CA Blockchain Working Group

Cybersecurity & Risk Management – Arshad Noor

Introduction

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 (https://en.wikipedia.org/wiki/Morris_worm) in 1988, began a long slide that resulted in California passing the first regulation of its kind anywhere in the world, in 2002, (https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386) mandating 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 (https://privacyrights.org/data-breaches) with 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 (https://en.wikipedia.org/wiki/Digital_signature), a benefit of *asymmetric key cryptography* (https://en.wikipedia.org/wiki/Public-key_cryptography) 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) (https://developer.mozilla.org/en-US/docs/Archive/Security/Introduction_to_Public-Key_Cryptography). 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 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 (https://www.theguardian.com/us-news/2019/aug/29/millennium-tower-san-francisco-settlement-leaning). The global financial crisis of 2007-2008 (https://duckduckgo.com/?q=global+financial+crisis+of+2007) occurred despite the banking and financial industry being the most regulated industry in the world.

Security Recommendations

It is our belief that governmental 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.

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 (https://www.comptia.org/certifications/network) or the security industry certifies security professionals (https://www.isc2.org/Certifications/CISSP).

While such a “Certified Blockchain Developer” (CBD) 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 development experts from academia and industry to define the curriculum and criteria for becoming a CBD.

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

Arguments Against CBD	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	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 CBD'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 CBD. However, possession of knowledge and 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	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 CBDs.
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 CBD. 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 CBD.

Disruptive Defenses

It is this author's reasoning that the vast majority of data-breaches since the passage of California's seminal data-breach disclosure law, resulted because of failures in protecting against specific vulnerabilities well-known within the ecosystem.

These vulnerabilities can be addressed using *disruptive defenses* – defenses that are based on current industry standard but are uncommon within applications (except for security-conscious ones). The *disruptive defenses* are:

1. **Eliminating *shared-secret authentication***: Invented in the 1960's, the *username/password* scheme which represents the progenitor of all *shared-secret authentication* schemes, including *One-Time Passcodes (OTP), Short Message Service (SMS) Codes, Knowledge Based Authentication (KBA), etc.*, is the least defensible security technology for the 21st century internet where nation-states are battling each other for economic supremacy. They also represent targets of "scalable attacks" where a compromise of the authentication scheme compromises everybody's credential.
    a. **Recommendation**: Mandating the use of *public-key cryptography* based authentication with purpose-specific cryptographic hardware will completely eliminate authentication secrets on the target machines, while dramatically reducing the vulnerability of authentication schemes on blockchain applications. Invented more than three decades ago, they are used to protect some of the most mission-critical systems around the world. Expensive and complex in the past, newer protocols such as those standardized by the FIDO Alliance and the World Wide Web Consortium, dramatically reduce the cost and complexity of integrating authentication protocols rated at *Authenticator Assurance Level 3* (NIST SP 800-63b: https://doi.org/10.6028/NIST.SP.800-63b), which provide "*very high confidence that the claimant controls authenticator(s) bound to the subscriber's account*" into modern web-applications.
        i. **Objections**: Some concerns were raised that the use of public-key cryptography with purpose-specific 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**: While there are many public-key cryptography based authentication schemes, the FIDO protocols in particular have been standardized at this time of writing across operating system platforms (Windows, Android), all modern browsers (except Internet Explorer) and purpose-specific cryptographic hardware are standard components in all modern business desktops, laptops and mobile devices. As such, the cost of consumers adopting this authentication scheme is merely reduced to web-applications supporting the use of this authentication scheme.

With respect to Quantum Computing, it is safe to say that the US NIST and its contemporaries in many parts of the world are well aware of the threat to public-key cryptography. While no one can predict what may happen in the future, to avoid using the most powerful authentication technology for the next decade of web-applications – and to fall back on half-a-century old technology that has proven to be futile – is to regress. Notwithstanding the risk, it is this author's recommendation that California be progressive and adopt this mandate for *strong-authentication* as we embark on the blockchain journey.

2. **Ensuring the *provenance* of a transaction before it enters the blockchain**: Almost all applications today, universally, assume that the data received on the server-end of a *client-server* application is the same data that was either captured or input at the client-end. That the application most likely uses the Transport Layer Security (TLS) protocol to secure data-transmission is provided as evidence that the data was transmitted securely from its source. However, such people fail to recognize that there are at least two vulnerabilities that TLS cannot protect from: I) The theft of a stolen credential (especially if it does not use strong-authentication as recommended in *Disruptive Defense #1*) permits a masquerader to submit a spurious transaction using a legitimate credential; or ii) The compromise of transaction data within the computer system after it is submitted by the legitimate user and before it has entered the TLS channel; this is possible if the computer system on which the user is executing the transaction has been compromised.

   a. **Recommendation**: Mandating that a blockchain transaction be *digitally signed* by the user before it is submitted will mitigate this risk. It is essential that the cryptographic key performing the digital signature be protected using purpose-specific cryptographic hardware to ensure that the *signing key* is not compromised on the user's computer. With such a digital signature, I) an attacker will not be able to submit a spurious transaction because he will not have possession of the user's *signing key* if the user has it in her possession; and ii) once digitally signed inside the cryptographic hardware in the possession of the user, the attacker might tamper with the transaction before it enters the TLS channel, but will be unable to compute a new digital signature, thus alerting the blockchain application on the server-end that this transaction cannot be trusted.
      It is noteworthy to mention that the latest version of the FIDO Alliance protocols – FIDO2 – includes the specifications for *Transaction Confirmation* that delivers precisely this capability.

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

3. **Preserving the confidentiality of sensitive information within and outside the blockchain**: While there are many ways to protect the confidentiality of sensitive information, encryption of information remains a time-tested and proven defense.

However, as with all matters of technology, there are many ways to implement encryption with the axiom that those that focus on developer, operational and security convenience tend to expose larger vulnerabilities in the system.

a. **Recommendation**: Mandating that only the application that has a need to see/use sensitive data be responsible for the encryption and decryption of that data would be in line with best-practices of the cryptographic community. While the application may leverage purpose-specific cryptographic elements to perform this sensitive operation, the cryptographic operation (encryption/decryption) should not be delegated to other 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 regardless of the security of the blockchain itself.
   Given that there are many technical details associated with the encryption of sensitive data, this submission will not go into implementation details, but recommend that *stakeholders* in blockchain applications understand specific implementation details of the encryption and key-management processes and controls before signing-off on the application.

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

4. **Preserving the integrity of transaction data even when outside the blockchain**: Mandating a *digital signature* on transaction data before the transaction enters the blockchain provides assurances about the *provenance* of the transaction. However, it is conceivable that the transaction may morph over its life.

   a. **Recommendation**: Mandating a *digital signature* each time the transaction undergoes a change ensures preservation of the integrity of the transaction over its lifetime. While the application may leverage purpose-specific cryptographic elements to perform this sensitive operation, the cryptographic operation (signing) should not be delegated to other general-purpose elements of the blockchain application, including the blockchain itself. It is imperative that the transaction be signed before it gets on the blockchain so its integrity is preserved within and outside the blockchain.
      Given that there are many technical details associated with digital signatures, this submission will not go into implementation details, but recommend that *stakeholders* in blockchain applications understand specific implementation details of the signing and key-management processes and controls before signing-off on the application.

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

5. **Using cryptographic hardware where cryptographic keys are used within the application**: A cardinal error of most application developers who are using cryptographic tools for the first time, is to underestimate the complexity of the task and to skimp on security controls around key-management – the discipline of managing the life-cycle of cryptographic keys. Many billion dollar companies have been caught flat-footed because they underestimated the tenacity of their attackers in compromising software based cryptographic *keystores* (which are protected by mere passwords), the most recent being the second largest breach in internet history – that of Marriott Hotel and the breach of 370 to 500 million sensitive data records (**https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach**).
    a. **Recommendation**: Mandating that blockchain applications that use cryptographic keys for encryption and signing use purpose-built cryptographic hardware (or cryptographic solutions that use purpose-built cryptographic hardware) will ensure the security of the application, keeping it in line with best-practices of the industry. Given that there are many technical details associated with key-management, this submission will not go into implementation details, but recommend that *stakeholders* in blockchain applications understand specific implementation details of key-management processes and controls before signing-off on the application.
        i. **Objections**: Some concerns were raised that the use of purpose-specific cryptographic hardware will be expensive and not provide the level of desired security (given that even Intel could not protect its own microprocessors from being compromised by design failures, leading to security vulnerabilities).
        ii. **Response**: There was a time when purpose-built cryptographic hardware was expensive – and remains expensive if the buyer is naive – but the industry has come a long way in delivering industry-standard security hardware at very reasonable prices. Currently, every business-class laptop, desktop, server and mobile device come embedded with *secure elements* that are purpose-built cryptographic hardware elements capable of sophisticated key-management functions when designed appropriately.
        Intel's vulnerabilities in its microprocessor were the result of their desire to optimize their central processing unit (CPU) for faster operations and did not take into account the fact that specific exploit software could take advantage of security gaps within this optimization to breach sensitive data. A purpose-built cryptographic element has a significantly less complex environment and firmware ensuring that there are fewer opportunities for compromise.
6. **Ensuring application access to cryptographic services remains within a *secure zone***: The emergence of cloud computing as an alternative deployment strategy for IT systems presents many opportunities, yet challenges traditional notions of data security. Companies have made the traditional mistake of taking their "on-premises" application to the public cloud on the assumption that cloud service providers (CSP)

have better security infrastructure and controls to protect their data. Sadly, evidence suggests the opposite. The most recent breaches of Uber (**https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453**) and Capital One (**https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html**) reflects that even billion-dollar companies have been naive in assuming that sensitive data can remain safe despite using sophisticated cryptographic key-management solutions available from the CSP.

a. **Recommendation**: Mandating that blockchain applications that use the public cloud leverage an application architecture (**https://www.ibm.com/developerworks/cloud/library/cl-regcloud/**) that defines a *secure zone* – distinct from the cloud's *public zone* – where the application has access to cryptographic services.
   Given that there are many technical details associated with the use of cryptographic services in public clouds, this submission will not go into implementation details, but recommend that *stakeholders* in blockchain applications understand specific implementation details of cloud-based cryptographic services before signing-off on the application.

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

Focused Stakeholders

Given the paradigm shift that blockchain-based systems are expected to have on current "systems of record", government must establish a permanent Blockchain Working Group 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 – <u>not</u> 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. No single group has a monopoly on knowledge; only by combining

the knowledge and expertise of a diverse group of professionals can one hope to achieve a balanced perspective on the path forward.

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 manage their use is logical. The same analogy applies to humans who participate in different ecosystems: healthcare, education, finance, government, employment, commerce, etc.

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 automobile, certain individuals and organizations must be able to ascertain these facts from an immutable record. This authorization must be defined in policy to ensure that the privacy of the asset owner and the public good is served with optimal efficiency, while systems with the appropriate access controls are used to implement such policy.

Just as a traditional relational database management system (RDBMS) – as is available from commercial and open-source implementations today – must be designed to solve a specific business problem to implement its attendant business rules and security constraints, so must a blockchain-based system.

Privacy is an independent property that must not be positioned as a contradiction to immutability. Privacy is an equally desirable feature in systems that are warranted. However, government 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 and the "hard fork" of the Ethereum blockchain - suggests that the State of California might consider defining an *experimental* period of perhaps 5-7 years, where State of California 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 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 creation of a business entity, 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), organizations must run parallel systems to ensure that in the event of a conflict, existing systems-of-record will prevail over blockchain-based systems.