GSGI Persönlich

Sehr geehrte Leserinnen und Leser

Die letzten zwei Jahre waren von einem spürbaren Digitalisierungsschub in allen Branchen geprägt. Der rapide Ausbau von Vernetzung, Kommunikation und Cloud führte nicht nur zu einer Verknappung von Elektronikkomponenten, sondern auch zu grassierender Cyber-Kriminalität. Die böswillige Verschlüsselung von Firmendaten mit nachfolgender Erpressung hat weltweit Schlagzeilen gemacht. Mittlerweile suchen sich die Angreifer lohnende Ziele in der Gebäudetechnik. Das globale Cyber-Sicherheitsunternehmen Kaspersky analysierte weltweit 40 000 intelligente Gebäude und fand heraus, dass fast 4 von 10 dieser Gebäude von einem bösartigen Cyberangriff betroffen waren. In den meisten Fällen versuchten diese Cyberangriffe, die Computer zu infizieren und im Nachgang die Steuerung der Gebäudeautomation zu übernehmen. Es wird höchste Zeit, dass sich unsere Branche dagegen rüstet.

Felix Gassmann
CTO Fr. Sauter AG

Autor: Felix Gassmann

Blockchain im Dienst der Gebäudeautomation

Mit dem Aufstieg von Bitcoin, der digitalen Internetwährung, wurde die Blockchain-Technologie plötzlich zum Hype. Internetgiganten planen eigene digitale Kryptowährungen und bedrohen die traditionelle Welt der Leitwährungen und der Banken. Abseits dieser Megatrends gehen wir ganz andere Wege und zielen auf eine «friedliche» technische Nutzung der Blockchain-Technologie, indem wir die Daten und Prozesse der Gebäudeautomation schützen.

Bei Blockchain denken viele zuerst an Bitcoin und damit an die Absicherung von Zahlungs-Transaktionen. Beim Bitcoin liegt unter einer dynamischen Transaktionsschicht eine statische, durch die Blockchain gesicherte, dezentrale (verteilte) Datenbank – eine Art Hauptbuch aller bisherigen Transaktionen. Mit jeder Transaktion wird diese Datenbank erweitert, vergleichbar einer Kette, der ständig neue Elemente hinzugefügt werden (daher auch der Begriff Blockchain = Blockkette). Jeder Rechner im Bitcoin-Netzwerk kann sehen, dass Teilnehmer A eine Transaktion an Teilnehmer B vornehmen möchte. Nun entsteht ein Rennen dieser Rechner: Dem Ersten, dem es gelingt, den Transaktionscode der Blockchain zu knacken, wird mit einer Beteiligung belohnt. Erst wenn alle Rechner in Netz zum Ergebnis kommen, dass die Transaktion gültig ist, wird sie in die Blockchain eingetragen und damit durch die Verkettung unfälschbar verewigt. Warum nun unfälschbar? Ein neuer Block enthält den digitalen «Fingerabdruck» des vorhergehenden Blocks. Wird in einem der Datenblöcke nur ein einziges Bit geändert, ändert sich der Fingerabdruck des betroffenen und allen in der Kette nachfolgenden Blöcke. Infolgedessen wird die Gültigkeit der Blockkette am Ort des Eingriffes ausgesetzt: Bildlich gesprochen bricht die Blockchain auseinander. Damit fliegen Fälschungen oder Fehler in einem Datenblock sofort auf und können durch Überschreiben aus unversehrten Teilen der verteilten Datenbank korrigiert werden.

Die Jagd nach dem Bitcoin-Transaktionscode – also das Bitcoin Mining – ist ausserordentlich rechenintensiv. Aufgrund des Börsengangs einiger grosser Bitcoin-Firmen, konnte man im 2019 deren Stromverbrauch ermitteln und auf das gesamte Bitcoin Netzwerk extrapolieren. Resultat: Die Kryptowährung Bitcoin allein benötigte damals für ihre Rechenoperationen rund 46 Terawattstunden Strom pro Jahr. Um diesen Energiebedarf zu decken, werden jährlich rund 22 Megatonnen Kohlendioxid freigesetzt. Das entspricht etwa dem CO_2-Fussabdruck von Hamburg oder ganz Sri Lanka.

Wir haben uns die Blockchain-Technologie auf ganz eigene Weise zunutze gemacht und übersetzen das Prinzip in die Welt der vernetzten Gebäudeautomation. Die Idee ist schnell erklärt: Die statischen Daten der Automationsstation im Netz werden zu einer Blockchain verkettet. Wie bei Bitcoin wird zunächst ein Genesis-Code erzeugt und verschlüsselt zur ersten Station im Netz geschickt. Danach werden die Daten der Station und der Genesis-Code miteinander verschmolzen und daraus ein digitaler Fingerabdruck erzeugt. In der Folge berechnet jede Automationsstation ihren digitalen Fingerabdruck auf der Basis ihrer eigenen Daten und eines Fingerabdrucks der im Blockchain-Ring vorangehenden Station. Die Block-Daten bestehen typischerweise aus Programmen, Firmware, Prozess- und Netzwerkparametern. Einfacher formuliert: Jede Station bildet mit ihren Daten einen Block der Blockchain. Wird die Integrität der Daten in einer Station verletzt – es genügt ein einziges Bit zu löschen oder zu ändern –, «zerbricht» die Blockchain sofort.

In einer ersten Entwicklungsvariante haben wir im Falle einer Integritätsverletzung unter anderem folgende Aktionen vorgesehen:

a) Nur Alarm auslösen und Übermittlung an Managementsystem via MQTT oder

Bild 1: Der «Building Data Integrity Manager» generiert den Genesis-Code der Blockchain und speichert die digitalen Zwillinge der im Netz befindlichen Automationsstationen.

E-Mail, betroffene Station und geänderte Daten identifizieren

b) Alarm auslösen, betroffene Station aus der Blockchain isolieren und neue Blockchain mit den unversehrten Stationen aufbauen

c) Alarm auslösen, betroffene Station isolieren, automatische Selbstheilung durchführen, Blockchain neu initialisieren

Die Funktion Selbstheilung setzt voraus, dass in der Inbetriebsetzungsphase von allen Stationen je ein digitaler Zwilling gebildet wurde. Diese Zwillinge, eine Kopie aller statischen Daten, werden in einer verschlüsselten Datenbank gespeichert, welche in einer dedizierten Automationsstation, dem «Building Data Integrity Manager» (BDIM) gesichert werden (Bild 1). Der BDIM übernimmt auch die Generierung des Genesis-Codes und die zyklische Prüfung des letzten in der Kette übertragenen digitalen Fingerabdrucks. Der Selbstheilungsprozess ist besonders interessant, weil er auch bei nicht autorisiertem Eingriff durch eigenes Servicepersonal dafür sorgt, dass die in der Inbetriebsetzungsphase vom Kunden validierten Daten unverfälscht überspielt werden. Damit haben wir für die wichtige Anforderung der Systemintegrität nach IEC 62443 einen bisher unerreichten Sicherheitslevel erreicht.

Da in unserem Verfahren kein Mining stattfindet und jede Station den digitalen Fingerabdruck ihrer Daten selbst berechnet, ist der Rechenaufwand und die anfallenden zusätzlichen Kommunikationsdaten im Netz vernachlässigbar. Von erhöhtem Strombedarf ist keine Rede, jedoch von einer hohen Datensicherheit schon!

Die Blockchain Technologie hat bereits in einem grösseren Projekt praktische Erkenntnisse geliefert: Ein einziger BDIM verkettet 50 Automationsstationen resp. Gebäudeklimazonen zu einer Blockchain (Bild 2).

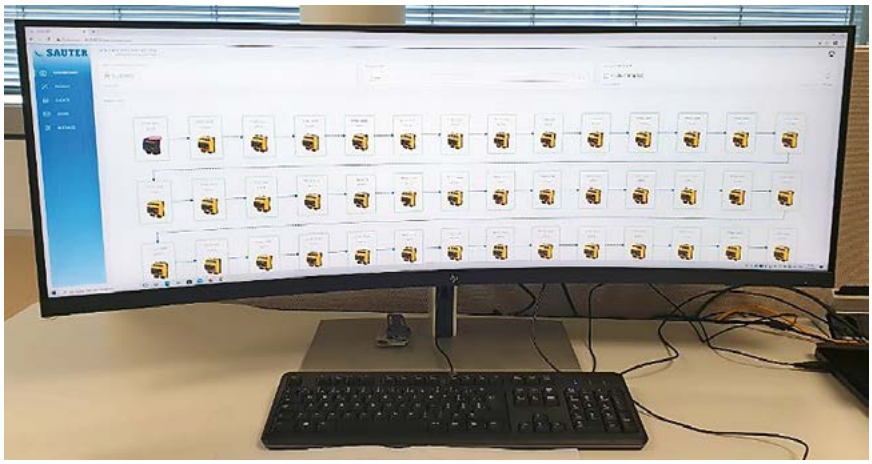

Bild 2: Visualisierung der Blockchain: Verkettung der Daten von 50 Automationsstationen.

GSGI-Mitglieder

BKW Building Solutions AG
www.bkwgt.ch

Bouygues Energies & Services InTec AG
www.bouygues-es.com

Burkhalter Group
www.burkhalter.ch

CKW Gebäudetechnik
www.ckw.ch

Hälg Group
www.haelg.ch

Honeywell AG
www.honeywell-schweiz.ch

Lippuner Energie- und Metallbautechnik AG
www.lippuner-emt.com

Sauter Building Control
www.sauter-building-control.ch

Schindler Aufzüge AG
www.schindler.ch

Securiton AG
www.securiton.ch

Siemens Schweiz AG
www.siemens.ch

VINCI Energies Schweiz AG
www.vinci-energies.ch

AKTUELL
Fachkurs Projektleitung Bauindustrie
Dauer: 10 Tage (3 × 3 + 1)
Zertifikat: Hochschule Luzern Technik & Architektur
Beginn nächster Kurs: 22.03.2022
www.hslu.ch

CAS Projektmanager/in Bau
Dauer: 25 Tage (5 × 5)
Zertifikat: Hochschule Luzern Technik & Architektur
Beginn nächster Kurs: 28.03.2022
www.hslu.ch

KONTAKT
Gruppe der Schweizerischen Gebäudetechnik-Industrie GSGI
Telefon 041 227 60 05
info@gsgi.ch I www.gsgi.ch