Een risk based-benadering

Blockchain security Auditing

22 december 2021

Reza Torabkhani

(Publicatiedatum: 22 december 2021)

Nu blockchain-technologie steeds vaker wordt toegepast en meer de aandacht trekt van bestuursleden en CxO's van veel organisaties, wordt het voor IT-auditors noodzakelijk om zich te verdiepen in de risico's die voortkomen uit de implementatie van deze technologie en de auditing ervan. Dit artikel wil inzicht geven in de risico's van blockchain-implementaties en enkele aanknopingspunten bieden voor een risk based-benadering van blockchain security auditing.

In dit artikel worden eerst de basisprincipes van blockchain geschetst. Dan wordt in hoofdlijnen een auditaanpak beschreven. Het artikel eindigt met een aantal afsluitende woorden.

Basisprincipes blockchain

De fundamentele functie van de blockchain is het kunnen delen en distribueren van gegevens of waarden, zonder de noodzaak van een vertrouwde tussenpersoon en zonder enig afgedwongen systeembeheer. Het ontwerp van de software en het netwerk zelf biedt de blockchaindeelnemers de mogelijkheid te vertrouwen op de waarheidsgetrouwheid van de informatie op de blockchain. [ISAC20] Bekeken vanuit een technisch perspectief is een blockchain een 'gedistribueerde append-only timestamped datastructuur'. [CASI18] Append-only timestamped houdt in dat een database chronologisch groeit en dat het alleen mogelijk is om gegevens (met tijdstempel) aan de database toe te voegen. Het wijzigen of verwijderen van eerder ingevoerde gegevens in eerdere blokken is onmogelijk.

Daarbij wordt gebruikgemaakt van beveiligingsfuncties zoals cryptografische hashes, digitale handtekeningen, gedistribueerde consensusmechanismen en peer-to-peertechnologie. De gegevens worden in blokken opgeslagen in een niet wijzigbare keten van transacties, zonder enige centrale vertrouwde autoriteit. De transacties vinden plaats tussen twee knooppunten (*nodes*) van het blockchain-netwerk. De gebruikers worden gekoppeld aan asymmetrische sleutels om op de blockchain te werken. Er zijn

softwareproducten in de vorm van digitale portemonnees (*wallets*) ontwikkeld om onder meer het sleutelbeheer te vereenvoudigen. Deze kunnen de vorm hebben van software-as-a-service of van een lokaal te installeren applicatie.
Een bekend voorbeeld van een transactie is de overdracht van een aantal digitale munten. Transacties kunnen complex zijn, tot aan een geautomatiseerd transactieprotocol dat zonder menselijke tussenkomst contractbepalingen uitvoert. [SZAB94] In dit geval wordt gesproken over *smart contracts*. Een smart contract functioneert als broncode die automatisch, onherroepelijk wordt uitgevoerd op het moment dat wordt voldaan aan vooraf afgesproken voorwaarden. Een voorbeeld is een smart hypotheekcontract, dat de aflossingen bijhoudt en het betreffende vastgoed overdraagt op het moment dat de gehele hypotheek is afgelost.

Een blockchain kan privaat of publiek zijn. Een private blockchain is *permissioned*. Dit houdt in dat de diensten in de keten gereguleerd zijn en de nodes alleen gebruikt mogen worden door gebruikers die daarvoor gemachtigd zijn. Publieke blockchains zijn *permissionless*, wat inhoudt dat de diensten vrijelijk door nodes kunnen worden aangeroepen. Bij permissionless blockchains is een deugdelijk consensusmechanisme van cruciaal belang. Door de afwezigheid van regulering is dit immers de enige manier om transacties te valideren.

Blockchain-audits

Bij de ontwikkeling van een toetsingskader voor blockchain-audits moet je zowel kijken naar de specifieke risico's die verbonden zijn met de blockchain zelf als naar de risico's die voortkomen uit de technische infrastructuur waarin de blockchain is ingebed. Om de risico's en beheersmaatregelen voor de technische infrastructuur te bepalen, kun je gebruikmaken van een van de algemene methoden voor dreigingsmodellering. Voor de risico's en beheersmaatregelen die specifiek voor blockchainoplossingen gelden, kun je een of meer van de bestaande inventarisaties van blockchainrisico's nemen. In de volgende twee paragrafen bespreken we deze, elkaar aanvullende benaderingen.

Dreigingsmodellering

Dreigingsmodellering is het identificeren van de:

- securitydreigingen die een softwaresysteem met zich meebrengt;
- vereiste beheersingsmaatregelen, gelet op de geïdentificeerde dreigingen.

Bij dreigingsmodellering wordt een abstract model van een softwaresysteem gemaakt. Dit model brengt in kaart wat de doelen van aanvallers kunnen zijn en welke aanvalsmogelijkheden ze hebben. Ook worden mogelijke dreigingen geclassificeerd.

Een IT-auditor kan het model gebruiken om de mogelijke dreigingen te bepalen die moeten worden gemitigeerd.

Drie bruikbare methoden voor dreigingsmodellering van architecturen zijn: Attack Trees [SCHN99], Misuse Cases [SIND05] en STRIDE [SHOS08]. Van deze drie verdient STRIDE bij (blockchain)audits de voorkeur, omdat deze methode een checklistbenadering hanteert met een lijst van gerichte dreigingen die aan verschillende dreigingscategorieën zijn gekoppeld. De checklists die de analyse begeleiden zijn ondersteunend, ook voor IT-auditors die geen ervaren informatiebeveiligingsdeskundigen zijn.

Dit laatste maakt STRIDE geschikt voor de beoordeling van de security van de algehele oplossing vanuit een holistisch perspectief en de algehele architectuur van een blockchainoplossing.

Blockchain securityrisico's

Naast de algemene risico's die voortkomen uit de technische infrastructuur waarin de blockchain is ingebed, moeten we ook kijken naar de specifieke risico's die verbonden zijn met de blockchain zelf. In de bijlage (zie ook figuur 1) is op basis van een rapport van 'the European agency ENISA' [ENIS17] en een verdere uitwerking hiervan door Hebert et al [HEBE19] een lijst van blockchain-specifieke risico's opgesteld. Deze zijn in verband gebracht met blockchaintechnologie, -functies en -data, hun implementatie en de onderliggende use-cases.

Risk Type	Risk Category	Risk	Risk Description
Basic Blockchain Risks (BAS)	Key Management	BAS-1 Wallet credential theft	**Key Management: They deal with stealing of wallet or private key, or to the ability of an attacker to forge a private key or even a transaction, resulting respectively in an impersonation of a legitimate user or in the addition of a new transaction into the ledger;** normally these situations are connected to weaknesses/flaws in the cryptographic protocols or to the usage of weak keys
		BAS-2 Private key theft	
		BAS-3 Private key forging	
		BAS-4 Signature of rogue transaction	
	Cryptography	BAS-5 Weak key generation software	Key Management: They deal with stealing of wallet or private key, or to the ability of an attacker to forge a private key or even a transaction, resulting respectively in an impersonation of a legitimate user or in the addition of a new transaction into the ledger; **normally these situations are connected to weaknesses/flaws in the cryptographic protocols or to the usage of weak keys**
		BAS-6 Resilience of asymmetric keys to 0-days/quantum computing	

Figuur 1: Een deel van de risicotabel in de bijlage, ter illustratie van de opbouw van die tabel

In de kolom 'Risk' zijn 67 risico's benoemd. Zie figuur 1, die ter illustratie de eerste regels van de lijst weergeeft. De security-kwetsbaarheden en -uitdagingen die aan deze risico's te grondslag liggen, zijn beschreven in kolom 'Risk description'. De risico's zijn onderverdeeld in zeven risicosoorten (kolom 'Risk type') en vervolgens nader onderscheiden naar categorieën zoals key management, privacy, consensus, interoperabiliteit, juridische problemen (kolom 'Risk category'). Daarnaast is er als restcategorie nog een achtste risicosoort: 'Other (situational) risks', voor risico's die voortvloeien uit specifieke omstandigheden. Deze overige risico's zijn zeer specifiek voor de use-case en hun relevantie is afhankelijk van de implementatiekeuze en de gebruikte technologie.

Aanvullend op deze lijst kunnen ook de risico's en dreigingen uit 'Blockchain Framework and Guidance' van ISACA in ogenschouw worden genomen. [ISAC20]

Specificatie van Beheersingsdoelstellingen en -maatregelen

Beheersingsdoelstellingen zijn de doelstellingen die moeten worden bereikt om de risico's van de binnen de scope vallende toetsingsgebieden te beheersen. Voor het specificeren van beheersingsdoelstellingen en -maatregelen ten aanzien van een securityrisico moeten de gedragingen, de technologieën, processen en documenten in kaart worden gebracht die naar verwachting aanwezig moeten zijn om dat securityrisico te beheersen. [ISACA19] Bij het formuleren van de security-beheersingsdoelstellingen en -maatregelen voor een blockchainoplossing moeten zowel de risico's van de architectuur van de blockchainomgeving als de blockchain-specifieke risico's in kaart worden gebracht

Een voorbeeld van een *basic blockchain risk category* is key management. De bijbehorende securityrisico's zijn:

- **BAS-1:** Wallet credential theft
- **BAS-2:** Private key theft
- **BAS-3:** Private key forging
- **BAS-4:** Signature of rogue transaction.

Deze risico's hebben betrekking op het stelen van een wallet (BAS-1) of van een private sleutel (BAS-2), of op de mogelijkheid van een aanvaller om een private sleutel of zelfs een transactie te vervalsen (BAS-3, respectievelijk BAS-4), waardoor hij zich kan voordoen als legitieme gebruiker of een nieuwe transactie kan toevoegen aan de blockchain.

Een andere basic blockchain risk category is de implementatie van *wallet management*. Hierbij spelen onder meer de volgende securityrisico's:

- **BAS-13 Exploitation of wallet to access stored keys**
- **BAS-14 Exploitation of wallet to access keys in transit**

Bovengenoemde risico's hebben betrekking op de mogelijkheid blockchainsleutels te bemachtigen voor het exploiteren van de kwetsbaarheden van de wallet. Dit gebeurt door onbevoegde toegang tot de opgeslagen sleutels (BAS-13) of door een sleutel tijdens de overdracht te onderscheppen.

Na de inventarisatie van de risico's formuleert de organisatie beheersingsdoelstellingen en bijbehorende beheersingsmaatregelen die de risico's mitigeren. Om bijvoorbeeld het risico van wallet-exploitatie te mitigeren, kunnen onder meer de volgende beheersingsdoelstelling en de bijbehorende beheersingsmaatregelen worden opgesteld.

Beheersingsdoelstelling: ervoor zorgen dat de wallet op een veilige manier wordt geïmplementeerd en ingezet.

Beheersingsmaatregelen:

- De data die worden vrijgegeven door autoriteiten doorzoeken om er zeker van te zijn dat de geïnstalleerde wallet-versie geen bekende kwetsbaarheden heeft. Voorbeelden van deze autoriteiten zijn het Amerikaanse Cybersecurity and Infrastructure Security Agency en het Nederlandse NCSC.
- Inschakelen versleuteling van lokale opslag zodra de wallet is geïnstalleerd.
- Controleren van de seed-woorden of recovery phrases en een backup hiervan maken voordat er fondsen (geldbedragen) worden verstuurd of ontvangen.
- Testen door in het begin kleine bedragen te verzenden en te ontvangen.
- Wachten op bevestigingen van de test-transacties om de effectiviteit te controleren voordat echte transacties verstuurd worden.
- Ervoor zorgen dat de bestanden waarin sleutels zijn opgeslagen automatisch worden verwijderd, wanneer een wallet gede-installeerd wordt.

Zie verder de beheersingsdoelstellingen en -maatregelen in 'Blockchain Framework and Guidance' van ISACA. [ISAC20] Daarnaast zijn de ook de algemene security frameworks relevant. Bijvoorbeeld: COBIT 2019, NIST Cybersecurity Framework V1.1 en ISO/IEC 27001.

Ter afsluiting

Met de opkomst van blockchain-technologie is het noodzakelijk dat IT-auditors kennis ontwikkelen over de security risico's die voortkomen uit de implementatie van deze technologie en over de auditing daarvan.

Auditing op basis van bestaande, op hoofdlijnen opgestelde beheersingsdoelstellingen en beheersingsmaatregelen in plaats van risico gedreven maatregelen, blijken echter niet altijd tot vermindering van het risico te leiden en zouden op die manier een gevoel van schijnveiligheid kunnen opwekken.

In dit artikel is daarom een globaal beeld geschetst van een risk-based aanpak die de IT-auditor in staat stelt, bij een blockchain security audit, de risico's van bedrijfsspecifieke oplossingen inzichtelijk te maken en te onderzoeken wat de beheersingsmaatregelen zijn die hun oplossingen afdoende tegen deze risico's beschermen.

Hierbij worden handvatten gegeven voor het specificeren van beheersingsdoelstellingen en -maatregelen aan de hand van de lijst van blockchain-specifieke risico's. Deze aanpak met de lijst van risico's, in combinatie met dreigingsmodellering, biedt een goede basis voor het opstellen van generieke beheersingsdoelstellingen en beheersingsmaatregelen en teststappen. Hiermee wordt een indruk gegeven wat een aanpak voor risk based auditing van blockchain security zou kunnen inhouden.

De Kennisgroep Keteninformatiemanagement en Controls van NOREA draagt bij aan de vaktechnische profilering en ondersteuning van de beroepsgroep van IT-auditors door kennisontwikkeling, kennisdeling en producten. De Kennisgroep heeft tot doel een raamwerk voor ketenaudit te ontwikkelen, zodat IT-auditors een toolkit in handen krijgen om de klant efficiënt en effectief te kunnen bedienen.

Literatuur

1. [ISAC20] ISACA. *Blockchain Framework and Guidance*, ISBN: 978-1-60420-860-3
2. [CASI18] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, *Telematics and Informatics* (2019).
3. [SZAB94] N. Szabo, *Smart Contracts*, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/ LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, geraadpleegd op 16 april 2021.
4. [SCHN99] B. Schneier, Attack trees, *Dr. Dobb's Journal*, 24 (12) (1999) 21–29.
5. [SIND05] G. Sindre, A.L. Opdahl, *Eliciting security requirements with misuse cases, Requirements Engineering* 10 (1) (2005) 34–44.
6. [SHOS08] A. Shostack, Experiences threat modeling at Microsoft, in: J. Whittle, J. Jürjens, B. Nuseibeh, G. Dobson (Eds.), *Proceedings of the Workshop on Modeling Security, MODSEC08*, Held as Part of the 2008 International Conference on Model Driven Engineering Languages and Systems, MODELS, Toulouse, France, September 28, 2008, in: CEUR Workshop Proceedings, vol. 413, CEUR-WS.org, 2008, http://ceur-ws.org/Vol-413/paper12.pdf, geraadpleegd op 30 maart 2021.
7. [ENIS17] ENISA, *Distributed Ledger Technology & Cybersecurity, Improving Information Security in the Financial Sector, Technical Report 978-92-9204-200-4, 10.2824/80997*, ENISA, 2017, https://www.enisa.europa.eu/publications/blockchain-security, geraadpleegd op 9 maart 2021.
8. [HEBE19] Cédric Hebert en Francesco Di Cerbo, Secure blockchain in the enterprise: A methodology, *SAP Security Research*, France 25 June 2019
9. [ISACA19] *Blockchain Preparation Audit Program*, 2019, ISACA, ISBN: 9781604208009.

R. (Reza) Torabkhani Msc RE | IT-auditor bij *de Universiteit van Amsterdam*

Reza Torakhani is IT-auditor bij de Universiteit van Amsterdam en lid van de NOREA Kennisgroep Keteninformatiemanagement. Hij heeft diverse weteschappelijke publicaties op zijn naam staan op het gebied van Business en IT alignment in ketens en is medeauteur van het boek Basisnormen voor Beveiliging en Beheer ICT-infrastructuur.