Smart Contracts Don't Monitor Themselves: Deploying Reliable Software on the Blockchain

amberdata

There's little disputing that blockchain technology is driving tremendous change.

Blockchain-based software is driving innovation at organizations large and small across a range of industries, from finance to agriculture to global trade to tourism and beyond.

What explains this momentum?

In large part, it's the result of the potential of the blockchain to make software systems and data more trustworthy and transparent. By decentralizing the control of resources and making information tamper-resistant, blockchain holds enormous promise for helping to build a fairer, more efficient future.

Yet the trust and transparency that blockchain has the potential to deliver are not a given. While it is indeed possible to build safer, more reliable software and services by taking advantage of blockchain's unique features, these benefits can be fully realized only when proper monitoring and oversight are applied to blockchain-based applications. To date, that has been difficult, as most insights into blockchain-based software were opaque at best.

This reality can be easy to overlook amid all of the excitement currently surrounding blockchain. The tremendous enthusiasm for blockchain technology has partly obscured the sobering fact that, at the end of the day, software that relies on the blockchain – such as Decentralized Applications (DApps) and smart contracts – requires the same types of monitoring and management as traditional software applications in order to be deployed reliably and effectively. Despite myths to the contrary, blockchain-based software is not immune to the same management challenges or reliability as other types of applications.

Indeed, not only do DApps and smart contracts require the same level of management and oversight as conventional applications, but in some respects blockchain poses special new monitoring challenges for software deployment teams. The unique requirements of features such as smart contracts and inter-blockchain data transactions increase the need for proper monitoring and analysis even further.

How can software development, deployment and management teams address these challenges?

This whitepaper explains by discussing the special monitoring needs of blockchain-based applications and offering guidance for meeting them. It explains what it takes to deploy software reliably on the blockchain and to make good on the promise of trust and transparency that the blockchain has the potential to unlock.

Why Trust Doesn't Happen Automatically on the Blockchain

Before delving into the specific challenges of deploying DApps and smart contracts, let's examine the myths surrounding trust, reliability and the blockchain.

Those myths hold that by storing data on the blockchain, or executing applications on the blockchain, organizations can somehow automatically guarantee that their software is reliable, trustworthy and perhaps even immune to being hacked.

This is not, in fact, the case. It is true that blockchain technology has the ability to help increase reliability and trust via immutable data storage, decentralized decision-making and transparent transactions that can be verified by all members of the network. Yet there are many ways in which DApps and smart contracts can suffer problems that undercut the user experience or the mission of the software provider:

- **Poor transaction processing speeds** could lead to unacceptably slow application performance. The Ethereum blockchain can process only about twenty transactions per second, whereas credit card processors handle tens of thousands. While there are methods for working around transaction delays in blockchain applications, those applications must be properly monitored to ensure that transactions proceed at an acceptable rate.

- **A lack of built-in auditing and reporting features** can make it difficult to maintain necessary levels of visibility into software and data. Without proper auditing and reporting, organizations that deploy blockchain applications may fail to meet compliance requirements. They may also lack data that is important for investigating security incidents.

- **Data could be manipulated by attackers** who discover vulnerabilities within blockchain protocols, or attempt to undermine the blockchain via an exploit such as the 51 percent attack.

- **Data could go out of sync** in the event that the blockchain used by an application is forked or there is a major disagreement between different sections of the network regarding state. Such a problem could also result from malicious activity like a 51 percent attack, or from more benign errors such as I/O problems.

In these ways and many more, blockchain-based software can easily go awry, failing to achieve the goals that its creators intend.

When that happens, the organization deploying the software as well as the users depending on it suffer because they can no longer trust the confidentiality and integrity of blockchain-based data and applications.

To make matters more complicated from a trust perspective, visibility into blockchain applications is often limited from a user's perspective due to a lack of open source code. Although blockchains are sometimes presented as "trust machines," there is no requirement that an application that runs on the blockchain be powered by open source code. When users lack the ability to inspect code and verify that an application does what its developers promise, their ability to trust it is limited. This does not mean that developers should never write closed-source Dapps, but it does mean that optimizing the performance and reliability of such applications is especially crucial in order to deliver fully on the trustability promise that blockchain offers.

And in an ecosystem where the number of startups created in the past few years reaches into the thousands – to say nothing of established companies competing to make the most of blockchain technology – even a small degradation in the trust and reliability of a DAapp or a smart contract can have dangerous effects for companies striving to succeed in this crowded market.

The Wide-Reaching Challenge of Trust

These challenges, by the way, apply broadly to any application that interacts with any blockchain in some way, not just those that meet narrow definitions of "Dapp" and "smart contract."

To be sure, there are significant technical differences between a blockchain such as Bitcoin, which was designed primarily to transfer value, and Ethereum, which enables smart contracts. There are also differences between a true Dapp or smart contract, which runs in a totally decentralized fashion via a blockchain that provides compute resources, and other applications that might store data on the blockchain but are not executed in a distributed fashion. Nonetheless, issues such as network contention and security vulnerabilities create serious problems for any blockchain application, no matter which category it falls into.

To date, the problems described above have received relatively little attention, perhaps because excitement about the potential of blockchain technology has overshadowed the reality that, like any other type of software, blockchain applications are subject to weaknesses and risks that need to be monitored and managed. As blockchain technology enters into widespread production use, however, and more organizations depend on blockchains for day-to-day operations, this fact is a fact that developers and IT operations teams everywhere will need to confront.

Finally, note that the challenge of guaranteeing trust applies in equal measure to public blockchains, such as Bitcoin, Multichain and Stellar; smart contract platforms like Ethereum; and permissioned, private blockchains like Hyperledger or Quorum, which are run via private networks that are not open to the public. Although permissioned blockchains, which are becoming popular within enterprise consortiums, make it possible to fine-tune access control for blockchain resources, they do not prevent the integrity, reliability and security problems described above that can undercut trust.

Properly Monitoring and Analyzing Blockchain Applications

With the right tools and processes, software delivery teams that deploy DApps and smart contracts can meet these challenges. Ensuring proper trust and reliability requires meeting the following specific challenges throughout the blockchain software delivery lifecycle.

Ensuring Data Integrity

Although blockchains provide special features that help to resist data loss or unintended data manipulation, they do not fully prevent the occurrence of these and other data integrity problems.

As a result, data integrity issues can arise within DApps and smart contracts in a variety of ways. As noted above, data may be manipulated maliciously by attackers who exploit vulnerabilities in blockchain protocols. Data could be lost in the event of a fork, especially because most blockchains can provide only probabilistic finality, with the result that the result of a transaction could be changed long after the transaction takes place. I/O errors could cause data corruption. And while some blockchains are designed with append-only data rules in an effort to prevent data loss, not all blockchains offer or strictly enforce this feature.

If data that your application depends on to meet the needs of users, such as account information or transaction histories, is lost or manipulated in these ways, your application will no longer meet user expectations or fulfill its intended task. This is true of any type of application, but it can be easy to forget this fact when managing Dapps and smart contracts, due to the myth that blockchain-based data is somehow immune to reliability and availability problems.

Monitoring Transaction Speeds

Slow transaction speeds have famously hampered the ability of some blockchains, like Ethereum, to provide the level of real-time performance that some DApps and smart contracts require in order to achieve their maximum potential. This is beginning to change as new blockchain platforms appear that boast transaction speeds as high as 35,000 transactions per second. In other cases, workarounds, such as paying higher transaction fees in order to speed transactions, can lead to better performance.

Yet no matter how fast your blockchain can complete transactions, or which strategies you employ to speed them up, the fact remains that continuously monitoring transaction speeds is critical in order to ensure that you are meeting SLAs and other commitments. The blockchain itself won't notify you if transactions are slowing down.

Tracking Third-Party Data

The blockchain itself doesn't necessarily record all of the data that your DApp or smart contract requires to operate properly. For example, transactional data, such as internal message calls between smart contracts, might not be stored on the blockchain on which the smart contract executes. Or an oracle may collect data from an external source in order to execute a smart contract without writing that data to the blockchain.

In these cases, it is important to monitor the state of such third-party data, and possibly to keep a record of it. Given that the data is not written to the blockchain itself, software delivery teams must ensure that they set up separate processes to keep track of this critical information in order to guarantee full visibility and auditability -- which represent another benefit that the blockchain is uniquely situated to enable, but only when managed properly.

Monitoring Multi-Blockchain Transactions

As more and more blockchains come into existence, it is increasingly common for DApps and smart contracts to interact with multiple blockchains at the same time. A number of protocols and platforms, such as Plasma (which enables the creation of "child" blockchains in the Ethereum ecosystem that run independently of the main Ethereum blockchain) and Aion (a protocol for integrating different blockchains via a federated network), help to smooth such integrations between blockchains.

They do not, however, provide the monitoring, reporting or automated failover features that are necessary to ensure that multi-blockchain transactions proceed as expected. If a flaw in a cross-chain transaction protocol causes a smart contract to fail to retrieve important information, for example, or an inter-blockchain transaction that is supposed to be atomic does not end up proceeding as such, software delivery teams must be immediately aware of the problem so that they can address it before it impacts end users.

Mapping Relationships

Your smart contract may not be an island. It may depend on other smart contracts or external processes to operate properly. The same could be true of a DApp that interacts with other DApps.

For this reason, mapping the relationships between different smart contracts and DApps is crucial in order to prevent a failure in one component from spilling over into another. If, for example, one smart contract fails to execute in time due to network congestion, you'll want to know whether other smart contracts that were waiting on the first one will also be impacted.

Security issues are at play, too, when mapping interactions between smart contracts. In order to identify problems such as man-in-the-middle attacks and contract identity spoofing, software management teams need to be able to understand how smart contracts are supposed to interact, then detect anomalies.

Access Control

Data access control is a persistent challenge on blockchains -- not least because most mainstream blockchains offer few built-in features to ensure that only certain groups have access to certain pieces of data. And even in cases where data access is restricted via add-on features or the uses of a permissioned blockchain, it's possible for access control policies to fail or be misconfigured, leading to a breach of privacy.

This is why monitoring permissions is vital for ensuring that blockchain-based data that is supposed to be confidential is actually confidential. Software management teams must be able to track the state of data access via graph map views and advanced search functionality that enables them to verify that permissions are properly configured and enforced.

Ensuring Auditability

Although some blockchains are designed in theory to create immutable records of data, in practice that is not a guarantee, as noted above. And even if it were, third-party transactional data that is important for auditing reasons may not be recorded on the blockchain.

You therefore can't rely on the blockchain itself to guarantee the level of auditability that you need to meet ensure full visibility into your DApps and smart contracts, and to meet compliance requirements. You must build your own auditability solutions by implementing the proper monitoring and reporting tools.

Data Actionability

Last but not least, software delivery teams must be able to translate the insights they collect about their DApps and smart contracts into action. That requires the ability to search and analyze the data, automatically detect anomalies and generate automated alerts about a potential problem with blockchain-based software.

Monitoring DApps and smart contracts is only half the battle for providing acceptable levels of software trust and reliability. Taking action to resolve problems as they occur is just as critical.

Blockchain Software You Can Trust: The SAP Example

What does properly managed and monitored blockchain software look like in practice? Consider SAP's track and trace supply-chain management solution as an example.

In SAP's definition, a blockchain application that is used to its maximum potential is distinguished by several key features:

- Use by multiple parties.
- The elimination of intermediaries.
- Transparency.
- The ability to transfer digital assets.

This is the approach to blockchain technology that is driving SAP's vision for a next-generation track and trace platform for managing the supply chain. SAP envisions the blockchain serving not just as a place to store data, but as a solution for ensuring transparent and reliable digital transactions among multiple parties, with no central group in control.

That level of transparency and reliability can be guaranteed only when the blockchain that powers the supply-chain management application is properly monitored and managed. Left unmonitored, the blockchain is at risk of problems such as the failure to record all relevant in a transaction or smart contracts that do not execute properly due to unanticipated conditions. With a way to identify and address these issues quickly, enterprises like SAP would not be able to use the blockchain to drive true innovation in supply-chain management.

Conclusion

Smart contracts, DApps and other applications that leverage the blockchain hold enormous potential for delivering a high level of trust and transparency. But they won't achieve this value on their own.

Instead, they must be deployed with the proper level of monitoring, insight, analysis and actionability to ensure that they perform as expected. Blockchain-based software that is not appropriately managed is at risk of failing to meet users' expectations in a variety of ways -- from slow responsiveness to a loss of data to improper data access and more -- and harming the competitiveness of the organizations that deploy it.

Amberdata, the first end-to-end blockchain monitoring and actionability solution, offers a solution to these challenges. By combining the monitoring features of tools like New Relic with the APM insights offered by solutions like AppDynamics and the analytics features of Splunk, Amberdata makes it possible to track blockchain applications continuously, in real time -- and to take effective action when problems arise. It provides enterprise-grade tools for monitoring and reporting critical information from blockchain apps, as well as APIs for building on top of the data. In so doing, Amberdata transforms blockchain application deployment from an opaque, ad hoc endeavor into a clear-cut, systematic process that meets the needs of production-quality software.

Amberdata is helping to enable a future in which companies can take full advantage of the potential of blockchain technology. No matter which blockchain you use, how your DApps and smart contracts are written and whether you work with permissioned or public data, Amberdata provides the visibility and actionability into blockchain-based applications and services that organizations need to leverage the blockchain responsibly and build trust and transparency into trustless platforms.

To learn more and sign up for a free Amberdata account, visit amberdata.io.

amberdata.io