Blockchain for Off-Chain Smart Contracts in an SAP® Environment

Trustworthy processing of private data from SAP HANA using SAP Blockchain on a Camelot Trusted Computing Appliance and Dell EMC Ready Solutions

ABSTRACT

Blockchains come with inherent privacy challenges. In a basic blockchain, all data is publicly available for all network participants without any encryption. This is a problem in cases where blockchain applications require data privacy. In this paper, we discuss an approach that allows blockchain-based applications to reliably process private data. This approach uses the Camelot Trusted Computing Appliance in an SAP HANA® database environment running on a Dell EMC infrastructure foundation. This approach keeps private data completely off-chain while registering the private data on-chain by storing a hash of it for later verification of its integrity.

February 2018


**BLOCKCHAINS AND PRIVACY**

Blockchains were originally used for authenticity-only purposes, not for privacy. That means a basic blockchain stores all data publicly available for all network participants without any encryption. In one of the first blockchain implementations, Bitcoin, this fact is even part of the concept. In order to let the simple smart contract of Bitcoin validate the distributed ledger continuously, it is necessary to have all transaction data, including amount, source account and target account, available in unencrypted form. The often-quoted anonymity on the Bitcoin network is rather a result of massive obscurity than of real security measures like encryption and privacy.

Many organizations forget this fact when they think about blockchain use cases. Also, use cases we thought about internally quite often turned out to have privacy requirements — basically almost every serious business use case comes with the need to secure blockchain transactions against read access from everybody.

This situation leads to the invention of so called **consortium blockchains** and **private blockchains**, which in contrast to the initial **public blockchains** have an authorization process on top of the authentication process. Nevertheless, for certain use cases consortium and private blockchains are not an option, and for another group of use cases even those closed blockchains are not good enough in terms of data privacy.

**BLOCKCHAIN APPLICATIONS THAT NEED DATA PRIVACY**

Ultimately, some public blockchain applications need data privacy. To tackle this situation, we implemented a first privacy layer on top of the Ethereum Blockchain, which encrypts data prior to putting it on the chain. Through the exchange of the symmetric decryption key, secured by asymmetric key-pairs, we realized a secure data exchange through the blockchain, like the Secure Socket Layer approach on the Internet (HTTPS).

This approach has the limitation that the encrypted data cannot be processed by smart contracts on-chain any longer. Why? The smart contracts would have to unencrypt the encrypted data on-chain. To enable them to do so we would have to send the decryption key to the blockchain, which then would be visible to all participants inside the transaction it was issued in. The privacy of the data to be processed would be gone in that moment. Thus, for the next group of use cases this privacy layer is not good enough.

**BLOCKCHAIN APPLICATIONS THAT NEED COMPLETELY PRIVATE DATA**

Some public or private/consortium blockchain applications need to trustworthily process completely private data. We identified several of these use cases.

As we noted above, the processing of private data is not possible on blockchains. Storing encrypted data on-chain excludes the possibility to process it with trustworthy smart contracts.

Example use cases for this type of application can be found wherever regulation processes meet intellectual property — for example, when certain components of a product construction plan (intellectual property, or IP) are controlled and need to be reported throughout the supply chain of a product (regulation process). None of the suppliers in such a scenario wants to reveal its construction plan, but each supplier still must report the regulated components that are part of the plan. So it is important to keep most of the data private and publish only, because of trustworthy processing, small amounts of it, which are defined by a central data pool (regulated data). Most parts of this scenario can be realized using any kind of blockchain except for the trustworthy processing of private data.
EXAMPLE USE CASES
Let’s consider a few examples of blockchain use cases that require data privacy.

PHARMACEUTICALS: DRUG APPROVAL
In this use case, a new drug produced by a pharmaceutical company needs to be registered with the complete recipe via hash on the blockchain in order to be reviewed by a regulatory body.

Via trusted computing, the regulatory body can be enabled to check the complete recipe against a publicly available list of regulated compounds, without getting to know the complete, secret recipe.

If existing regulated substances are inside the new drug, information on them would be visible to the regulatory body and appropriate measures could be triggered, such as no approval, prescription only or requirements to keep certain threshold levels.

ADDITIVE MANUFACTURING: TRUSTWORTHY PRODUCTION NETWORK
Additive manufacturing, such as 3D printing or Selective Laser Sintering (a 3D-printing method), enables many trustworthy use cases supported by blockchains and trusted computing. For example, these use cases can include:

• Protecting intellectual property (3D models) during manufacturing by subcontractors
• Establishing trust with new suppliers and subcontractors through trustworthy sampling, such as analysis of print logs and deriving respective quality information from them

As the results of additive manufacturing steps are "real digital twins," the production logs (if there is trust in them) can be used to judge the quality of the product.

In these use cases trusted computing needs to be implemented in the producing devices, such as the 3D printers.

THE SOLUTION
To help organizations implement use cases like these, Camelot Innovative Technologies Lab (Camelot ITLab) and Dell EMC are collaborating on a solution that enables organizations to capitalize on the unique capabilities of blockchains in a manner that protects the privacy of sensitive data.

Camelot IT Lab
Camelot Innovative Technologies Lab (Camelot ITLab) is the leading SAP consultancy for digital value chain management, with more than 20 years of experience. Camelot guides clients in their digital transformations from strategy to the implementation of innovative solutions. The company’s blockchain journey started in 2015, and today Camelot offers a comprehensive portfolio of blockchain products and services leveraging Camelot Hypertrust Platform and SAP Leonardo.

Dell EMC
Dell EMC, a part of Dell Technologies, services its customers — including 98 percent of the Fortune 500 — with a broad, innovative infrastructure portfolio from edge to core to cloud. A strategic SAP technology and software partner for more than 20 years, Dell EMC is a leader in server and storage performance benchmarks for SAP HANA® and SAP applications.
Blockchain-based applications can reliably process private data. To achieve this, the Camelot Trusted Computing Appliance can be used in deployments powered by a Dell EMC infrastructure foundation. This approach keeps private data completely off-chain. It lets all parties store their private data in their local environment/network only. Nonetheless, it registers the private data on-chain by storing a hash of it for later verification of its integrity.

The processing of this data is kept completely off-chain. All involved parties agree on an algorithm to be used to process their private data, which can be achieved on-chain with voting machines. This algorithm is then distributed to all parties as an executable program. The important fact: The algorithm result is specifically authorized to be published to the blockchain.

The danger of this approach: The parties could alter the algorithm that was agreed on when it is running on their off-chain infrastructure. This is where trusted computing comes into action. This concept uses a hardware-based measure to prevent the unauthorized modification of executables in local environments and to circumvent the manipulation of their processes at runtime. By doing so, trusted computing can solve the old “never trust the client” problem.

**A SCENARIO**

In this white paper, we set up the following scenario to demonstrate the feasibility of trusted computing in an SAP environment. This scenario includes the use of:

- Camelot Trusted Computing Appliance on a Dell Enterprise Workstation
- SAP Leonardo Blockchain as a Service as the blockchain network
- SAP HANA database as persistency of the private data on Dell EMC Ready Solutions for SAP

**CAMELOT TRUSTED COMPUTING APPLIANCE**

Camelot Trusted Computing is based on the Camelot Hypertrust Platform. It involves an SAPUI5 frontend, Node.js middleware, and interfaces to different blockchain backend technologies and trusted computing enclaves, the so called Camelot Trustlets. The

---

**Figure 1.** Solution overview: SAP Leonardo – Blockchain and SAP HANA® for Trusted Computing.
middleware also contains local storage. These components are provided by an appliance based on a Dell Enterprise Workstation using Intel® Software Guard Extensions (Intel® SGX) and accessing blockchain as a service (BaaS) via HTTPS.

It is possible to use SAP HANA as an additional local persistency. Upon the creation of relevant records in SAP HANA, a hash is created on the blockchain to uniquely identify these records and to guarantee their integrity later on. Those records registered via hash on the blockchain can be processed later using Camelot Trusted Computing. SAP HANA is accessed through the middleware and the available SAP HANA database client for node. The SAP HANA database is operated on a Dell EMC Ready Solution for SAP HANA.

In this scenario, only the blockchain and the trustlets are trusted areas. All other components of the landscape are alterable and potentially unsafe. To ensure a reliable communication between the secure blockchain and trustlet components through insecure channels (middleware), asymmetric encryption with digital signatures is used to verify the validity of the communication messages.

DELL EMC INFRASTRUCTURE: READY SOLUTIONS FOR SAP

The SAP HANA platform in this solution is based on the Dell EMC PowerEdge™ R940 server with Intel® Xeon® processors, the most powerful enterprise server platform in the Dell EMC portfolio. This platform is built for speed and scalability while offering value-added features that enhance management and reliability. With 48 DDR4 DIMM slots and 24 hard drives (including up to 12 Express Flash NVMe PCIe SSDs), the system scales to handle the most demanding workloads. To streamline and accelerate deployment, the Dell EMC infrastructure is available in Ready Solutions that are optimized for SAP HANA.

Dell EMC Ready Solutions include:

- **Ready Nodes** — Dell EMC offers Ready Nodes dedicated to SAP HANA. Built on Dell EMC PowerEdge servers with Intel Xeon processors, these Ready Nodes are pre-sized, pre-built and delivered with SAP HANA software pre-loaded.

- **Ready Bundles** — Dell EMC Ready Bundles bring together SAP-certified Dell EMC servers, storage and networking, including support for SAP HANA Tailored Data Center Integration (TDI).

- **Ready Systems** — These pre-built systems deliver the convenience of an appliance and the flexibility of TDI, including options that incorporate Dell EMC V[x]Block, VxRail and VxRack.
Dell EMC hybrid and cloud options:
In addition to on-premises deployments, Dell EMC offers a choice of hybrid cloud and off-premises platforms for SAP HANA environments.

- **Hybrid cloud** — The Dell EMC Enterprise Hybrid Cloud solution combines hardware, software and services from Dell EMC and VMware into a platform built on converged systems to deliver the foundation for infrastructure-as-a-service. Dell EMC and VMware have spent thousands of hours of engineering time designing, testing and proving the platform in a lab setting, so organizations deploying cloud solutions don’t have to expend that effort.

- **Off-premises managed cloud for SAP** — Virtustream, a Dell Technologies business, offers an unparalleled platform for running SAP in the cloud. The platform was purpose built for handling complex, mission-critical enterprise applications. Virtustream experts have extensive experience working directly with SAP applications. They have the expertise to seamlessly migrate SAP deployments to the cloud.

**SAP LEONARDO BLOCKCHAIN AS A SERVICE**

With SAP Leonardo, SAP is offering a digital innovation system that meaningfully integrates next-generation technologies, including ready-to-use blockchain technology, as cloud computing based services via SAP Cloud Platform. The blockchain element is based on the Hyperledger open source blockchain platform, using its standards and protocols.

**KEY TAKEAWAYS**

In the blockchain context, trusted computing can serve as a complement to the existing technology to realize different technical use cases. Here are a few examples:

**TRUSTWORTHY PROCESSING OF SECRET DATA CONNECTED TO A BLOCKCHAIN**

The 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 the 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.

![Figure 3. Use case: Trustworthy processing of secret data](image)
**INTER-BLOCKCHAIN DATA EXCHANGE**

Today there is no standardized way to exchange data between two separate blockchains. A Camelot Trusted Computing Appliance can be used to realize this by establishing a secure and trustworthy data channel. Even possibly necessary data transformations can be implemented inside the data exchange trustlet, onboarded on the blockchains on both sides.

![Diagram of inter-blockchain data exchange](image)

**Figure 4.** Use case: Inter-blockchain data exchange.

**SECURE BLOCKCHAIN INJECTION OF OFF-CHAIN DATA**

Smart contracts cannot consume data from outside the blockchain. Data from trustworthy sources (e.g., public websites secured with a trusted SSL certificate) can be pushed into blockchains using the Camelot Trusted Computing Appliance.

![Diagram of secure blockchain injection of off-chain data](image)

**Figure 5.** Use case: Secure blockchain injection of off-chain data
GETTING STARTED
To help your organization get started with SAP HANA and SAP Leonardo Blockchain, the Dell EMC Global SAP Center of Excellence provides a wide range of resources to accelerate deployment and time to value.

Using the Center of Excellence, your IT leaders can consult with experts, explore demonstrations of the SAP HANA platform and SAP Leonardo, and access test systems to size your projects. These activities can help your organization reduce project risks and enable analytic success.

Located near SAP’s worldwide headquarters in Walldorf, Germany, the Dell EMC Global SAP Center of Excellence can be accessed through scheduled engagements virtually or on-site. DellEMC.com/Global SAP Center of Excellence

LEARN MORE
To learn more about Trustworthy Processing of Private Data from SAP HANA using SAP Blockchain on Camelot Trusted Computing Appliances and Dell EMC Ready Solutions:

• Contact your Camelot ITLab or Dell EMC representative.
• Visit any of the following sites:
  – SAP HANA and SAP Leonardo Blockchain as a Service sap.com/products
  – Camelot camelot-itlab.com/hypertrust-network or camelot-itlab.com/trusted-computing
  – Dell EMC DellEMC.com/hana or DellEMC.com/techcenter

Dr. Marten Neubauer is SAP Enterprise Solution Consultant at Dell EMC’s Global SAP Center of Excellence, responsible for developing and driving new solution approaches for the healthcare and life sciences business. A former CIO for a national German healthcare provider himself and a Ph.D. for system integration into OR theaters, Marten has a breadth of experience in the healthcare and life sciences segment. Marten is driving a number of thought leader initiatives to support SAP solutions with Dell EMC infrastructure.
Email: Marten.Neubauer@dell.com

Andreas Goebel is head of Center of Digital Innovation Camelot ITLab in Mannheim, Germany. After spending more than 15 years in R&D at SAP in Walldorf and several years in blockchain technologies and cryptocurrencies, he decided to combine this expertise in his new role at Camelot to find real business applications of blockchain technology. Today, he is passionately evangelizing the blockchain topic throughout the SAP ecosystem and among Camelot’s customers.
Email: agobi@camelot-itlab.com

To learn more, visit: DellEMC.com/sap or contact your Dell EMC representative for a one-on-one conversation about your needs and goals.