Congratulations! You have decided to use blockchain in your organization. Its possibilities are apparently endless, and your business leaders are excited about how it can increase efficiencies and reduce costs.

How to operationalize blockchain

That said, blockchain is in its early stages of development and no one really knows what it will look like in a year—or even six months. What is certain is that many financial services organizations globally—from investment banks to exchanges and retail banks—are investigating the benefits of using blockchain. All of these organizations have complex business lines, legacy technology and regulatory obligations to take into consideration.

There will be private blockchains, such as those used for customer authentication, and public blockchains, such as blockchain for settlements. There will be semi-private consortium blockchains, where banks or exchanges can connect partners for anything from transactions to reporting.

Once you have decided on a blockchain application that suits your business, the next step is to move it out of the incubator and incorporate it within your enterprise applications. And that is where the fun starts; making blockchain applications work in the real world is as much of a challenge as building the blockchain application itself.

Any organization that is serious about blockchain also needs to be serious about connectivity to a partner ecosystem, access controls, governance, integrating blockchain with internal systems and data repositories, visibility into—and real-time monitoring of—blockchain-based transactions and more. Therefore, you will need to operationalize blockchain. Because, despite the hype, blockchain is still largely a stranger to IT departments. Its future is uncertain and, once integrated with legacy systems, it could become a virtual chain around their necks. And, as secure as blockchain is reputed to be, there is still the possibility of errors (see sidebar on page 4).
Blockchain in capital markets

The industry is investigating the uses of blockchain in a variety of ways:

- **R3** leads a consortium partnership with more than 50 of the world’s leading financial institutions, helping them to design and deliver advanced distributed ledger technologies for the global financial markets.
- **Ethereum** is a public blockchain-based platform with smart contract functionality. It is primarily used by fintech start-ups as the basis for building their apps. Larger companies are considering using Ethereum as a platform upon which to base their own private blockchains.
- The Australian Securities Exchange has invested more than $10 million in industry startup Digital Asset Holdings to build a new post-trade settlement system using distributed ledger architecture.
- **Nasdaq** became the first financial institution to take a blockchain proof-of-concept live when it debuted its private shares trading platform, Linq, in 2015.
- Banks including J.P. Morgan Chase and Citigroup have successfully tested blockchain on credit-default swaps.

Blockchain in banking

- Some financial institutions and fintech startups are looking at ways to leverage blockchain in the area of identity and authentication, using the secure data to create an identity on blockchain.
- Others want to enable real-time money transfers. A group of banks, including UBS, Santander and UniCredit, experimented with moving money across borders using a blockchain platform that payment network Ripple created.

Blockchain in insurance

The insurance industry is also investigating ways to use blockchain.

One of these is for customer engagement, where the company’s users may be concerned about handing over their personal data and are frustrated by having to enter the data repeatedly. A customer-controlled blockchain could be used for identity verification or medical data; the blockchain remains on the customer’s device. Start-ups are working on blockchain solutions for Know Your Customer (KYC) data, where users can simply forward their secure identity data to other parties for on-boarding. This can also be used in other areas of financial services.

Another use for blockchain is in the area of smart contracts to automate underwriting and claims handling. The idea is that it will pay out against the insurable event without the policyholder having to make a claim or the insurer having to administer the claim.

This could greatly reduce the cost of claims processing and insurance fraud. Also, any customer who has waited for days or weeks for an insurance agent to come around and survey any damage will be much more satisfied if the claim can be made immediately. The Internet of Things (IoT) will accelerate the use of blockchain in insurance; devices from cars to home appliances can have their insurance policies registered and administered by smart contracts in a blockchain network. Sensors would detect damage and then trigger the repair process, as well as claims and payments.

Whatever a firm uses blockchain for, the challenge lies in incorporating, monitoring and managing the technology within the enterprise architecture.

“Distributed ledger technology has the potential to change financial services as profoundly as the Internet changed media and entertainment.”

— **R3 consortium**
What has to be done to operationalize blockchain?

While much of the emphasis is on blockchain itself and possible use cases, an equally important question is, “how will we introduce blockchain into the enterprise?”

To put it another way, “how will we operationalize blockchain?”

First, you need to connect to a private or public blockchain ecosystem and/or with external parties using the blockchain.

Second, you have to integrate blockchain applications with existing technology. This is not as easy as it sounds, as you have to decide how to manage and plan for future architectural transformations caused by other disruptive technologies. Plus, you have to manage that infrastructure as blockchain standards evolve.

Third, you will have to decide how to interact with the blockchain ecosystem, with regards to security and access controls.

Fourth, you have to figure out how to monitor transactions and events on the blockchain and react to them in real time.

Fifth, you have to decide how to reconcile data that exists in blockchains and legacy applications.

Sixth, you have to automate, coordinate and manage processes that span existing technologies and blockchains.

In short, you must rapidly and seamlessly utilize blockchain to gain the advantages of the technology today without having to run complex, costly and lengthy programs of re-architecture.

Lifecycle events need to be managed too. For example, when a counterparty exercises an option on a smart derivatives contract in the blockchain, that event needs to be captured and propagated to the same downstream systems. Similarly, external events, such as those relating to market data, will also need to be monitored and applied to the smart contracts. You will need to plan for integrating those systems, having first identified what systems are affected and how.

New higher-level processes may also need to be established to exploit the benefits from the blockchain ecosystem. The interoperability between systems will have to be agile, secure and have robust governance. Enterprise applications should not be exposed to any complexities of the blockchain and should be abstracted away.

Operationalizing blockchain also addresses the need for access controls over the participants, from an application and business context, be it internal or external to the enterprise.

Integration that is technology-agnostic and the ability to establish and execute the policies required for governance are key to the blockchain access layer. API-based integration will be a popular choice.

Critical aspects of operationalizing blockchain:

- Existing applications have to work seamlessly with blockchain by using an integration access layer to manage the interoperability.

  Every enterprise has legacy technology that must be interoperable with blockchain. From KYC to risk management and settlements, these applications have to engage seamlessly with the new blockchain applications to ensure complete interoperability.

- It is important to have complete visibility of every event in the blockchain network.

  Enterprises must monitor blockchain and query and search the blockchain for transactions based on all manner of criteria, with response times equivalent to existing technologies.

“A blockchain is essentially an incorruptible ledger of blocks of data, and that data can be just about anything.”

— John Naughton | Professor of the public understanding of technology at the Open University

Smart contracts

A smart contract is an automated agreement that executes pre-programmed instructions to reach a pre-defined outcome. For example, in a blockchain payments application the contract would automatically calculate the amount of the payment and then arrange for it to be made. The automated execution takes place via software which has been programmed with the instructions.

Smart contracts are the key to using blockchain technology in complex financial transactions, because they can drastically speed up the affirmation and confirmation process. Smart contracts reduce complexity so there are fewer reconciliation issues, which increases efficiency and reduces costs.
Making blockchain smart

Smart contracts are only as smart as their programmers and their logic could contain bugs, or there may be unforeseen and therefore untested conditions, such as negative interest rates, or buying and selling at the wrong price (such as when Knight Capital’s algorithm lost it $440 million in 30 minutes). The impact of such conditions may reveal themselves months, or even years, after a transaction was executed, upon maturity or an option exercise for example.

News that a blockchain-based investment fund known as the Decentralized Autonomous Organization (DAO) was compromised in June to the tune of $55 million worth of Ether digital currency, rattled blockchain enthusiasts and crashed the share price of operator Ethereum. A participant exploited weaknesses in the smart contracts upon which the fund’s transactions were based, enabling him/her to withdraw other investors’ Ether money. If a smart contract has bad code that is immutable and distributed on the blockchain, the potential for damage could be huge, especially if that code is intentionally malicious. How do you monitor and detect such rogue code? And how do you stop it, how do you pull the plug? IT and compliance departments are right to be concerned about the security and sovereignty of blockchain smart contracts that are operating within their enterprise.

"[Blockchain] was created to solve a problem that had been puzzling digital activists for decades: how to create digital property without a central authority keeping track of who owns what.”

— Alex Hern | Technology reporter for the Guardian®

• Automate process orchestration and enable blockchain events to trigger processes across multiple off-chain and on-chain applications.

Although blockchain transactions occur in a closed environment, they can impact events both inside and outside the chain. Technology is critical to make these on- and off-chain applications interoperable in an automated fashion.

• Provide for the governance, risk management and security of the blockchain network.

What happens in a blockchain application can have an impact across an enterprise, so careful monitoring off- and on-chain is necessary in order to enable proper governance, risk management and security of the entire network.

Access, manage and control

Interoperability of blockchain within an enterprise requires:

• A blockchain access layer that seamlessly integrates blockchain with legacy technology for interoperability
• The ability to correlate and validate data and apply business context going into blockchain
• Governance and security to enterprise or industry-wide blockchains
• Event processing and aggregation for complete visibility on- and off-chain activities
• Monitoring, exception management and alerting of blockchain events
• Process automation for off-chain process orchestration
• An overlay service layer to enrich functionality of blockchain apps

Conclusion

In order to enable existing applications to work with blockchain seamlessly, organizations need to use an access layer to manage the interoperability. Acting as a broker, the access layer offers the ability to abstract the complexities of blockchain and smart contracts, expose the functionalities of the blockchain application and communicate them to legacy applications. Through a total surveillance module, the access layer has complete visibility of every event in the blockchain network, with that visibility the analytics engine can detect anomalies and gather intelligence. Automated process orchestration enables blockchain events to trigger processes across multiple off-chain and on-chain applications. Another module can provide for the governance, risk management and security of the blockchain network.

Ask your Software AG representative how you can efficiently operationalize blockchain using the Digital Business Platform. Or, learn more on our website.

ABOUT SOFTWARE AG

The digital transformation is changing enterprise IT landscapes from inflexible application silos to modern software platform-driven IT architectures which deliver the openness, speed and agility needed to enable the digital real-time enterprise. Software AG offers the first end-to-end Digital Business Platform, based on open standards, with integration, process management, in-memory data, adaptive application development, real-time analytics and enterprise architecture management as core building blocks. The modular platform allows users to develop the next generation of application systems to build their digital future, today. With over 45 years of customer-centric innovation, Software AG is ranked as a leader in many innovative and digital technology categories. Learn more at www.SoftwareAG.com.

© 2016 Software AG. All rights reserved. Software AG and all Software AG products are either trademarks or registered trademarks of Software AG. Other product and company names mentioned herein may be the trademarks of their respective owners.