DXC.technology

White Paper

How to overcome the security questions facing blockchain technology

Overcoming security questions about blockchain ecosystems will help ensure that blockchain continues to evolve in the financial services industry and matures into a disruptor in other businesses. This paper identifies security implications and potential threats, and offers 10 recommendations for embedding security into blockchain transactions.

Until recently, blockchain technology was not on the radar of most organizations. In fact, just 18 months ago, an executive of a major financial organization referred to blockchain asa "technology looking for a solution."

Attitudes changed by the time of the World Economic Forum 2018 conference in Davos, Switzerland, where the future of blockchain was in the spotlight and the *Financial Times* reported[1] that Nasdaq was investigating blockchain-based cryptocurrency product opportunities. Nasdaq would join a cadre of believers that includes venture capitalists and an array of startups investing significant time and money — $4.5 billion in 2017 — exploring blockchain technology.[2]

While blockchain is best known as the foundation for cryptocurrencies such as bitcoin and Ethereum, many think the technology will emerge as the bedrock of a peer-to-peer economy, transforming industries in the process — that is, if the security of blockchain ecosystems can be ensured. A major hack that resulted in the theft of $45 million in Ethereum[3] has raised some eyebrows.

Overcoming the security questions discussed in this paper will help ensure the continued evolution of blockchain in the financial services industry and help it mature into a disruptor in other businesses.

Blockchain basics
Learn more about creating applications exclusively on blockchain or hybrid applications that access blockchains over the internet. Get the basics at **www.dxc.technology/blockchain_basics**.

The promise of blockchain networks

Blockchain is software technology that supports a distributed digital ledger and enables electronic transactions to be performed between two or more parties without the need for a trusted intermediary such as a bank. It's like a banknote passing from one hand to another. From that point on, it becomes possible to confer intrinsic value on the information, whose authenticity, integrity and legitimacy are guaranteed from owner to owner. A blockchain, therefore, makes it possible to create unassailable, tamper-proof digital assets and to achieve digitization and disintermediation for documentation (identity, authenticity, ownership, provenance, etc.); rights (usage, access, authorization, etc.); traceability (receipt, reading, editing, time-stamping, etc.); and even units of account (loyalty points, currency, etc.). These enable businesses to increase speed, improve the customer experience, enable innovative processes and reduce costs.

Since blockchain empowers individuals, entities or things to connect directly through a software-driven exchange, it potentially disintermediates value exchanges — thereby reducing transaction costs and inhibitors to market entry. As such, blockchain can create game-changing products and new business models that could deliver remarkable business value.

[1] "World of banking and cryptocurrencies collide," *Financial Times* video, January 24, 2018. https://www.youtube.com/watch?v=GUBLGbL3-k0

[2] "Blockchain Tops $4.5 Billion in Private Funding This Year, but Deal Growth Stalls," *Wall Street Journal*, September 22, 2017. https://www.forbes.com/sites/jonathanponciano/2017/09/22/blockchain-tops-4-5-billion-in-private-funding-this-year-but-deal-growth-stalls/#16b9aeba74c6

[3] "Here's how an ex-Ethereum developer describes the night the cryptocurrency was hacked," Scott Carey, *TechWorld*, June 22, 2016. https://www.techworld.com/security/ex-ethereum-developer-describes-night-crypto-currency-was-hacked-3642315/

Potential uses include: food traceability to reduce fraud, thereby protecting revenue and increasing brand provenance; resilient supply chain management in the defense sector; and the ability to provide farmers in the developing world with access to financial tools in exchange for sustainable land-usage best practices.

Blockchain has been around for some time but spent several years in the "hype shadow" of cryptocurrencies such as bitcoin, virtual money transferred as securely and simply as sending an email. Over time, blockchain has become a more established and more viable alternative to traditional transactions. While blockchain 1.0 mainly focused on currency transactions, blockchain 2.0 aims to enable the execution of programmable business logic and autonomous enforcement. Potential business applications include the exchange of digital assets such as bonds, health records, digital rights, payments or supply chain processes.

Don't underestimate the transformative potential of blockchain vs. traditional techniques. Blockchain technology promises to remove complexity, cost and time delays, while adding transparency and trust to the mix. Because electronic transactions can be performed without a trusted intermediary, blockchain offers the opportunity to reduce transactional friction in the way we do business today.

A corporate social responsibility risk?
The prevailing consensus algorithm — used to validate blockchain transactions — is known as "proof of work" and relies on various "miner" computer nodes within the blockchain network to perform complex mathematical operations. This role is computationally expensive to perform but, as is the case with bitcoin, is a lucrative one: The first miner to solve the equations gets to validate the transaction and receives a reward of bitcoins. This incentive has led to many players becoming miners.

Unfortunately, demand to build miners has tied up the world's supply of graphics processing units (hardware that can accelerate the computation), which may be better utilized for applications such as medical research, astronomy, defense intelligence and, more generally, machine learning. Additionally, these systems increase power consumption, raising corporate social responsibility questions about the impact on the environment.

Security implications

But as transactions move from a traditional centralized model toward a decentralized model, the security challenges change. For one thing, the main target for attack shifts. Rather than attacking a large institution entrusted to safeguard the assets, the preferred target may be an individual using the blockchain. Reports are already surfacing of individuals being attacked and forced to transfer their cryptocurrency.

Then there are all the questions swirling around key security. Blockchain uses public key cryptography, which relies on key pairs — a public key to be shared and a corresponding private key kept safe by its owner. Secure value exchange between two peers can be done by encrypting information with the receiver's public key — meaning the message can be decrypted only with the corresponding private key.

With blockchain, control of private keys is crucial. Whoever controls the private keys controls the value within the chain. Losing a private key may mean losing the value. Further, adversaries submitting transactions with stolen keys to a verifying node are indistinguishable from legitimate transactions. A possible way to mitigate this risk is by blacklisting stolen private keys. However, this would be controversial, since it would introduce the possibility of a central control point, which goes against the concept of the distributed nature of the chain.

The importance of private keys raises several issues for organizations interested in using blockchain. When a company is a member of a blockchain, who has access to the private keys? How is that access guarded and maintained? What happens if access to the company's private keys is compromised, and what are the subsequent implications for the integrity of the blockchain? What is the best way to revoke private keys? Powerful and sophisticated solutions are needed to securely and effectively generate, manage and control private keys.

Another security concern involves the vulnerability of nodes in a chain. Once a transaction is formed, in the case of some blockchain platforms, it is sent to a blockchain peer-to-peer network of consensus nodes. A consensus algorithm, of which there are a number, is used to agree upon the next block to be added to the chain.

A concerted attack against a number of the lesser-protected nodes in the network could lead to the attacker gaining majority control[4] and, therefore, the ability to game a consensus — an unfortunate side effect of peer-to-peer systems, known as the Sybil attack.[5] This could result in a group of legitimate transactions becoming invalid due to the block's integrity being compromised. Common policies may be required to defend the system as a whole.

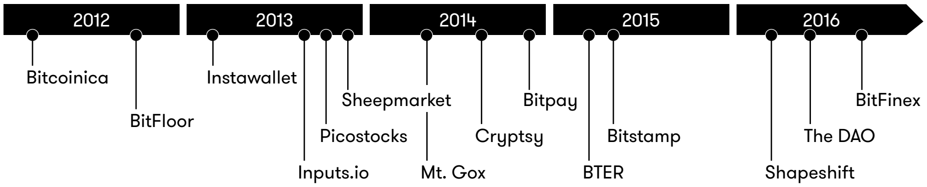
And finally, additional attacks and compromises related to blockchain also pose threats. For example, recent "cryptojacking" approaches plant malware onto a system to enable the mining of cryptocurrencies through parasitic consumption of the host's spare resources. While these are not attacks on a blockchain per se, they are driven by the change introduced by the technology.

Understanding the risk

Adversaries looking to exploit these attack surfaces are getting far more sophisticated and are also constantly innovating. These attackers, which range from criminal organizations to nation-state actors, have different motivations and capabilities for mounting an attack on a blockchain implementation.

Considering the history of blockchain hacks (see **Figure 1** and **Table 1**), it's evident that even though blockchain technology itself is secure, the ecosystem is vulnerable to attacks. Looking at the amounts of virtual money stolen, it's clear that adversaries are focusing on blockchain-based value exchange solutions.

Figure 1. Timeline of blockchain attacks



[4] "51% Attack, Majority Hash Rate Attack," Bitcoin.org. https://bitcoin.org/en/glossary/51-percent-attack

[5] John (JD) Douceur, "The Sybil Attack," Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS), Microsoft, January 1, 2002. https://www.microsoft.com/en-us/research/publication/the-sybil-attack/

Table 1. Blockchain hacks. In the table, amounts are represented in bitcoin (BTC), ether (ETH) and litecoin (LTC).

Date	Platform	Method/ vulnerability	Loot	Value at the time
2012 – February	Bitconica	Security breach — API	40,000 BTC	$350,000
2012 – July	BitFloor	Unencrypted wallet backup	25,000 BTC	$250,000
2013 – April	Instawallet	Security breach — wallet hack		
2013 – October	Inputs.io	Account hack	4,100 BTC	$1,000,000
2013 – November	PicoStocks	Stolen wallet keys	6,000 BTC	$6,000,000
2013 – December	Sheep Marketplace	Inside job	5,400 BTC	$4,000,000
2014 – February	Mt. Gox	Security breach — codebase	850,000 BTC	$700,000,000
2014 – June	Cryptsy	Security breach — codebase	1,300 BTC	$6,000,000
2014 – December	BitPay	Social engineering — account hack	5,000 BTC	$1,800,000
2015 – January	Bitstamp	Phishing — hot wallet hack	19,000 BTC	$5,000,000
2015 – February	Bter	Cold wallet hack	7,170 BTC	$1,650,000
2016 – April	ShapeShift	Security breach — hot wallet hack	• 469 BTC • 5,800 ETH • 1,900 LTC	• $200,00 • $46,000 • $7,600
2016 – June	The DAO	Smart contract code “hack”	3,600,000 ETH	$60,000,000
2016 - August	Bitfinex	Governance flaw — wallet signature	119,756 BTC	$60,000,000

The essence of the most popular incarnation of blockchain — cryptocurrencies — is that they void the need for central regulation and compliance. However, efforts to bring controls to this market are likely to ensure that criminal elements don’t exploit loopholes in a transaction life cycle — so the days of regulatory compliance are not over.

Other security factors to be considered

Due to the combination of complicated concepts, blockchain technology requires a high level of expertise to grasp the many technical nuances that need to be mastered before adoption. Here are some other security factors to consider:

- **While data is shared across the blockchain network, confidentiality requirements need to be taken into account.** Depending on the applications and risks, it may be desirable to encrypt blockchain data in transit. While encryption of transactions may be desirable for assets that will be exchanged only once — preserving the confidentiality of the exchanging parties — this may restrict the resale of assets. Resale transactions are possible only if the blockchain application is aware of the identity of all parties.
- **If both asset liquidity and confidentiality are desirable, alternatives such as the use of a zero-knowledge proof of a transaction may best meet the confidentiality/liquidity trade-off.** Therefore, to maximize market value and liquidity, the cryptographic design of an application should take into account the asset class being traded, such as currency, commodity or collectible goods.
- **As with any corporate application, a security posture of assumed compromise that utilizes a defense-in-depth protection strategy would benefit the design of blockchain applications.** A subtle difference with blockchain is the need to understand the operational risk posed by collateral obligations resulting from the execution of a smart contract. For example, smart contracts can trigger functions from other smart contracts and call for action. An attack on a poorly developed smart contract might have a cascading effect on others. Whenever existing smart contracts have to be updated or deleted, they can be retired only if they had been initially designed for retirement or self-destruction.
- **It may seem as if blockchain provides strong inter-firm trust, and while that is largely true, firms should be mindful of an obvious but easily overlooked point: Blockchain covers only the trust concerns of the ledger itself.** Parties recording transactions onto the ledger — be those human or internet-of-things agents — are still open to corruption, collusion and manipulation. Blockchain technology certainly raises the bar of trustworthy multiparty systems, but dark forces should not be underestimated.

10 ways to embed security into blockchain transactions

If the upsides of blockchain for your application outweigh the concerns evaluated here, the next step may be to launch a proof of concept. We advise you to consider these 10 recommendations to embedding security into blockchain transactions:

1. Develop role-based authentication, authorization and access control applicable to the business solution.
2. Understand the risks and the ownership of the weak points in the value chain and ecosystem.
3. Ensure end-to-end encryption to properly protect data.
4. Adopt a secure-by-design approach that will ensure backward compatibility for the algorithms as they change over time.
5. Develop secure key governance practices.
6. Identify secure coding and secure smart contract life-cycle management frameworks.
7. Focus on proper and trustworthy data entry that reduces the threat of collusion to the system.
8. Implement operational resilience, governance, risk, compliance and management.
9. Conduct threat-based risk assessments.
10. Keep abreast of developments that will enable cyber security monitoring and incident response for block chain solutions.

With market interest in blockchain increasing, and interest in solutions based on the technology emerging, it is time to think about the security implications that will come with the promised benefits and how to manage that risk.

Learn more at www.dxc.technology/secureblockchain

About the authors

Richard Archdeacon
Head of Security Strategy,
DXC Technology

Simon Arnell
Security Chief
Technologist,
DXC Technology

Faisal Siddiqi
Enterprise Architect,
DXC Technology

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, serving nearly 6,000 private and public-sector clients from a diverse array of industries across 70 countries. The company's technology independence, global talent and extensive partner network deliver transformative digital offerings and solutions that help clients harness the power of innovation to thrive on change. DXC Technology is recognized among the best corporate citizens globally. For more information, visit **dxc.technology**.