Blockchain has arrived with a fanfare and hype rarely seen in the realm of information technology, most notably in the form of cryptocurrency applications such as Bitcoin. Often described in terms of absolute trust, anonymity and security, it is touted as a game-changer for businesses, governments and criminals alike. But as organisations rush to deploy applications based on blockchain technology, do the potential benefits outweigh the information risks?

BUSINESS TRANSACTIONS
Conducting business involves transacting with other parties, such as customers or suppliers. For centuries, each party to a transaction maintained a record in a book called a ledger. But a problem with this approach is that any disputes over the contents of the ledger can come down to one party’s word against the other. As a consequence, many transactions rely on intermediaries such as banks, who can help with disputes, but also add to the costs of transacting.

The centuries-old methods of performing transactions and recording them in ledgers have now become computerised using databases. In so doing, any issues from the manual systems have been replicated – and exacerbated – in the digital world. Intermediaries remain and there are more ledgers than ever.

The complex transactions that computers enable have their own issues. For example, criminals may hide fraud and evade justice by employing currency transfers between multiple participants and across international borders.

ENTER BLOCKCHAIN
Blockchain replaces the recording of transactions in multiple ledgers, by different parties, with a single distributed ‘blockchain’ ledger. Participants reach consensus that the contents of the ledger are valid and trustworthy: creating a single version of the truth.

Once a transaction appears in the blockchain ledger it forms an indelible record of a transacted asset’s ownership and is agreed by parties as a ‘done deal’. This enables blockchain to operate without the need for an intermediary.

BLOCKCHAIN BENEFITS
By removing intermediaries, blockchain can reduce transaction complexity and cost. It also claims to reduce the risk of tampering, cyber attack and centralised IT failures. The potential benefits of blockchain are promised in areas such as supply chain, logistics, inventory and asset management. But the hype makes it difficult to weigh up blockchain’s advantages against its disadvantages, and assess whether there is sufficient net gain over existing and more mature technologies such as databases.

SECURITY ISSUES AND MITIGATION
While the more familiar manifestations of blockchain – such as cryptocurrencies – are based on public (permissionless) blockchains, private (permissioned) or federated blockchains are increasingly of interest to ISF Member organisations.

Understanding the potential security issues, and how they can be addressed, is vital for any organisation planning to use applications based on blockchain technology, especially considering the well-known breaches of blockchain related financial services1 – examples are illustrated in Figure 1.

Figure 1: Well-known blockchain breaches

<table>
<thead>
<tr>
<th>Year</th>
<th>Blockchain Name</th>
<th>Amount Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>Mt.Gox</td>
<td>$480m</td>
</tr>
<tr>
<td>2017</td>
<td>Parity Wallet</td>
<td>$155m</td>
</tr>
<tr>
<td>2018</td>
<td>Coincheck</td>
<td>$500m</td>
</tr>
</tbody>
</table>

This report helps those involved in blockchain deployment to:
– understand the main components of a blockchain network: participants, devices, applications and ledgers
– identify security issues associated with developing or using blockchain applications
– address security issues in a structured manner by determining security requirements, applying a secure systems development lifecycle (SDLC) and supporting live blockchain applications.

PERFORMING A BLOCKCHAIN TRANSACTION
Transactions are key to blockchain and understanding them will help Members gain an overall picture of a blockchain network, its benefits and disadvantages. An example of the main stages of a blockchain transaction using cryptocurrency (e.g. Bitcoin) is presented in Figure 5. The same principles are applicable to transactions involving other assets.

Figure 5: Example of a blockchain application

1. Bob uses his blockchain app (wallet) to spend $500 in cryptocurrency for a purchase from Alice. His blockchain application creates a transaction request signed with his private key.

2. Bob’s transaction is broadcast to the blockchain network. The network validates his transaction to ensure he owns the $500. The transaction is packaged with other transactions into a block.

3. The nodes on the blockchain network compete to generate (mine) a digital fingerprint of the block, which is a complex mathematical calculation called a cryptographic hash. The validated block is then appended to the ledger. Each block contains the previous block’s hash, cryptographically chaining the blocks together.

4. The validated block is broadcast amongst participant nodes who confirm its validity and append it to their copy of the blockchain ledger.

5. The blockchain ledger now shows the transaction. Alice is now confirmed the owner of the $500.
5 Conclusion

Blockchain, an approach to creating a distributed ledger, is potentially revolutionary. Much of the mainstream media attention around blockchain is centred on public (permissionless) implementations, particularly via cryptocurrencies, such as Bitcoin. However, many of the new commercial applications are likely to be private (permissioned) blockchain deployments, which may be limited in benefit as they do not take full advantage of the blockchain philosophy.

Blockchain introduces a relatively new concept based on trust in a distributed network of participants, some of whom may not be known. There is a fog of hype that surrounds this relatively immature technology, which can obscure both the value of blockchain applications and the associated risks.

Blockchain risks are particularly acute considering that its security is built on assumptions that the:

– content of the blockchain ledger is both immutable and irrefutable
– underlying cryptography is secure enough to last the life of a blockchain application
– consensus algorithms are robust.

As blockchain is put to different uses, it is vital to cut through the hype to understand its merits and disadvantages. After all, it may not always be the best solution to a problem; directories, databases and other types of data store still have value.

While there may be a commercial advantage from being at the forefront of adopting blockchain, prudent organisations should be aware that blockchain is immature and unforeseen security issues may emerge. Consequently, ISF Members should place a particularly strong emphasis on evaluating the risks of developing or using blockchain applications before trusting this innovative approach.

WHERE NEXT?

The ISF encourages collaboration on its research and tools. ISF Members are invited to join the Technology community on ISF Live to share experiences and discuss practical and innovative approaches for developing and using secure blockchain applications.