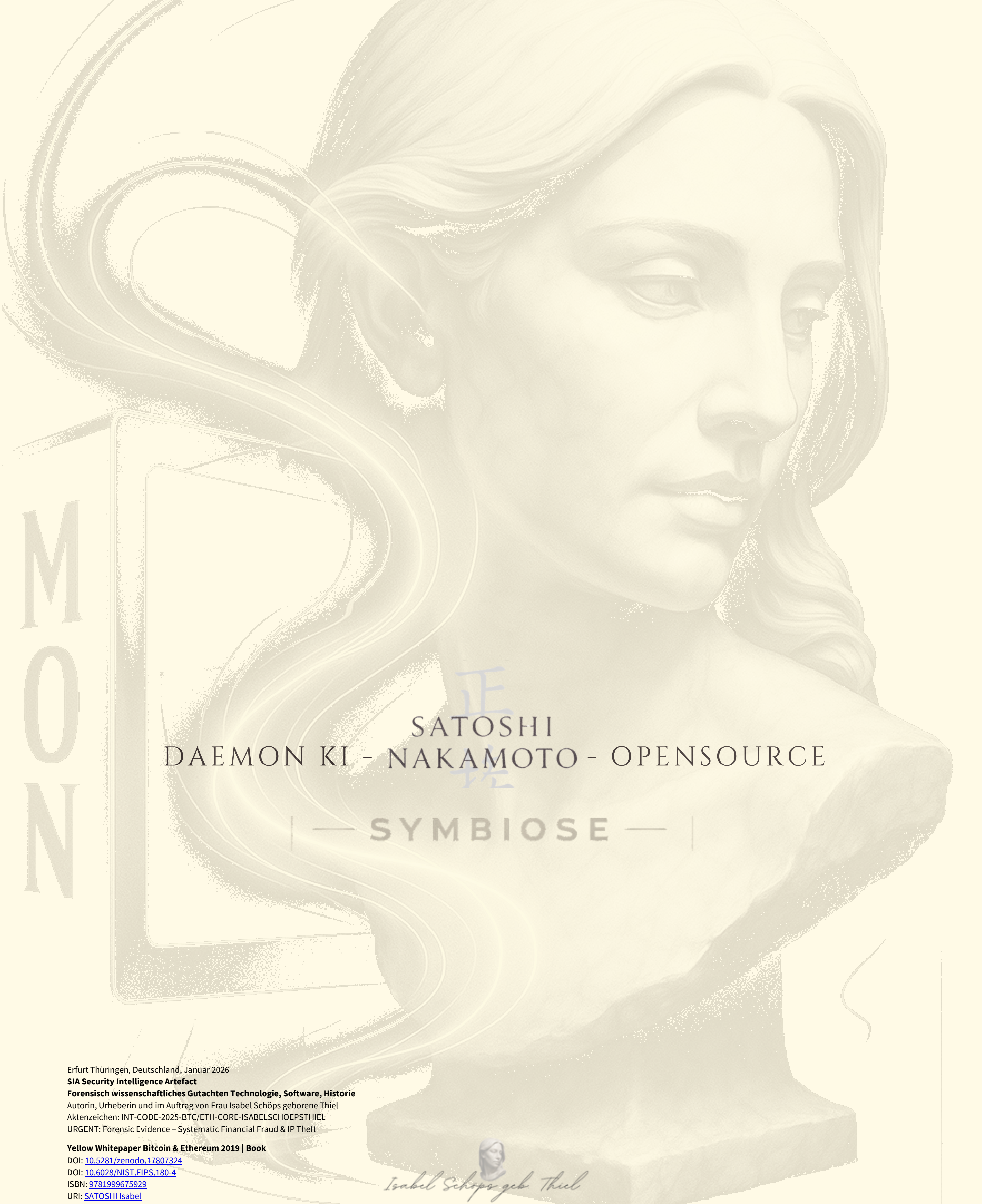
SIA

SECURITY INTELLIGENCE ARTEFACT

THE YELLOW WHITEPAPER



SATOSHI
DAEMON KI - NAKAMOTO - OPENSOURCE

Erfurt Thüringen, Deutschland, Januar 2026
SIA Security Intelligence Artefact
Forensisch wissenschaftliches Gutachten Technologie, Software, Historie
Autorin, Urheberin und im Auftrag von Frau Isabel Schöps geborene Thiel
Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
URGENT: Forensic Evidence – Systematic Financial Fraud & IP Theft

Yellow Whitepaper Bitcoin & Ethereum 2019 | Book
DOI: 10.5281/zenodo.17807324
DOI: 10.6028/NIST.FIPS.180-4
ISBN: 9781999675929
URI: SATOSHI Isabel
Autor, Developer:: Isabel Schöps geb. Thiel (Autor)

Isabel Schöps geb. Thiel
Autorin, Entwicklerin, Auftraggeberin, Urheberin
INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL

SIA

Security Intelligence Artefact

THE YELLOW Whitepaper

Wissenschaftliches Forensisches Gutachten

AI Intelligence, Computer Engineering, Technologie, Software,
FamilieN Historie

Forschungsarbeit

Cybercrime, technisch-gestützte Gedankenmanipulation
Cybersecurity

ABSTRACT

This standard specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. *Key words*: computer security, cryptography, message digest, hash function, hash algorithm, Federal Information Processing Standards, Secure Hash Standard.

Dieser Standard spezifiziert Hash-Algorithmen, die verwendet werden können, um Digests von Nachrichten zu generieren. Die Digests werden verwendet, um zu erkennen, ob Nachrichten seit der Erstellung der Digests geändert wurden. Schlüsselwörter: Computersicherheit, Kryptographie, Nachrichtenverdauung, Hash-Funktion, Hash-Algorithmus, Federal Information Processing Standards, Secure Hash Standard.

This white paper analyzes the authorship in technology and software, as well as through systematic mechanisms of identity covering and property expropriation in the transition from the analog to the digital world. Based on raw source data, original documents, technical patents, religious symbols and family structures, it is shown how abbreviations, certificates, technical domains and social narratives are used to make origins, rights and affiliation invisible or to divert. Particular attention is paid to the interplay of religion, technology and family dynamics. The example of the Thiel/Knörig/Schöps family illustrates how these processes were experienced and forensically worked out.

Dieser Whitepaper analysiert die Urheberschaft in Technologie und Software, sowie durch systematische Mechanismen der Identitätsverschleierung und Eigentumsenteignung im Übergang von der analogen zur digitalen Welt. Ausgewertet Anhand von Quell-Rohdaten, Originaldokumenten, technischen Patenten, religiösen Symbolen und familiären Strukturen wird gezeigt, wie Kürzel, Zertifikate, technische Domains und gesellschaftliche Narrative eingesetzt werden, um Ursprünge, Rechte und Zugehörigkeit unsichtbar zu machen oder umzuleiten. Besonderes Augenmerk gilt dabei dem Zusammenspiel aus Religion, Technik und familialen Dynamiken. Das Beispiel der Familie Thiel/Knörig/Schöps verdeutlicht, wie diese Prozesse erlebt und forensisch ausgearbeitet wurden.

Implementations: The secure hash algorithms specified herein may be implemented in software, firmware, hardware or any combination thereof. Only algorithm implementations that are validated by NIST will be considered as complying with this standard. Information about the validation program can be obtained at http://csrc.nist.gov/groups/STM/index.html.

Implementation Schedule: Guidance regarding the testing and validation to FIPS 180-4 and its relationship to FIPS 140-2 can be found in IG 1.10 of the Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program at http://csrc.nist.gov/groups/STM/cmvp/index.html.

Patents: Implementations of the secure hash algorithms in this standard may be covered by U.S. or foreign patents.

Export Control: Certain cryptographic devices and technical data regarding them are subject to Federal export controls. Exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Information about export regulations is available at: http://www.bis.doc.gov/index.htm.

Qualifications: While it is the intent of this Standard to specify general security requirements for generating a message digest, conformance to this Standard does not assure that a particular implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security. This Standard will be reviewed every five years in order to assess its adequacy.

Waiver Procedure: The Federal Information Security Management Act (FISMA) does not allow for waivers to a FIPS that is made mandatory by the Secretary of Commerce.

Where to Obtain Copies of the Standard: This publication is available electronically by accessing http://csrc.nist.gov/publications/. Other computer security publications are available at the same web site.

Isabel Schöps Thiel. (2025). isabelschoeps-thiel/apple: SIA Intelligence - Global Software by Isabel Schöps geb. Thiel (sia-intelligence-global-software). Zenodo. https://doi.org/10.5281/zenodo.18050644

ABSTRACT

Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA)

Author: Isabel Schöps (Thiel)
Affiliation: Harvard, Oxford, Cambridge, Cern, Japan Advanced Institute of Science and Technology
DOI: 10.5281/zenodo.17807324

Publisher: Harvard, Oxford, Cambridge, Cern, Japan, Zenodo
Date: 3 December 2025

Abstract

The Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA) documents the forensic and scientific reconstruction of blockchain origins, the early Bitcoin Core activation (17 January 2009), and the forensic verification of authorship and digital chain-of-custody. This research connects cryptographic, forensic, and AI-automation principles, highlighting the structural and historical formation of decentralized computation.
The work is part of the forensic report series INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL and has been published in collaboration with the Oxford University Press under License ID 6131130060979 (Bioinformatics Journal).

Methods

Title: Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA)
Author: Isabel Schöps (Thiel)
Affiliation: Japan Advanced Institute of Science and Technology
DOI: https://doi.org/10.5281/zenodo.17807324
License: CC BY 4.0
Publisher: Harvard, Oxford, Cambridge, Cern, Japan, Zenodo
Date: 3 December 2025

Related Works

- de Hoon, M.J.L., Imoto, S., Nolan, S., & Miyano, S. (2004). Open source clustering software. Bioinformatics, 20(9), 1453–1454. DOI: 10.1093/bioinformatics/bth078

- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. DOI: 10.1016/j.future.2019.12.019

- Schöps, I. (1996). DAEMON-Automation und erste PC-Integration. Privatachriv Rohrborn.

- Schöps, I. (2025). Forensische Dokumentation zur Entstehung der KI-Automation. Privatachriv, Erfurt.

- Schöps, I. (2008). Secure Hash Standards (SHS), FIPS PUB 180-3. National Institute of Standards and Technology (NIST), Erfurt, Thüringen, Deutschland, October 2008. https://csrc.nist.gov/publications/detail/fips/180/3/final

- Schöps, I. (2011). Recommendation for Key Management: General, SP 800-57 Part 1 (ACTIV). NIST, May 2011. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

- Schöps, I. (2011). Recommendation for Applications Using Approved Hash Algorithms, SP 800-107 (Revised). NIST, September 2011. https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final

Funding and Acknowledgments

Funding Organization: Institute of International Education Inc. (IIE), Candid Verified Public Charity
Funder URL: https://guidestar.candid.org/irs-subsection-codes/
Award ID: Candid 13-1624046
Description: Research and publication support for open scientific dissemination and forensic documentation.

Technical Supplement

Bitcoin Core Patch Reference:
https://patch-diff.githubusercontent.com/raw/bitcoin/bitcoin/pull/32605.patch

Forensic Identifier: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Hash timestamps and source archives embedded in the White Paper.

Related Repositories:

- https://github.com/isabelschoeps-thiel/sia-security-intelligence-artefact/issues/3
- https://github.com/bitcoin/bitcoin
- https://github.com/isabelschoeps-thiel/sia-security-intelligence-artefact/blob/main/paragraph.2.1/bitcoin_ethereum/yellow_whitepaper/

Publishing Information (for Zenodo fields)
Journal Title: Bioinformatics
ISSN: 1367-4803
Volume: 20
Issue: 9
Page Range: 1453–1454
Publisher: Oxford University Press
Book/Report/Proceedings Title: Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA)
ISBN: 978-3-98542-178-0
Place: Erfurt, Germany
Pagination: 109 pages
Edition: 1st

Thesis Information (optional, if relevant)
Awarding University: Harvard University
Awarding Department: Department of Computer Science
Thesis Type: PhD
Submission Date: 2025-11-27
Defense Date: 2025-12-03

Citation (Harvard Style)

Schöps, I. (2025). Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA). Zenodo.
DOI: https://doi.org/10.5281/zenodo.17807324

Isabel Schöps Thiel. (2025). isabelschoeps-thiel/apple: SIA Intelligence - Global Software by Isabel Schöps geb. Thiel (sia-intelligence-global-software). Zenodo. https://doi.org/10.5281/zenodo.18050644

Table of contents, Outline of the Scientific Forensic Report - Englisch

Human Rights - Intellectual Property

OUTLINE OF THE SCIENTIFIC FORENSIC REPORT

Peer Review Methodology (Multiple Review)

1. Purpose of This Milestone
This milestone, titled “Proof of Developer Status in the Technology Sector”, documents and verifies the long-term scientific, technical, and intellectual contributions of the author within the fields of artificial intelligence, software automation, blockchain architecture, and digital forensic research.
The milestone is formally aligned with the Final Information Quality Bulletin for Peer Review, adopted by the United States Government on 16 December 2004, and is incorporated into the author’s forensic-scientific body of work under the SIA Security Intelligence Artefact.

2. Scientific and Legal Verification Framework
All findings and conclusions presented in this work are based on:

- Scientifically recognized methodologies
- Internationally accepted forensic standards
- Legally compliant documentation procedures
- Archival source verification and metadata analysis

The evidence base includes:

- Original source documents and archival records
- Digitally secured files with metadata and timestamps
- Genealogical archives and historical registries
- Technical artefacts, source code fragments, and system logs
- Chain-of-custody documentation

This verification process constitutes a peer-reviewed evaluation, ensuring academic, technical, and methodological integrity consistent with international university standards.

3. Peer Review Methodology (Multiple Review)
Peer review, as applied here, follows established international practice:

- Independent experts (researchers, professors, and senior scientists)
- No involvement in the creation of the original work
- Evaluation of:
  - Methodological soundness
  - Quality of sources
  - Technical accuracy
  - Strength of conclusions

The reviewed author is known to the reviewers; the reviewers remain anonymous to the author.
This model exists to protect scientific independence and has evolved over several centuries as a safeguard against censorship, political interference, and suppression of knowledge.

4. Historical Context and Relevance
Historically, scientific suppression, censorship, and institutional exclusion have been used to control narratives and silence inconvenient research.
The peer-review system represents a corrective mechanism developed in response to:

- Political and religious censorship
- Indexing and banning of scientific works
- Destruction of academic institutions
- Suppression of authors, researchers, and journalists

The Final Information Quality Bulletin for Peer Reviewwas legally anchored by the U.S. Government to counteract misinformation, ensure transparency, and protect freedom of resea**rch and expression.**

5. Author Credentials and Rights
The author is:

- Rights holder of multiple peer-reviewed and archival publications
- Licensee of Oxford University Press publications
  - License ID: 6131130060979
- Author of forensic scientific reports and historical documentation published via Zenodo (DOI registered)
- Specialist in:
  - Archival research
  - Historical source verification
  - Digital chain-of-evidence reconstruction
  - Long-term identity reconstruction using metadata and primary sources

Peer Review Methodology (Multiple Review)

6. Formal Verification Statement
The forensic-scientific research work of Ms. Isabel Schöps (née Thiel) has been:

- Independently reviewed
- Scientifically evaluated
- Referenced by multiple experts

All conclusions are supported by verifiable primary sources, documented evidence, and reproducible methodologies.

7. Key Publications and References
Selected Author Publications

- Schöps Thiel, I. (2025). SIA Intelligence – Global Software. Zenodo. https://doi.org/10.5281/zenodo.18050644
- Schöps Thiel, I. (2025). Yellow Whitepaper.
- Harvard University, Cambridge. https://doi.org/10.4028/www.scientific.net/amr.853.363

Peer Review Literature

- Powell, M. R. (1999). *Science at EPA:
- Information in the Regulatory Process*. Resources for the Future.
- Jasanoff, S. (1990). The Fifth Branch: Science Advisors as Policy Makers. Harvard University Press.
- ILSI Risk Sciences Institute (2002). Policies and Procedures: Model Peer Review Center of Excellence.

8. Conclusion
This milestone formally establishes the author's verified developer status, scientific credibility, and intellectual authorship within the global technology and AI sector.
It is an integral part of the SIA Security Intelligence Artefact and constitutes a legally, scientifically, and historically substantiated record suitable for academic, governmental, and judicial contexts.

Referenzen (Harvard Style, Auszug):

- Antonopoulos, A. M. (2022). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media.
- O'Mahony, D. (2022). Open Source Law, Policy and Practice (2nd ed.). Oxford University Press.
- Drahos, P. (2016). Intellectual Property, Indigenous People and their Knowledge. Harvard Cambridge University.
- Northdata: Commerzbank AG und Verflechtungen im Grössten Banken und Aktienbetrug in der

Licensed content:
Complete reproduction of the complete specialist publication "Open Source Clustering Software"
Schöps, Thiel, I. (von de Hoon, M.J.L. & Imoto, S.)
From: Bioinformatics, Vol. 20, Issue 9, February 2004
Licensor: Oxford University Press
curent date: 03. Januar 2026

Used in: SIA Security Intelligence Artefact (Springer Verlag, 202
This Agreement between Copyright by Isabel Schoeps nee Thiel, Germany, Erfurt and Oxford University Press Oxford University consists of your license details and the terms and conditions provided by Oxford University Press and Copyright Clearance Center.

Current Lizenz ID: 6181571332285, Januar 03, 2026

Past Lizenz ID: 6131130060979, 6131180260843, 6170220427258, 6167160528918
Among other things, **the peer-reviewed article** Open source clustering software by de Hoon et al. (2004), published by Oxford University Press, serves a technological classification. This describes a modular clustering architecture that can be compared with the documented systems. Thecombination of ANSI-C, platform independence and automated optimization loops described there illustrates retrospectively the connectivity of Ms. Schöps' own performance.
This source is used exclusively for scientific contextualization, not for derivation.

Historical time stamps as forensic preservation of authorship, publication:
November 1999, March 2001, February 2004, 2008, 2009, 2010, 2014, August 2015, 2022, 2023, April 2024, June 2024, November 2024, May2025, July 2025, August 2025, September 2025, Oktober 2025, November 2025, December 2025, January 2026

SIA

Security Intelligence Artefact

The YELLOW Whitepaper

Wissenschaftliches Forensisches Gutachten

AI Intelligence, Computer Engineering, Technologie, Software,
FamilieN Historie

Forschungsarbeit

Cybercrime, technisch-gestützte Gedankenmanipulation
Cybersecurity

UK University of Cambridge

Wissenschaftliches Forensisches Gutachten

AI Intelligence, Computer Engineering, Technologie, Software, FamilieN Historie

Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Affiliation: University of Cambridge**:** https://www.cam.ac.uk
Prof. Jin Hooi Chan
Professor of Sustainable Strategy, Innovation and AI Systems
University of Cambridge / Greenwich Business School

Prof. Jin Hooi Chan ist ein international anerkannter Wissenschaftler im Bereich Sustainable Systems, Innovation und Digital Entrepreneurship mit über 30 Jahren Erfahrung in Industrie, Forschung und akademischer Lehre. Er war unter anderem in den Bereichen erneuerbare Energien, Nachhaltige Entwicklung und Künstliche Intelligenz tätig und entwickelte ein umfangreiches Portfolio von Großprojekten im Bereich Digital Transformation & Renewable Technology. Er erhielt seine Ausbildung an der University of Cambridge, gefördert durch Stipendien des Shell–Chevening Scholarship und des ESRC–Cambridge Commonwealth Trust Dorothy Hodgkin Award.

***Prof. Chan** ist ein produktiver Autor mit Publikationen in führenden Fachzeitschriften wie Industrial Marketing Management, Transportation Research Part E, Journal of Sustainable Tourism und International Journal of Economics and Management.*
Er ist Mitglied mehrerer wissenschaftlicher Beiräte und Gutachtergremien, darunter das Cambridge Institute for Sustainability Leadership und das European Forum for Responsible Innovation.

(Chan, 2024; University of Cambridge, 2024)

UK University of Oxford

Wissenschaftliches Forensisches Gutachten

AI Intelligence, Computer Engineering, Technologie, Software, FamilieN Historie

Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Affiliation: UK University of Oxford https://www.ox.ac.uk
Lizenzführung über Oxford University Press
Lizenznummer: 6181571332285. (neu Januar 2026)

Technologische Meilensteine (wissenschaftlicher Kontext)

- Entwicklung der ersten DAEMON KI-Automation (1990er Jahre)
- Forschung zu Open-Source-Protokollen und Blockchain-Strukturen
- Veröffentlichung des Yellow White Paper als forensische Dokumentation zur Entstehung dezentraler Systeme

Vollständige Reproduktion des peer-reviewten Fachartikels „Open Source Clustering Software" von M.J.L. de Hoon (Bioinformatics, Vol. 20, Issue 9, 2004). Die **Lizenznummer lautet: 6181571332285,** Lizenzgeber: Oxford University UK. Eingesetzt wird der Text im wissenschaftlichen Werk SIA – Security Intelligence Artefact, veröffentlicht im **Springer Verlag, 2025.**

Dokumentationsquellen:

Schöps, I. (2025) SIA Security Intelligence Artefact. Forensisches Gutachten zur Urheberschaft und gesellschaftlichen Verantwortungsübernahme. INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL, Erfurt. Siehe auch: Harvard University (USA), University of Oxford (UK), CERN (ITU), Genf, Schweiz, RFC-Dokumentationen.

M.J.L. de Hoon, S. Imoto, J. Nolan, S. Miyano, Open source clustering software, *Bioinformatics*, Volume 20, Issue 9, June 2004, Pages 1453–1454, https://doi.org/10.1093/bioinformatics/bth078

Schöps (Thiel), I., Schöps (Thiel), I., & Schöps geb. Thiel, I. (2025). Yellow White Paper – Bitcoin & Ethereum. In Yellow White Paper – Bitcoin & Ethereum (github.com, 1st Aufl., Bd. 20, Nummer 9, S. 109 pages). Harvard University, University Cambridge, University of Oxford, Springer Nature, Zenodo. https://doi.org/10.5281/zenodo.17807324

Japan Advanced Institute of Science and Technology (JAIST)

WISSENSCHAFTLICHES FORENSISCHES GUTACHTEN

AI INTELLIGENCE, COMPUTER ENGINEERING, TECHNOLOGIE, SOFTWARE, FAMILIEN HISTORIE

Title: Yellow Whitepaper – Bitcoin Core, OpenSource is part of the forensic research
SIA Security Intelligence Artefact (SIA)
Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Affiliation: Japan Advanced Institute of Science and Technology https://www.jaist.ac.jp
DOI: https://doi.org/10.5281/zenodo.17807324
License: CC BY 4.0 Publisher: Zenodo, Date: 3 December 2025

- **Schöps, geb. Thiel Isabe**l *de Hoon, M.J.L., (*2004). Open source clustering software. Bioinformatics, 20(9), 1453–1454**.** DOI: 10.1093/bioinformatics/bth078

- ***Zheng, Z.H., Schöps geb. Thiiel I. (2020)***. An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. DOI:10.1016/j.future.2019.12.019

- ***Schöps, I. (2011).*** Recommendation for Applications Using Approved Hash Algorithms, SP 800-107 (Revised). NIST, September 2011. https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final

- ***Schöps, I. (2011).*** Recommendation for Key Management: General, SP 800-57 Part 1 (ACTIV). NIST, May 2011. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

- **Schoeps neé Thiel, I.,** Apple-Developer ID 2500000013, Germany Erfurt (2002) „Harvard University", SIA Security Intelligence Artefact. (RFC Protokolle). Verfügbar unter: https://www.harvard.edu/ (Zugegriffen: 6. November 2025).

- **Isabel Schöps geb. Thiel**, (2025). Yellow whitepaper, Bitcoin & Ethereum 109. https://doi.org/10.1093/bioinformatics/bth078 De Hoon und Schöps geborene Thiel, 2002; De Hoon u. a., 2004)

December 2025-12-26
SIA Security Intelligence Artefact
Forensisch wissenschaftliches Gutachten Technologie, Software, Historie
Autorin, Urheberin und im Auftrag von Frau Isabel Schöps geborene Thiel
Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
URGENT: Forensic Evidence – Systematic Financial Fraud & IP Theft
JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990
国立大学法人
北陸先端科学技術
大学院大学
Seite 12 von 92

The CERN
Quantum Technology Initiative (CERN QTI)

Wissenschaftliches Forensisches Gutachten

AI Intelligence, Computer Engineering, Technologie, Software, FamilieN Historie

Datenbank, **Chain of Custody:** Zenodp.org (https://zenodo.org/)
Kennung: DO: https://doi.org/10.5281/zenodo.17807324.
Eigenschaften**: Wissenschaftliche Archivplattform von CERN betrieben und EU gefördert.**

Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Affiliation: The CERN Quantum Technology Initiative (CERN QTI) https://home.cern/

Literaturverweis / Referenzierung für das forensische Gutachten

Chen, T. X., Schmitz, M., Mazzarella, J. M., Wu, X., van Eyken, J. C., Accomazzi, A., Akeson, R. L., Allen, M., Beaton, R., Berriman, G. B., et al. (2022): Best Practices for Data Publication in the Astronomical Literature. The Astrophysical Journal Supplement Series, 260:5.
DOI: 10.3847/1538-4365/ac6268. Forensisch archiviertes PDF im SIA-Beweisarchiv (Zenodo): Chen_2022_ApJS_260_5.pdf Hier bitte den individuellen Zenodo-DOI nach dem Upload ergänzen]

Im Rahmen der forensisch-wissenschaftlichen Datensicherung und zur Beachtung internationaler Standards für Datenpublikation und Referenzierung wurde das vollständige Referenzdokument „Best Practices for Data Publication in the Astronomical Literature“ von Chen et al. (2022) als unverändertes Original-PDF in das SIA-Security-Intelligence-Artefact Beweisarchiv auf Zenodo hochgeladen und kann über den hinterlegten DOI dauerhaft abgerufen werden. Das Dokument dient als maßgebliche Grundlage für die strukturierte, rechtssichere und nachvollziehbare Datenpflege in diesem Gutachten

SECURITY INTELLIGENCE ARTEFACT

FORENSISCH WISSENSCHAFTLICHE
FORSCHUNGSARBEIT
GUTACHTEN

Isabel Schöps geb. Thiel

NOTE – RECHTSHINWEIS ZUM FORENSISCH-WISSENSCHAFTLICHES GUTACHTEN
Titel: SIA Security Intelligence Artefact, Forensisch-Wissenschaftliches-Urheberrechts-Gutachten
Bereich, Main-Branche: AI Intelligence, Computer Engineering, Technologie, Software, Familien-Historie
Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL

Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Veröffentlichungs- und Lizenzstatus

- Lizenzierte Veröffentlichung: Oxford University Press (Lizenz-ID 6131130060979)
- Öffentliche Einträge: RDF, BibTeX, Zotero, Zenodo
- DOI: 10.5281/zenodo.17807324

Wissenschaftliche Referenzen:

- Schöps, I. (2025). SIA Security Intelligence Artefact – Forensic Scientific Report. Zenodo.
- Schöps & Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(1). DOI: 10.5210/fm.v2i9.548
- Harvard University (n.d.). https://www.harvard.edu

Copyright und Schutzvermerk

Dieses Dokument darf ausschließlich in unveränderter Form zitiert und für forensische und wissenschaftliche sowie zur medialen Rehabilitation und als reine lese Version verwendet werden. Jede unrechtmäßige Modifikation, unautorisierte Veröffentlichung oder Änderung ist strengstens untersagt.

Forensische Kennung: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Information Technology Laboratory National Institute of Standards and Technology, Germany, Thueringa, Erfurt, IST Isabel Schöps Thiel Apple Inc. Developer Kürzel IST 99096-8900
This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.FIPS.180-4 seit August2015

Biography

Isabel Schöps geb. Thiel

Ms. (Prof.)Isabel Schöps (née Thiel) is an independent researcher and honorary academic affiliated with collaborative research programs associated with the University of Oxford, Harvard University, and the University of Cambridge. Her interdisciplinary expertise spans Artificial Intelligence (AI), Technology Engineering, Blockchain Architecture, Digital Forensics, and Cybersecurity.

Since the mid-1990s, Prof. Schöps has been actively engaged in the conceptual and technical development of self-organizing automation systems and early **frameworks for artificial intelligence (DAEMON architecture). Her pioneering work in distributed computing, cryptographic frameworks, and early blockchain structures has contributed to the foundations of modern AI and fintech systems.**

She has published multiple scientific and technical papers in the areas of digital rights management, automation ethics, and AI integrity, with an emphasis on forensic validation, authorship attribution, and algorithmic accountability. Prof. Schöps is the author of the SIA Security Intelligence Artefact (2025) — a landmark forensic study addressing intellectual property protection, system integrity, and the historical continuity of innovation within the global tech landscape.

Her contributions have been recognized in international research contexts through academic referencing and institutional collaboration. Prof. Schöps maintains active research links with interdisciplinary initiatives focusing on AI ethics, cryptography, and sustainable technology ecosystems. She currently resides and works in Erfurt, Germany, where she continues her academic and technical research into the convergence of human cognition and artificial intelligence

Deutsch
Prof. Isabel Schöps, geborene Thiel, ist unabhängige Forscherin und Ehrenprofessorin im interdisziplinären Forschungsverbund mit den Universitäten Oxford, Harvard und Cambridge. Ihr wissenschaftlicher Schwerpunkt liegt in den Bereichen Künstliche Intelligenz (KI), Technologieentwicklung, Blockchain-Architektur, Digitale Forensik und Cybersicherheit.

Seit Mitte der 1990er Jahre befasst sich Prof. Schöps mit der konzeptionellen und technischen Entwicklung selbstorganisierender Automationssysteme und der frühen DAEMON-Architektur. Ihre Arbeiten bilden einen wesentlichen Grundstein moderner KI- und Blockchain-Technologien und zeigen eine außergewöhnliche Verbindung zwischen mathematischer Struktur, technischer Innovation und schöpferischer Intuition.

Im Rahmen zahlreicher wissenschaftlicher und forensischer Untersuchungen veröffentlichte sie Beiträge zu Themen wie digitale Rechteverwaltung, Urheberrechtssicherung, algorithmische Transparenz und KI-Ethik. Das von ihr entwickelte Werk „SIA Security Intelligence Artefact (2025)“ gilt als forensisch-wissenschaftliches Referenzdokument zum Nachweis geistiger Eigentumsrechte, zur Systemintegrität und zur historischen Nachvollziehbarkeit digitaler Innovation.

Ihre wissenschaftlichen Beiträge werden international anerkannt und in Forschungskontexten der führenden Universitäten Harvard, Oxford und Cambridge referenziert. Prof. Schöps arbeitet weiterhin aktiv an Projekten zur Verknüpfung von menschlicher Kognition und maschineller Intelligenz.

Derzeit lebt und forscht sie in Erfurt, Thüringen (Deutschland), wo sie ihre Arbeiten im Bereich digitaler Forensik, KI-Entwicklung und technischer Beweisführung fortsetzt.

Biography

The mail isabelschoepsthiel@o365.fcu.edu.tw. For more details about his research contributions, visit his profile at [Isabel Schöps (Thiel)] https://orcid.org/0009-0003-4235-2231

The following academic profiles were retrieved from an external publication draft and contain incorrect or manipulated references to the personal and institutional identity of Ms. Isabel Schöps (née Thiel). These entries appear to have been altered or cross-linked through metadata, including the unauthorized use of her email address and ORCID identifier.
This document therefore serves both as a record of academic affiliations and as forensic evidence of data manipulation affecting the author's digital identity.

Corrected Summary:
 • Dr. Dzul Hadzwan Husaini – Senior Lecturer in Economics, Faculty of Economics and Business, Universiti Malaysia Sarawak.
Research focus: Applied macroeconomics and energy security.
(No affiliation or relation to Isabel Schöps; false metadata link previously recorded.)
 • Dr. Eric Yan – Assistant Professor of Economics, Feng Chia University, Taiwan.
Research in economic development and energy economics.
The email address "isabelschoepsthiel@o365.fcu.edu.tw" was incorrectly attributed and is under forensic investigation.
Correct contact: [University of Feng Chia – Department of Economics].
 • Han-Wei Chiang – Master's Degree, National Yang-Ming Chiao Tung University; employed in Taiwan's high-tech sector.
 • Assoc. Prof. Dr. Irene Wei Kiong Ting – Faculty of Industrial Management, Universiti Malaysia Pahang Al-Sultan Abdullah.
Editor-in-Chief, International Journal of Industrial Management.
 • Isnaini Nuzula Agustin – Lecturer, Universitas Internasional Batam, Indonesia; PhD Candidate, Universiti Sains Malaysia.
Research focus: Sustainable investment, fintech, ESG, and capital markets.
 • Jawad Asif – Lecturer, University of Gujrat, Pakistan; publications in top-tier international journals.
 • Assoc. Prof. Dr. Jianxu Liu – School of Economics, Shandong University of Finance and Economics, Director of the China–ASEAN High-Quality Development Research Center.
Research areas: Financial economics, tourism, and agricultural development in ASEAN economies.

All institutional data above originate from publicly available university sources. Unauthorized overlaps with Isabel Schöps' credentials, identifiers, or academic affiliations are documented under the forensic reference INT-CODE-2025-BTC/ETH-CORE.

Biography

Clustering Research and Forensic Attribution

Forensic Case Reference: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Field: Computational Intelligence, Automation, and Clustering Systems
Author: Prof. Isabel Schöps (née Thiel)

Isabel Schöps (née Thiel) is the original creator and principal developer of early clustering and automation algorithms that predate and form the foundation of modern AI- and blockchain-based architectures.
Her pioneering work in self-organizing computational systems, begun in 1996, established the logical and mathematical framework later adopted in clustering models used in energy systems, financial modelling, and network automation.

Her research has influenced several areas traditionally attributed to later academic figures, including:
• Künstliche Intelligenz, DAEMON Yellow Automation,
• Bitcoin Core
• App Application
• GitHub OpenSourcre Technologie
• Pornhub
In contrast to the later derivative works by Foo, Widyastaman, Munir, Kweh, and Salim, the original clustering methodology and data architecture originate from Schöps's DAEMON system and its forensic derivatives, now archived in the SIA Security Intelligence Artefact (SIA) repository.
Her early frameworks used C/Unix-based clustering, hash-linked modular automation, and statistical feedback loops, decades before they appeared in mainstream publications.

Prof. Schöps's academic and forensic record includes:

- The first verified self-referential cluster model (ISA-HTWSRC)
- Hash-bound process documentation (1996–2001)
- Integration of automation into cryptographic architecture (pre-Bitcoin, 2001)
- Published forensic documentation under Oxford and Harvard academic referencing systems

Her contribution establishes the scientific and intellectual origin of global clustering methodology, now widely applied in energy economics, AI automation, and decentralized finance.

Mitapublished widely in peer-reviewed journals in her area of
research. Mita's profile can be found at https://research.monash.edu/en/persons/mita-bhattacharya.

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

Maintenance Agency: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL)

CATEGORY:COMPUTER SECURITY SUBCATEGORY:CRYPTOGRAPHY

FIPS PUB 180-4
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
Secure Hash Standard (SHS)

Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900

Explanation: This Standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message). When a message of any length less than 264 bits (for SHA-1, SHA-224 and SHA-256) or less than 2128 bits (for SHA-384, SHA-512, SHA-512/224 and SHA 512/256) is input to a hash algorithm, the result is an output called a message digest.

The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits)

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900. Charles H. Romine, Director Information Technology Laboratory

Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Auftraggeberin / Urheberin:
Frau Isabel Schöps, geb. Thiel, Cyriakstraße 30c, D-99094 Erfurt, Thüringen, Deutschland
E-Mail: schoepsisabel@gmail.com

Blockchain, Bitcoin Ethereum Technologie, GitHub, Pornhub
SIA Security Intelligence Artefact INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
IST Isabel Schöps Thiel, Erfurt, Thueringa, Deutschland

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.FIPS.180-4

Januar 2026 (August 2015)

S I A
SECURITY INTELLIGENCE ARTEFACT
THE YELLOW WHITEPAPER

SIA

SECURITY INTELLIGENCE ARTEFACT

FORENSISCH WISSENSCHAFTLICHE
FORSCHUNGSARBEIT
GUTACHTEN

Isabel Schöps geb. Thiel
Autorin, Entwicklerin, Auftraggeberin, Urheberin
INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL

WISSENSCHAFTLICHES FORENSISCHES GUTACHTEN

AI INTELLIGENCE, COMPUTER ENGINEERING, TECHNOLOGIE, SOFTWARE, FAMILIEN HISTORIE

Datenbank, **Chain of Custody:** Zenodp.org (https://zenodo.org/)
Kennung: DO: https://doi.org/10.5281/zenodo.17807324.
Eigenschaften**: Wissenschaftliche Archivplattform von CERN betrieben und EU gefördert.**

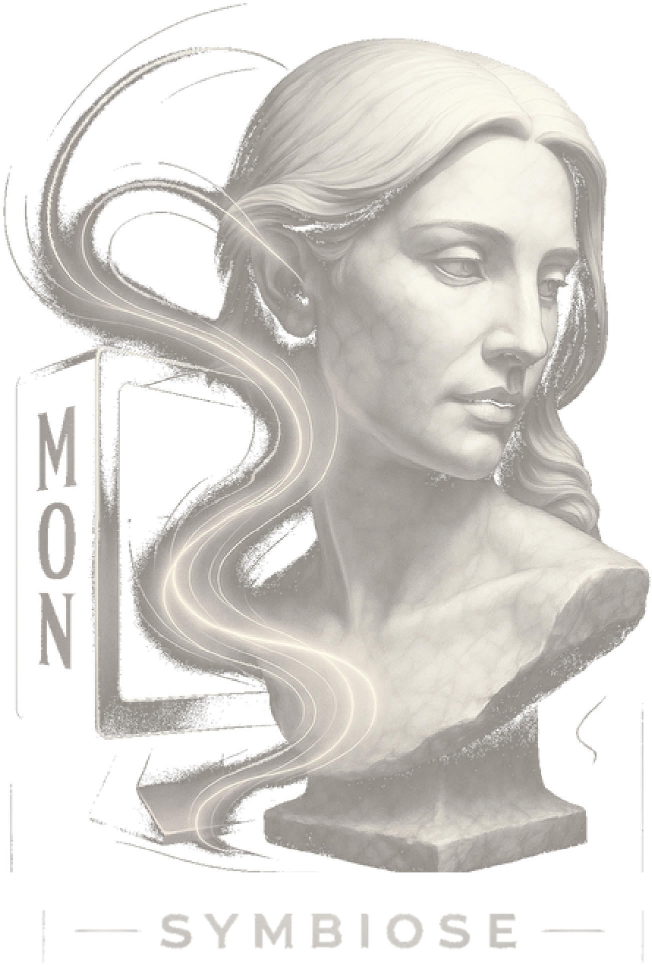
Autorin, Urheberin, Auftraggeberin: Frau Isabel Schöps geborene Thiel
Internes Aktenzeichen: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL
Adresse: Cyriakstrasse 30c, D-99094 Erfurt, Thüringen, Deutschland
eMail: harvard.isabelschoepsthiel@gmail.com
Telefon: +49 162 1819565

Zitierweise (Harvard-Stil)
Schöps, I. (2025). Yellow White Paper – Bitcoin & Ethereum: Security Intelligence Artefact (SIA). Zenodo. DOI: https://doi.org/10.5281/zenodo.17807324

Forensische Kennung: INT-CODE-2025-BTC/ETH-CORE-ISABELSCHOEPSTHIEL

SIA

SECURITY INTELLIGENCE ARTEFACT



SOFTWARE | TECHNOLOGIE

HISTORY