# CA Blockchain Working Group

## *Cybersecurity, Privacy & Risk Management (Arshad Noor – v3 - 11/21/2019)*

**What considerations should public or private organizations undertake regarding the security requirements of a proposed implementation of blockchain?**

The answer to this question relates to anticipated business benefits to public and/or private organizations from proposed implementations of blockchains.

Blockchain is touted to have many unprecedented business benefits, 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* <u>*cost-effective*</u> *shared ledger – where each party may view and verify each others' 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. *Distributed databases* across networks have been in use for over three decades. <u>*All*</u> 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 infrastructre (PKI).

What blockchain has done is to demonstrate that these benefits can be combined together to provide, hitherto, unrealized benefits to businesses and government. It must be said, that without the advancements in other areas of technology, the cost of realizing these benefits might still be high.

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 two decades.

Blockchain heralds a movement to eliminate time-tested procedures of trust, understandable to lay-people, and to replace them with cryptographic procedures transparent to only advanced professionals. It is imperative, that in order to preserve trust, every element of application security that can cast aspersions on the system must be considered carefully before it can be deemed trustworthy.

There was a time when builders 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 so 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 industry likely being the most regulated industry in the world.

It might be prudent for the State of CA to consider practices followed in other areas of information technology to minimize risk: specifically, the practice of certifying blockchain application developers through a course of study, 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" 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 (https://privacyrights.org/data-breaches).

Finally, 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 CA might consider defining an *experimental* period of perhaps 5-7 years, where State of CA 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 itcan 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.

**Which stakeholders should be involved in such discussions? Should different blockchain systems be associated with different application contexts?**

The following stakeholders must be involved where blockchain-based systems replace existing systems-of-record:

- Business representatives
- Government representatives of existing systems-of-record (where public records are involved)
- Independent legal and privacy advisors
- 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

Almost certainly, different blockchains for different application contexts must be used 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.

This model may be extended to ecosystems that serve the specific ecosystem while leaving others unaffected.

**What components of blockchain should be highlighted? Can the immutability of blockchain architecture be reconciled with requirements of emerging privacy policies, such as GDPR in the EU and CCPA in California? How should these components be incorporated into a decision-making and assessment process to determine its appropriateness for any use case?**

The immutability of transactions is always a desired capability in any system – fraud flourishes in systems where transactions can be modified without a trace. Where legitimate, transactions can be reversed to correct errors of commission – with blockchain-based systems, a second transaction is essential to correct the error (much as in any banking transaction-based system).

However, 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.

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 lifecycle 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.

**How can we ensure that we forge an adaptive path forward for blockchain implementation in California, one that is neither too permissive nor too constrained? Consider implications beyond this legislation.**

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 representaties 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 advisors
- 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

The legislature made the right decision to convene such a group before enacting any law that broached blockchain; 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.