MARKET PERSPECTIVE

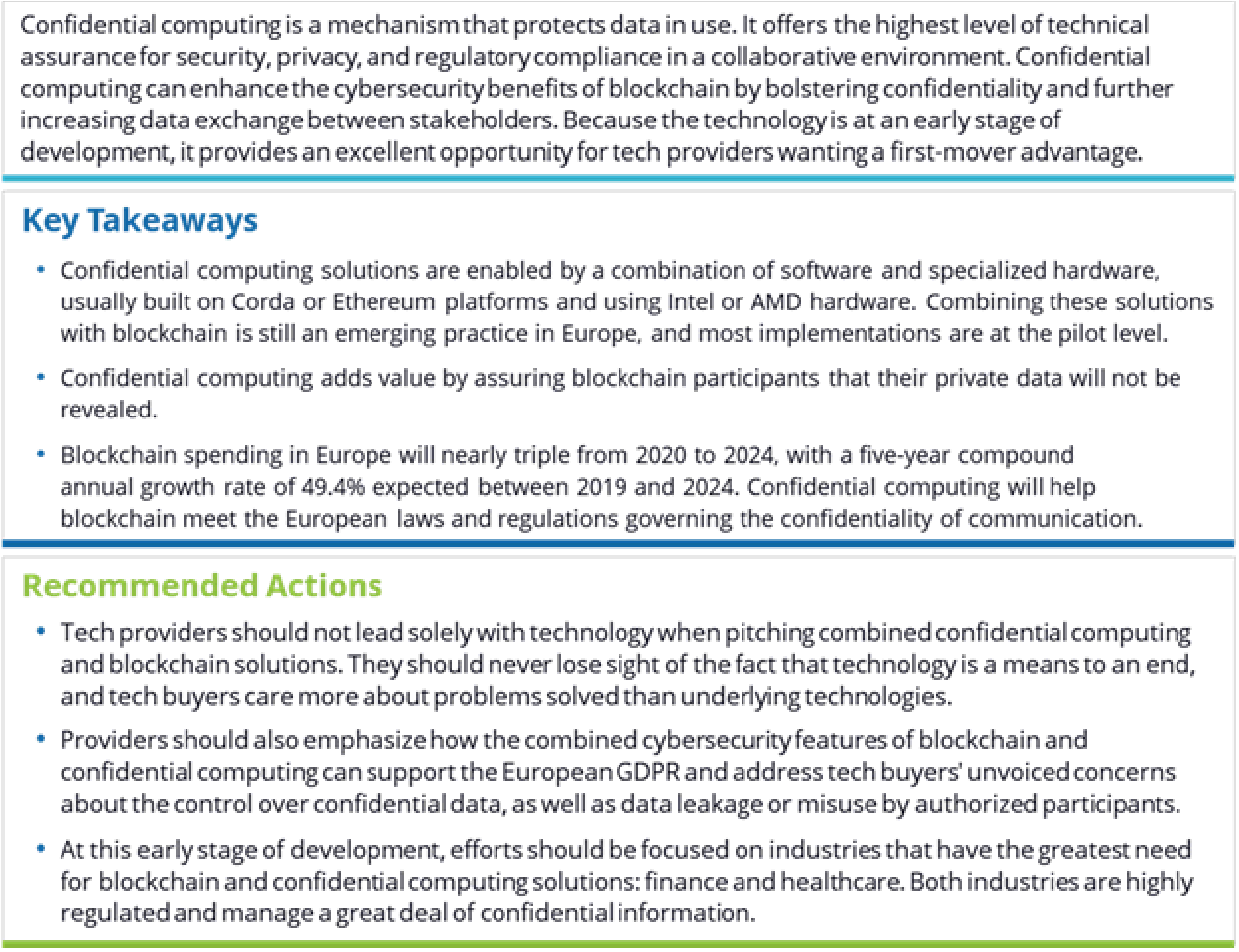
What Confidential Computing Can Bring to the European Blockchain Landscape

Radoslav Dragov Mohamed Hefny

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: What Confidential Computing Can Bring to the European Blockchain Landscape



Confidential computing is a mechanism that protects data in use. It offers the highest level of technical assurance for security, privacy, and regulatory compliance in a collaborative environment. Confidential computing can enhance the cybersecurity benefits of blockchain by bolstering confidentiality and further increasing data exchange between stakeholders. Because the technology is at an early stage of development, it provides an excellent opportunity for tech providers wanting a first-mover advantage.

Key Takeaways

- Confidential computing solutions are enabled by a combination of software and specialized hardware, usually built on Corda or Ethereum platforms and using Intel or AMD hardware. Combining these solutions with blockchain is still an emerging practice in Europe, and most implementations are at the pilot level.
- Confidential computing adds value by assuring blockchain participants that their private data will not be revealed.
- Blockchain spending in Europe will nearly triple from 2020 to 2024, with a five-year compound annual growth rate of 49.4% expected between 2019 and 2024. Confidential computing will help blockchain meet the European laws and regulations governing the confidentiality of communication.

Recommended Actions

- Tech providers should not lead solely with technology when pitching combined confidential computing and blockchain solutions. They should never lose sight of the fact that technology is a means to an end, and tech buyers care more about problems solved than underlying technologies.
- Providers should also emphasize how the combined cybersecurity features of blockchain and confidential computing can support the European GDPR and address tech buyers' unvoiced concerns about the control over confidential data, as well as data leakage or misuse by authorized participants.
- At this early stage of development, efforts should be focused on industries that have the greatest need for blockchain and confidential computing solutions: finance and healthcare. Both industries are highly regulated and manage a great deal of confidential information.

Source: IDC, 2021

NEW MARKET DEVELOPMENTS AND DYNAMICS

Enterprises are becoming more and more reliant on digital infrastructure as they transform their services and operations through the steady application of digital technologies – i.e., as they undertake digital transformation (DX). Given their need to accelerate digital transformation and simultaneously minimize costs, numerous businesses in Europe are using cloud computing or remote servers to store and process critical data, instead of hosting infrastructure on premises. These enterprises that are migrating workloads to the cloud naturally have concerns about the security of their sensitive data. IDC's *Future of Trust Survey* revealed that the top three challenges to establishing trust today are **increasingly sophisticated cyberattacks**, **complex regulatory requirements,** and **fragmented IT and security infrastructure**.

Companies use the confidentiality, integrity, and availability (CIA) triad model to gauge their level of information security and guide cybersecurity policies. **Confidentiality** describes the ability of enterprises to maintain privacy and secrecy of their data (e.g., by only allowing access to authorized persons). **Integrity** is about guaranteeing that code/data can be trusted because it has not been tampered with by anybody. **Availability** refers to the ability of enterprises to provide users with timely and reliable access to the systems and applications they need (see Figure 2).

Confidentiality (or privacy) is the biggest concern enterprises have when using a third-party cloud provider. IDC's Future of Trust framework regards privacy as a strategic pillar that drives trusted outcomes. To mitigate privacy concerns, cloud vendors have started providing protection services for both *data at rest* and *data in transit*. Data in transit refers to data that is being transferred from one location to another, usually via the Internet. Because data in transit is thought to be more vulnerable, it requires stricter data protection measures. Meanwhile, data at rest is data that is not actively moving from location to location. While data at rest is viewed as more secure than data in transit, its content often makes it a more valuable target for malicious actors.

However, a gaping hole vis-à-vis security pertains to **data in use** (i.e., data that is currently being processed or read). Data has to be unencrypted prior to processing, which leaves it vulnerable to various malicious attacks. **Confidential computing** substantially reduces this security weakness by separating confidential data into a CPU enclave when it is processed. Any data inside the enclave can be accessed only by authorized programming code and no other party.

IDC defines confidential computing as a mechanism that protects (encrypts) data in use. Confidential computing thus offers the highest level of technical assurance for security, privacy, and regulatory compliance in a multitenant, geo-dispersed, or collaborative environment. Isolation and sandboxing techniques are designed to give the data owner complete authority over data and ensure that only authorized code accesses this data. Confidential computing guarantees enterprises that their confidential data is secure (and thus encourages them to transfer more of their data to off-premises services). These twin capabilities of confidential computing – ensuring data protection and facilitating greater data exchange between different stakeholders – broadly mirror those of blockchain. While there are important differences between the two technologies, they complement rather than compete with each other in a powerful way. The next section discusses how confidential computing can resolve some blockchain problems and facilitate its wider adoption.

How Is Confidential Computing Relevant to Blockchain?

Blockchain scores very highly on the integrity and availability fronts in the CIA triad model discussed earlier. However, blockchain ranks comparatively poorly in terms of confidentiality. Confidential computing can thus play an important role in this respect.

When it comes to ***data integrity,*** blockchain – the immutable ledger of transactions – can be safely considered as a very secure technology. By combining its decentralized structure with cryptography and sequential hashing, blockchain provides much greater security than a standard database.

In terms of ***data availability***, blockchain guarantees operational resilience with its peer-to-peer structure that has multiple nodes operating in a distributed manner. Blockchain is very resilient against distributed denial of service (DDoS) attacks because it operates in a distributed manner with no single point of failure. A DDoS attack is a malicious attempt to overwhelm a network or its surrounding infrastructure with a flood of Internet traffic. During such an attack, some of the multiple nodes of a blockchain can be made redundant without disrupting the entire network. The information on a blockchain is only in danger of being compromised if 51% or more nodes are commandeered by malicious actors.

Blockchains have made tremendous strides in terms of ***data confidentiality*** since their introduction. Initially, the only blockchains were public (meaning that there were no restrictions on who could access and participate in the network). Naturally, the public availability of all blockchain information made it very impractical for enterprises that wanted to keep most of their data private. This impediment led to the development of private blockchains with appropriate access and security controls. On such blockchains, only authorized individuals and businesses can see certain confidential information. The fact that a blockchain provides a single source of truth that cannot be disputed or altered without another party's knowledge encourages different businesses to voluntarily share more information with each other without the need for middlemen.

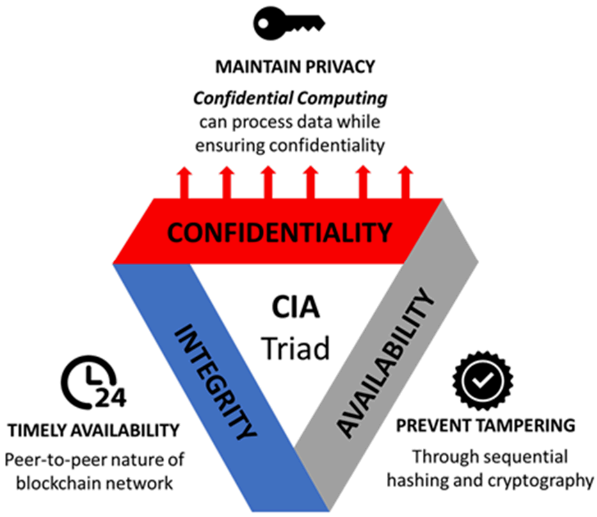
However, there are certain scenarios where the guarantee of a "single source of truth" and strong access controls are not enough to attract companies to a blockchain. In a blockchain, any authorized party inside or outside the organization can see shared information. Organizations have no control over what authorized parties do with that information. There is always a risk that the information shared with external parties will be abused or purposefully leaked by malicious actors. Since that risk is ever present, organizations are reluctant to share information. The utility of blockchain largely comes from its ability to let multiple parties exchange information more freely.

Financial fraud detection is a good example in this regard. It is difficult to detect illicitly acquired funds if they are transferred from several banks and not detected when deposited at an initial bank. Blockchain minimizes this problem as transactions are time stamped and signed — allowing them to be traced back to a corresponding party as well as a specific time. This built-in audit capability boosts reliability and gives enterprises more security and transparency over interactions. However, banks are reluctant to share all their transaction history with competitor banks for fear of giving away strategically important information. They are even reluctant to share such history with "trusted" third parties in case it may be misused by a rogue employee.

In such instances, **confidential computing is of great benefit — it can protect such sensitive data by performing computation in a hardware-based trusted execution environment (TEE), which is a secure enclave within a CPU**. In essence, this means that inputs are protected and inaccessible to the parties processing the data. For example, data from all banks can be collected and fed into a secure enclave. This data can then go through fraud detection processing without exposing the underlying transaction data to anyone. Confidential computing assures users that data is processed in a secure and tamperproof way. This capability encourages companies to share confidential data since they know it will not be revealed to other entities or parties processing the transactions. Thus, confidential computing further enhances the cybersecurity benefits of blockchain by bolstering confidentiality and increasing data exchange between stakeholders.

FIGURE 2

Outline of the Intersection of Blockchain and Confidential Computing


MAINTAIN PRIVACY
Confidential Computing can process data while ensuring confidentiality
CONFIDENTIALITY
CIA Triad
INTEGRITY
AVAILABILITY
24
TIMELY AVAILABILITY
Peer-to-peer nature of blockchain network
PREVENT TAMPERING
Through sequential hashing and cryptography

What is confidential computing?

Confidential computing is a hardware-enabled mechanism that protects data in use. It offers the highest level of technical assurance for security, privacy, and regulatory compliance in a collaborative environment.

How is confidential computing relevant to blockchain

Confidential computing can further enhance the cybersecurity benefits of blockchain by bolstering the confidentiality of private data and thereby increasing data exchange and collaboration between stakeholders.

Where can both technologies be applied?

At this early stage, it is best to focus efforts on the industries that have the greatest need for confidential computing solutions: finance and healthcare. Both industries are highly regulated and must comply with disparate regulatory frameworks.

Source: IDC European Blockchain Practice, 2021

The Small but Growing Ecosystem of Solutions that Combine Blockchain and Confidential Computing

While discussions of both confidential computing and blockchain can become very technical and abstract, there are real-life examples that demonstrate the benefits of both. However, the confidential computing examples in Europe are small and have not yet reached industrial scale, chiefly because the technology is still at a nascent stage of emergence. Nevertheless, both technologies have clear and tangible benefits, so it is only a matter of time until they become more widespread.

Due to its nature, confidential computing solutions encompass both hardware and software. Hardware enables the confidential processing of information that software (which does not necessarily have to be based on blockchain) takes advantage of. Since confidential computing protects data in use, it needs specific hardware-based protections built into the CPU. CPUs process and execute instructions and are distinctly separate from computer memory. There are a handful of CPU manufacturers that dominate the computing market. Among the hardware leaders in the market, AMD and Intel stand out for their confidential computing-enabling hardware. This hardware allows an enterprise software solution provider like R3 to build its confidential computing platform Conclave on a solid footing.

Major Players

Intel

As part of its continuing efforts to secure sensitive data, Intel developed the Software Guard Extension (SGX). SGX is a security instruction set baked into many of Intel's x86-based CPUs (most PCs and laptops are based on the x86 architecture). SGX offers hardware-based memory encryption that isolates specific application code and data in memory. Developers can use SGX hardware to protect sensitive portions of application code and data. This environment keeps blockchain data in an encrypted form until it is needed for a transaction. When ready for processing, data is then decrypted in a secure enclave which is only accessible to permitted participants. Essentially, Intel SGX helps keep users' sensitive data from being revealed or modified by creating a trusted execution environment within memory. However, it is important to point out that the SGX is not built only for blockchain.

Recently, Intel released the third generation of its **Xeon** scalable processors with a host of specialized security features. Xeon's new SGX allows it to turn parts of a server's memory into secure enclaves that store sensitive data such as encryption keys. The new Xeon processors also have a built-in crypto acceleration feature, fittingly called Intel Crypto Acceleration. This feature improves the functioning of major cryptographic algorithms such as AES, SHA, and GFNI, allowing for real-time encryption without affecting performance. Overall, Intel has a head start in the chip manufacturer space, but competition will soon heat up.

A Real-Life Use Case Example — Trusted Compute API

Intel, along with other Ethereum community leaders, launched the Trusted Compute application programming interface (TC API) to extend the notion of decentralized trust to off-chain workloads. This API was developed for business-oriented Ethereum networks, but can be extended to support other blockchain frameworks.

Developers can accelerate the execution of complex smart contracts while preserving the privacy of sensitive off-chain data with TC API – in other words, transactions can execute in an off-chain compute environment and then return results to the main Ethereum blockchain.

AMD

AMD is a large multinational semiconductor company that develops computer processors for business and consumer markets. The company's EPYC processor offers hardware-accelerated protection that supports data-in-use encryption. The processor's AES-128 encryption engine, which is embedded in the memory controller, automatically encrypts and decrypts data in main memory when an appropriate key is provided. At the same time, the AMD Secure Processor provides cryptographic functionality for secure key generation and key management.

AMD's capability to encrypt the entire main memory space of a virtual machine, and its use of one key per virtual machine to isolate guests and the hypervisor from each other through an advanced security feature called Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP), make it perfect for the cloud.

Microsoft recently announced that it would be the first major cloud provider to offer confidential Azure virtual machines based on the new AMD EPYC 7003 series processors. Blockchain services deployed on Azure and built on top of confidential computing will thus be more private, confidential, and secure; they will also support hardware-accelerated computations. In addition, the virtual machines will secure inefficient and complicated applications that are offloaded from a blockchain, including artificial intelligence and Internet of Things workloads.

Going forward, most CPU products will likely have inbuilt security features that support confidential computing. In such an environment, where most hardware supports confidential computing, the rapid deployment of a variety of use cases will depend on software and solutions.

R3's Conclave

When it comes to software that enables the development of confidential computing solutions for blockchains, one provider has achieved a head start – R3. R3 has a solution called Conclave, which complements its enterprise blockchain called Corda. Like other confidential computing solutions, Conclave is designed to solve business problems in which data needs to be shared with other organizations or people without content being revealed.

With Conclave, confidential data is pooled into an Intel SGX enclave where it is protected even when being processed. The solution makes it easy for multi-party applications to be cryptographically verified for integrity before the transfer of sensitive data. Conclave, which is currently available as a standalone platform, is compatible with R3's blockchain platform Corda Enterprise. A full integration is forthcoming.

Conclave has a high-level API for writing applications on any operating system, as well as for code written in several popular computer languages. Firms can build new solutions and services on the platform or develop and run existing solutions across new private data sets.

It is worth noting that confidential Computing applied to blockchain in R3's Conclave platform adds an additional security layer to the data exchange network between participants, ensuring data that *should be* synchronized *is* synchronized. In addition, Conclave allows network infrastructure to be used in situations where data absolutely *must not be* synchronized or shared, but where it must, nevertheless, be pooled. This opens the door to a series of additional application scenarios and use cases.

A Real-Life Use Case Example — IntellectEU's ClaimShare

The Belgian digital finance technology company IntellectEU developed the ClaimShare solution that employs confidential computing and blockchain to reduce fraudulent claims in the insurance industry. The solution utilizes R3's Corda blockchain and Conclave confidential computing platform enabled by Intel SGX. One of the most common fraudulent activities is the taking out of multiple claims across different insurers for the same loss event. This practice is especially difficult to detect since there is no industry data-sharing standard. In addition, there are regulatory constraints to sharing sensitive and personal information.

ClaimShare aims to reduce the number of fraudulent claim payouts by offering a fraud claim verification solution across insurers. The solution enables insurers to submit public claims data on the ClaimShare ledger (after verification); it then checks if a claim has been paid out by another insurer while guaranteeing total privacy so than no competitive information is revealed. If submitted data matches one on record, insurers can be sure that that claim is fraudulent. They can then prevent a second payout to the end user.

T-Mobile's NEXT

T-Mobile developed NEXT, an open-source identity and access management platform for enterprises. Primarily intended for internal use, NEXT reduces friction, improves security, and increases auditability and historical reporting. NEXT is built upon the Hyperledger Sawtooth framework and utilizes the hardware TEE provided by Intel SGX in the consensus algorithm.

SAP Leonardo Blockchain as a Service

SAP offers ready-to-use blockchain technology via its SAP Cloud Platform. The blockchain element is based on the Hyperledger open source blockchain platform and uses its standards and protocols. A trusted executable deployed on a host with Intel SGX support can act as a local blockchain extension. After a secure onboarding of the host to a trustworthy network, it can execute local programs that can be seen as off-chain smart contracts. The processed data remains completely unknown to the network.

ADVICE FOR THE TECHNOLOGY SUPPLIER

Educate Tech Buyers

In many ways, confidential computing's first steps mirror those of blockchain: Little is understood about the technology and it is very technical to explain, but it has the potential to add enormous value across industries. At this stage, most effort should be spent on educating potential tech buyers about what confidential computing is and how it works. However, the primary goal should be to demonstrate the benefits and synergies that tech buyers can derive from confidential computing *and* blockchain combined. Blockchain enables secure and effortless collaborations between multiple stakeholders, while confidential computing allows certain private information to be shared for a specific purpose without being revealed.

Make a Clear Case for Creating a Worry-Free Environment

Some companies are reluctant to adopt blockchain-based solutions (especially if it means becoming part of a wider ecosystem) chiefly because they have lingering worries that the data they send to a blockchain is out of their control and can be leaked.

The combined blockchain and confidential computing solutions built so far, which are based on Corda or Ethereum platforms, take advantage of Intel or AMD's hardware execution and acceleration features. Just as early commercial blockchain applications turned into consortium-based solutions, IDC believes that groups of buyers will come together to adopt the same confidential computing solutions and collaboratively exchange information with each other without confidentiality risks. For example, financial institutions can unite to create specific applications for preventing money laundering and fraud. These financial institutions can pool private information for the sole purpose of fraud detection. Moreover, such groups of buyers do not have to be created from scratch; rather, they can piggyback on existing consortia or alliances formed around a specific blockchain.

Target the Two Most Prospective Industries

Confidential computing software platforms and solutions are still developing, and blockchain applications in Europe are still on the emerging technology fringes. At this early stage, suppliers should focus efforts on the two industries that have the greatest need to enhance blockchain trust and security with confidential computing solutions: finance and healthcare. Both industries are highly regulated and need to comply with disparate industry and regional regulatory frameworks. These industries also manage a great deal of personal and sensitive data. The cost of a data breach is an increasing concern for finance and healthcare organizations, not only in terms of regulatory fines for the loss or breach of sensitive data, but also in terms of the erosion of organizational trust in the eyes of customers and the general market. Moreover, finance is by far the largest sector in terms of blockchain spending in Europe, and healthcare will be the fastest growing industry between 2021 and 2024 (according to the IDC Worldwide Blockchain Spending Guide).

LEARN MORE

Related Research

- *IDC TechBrief: Extend the Circle of Trust with Confidential Computing in Public Cloud* (IDC #US47510421, April 2021)
- *The Blockchain Trilemma and Its Impact on the European Blockchain Market* (IDC #EUR145773120, December 2020)
- *The Importance of Interoperability for the Development of the European Blockchain Industry* (IDC #EUR145774120, November 2020)
- *IDC Market Glance: Blockchain in Europe, 2Q20* (IDC #EUR145773920, April 2020)
- *Barriers to Blockchain Adoption in Europe* (IDC #EUR145773720, March 2020)
- *Blockchain Adoption in Europe, 2020: Awareness and Growth by Country and Industry* (IDC #EUR145773520, March 2020)

Synopsis

This Market Perspective describes confidential computing and reveals how it enables a high level of technical assurance for security and privacy in a collaborative environment. This paper also details how confidential computing can complement blockchain by bolstering the confidentiality of private data and further increasing data exchange between stakeholders. Because confidential computing is at an early stage of development, it provides an excellent opportunity for tech providers wanting a first-mover advantage.

"Blockchain spending in Europe will nearly triple from 2020 to 2024, making it an interesting market for confidential computing. Blockchain can help this emerging technology meet the European laws and regulations governing confidentiality of communication and increase trust in transactions between network partners." – Senior Program Manager, Mohamed Hefny, Virtualization, Systems and Infrastructure Solutions, IDC EMEA

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
blogs.idc.com
www.idc.com