accenture

BELIEVE IT OR NOT

Blockchain's potential starts with security

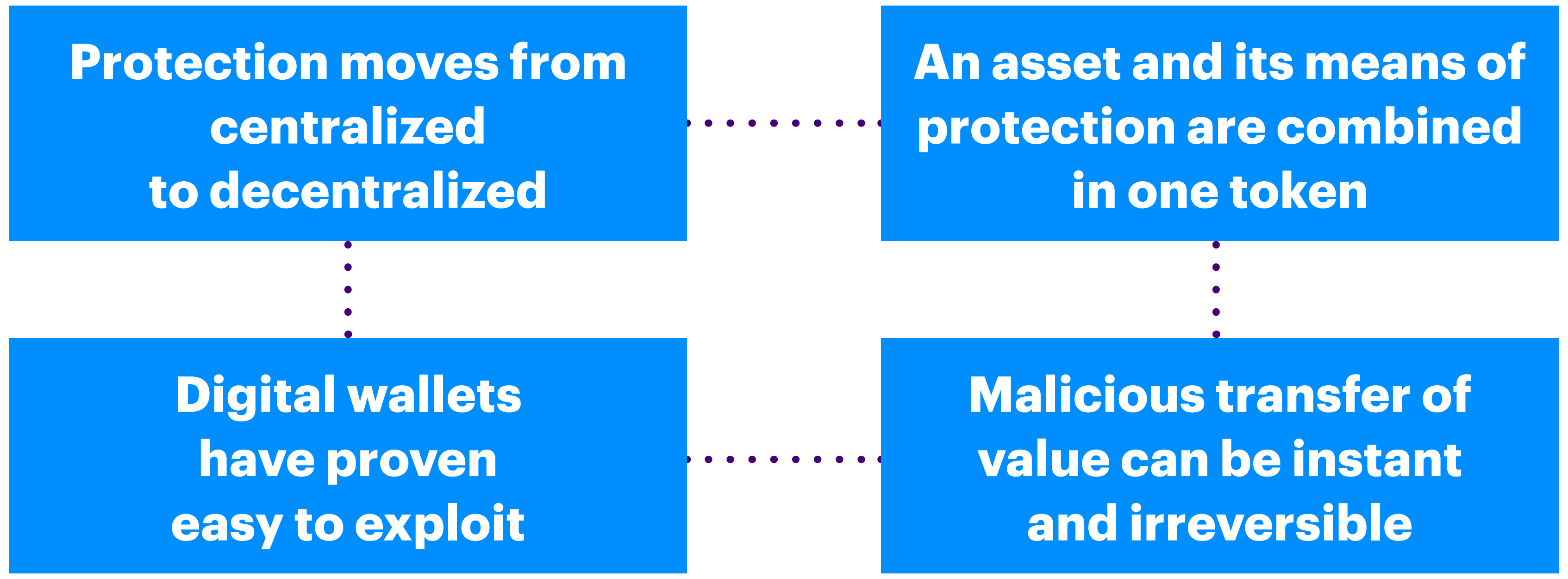
CONTENTS

BLOCKCHAIN SECURITY

Blockchain technology will likely revolutionize the way we live and work. It has the potential to give us greater control over our healthcare and well-being, provide greater insight into the origins and quality of the food we eat and the products we buy, financial transactions will execute faster and be simultaneously more transparent and private, and business will be conducted with greater efficiency and less risk. It can also provide verifiable identification to the 1.1 billion individuals without documented proof of existence, or a bank in the pocket of the 2 million unbanked[1]. And if the World Economic Forum's survey prediction is correct, by 2027, 10 percent of global gross domestic product (GDP) will be contributed by blockchain technology[2].

Blockchain's unique attributes will provide a new infrastructure on which the next generation of streamlined business applications will be built. But it also creates unique security challenges.

Here's why:



Protection moves from centralized to decentralized

An asset and its means of protection are combined in one token

Digital wallets have proven easy to exploit

Malicious transfer of value can be instant and irreversible

Sources: (1) https://globalfindex.worldbank.org/
(2) www.coindesk.com/world-economic-forum-governments-blockchain/

While blockchain technology has proved to be highly-tamper resistant, the vulnerabilities in blockchain applications have been exploited with some significant consequences.

In 2014, nearly half a billion dollars' worth of Bitcoin was stolen from Mt. Gox, the largest Bitcoin exchange in the world at the time. Two years later, roughly US$60 million worth of Ether, a value transfer token, was redirected to a hacker's account via The DAO, a decentralized autonomous organization built upon Ethereum. Another year later, 2017, the second largest Bitcoin attack occurred at the Hong Kong-based cryptocurrency exchange platform, Bitfinex. This time the hackers made off with US$72 million worth of Bitcoin. The attackers have not been caught. Where money exists, so does the possibility of theft and these threats are likely to continue.

And starting in 2018, the once-feared 51% attack often discussed as a more theoretical distant concern than anything of immediate relevance, has become far too common. Attackers in at least 5 instances have identified vulnerabilities in the lack of miners on smaller coin networks, leveraging mining marketplaces to rent mining power and spin it up quickly. The most notable attack to date was in the first week of 2019, capturing around $1.1 million on the Ethereum Classic blockchain.

MYTH BLOCKCHAIN HAS BEEN HACKED

With these high-profile breaches, it’s not surprising that there is a misperception that blockchain has been hacked. In reality, there is a full spectrum of touchpoints across an end-to-end blockchain-based solution. Taking that into consideration is imperative to securing the entire solution. The vulnerabilities outlined up until this point illustrate the fact that, while at no point was the underlying blockchain technology hacked, and these hacks occurred on permissionless platforms, each nefarious actor identified a vulnerability within these blockchain ecosystems. And, while permissionless platforms are unlikely to be the basis of an enterprise solution, there are valuable lessons to be learned. The ability to secure distributed ledgers, digital wallets and other applications is mission critical.

Blockchain technology will be just one component of the new IT stack. Security needs to be baked into the entire architecture of any blockchain solution.

There is quite a bit of confusion and hype around blockchain security and there are many variables that need to be considered when designing a security solution, but, in general, security threats fall into three main buckets:

- **ENDPOINT VULNERABILITIES**
- **UNTESTED CODE**
- **ECOSYSTEM / THIRD-PARTY RISKS**

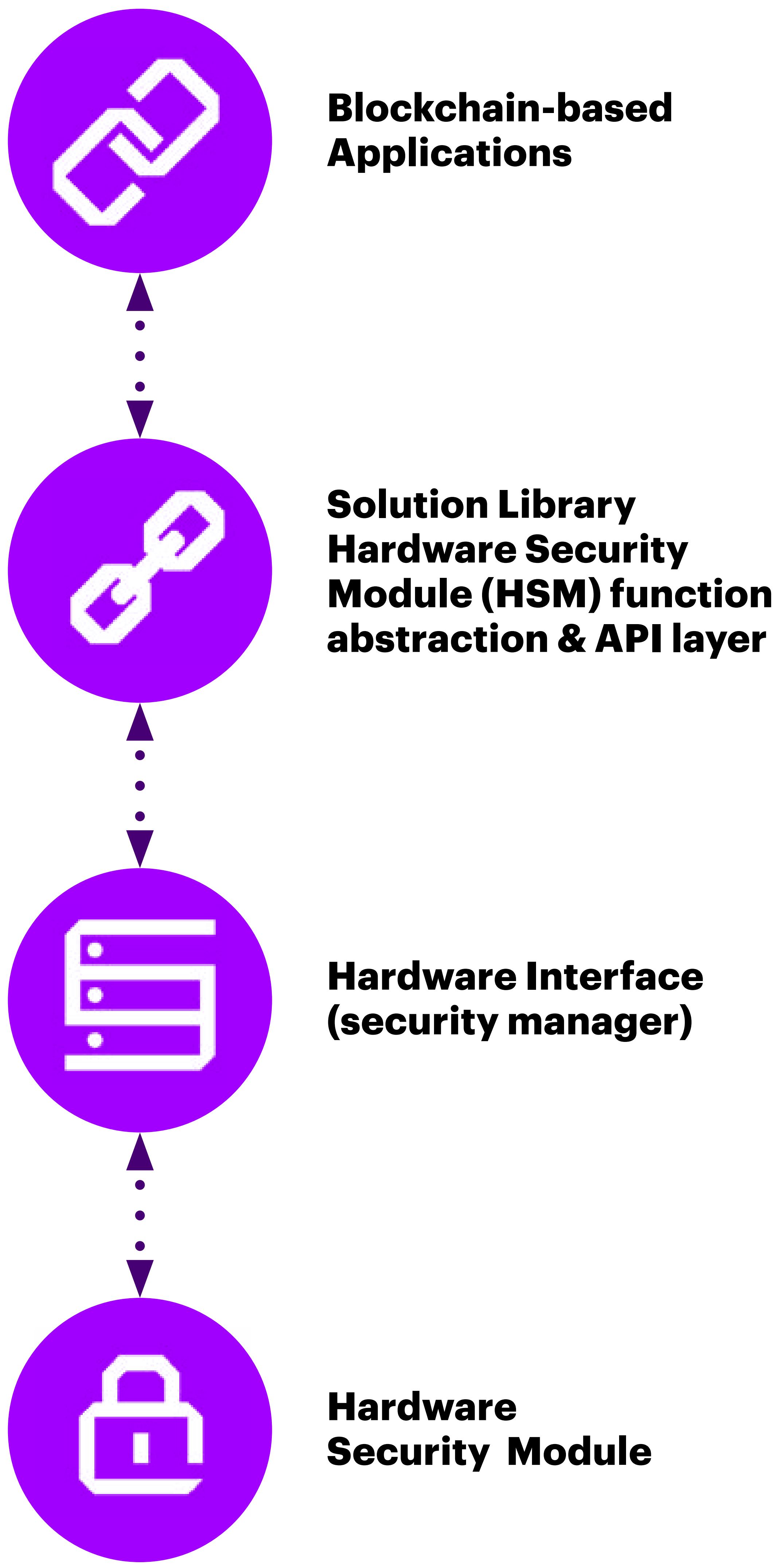
Endpoint Vulnerabilities

The most direct and potentially easiest method of attacking any technology solution is through the endpoint vulnerabilities. This is where humans and technology connect and, with blockchain-based solutions, can include digital wallets, devices, or the client-side of the application. For the users, this means potential vulnerabilities in the protection of their private key and password, or physical access to their phone or computer.

If one of these end points becomes compromised, and a malicious actor gains access to an account, unless additional security protections exist (e.g., two-factor authentication on asset transfers), everything within the account can be at risk. Further, using the compromised account, the hacker can commit fraud without setting off any external alarms or signs of abnormal behavior. Unlike banks that can cancel transactions or make corrections after the fact, public permissionless blockchains' permanence makes it more difficult to correct the implications of the breach. And when an attack takes place beyond one account, expanding to a data warehouse managing access to all accounts, the potential damage can be monumental.

Progress has been made recently with many companies stating they are using cold wallets – often in combination with HSMs (hardware security models). Hot wallets are applications connected to the internet for storing the private cryptographic keys that anyone who owns cryptocurrency needs in order to spend it. Cold wallets are not connected to the internet making them more difficult to compromise. Coinbase, for example, claims to hold 98 percent of their cryptocurrency in cold storage, while maintaining insurance for assets in all hot wallets. In January 2017, however, hackers broke into Tokyo-based cryptocurrency exchange Coincheck Inc. and made off with nearly US$500 million in digital tokens. The company admitted that it had kept customer assets in a hot wallet, which is connected to external networks, which was the cause of the security lapse[3].

Sources: (3) fortune.com/2018/01/31/coincheck-hack-how/



Blockchain-based Applications

Solution Library Hardware Security Module (HSM) function abstraction & API layer

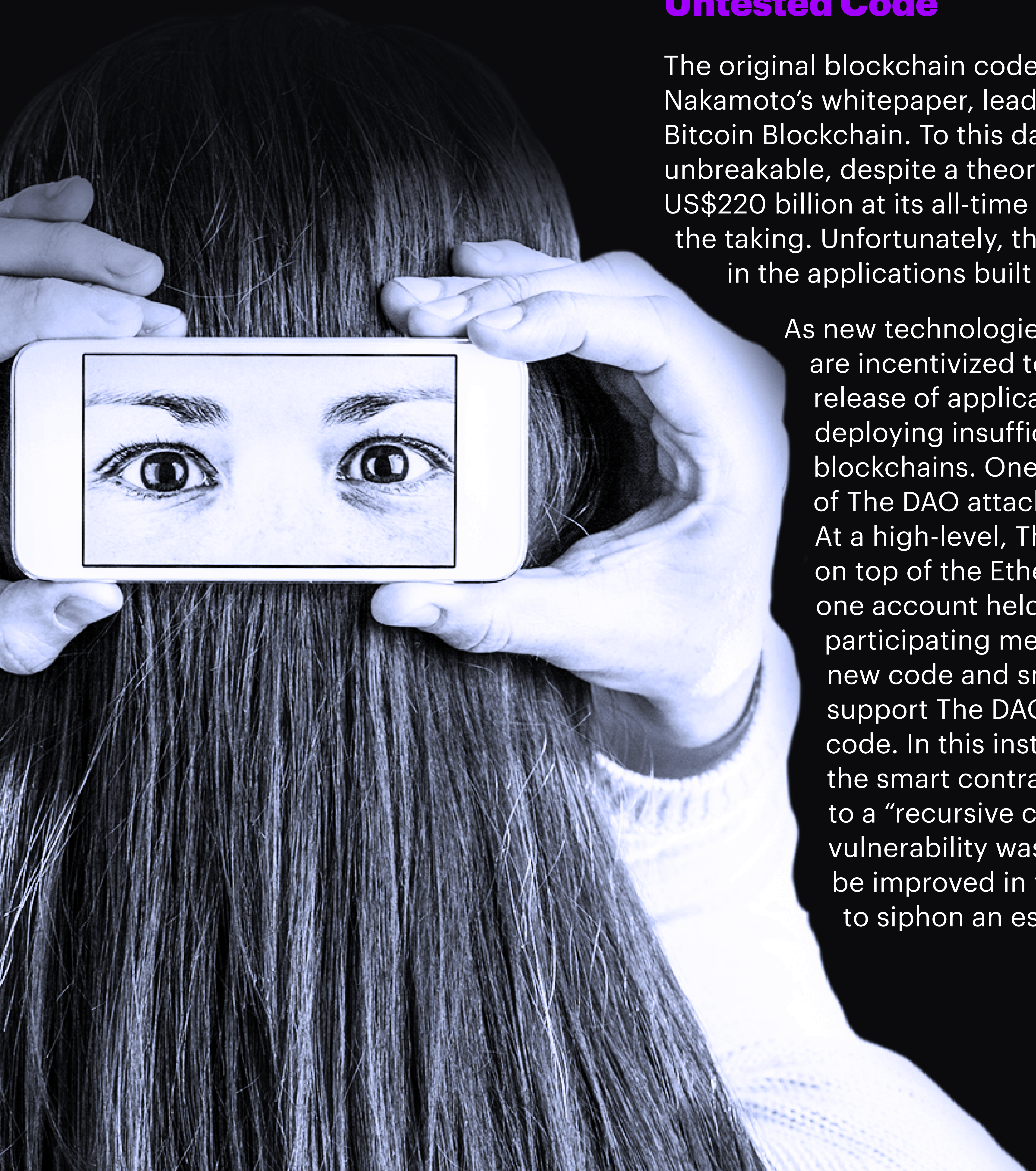
Hardware Interface (security manager)

Hardware Security Module

In addition, these risks can be mitigated with an HSM. HSMs are industrial-grade, crypto-processors that securely generate, protect, and store keys. HSMs are already broadly used by banks to safeguard and manage digital keys so that they are not simply stored on a server or in the software which makes them essentially impossible for unauthorized users to extract. Nevertheless, endpoint vulnerabilities remain susceptible through methods such as social engineering, phishing, or real-world kidnapping or theft. These keys hold such a great deal of significance as they are the only method of proving identity in a virtual network. Though many of the attacks and discussion is around public permissionless blockchains, private permissioned blockchain solutions must also take these risks into consideration because the losses could potentially be more catastrophic.

On public permissionless blockchains, such as Bitcoin or Ethereum, if one person's wallet or account is compromised, the threat is contained as no assets are at risk outside of the victim's possession. The malicious actor could do as he or she pleases with the compromised wallet and account, but nothing further. On a private permissioned blockchain, those that enterprises will likely be using for their implementation, the risk could potentially extend beyond one account.

Consider the implications if malicious actors gained access to the controls of an ecosystem operator. Unbeknownst to the network, they could track and steal the data of all activity on network. Given edit and write controls, they could start manipulating the network and masking activity as the original operator. If this account had unilateral governance controls, they would potentially be able to onboard fraudulent actors, wreaking additional havoc on the network. It is important to consider what is at stake on each network, and which parties have different levels of access. Despite a network being between trustworthy parties, security precautions may dictate controls and limitations being placed on all users, guided by business necessity. These risks highlight the importance of network design, access control, and authority balance on private networks.



Untested Code

The original blockchain code came as a result of Satoshi Nakamoto's whitepaper, leading to the creation of the Bitcoin Blockchain. To this day the code has proven unbreakable, despite a theoretical bounty of over US$220 billion at its all-time high to-date being there for the taking. Unfortunately, that is not the case for all code in the applications built upon the blockchain.

As new technologies enter the market, developers are incentivized to be first or early with the release of applications, often at the risk of deploying insufficiently tested code on live blockchains. One now infamous example is that of The DAO attack on the Ethereum network. At a high-level, The DAO was a program built on top of the Ethereum network, in which one account held the investments for all participating members. However, with the new code and smart contracts developed to support The DAO, came vulnerabilities in the code. In this instance, the ability to manipulate the smart contracts to drain money due to a "recursive call bug." Even though the vulnerability was identified, the code could not be improved in time and the hacker was able to siphon an estimated US$60 million.

These types of untested code risks are common among start-ups and applications that are trying to quickly enter the market. However, given the decentralized model of many blockchain solutions, the risks are often greater due to the irreversibility of the technology. As enterprises continue to build and deploy blockchain solutions, standard best practices for code review are encouraged, adding emphasis to peer review and independent testing prior to releasing new features or applications. Smart contracts, a new technology for most enterprises, can be particularly risky but Digital Asset now includes a testing protocol in its DAML language that allows users to test drive smart contracts at the development stage. Hyperledger, a Linux Foundation project, is leveraging its open source culture to bring more attention to detecting bugs and solving problems in its frameworks via its "Bug Bounty" program. There are also initiatives, such as Zeppelin, which focus solely upon creation of secure smart contracts. They have proposed secure coding and design principles that can be taken into consideration while writing business logic and smart contracts on top of any private blockchain. These are just a few of the design principles that should be considered early in the development process.

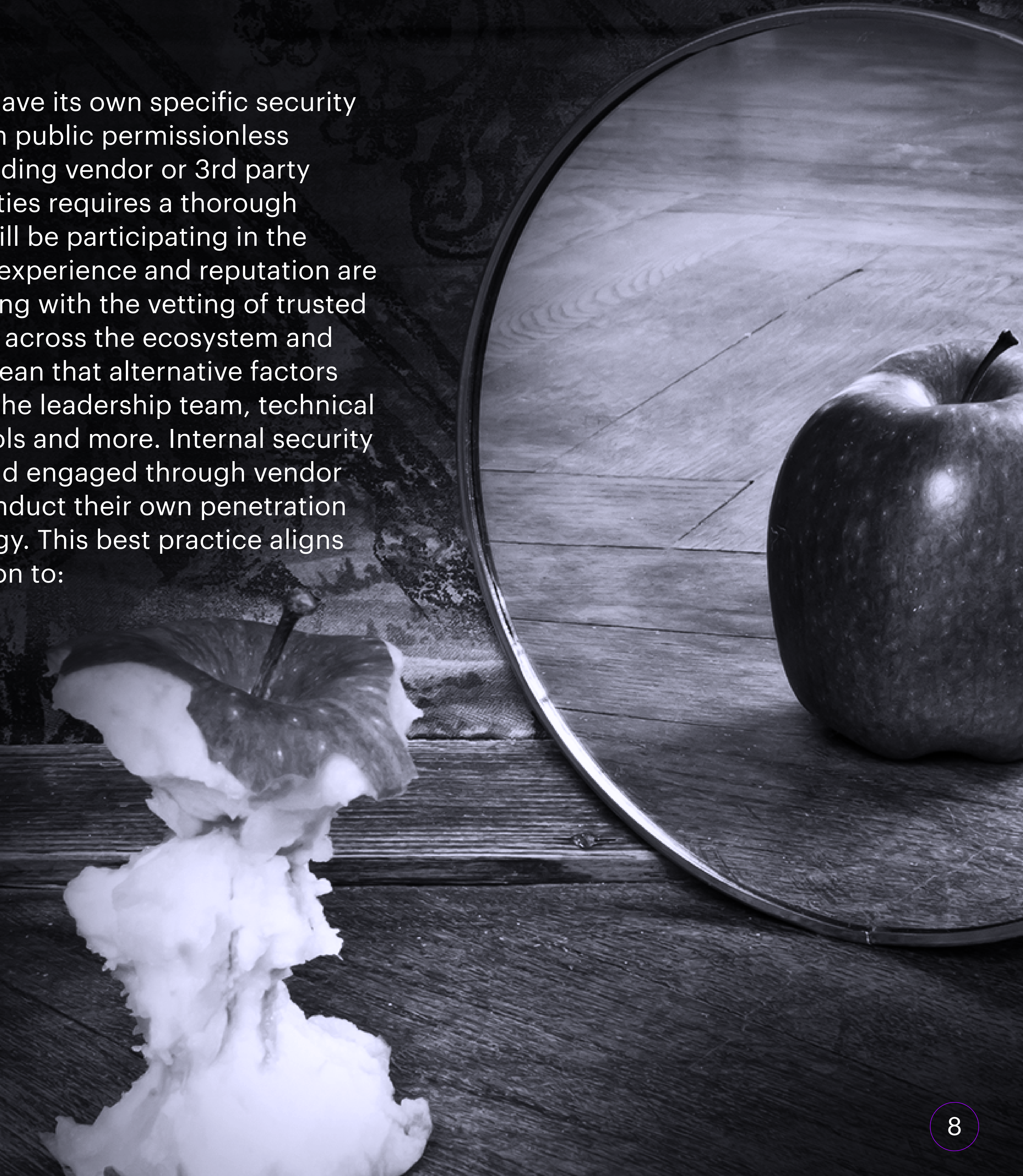
Ecosystem / Third-Party Risks

As discussed previously, blockchain platforms have proven secure to-date, but the security of a blockchain solution depends upon the entire ecosystem of the application. Often, this will include partnering with third-party solution providers, including blockchain integration platforms, payment processors, wallets, fintech, payment platforms, and smart contracts. Organizations wishing to deploy third-party blockchain applications and platforms must be aware that the security of their blockchains is only as strong as its weakest link across all technology provided. Pourous system security, flawed code, and even personnel vulnerabilities can expose their clients' blockchain credentials and data to unauthorized persons.

The Bitfinex hack in 2016 is a public permissionless example of a realized partner risk. Thanks to poor security on the part of Bitfinex, BitGo, a cold storage wallet service that often partners with cryptocurrency exchanges, lost US$72 million of customer deposits. Bitfinex had designed the architecture so that whatever BitGo was directed to do with their linked wallets, BitGo would automatically comply. So when Bitfinex's server got hacked, the hackers could make unlimited requests to the BitGo wallets and send those assets to their private wallets. While BitFinex used a best practice in storing cryptoassets in cold wallets, they still put themselves at risk for having poor security and a system with a single point of failure.

Each enterprise solution will have its own specific security needs and they will differ from public permissionless considerations. However, avoiding vendor or 3rd party related blockchain vulnerabilities requires a thorough vetting of each partner that will be participating in the blockchain ecosystem. While experience and reputation are often the key factors in assisting with the vetting of trusted partners, the new innovations across the ecosystem and the wealth of start-ups may mean that alternative factors must be considered, such as the leadership team, technical acumen, code testing protocols and more. Internal security teams should be consulted and engaged through vendor selection so that they may conduct their own penetration tests of the relevant technology. This best practice aligns with Gartner's recommendation to:

"be cautious of over optimistic vendor claims by evaluating the technical security aspects of blockchain platforms under consideration."[4]



Sources: (4) Gartner, Innovation Insight for Blockchain Security, Aug 2017

CONSIDERATIONS FOR DEVELOPMENT

> “
>
> If we’ve learned anything from the past couple of years, it’s that computer security flaws are inevitable.
>
> Bruce Schneier

As cryptography expert Bruce Schneier coined in 2000, security is a process, not a product[5]. Security should not be a go-to-market consideration, or something wrapped around an application once developed. It should be intrinsically considered through various stages of the product development lifecycle. It may not necessitate the same level of rigor in the early planning stages as when scaling the application, but it should still be a consideration nonetheless.

Sources: (5) www.schneier.com/essays/archives/2000/04/the_process_of_secur.html
Photographer Lynne Henry https://www.schneier.com/photo/

EMBEDDED SECURITY

Blockchain implementations and solutions should consider security embedded in the blockchain technology stack. Imagining and positioning security as a protective peripheral component around the blockchain network will weaken the cyber resilience of the platform. Security measures should be implemented at each layer with a risk-based approach. This will strengthen the defense and build up the cyber resilience of the platform against attacks from foreseeable vectors. As implementations mature and the risks evolve, organizations should consider reviewing the risks at each layer and strengthening their security measures appropriately. In the graphic below, security measures are listed as a starting baseline for each layer.

Five areas are:

Governance

Application

Data

Transactions

Infrastructure

Governance

The business and operating model of its members is as important as the technology of a private enterprise blockchain network. Before a successful implementation of a private blockchain, a governance body should be appointed or established to create and manage guidelines and standards for the technology and surrounding processes. With regards to security, standards must be set around identity and access management, onboarding new members, secure key management, data management policies and more. Often these governing bodies require an objective third-party to implement best practices and mediate the conversations.

Back to **Embedded Security**

Application

At the application layer, self-executing smart contracts and the third-party applications that integrate with the blockchain network enable the business logic in the ecosystem. As discussed above, any bugs or vulnerabilities can have permanent, real-time damage to the network. Therefore, secure code development and application security in general will play a vital role in development of smart contracts and third-party applications.

Back to **Embedded Security**

Data

By default, there is no confidentiality in blockchain design, as all data on-chain is visible to all participants. Confidentiality and data protection are important considerations in design and implementation. The level of confidentiality of the network depends on the design of the platform. Utilizing an off-chain approach, companies can keep parts of the data in a local storage and upload the hash of the data to keep its integrity within the transaction. This approach requires minimal advanced cryptology.

Alternatively, companies can keep information on the chain while still maintaining a level of confidentiality. Cryptographic techniques are still being developed but an early example is zk-SNARKs, a version of Zero-Knowledge Proof, meaning validating a statement about encrypted data without revealing the decrypted data. One additional alternative is to avoid the global broadcast model of transactions and limit the visibility to only related and needed parties in the network. An example of this design can be found in R3 Corda distributed ledger technology (DLT) which uses an Unspent Transaction Output (UTXO) set model.

Back to
Embedded Security

Transactions

Security for transactions is widely based around the consensus algorithm and underlying protocol that dictate how consensus on transactions is reached, resulting in an updated shared ledger. As DLT advancements continue, developers have more choices regarding which to implement for their solution. The algorithms and accompanied rule set shape the network, transaction speed, and network scalability, each providing its own benefits and limitations. While likely included in a requirements assessment prior to developing a proof-of-concept, it is important for both developers and security engineers to carefully consider which algorithm and protocol are best for their use case.

Back to **Embedded Security**

Infrastructure

Blockchain solutions have nodes and application program interfaces (APIs) that communicate over public and private networks. Nodes and their roles can differentiate in solutions, as they are the communicating entities in the blockchain network. They run on participants' own infrastructure and network which requires fundamental security controls and measures, like periodical vulnerability assessments and penetration testing, logging and monitoring, endpoint security and patch management. Compromising a single node may result in a malicious actor stealing the assets of the end user in public blockchains or actor remaining undetected and monitoring the transactions and activities in a private blockchain network.

These considerations align to the blockchain security recommendations set out by Gartner, including taking a holistic view of security, ensuring the risks are clear at the business, technical, and cryptographic levels. In addition, as should be done with any technology implementations, each project should be evaluated by preparedness and with incident response plans that address critical security events during the blockchain life cycle[6].

	BLOCKCHAIN	SECURITY
Governance	**Blockchain Ecosystem Rules and Permissions** manage onboarding of participants into the network and the roles within the network.	• Identity and Access Management • Key Management via Hardware Security Modules • Information Security Guidelines and Policies • Security Training
Application	**Smart Contracts** are self-executing, logical workflow agreements between parties to manage the access and use of value and data. **third-party applications** also can be integrated within the platform.	• Application security • Secure code development and guidelines • Vulnerability assessment of third-party applications
Data	**On-chain Data Encryption** Each data item can be encrypted individually and data can be segregated into on- and off-chain.	• Encryption and Key Management • Privacy policies and controls • Industry specific standards and regulation • Off-chain Data Security
Transactions	**Blockchain Consensus and Rules** Participants' must agree on rules to commit transactions and to update the shared ledger with consensus algorithms.	• Secure and sustainable choice of consensus algorithm in design against double-spending, censorship • Fork management and maintenance
Infrastructure	**Blockchain Network & Systems** Participants' nodes stand in their infrastructure and network, communicating through public or private connections.	• Periodical Vulnerability Assessment and Penetration Testing • Logging and Monitoring • Endpoint Security and Patch Management

Sources: (6) Gartner, Evaluating the Security Risks to Blockchain Ecosystems, March 2018

Back to **Embedded Security**

SAFEGUARDING FOR THE FUTURE

In the ten years since Satoshi’s Bitcoin whitepaper, and three years since the first release of Ethereum, we’re seeing an acceleration of enterprise applications with blockchain technology. Aspirations are grand. Just as use cases are examined for their long-term potential, security must also be built to address increasingly sophisticated threats. We must accept that potential black swans exist but not use that as a reason to ignore future possibilities.

There are a few hints today that can help uncover what security risks may exist in the future.

Identity

Quantum

Identity

Consider biometric identification and its rapid spread in the physical world. Casinos employ facial recognition to spot known card counters, while banks use voice recognition to verify customers over the phone. The Nymi wristband uses employees' heartbeats as a means to authenticate them to a corporate network. And hospitals around the country use Imprivata's PatientSecure to identify patients via the unique vein patterns in the palms of their hands. Soon, biometric identification will likely be a common method of identity verification, where multiple security protocols will create a unique identifier that can be indexed on a blockchain. No data will be kept on chain, but it will allow the user to prove they are who they say they are and determine what data they share, with whom, and for how long.

Back to
Safeguarding for the future

Quantum

Looking further ahead, quantum computing has the potential to be the most impactful advancement to modern technology. What currently would take computers years to complete could be done in seconds. Google has already shared details about their quantum efforts that have been running algorithms at 100,000,000 times faster than traditional computer chips. While the opportunities for innovation are exciting, the security implications should not be understated or overstated. Blockchain technology is unlikely to be a high priority target for quantum, but if it were, two key components have been discussed as being at risk:

1) Proof-of-work mining

Traditional mining for public blockchains is built on the concept of computers competing to solve difficult math problems – ones that can only be solved through guessing with brute force. This has led to the rise of a multibillion-dollar industry, competing to build mining supercomputers. This natural competitive balance has been created using similar styles of chips which mitigates a 51 percent attack risk (or even in the case of 51 percent market share, mitigates the risk of any adverse activity). However, many speculate that when the first quantum computer is used to compete in proof-of-work mining, it will retain such a significant advantage that it will have access over the network. According to research conducted at the National University of Singapore[7], an attacker with a quantum computer would be able to alter the transactions before the blocks are processed. Eliminating any checks and balances, the attacker can also decide which transactions are processed, increasing the risk to a variety of additional issues (e.g., double spend).

2) Private keys

The second vulnerability believed to be brought on by quantum computing relates to private key cryptography, a technology not unique to blockchain. Classic public / private key cryptography leverages integer factorizations, math problems that are very difficult to solve, but easy to prove correct. This cryptography is safe from today's computers due to the large complexity and amount of time it would take to solve the problems. However, quantum computing technology could potentially solve these in minutes, if not seconds. This means all technology that uses this type of cryptography – effectively the entire financial infrastructure as well as most other forms of technology – would be at risk.

Sources: (7) https://arxiv.org/abs/1710.10377

Despite the potential chaos quantum could create, most researchers note the quantum's risk to blockchain is more of a red herring than anything else. Nevertheless, solutions to these risks are already being developed. In preparation for Q-Day, the term the senior adviser for American Defense International coined for the day quantum computers can break classic computer encryption methods, many have begun working to develop quantum-proof solutions.

Quantum key security leverages randomness in the atmosphere to create and protect against quantum attacks. Post-quantum cryptography has arisen as the study of quantum-resistant cryptographic algorithms. And quantum-secured blockchain networks are in early development with the potential to develop mining and private key cryptography that is safe from quantum attacks. While the risk is real, research suggests the advancements in quantum-resistant cryptography and correlated security advancements will solve any potential quantum risks. As a Quantum-Proofing the Blockchain report from the Blockchain Research Institute recommends, blockchain protocols should be developed with agile frameworks, often leveraging modular digital signature schemes that can be switched out with quantum-resistant ones as developed and necessary. Open source efforts like the Open Quantum Safe project can be used to test and develop best practices as quantum-resistant key exchange and signature schemes mature[8].

Conclusion: blockchain is here

According to an Accenture survey of global executives, 80 percent expect blockchain technology to be integrated into their organizations' systems in the next three years[9]. That means the time to be begin thinking about development, and its security implications, is now. Deciphering between the hype and reality of security threats to blockchain technology is a major first step. Be it endpoint vulnerability, untested code, or the larger ecosystem, protecting against these risks is best done throughout the development lifecycle – embedding security within each layer of the stack.

...and so is the time for security

Just as blockchain technology is not a magic pill to solve data security, these security principles should be relied upon to cover the entirety of a blockchain application. Traditional security best practices should be combined with application specific enhancements to ensure the security of the application, and its surrounding ecosystem. It is the preparation and efforts of today that protect the organization tomorrow.

Back to
Safeguarding for the future

Sources: (8) Source: BRI, Quantum-Proofing the Blockchain, Nov 2017
(9) Tech Vision Survey, 2018

About our authors

John Velissarios
Managing Director, Global Blockchain Security Lead

Justin Herzig
Sr. Principal, Global Blockchain Research Lead

Didem Unal
Blockchain Security Consultant

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at www.accenture.com.

About Accenture Research

Accenture Research shapes trends and creates data-driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 250 researchers and analysts spans 23 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research – supported by proprietary data and partnerships with leading organizations such as MIT and Singularity – guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients.