensure that data integrity was maintained. Data confidentiality was not questioned since even vast swaths of people within the company implementing such technology, were prevented from accessing such systems and data.

It can be said, that at the peak of mainframe and mini-computer usage for data-processing, computers were viewed to offer dramatic improvements in productivity to business transaction processing without the loss of data-authenticity, confidentiality or integrity. The advent of the Personal Computer (PC), Local Area Networks (LAN), the internet and eventually, the world-wide web (WWW) heralded the erosion of trust.

The cost of deploying PCs and LANs were insignificant compared to the cost of deploying a mainframe and/or mini-computers; as a result, the discipline inculcated over years in managing mainframes and mini-computers were largely ignored as business processes transitioned to PCs and LANs. But, with the introduction of the internet and the WWW, businesses began to experience the consequences of ignoring security in the newly transitioned/created business processes that leveraged PCs, LANs and the WWW.

The outbreak of the Morris Worm[24] in 1988, began a long slide that resulted in California passing the first regulation of its kind anywhere in the world in 2002[25]. It mandated businesses to disclose data-breaches affecting California residents. Since the passage of this law, more than 10,000 publicly disclosed breaches and more than 11 billion breached data-records have been recorded[26] with

[24] Morris Worm, Wikipedia, https://en.wikipedia.org/wiki/Morris_worm

[25] SB-1386 Personal Information: privacy (2001-2002), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386

[26] Data Breaches, Privacy Rights, Clearinghouse, https://privacyrights.org/data-breaches

dozens of jurisdictions around the world passing new data-security and privacy regulations of which the most notable are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA). [*NOTE: When this document is merged with other submissions in the final recommendation, please include a cross-reference to Jason Albert's Privacy related submissions, here. Thank you.*]

What this suggests is that while businesses have invested hundreds of billions of dollars – if not trillions over the last two decades – in building new business applications on the internet, there has been woeful attention paid to the security of data: ensuring its provenance, confidentiality and preserving its integrity.

Blockchain

Blockchain is touted to have many unprecedented business benefits, including security; but when dissected technically, there is only one unique benefit that blockchain offers: *the ability of multiple parties to participate in a distributed database system – a cost-effective shared ledger – where each party may view and verify each others' transactions, as well as participate in those transactions, without excessive friction.* All other stated benefits of blockchain have been feasible in the past but have remained unimplemented – or not implemented effectively enough to accrue benefits - for a variety of reasons.

For instance, the single most touted benefit of blockchain – *immutability of transactions* – has been possible within applications for over two decades with the use of digital signatures[27], a benefit of *asymmetric key cryptography*[28] introduced as early as in the late '70s. *Distributed databases* across networks have been in use for over three decades. *All* applications currently in use are *permissioned* applications. And, *multi-party trust* has also been in use for over two decades with the use of public key infrastructure (PKI)[29]. What blockchain has done is to demonstrate that these benefits can be combined together to provide, hitherto, unrealized benefits to businesses and government.

Given the above, the single most important consideration public and private organizations must undertake regarding the security of any proposed solution relying upon blockchain technologies is to make a commitment that security will not play a secondary role within the application, as has been so for the last few decades.

Blockchain heralds a movement to eliminate time-tested procedures of trust which were simple to understand by lay-people, and to replace them with cryptographic procedures transparent to only advanced professionals. While it might be argued that this is the natural evolution of science and technology, when it comes to human interactions with government and businesses, in order to preserve trust in institutions and an orderly society, it is imperative that every element of application

[27] Digital Signatures, Wikipedia, https://en.wikipedia.org/wiki/Digital_signature

[28] Public-key Cryptography, Wikipedia, https://en.wikipedia.org/wiki/Public-key_cryptography

[29] Introduction to Public-key Cryptography, Mozilla Developer Network, https://developer.mozilla.org/en-US/docs/Archive/Security/Introduction_to_Public-Key_Cryptography)

security that can cast aspersions on the system be considered carefully before it can be deemed trustworthy.

This is analogous to a time when the construction industry could build homes without licenses, permits, building codes, inspections and certificates of occupancy. Many people paid a price with their lives, livelihoods and finances for such a *laissez-faire* mode of operations – some still do even in this 21st century despite the industry being heavily regulated in California[30]. The global financial crisis of 2007-2008[31] occurred despite the banking and financial industry being the most regulated industry in the world.

[30] Settlement reached over San Francisco's notorius sinking tower, The Guardian, https://www.theguardian.com/us-news/2019/aug/29/millennium-tower-san-francisco-settlement-leaning

[31] Search results for 'Global Financial Crisis', Duck Duck Go, https://duckduckgo.com/?q=global+financial+crisis+of+2007