Zero Knowledge Proof Gamification (ZKPG+)

Thomas Wernbacher & Alexander Pfeiffer

University of Krems Press

ZKPG+ Modell

Autoren: Mag. Dr. Alexander Pfeiffer, PhD MA MBA und Mag. Thomas Wernbacher, MA MSc

Herausgeber: Zentrum für Angewandte Spieleforschung in Kooperation mit dem Department für Sicherheitsforschung, Universität für Weiterbildung Krems; University of Krems Press

Im Auftrag von: LimeSoda Interactive Marketing GmbH

Projektbericht: Innovationsscheck ZKPG+ Framework (Zero Knowledge Proof Gamification)

Gefördert im Rahmen eines FFG Innovationsschecks

DOI: https://doi.org/10.48341/j2r8-3x86

KI Disclaimer:

DeepL Pro: Rechtschreibkontrolle

Manus: Umwandlung von Word in ein optimal formatiertes PDF für den Publikationsprozess

University of Krems Press

Inhalt

Einleitung

Die Herausforderung der modernen Unternehmensverantwortung

In einer Unternehmenswelt, die in der öffentlichen Diskussion zunehmend von Transparenz, Nachhaltigkeit und ethischem Handeln geprägt sein sollte, stehen Unternehmen vor einer dreifachen Herausforderung.

- Erstens müssen sie ihre Corporate Social Responsibility (CSR) Ziele nicht nur definieren, sondern auch glaubwürdig kommunizieren.
- Zweitens müssen sie ihre Mitarbeiter_innen und Stakeholder_innen aktiv in diese Bemühungen einbinden.
- Drittens müssen sie dabei die Privatsphäre aller Beteiligten schützen und gleichzeitig Vertrauen aufbauen.

Dieses Mini-Buch präsentiert das ZKPG+ Modell, einen innovativen Ansatz, der drei auf den ersten Blick unterschiedliche Konzepte – Corporate Social Responsibility, Gamification und Zero-Knowledge Proofs – zu einem gemeinsamen Framework verbindet. Dieses Modell soll Unternehmen ermöglichen, ihre CSR-Initiativen auf eine Weise zu gestalten, die sowohl engagierend als auch vertrauenswürdig sein können, ohne die Privatsphäre der teilnehmenden Akteur_innen zu gefährden.

Das Buch ist das Ergebnis aus der Zusammenarbeit von Mitarbeiter_innen der Universität für Weiterbildung Krems und zwar namentlich Alexander Pfeiffer, Simon Wimmer, Constantin Kraus und Thomas Wernbacher, mit der Wiener

Agentur Limesoda GmbH, welche CSR nicht nur im eigenen Unternehmen lebt, sondern für ihre Kund_innen mit Bedacht umsetzt. Im Rahmen des von der FFG geförderten Innovationsschecks wurden nicht nur interne Handlungsempfehlungen für das Unternehmen ausgearbeitet, sondern vor allem auch ein öffentlich zugängiges Dokument versprochen, welches auch anderen Agenturen und vor allem KMUs die Möglichkeit geben soll neue Ideen in die Reflektion und Diskussion aufzunehmen.

Aufbau dieses Buches

Das Buch ist in drei Teile gegliedert. Teil I führt in die Grundkonzepte ein: CSR, Gamification, Zero-Knowledge Proofs sowie die unterstützenden Konzepte Blockchain und Need to Know. Jedes Konzept wird zunächst isoliert betrachtet, um ein solides Fundament für das Verständnis der späteren Verbindungen zu schaffen.

Teil II untersucht die paarweisen Verbindungen zwischen diesen Konzepten. Wie kann Gamification CSR-Initiativen unterstützen? Wie können Zero-Knowledge Proofs Vertrauen in CSR-Berichte schaffen? Wie können Gamification-Systeme datenschutzfreundlich gestaltet werden?

Teil III präsentiert das integrierte ZKPG+ Modell und illustriert seine Anwendung anhand konkreter Fallstudien. Der Anhang enthält das begleitende Kartenspiel “The Ethical Enabler”, das als Lern- und Awareness-Tool für die im Buch behandelten Konzepte dient. Dieses ist unter www.zkp-gamification.com verfügbar.

Die Grundkonzepte

Corporate Social Responsibility (kurz CSR)

Definition und Bedeutung Corporate Social Responsibility (kurz CSR) bezeichnet die Verantwortung von Unternehmen, über ihre wirtschaftlichen und rechtlichen Pflichten hinaus einen positiven Beitrag zur Gesellschaft und Umwelt zu leisten. Es ist ein Konzept, das die Integration sozialer und ökologischer Belange in die Geschäftstätigkeit und die Interaktion mit Stakeholder_innen beschreibt.

Die Bedeutung von CSR hat in den letzten Jahrzehnten erheblich zugenommen. Verbraucher_innen, Investor_innen und Mitarbeiter_innen erwarten heute von Unternehmen, dass sie nicht nur profitabel sind, sondern auch ethisch handeln und zur Lösung gesellschaftlicher Probleme beitragen. Unternehmen, die diese Erwartungen ignorieren, riskieren Reputationsschäden, den Verlust von Kund_innen und Schwierigkeiten bei der Gewinnung von Talenten.

Historische Entwicklung Die Geschichte von CSR lässt sich in vier Phasen unterteilen:

- **Die Philanthropische Ära (vor 1950)** In dieser frühen Phase war die soziale Verantwortung von Unternehmen hauptsächlich durch Philanthropie und paternalistische Wohlfahrtsprogramme für Mitarbeiter_innen gekennzeichnet. Unternehmer_innen wie Andrew Carnegie und John D. Rockefeller spendeten große Teile ihres Vermögens für wohltätige Zwecke, aber diese Aktivitäten waren oft von den Kerngeschäftsaktivitäten getrennt.
- **Die Bewusstseinsära (1950er-1960er Jahre)** Die Veröffentlichung von Howard R. Bowens Buch "Social Responsibilities of the Businessman" im Jahr 1953 markierte einen Wendepunkt. Bowen, oft als "Vater der CSR" bezeichnet, argumentierte, dass Unternehmen eine Verpflichtung gegenüber der Gesellschaft haben, die über die reine Gewinnmaximierung hinausgeht. Diese Ära sah den Beginn eines bewussten Dialogs über die Rolle von Unternehmen in der Gesellschaft.
- **Die Themenära (späte 1960er-frühe 1970er Jahre)** Mit dem Aufkommen sozialer und ökologischer Bewegungen begann CSR, sich auf spezifische Themen wie Umweltverschmutzung, Verbraucherschutz und Arbeitssicherheit zu konzentrieren. Unternehmen wurden zunehmend aufgefordert, ihre negativen externen Effekte zu adressieren.
- **Die Reaktionsfähigkeitsära (Mitte der 1970er Jahre bis heute)** Diese Ära sah einen Wandel von einem reaktiven zu einem proaktiven Ansatz. Unternehmen begannen, Managementsysteme zu entwickeln, um soziale Anforderungen zu antizipieren und darauf zu reagieren. Dies führte zur Entwicklung von Konzepten wie Corporate Social Performance (CSP) und Corporate Social Responsiveness.

Carrolls CSR-Pyramide Eines der einflussreichsten Modelle zur Konzeptualisierung von CSR ist die von Archie B. Carroll entwickelte CSR-Pyramide. Sie definiert vier Ebenen der Unternehmensverantwortung:

Ebene	Verantwortung	Beschreibung
1	Ökonomisch	Profitabel sein – die Grundlage für alle anderen Verantwortlichkeiten
2	Legal	Das Gesetz befolgen – Einhaltung von Vorschriften
3	Ethisch	Das Richtige tun – moralisch über die gesetzlichen Anforderungen hinaus handeln

Ebene	Verantwortung	Beschreibung
4	Philanthropisch	Zur Gesellschaft beitragen – freiwillige Verbesserung der Gemeinschaft

Die Pyramide verdeutlicht, dass wirtschaftliche Verantwortung die Basis bildet, auf der alle anderen Verantwortlichkeiten aufbauen. Ein Unternehmen muss zunächst wirtschaftlich lebensfähig sein, bevor es sich höheren Verantwortlichkeiten widmen kann.

Moderne CSR-Berichterstattung In den letzten Jahren hat sich die CSR-Berichterstattung durch standardisierte Rahmenwerke professionalisiert:

- **Global Reporting Initiative (GRI):** Das weltweit am weitesten verbreitete Rahmenwerk für Nachhaltigkeitsberichterstattung. Es bietet umfassende Standards für die Berichterstattung über wirtschaftliche, ökologische und soziale Auswirkungen.
- **Sustainability Accounting Standards Board (SASB):** Konzentriert sich auf branchenspezifische Standards für wesentliche ESG-Faktoren und hilft Investor_innen, die finanziellen Auswirkungen von Nachhaltigkeit zu verstehen.
- **Corporate Sustainability Reporting Directive (CSRD):** Eine EU-Richtlinie, die ESG-Berichterstattung für große Unternehmen verpflichtend vorsieht; der ursprünglich kommunizierte Anwendungsbereich von rund 50.000 Unternehmen wurde durch spätere politische Anpassungen deutlich eingegrenzt.
- **Die Triple Bottom Line:** Das Konzept der Triple Bottom Line (TBL), geprägt von John Elkington, argumentiert, dass Unternehmen ihren Erfolg nicht nur an ihrer finanziellen Leistung (Profit) messen sollten, sondern auch an ihren sozialen (People) und ökologischen (Planet) Auswirkungen. Diese ganzheitliche Sichtweise der Unternehmensleistung ist zentral für modernes CSR.
- **CSR und ESG:** Während CSR das breitere Konzept der Unternehmensverantwortung gegenüber der Gesellschaft darstellt, bezieht sich Environmental, Social, and Governance (ESG) auf die spezifischen, messbaren Kriterien zur Bewertung der Unternehmensleistung in diesen Bereichen. Der Aufstieg von ESG hat CSR von einem qualitativen Konzept zu einer datengetriebenen Praxis transformiert.

Aktuelle Trends Die CSR-Landschaft entwickelt sich ständig weiter. Die Implementierung von CSR variiert stark je nach Branche und Unternehmensgröße. Einige Beispiele illustrieren die Vielfalt der Ansätze:

- **Technologiebranche** Technologieunternehmen fokussieren sich häufig auf Datenschutz, ethische KI-Entwicklung und die Reduzierung des ökolo-

gischen Fußabdrucks ihrer Rechenzentren. Große Cloud-Anbieter_innen investieren in erneuerbare Energien und setzen sich Ziele zur Klimaneutralität.
- **Finanzsektor** Banken und Versicherungen integrieren ESG-Kriterien in ihre Investitionsentscheidungen und bieten nachhaltige Finanzprodukte an. Sustainable Finance ist zu einem wichtigen Geschäftsfeld geworden.
- **Einzelhandel** Einzelhändler_innen konzentrieren sich auf nachhaltige Lieferketten, faire Arbeitsbedingungen und die Reduzierung von Verpackungsmüll. Transparenz gegenüber Verbraucher_innen über die Herkunft von Produkten gewinnt an Bedeutung.
- **Produktion** Produzierende Unternehmen arbeiten an der Reduzierung von Emissionen, der Implementierung von Kreislaufwirtschaftsprinzipien und der Verbesserung der Arbeitssicherheit.

Die Herausforderung der Glaubwürdigkeit Eine der größten Herausforderungen für CSR ist die Glaubwürdigkeit. Der Begriff "Greenwashing" beschreibt die Praxis, sich ein umweltfreundliches Image zu geben, ohne substanzielle Maßnahmen zu ergreifen. Stakeholder_innen werden zunehmend skeptisch gegenüber CSR-Behauptungen, die nicht durch unabhängige Verifizierung gestützt werden.

Diese Glaubwürdigkeitslücke ist einer der Hauptgründe, warum Zero-Knowledge Proofs für CSR so relevant werden könnten. Sie bieten eine Möglichkeit, Behauptungen kryptographisch zu verifizieren, ohne sensible Daten offenzulegen.

Die verpflichtende Berichterstattung nimmt weltweit zu. Was einst freiwillig war, wird zunehmend gesetzlich vorgeschrieben. Die doppelte Wesentlichkeit erfordert, dass Unternehmen sowohl über ihre Auswirkungen auf Gesellschaft und Umwelt als auch über die Auswirkungen von Umwelt- und Sozialfaktoren auf ihr Geschäft berichten. Die Lieferkettentransparenz erstreckt sich über die eigenen Betriebe eines Unternehmens hinaus auf die gesamte Wertschöpfungskette.

Gamification

Gamification ist die Anwendung von Spieldesign-Elementen und Spielprinzipien in zumeist spielfremden Kontexten. Es ist ein Designansatz, der die menschliche Motivation und das Engagement in den Mittelpunkt stellt. Angelehnt an Yu-kai Chou ist Gamification die Kunst, alle unterhaltsamen und fesselnden Elemente aus Spielen zu extrahieren und auf reale oder produktive Aktivitäten anzuwenden. Pfeiffer und Wernbacher haben die Definition auch erweitert. Sie betonen, dass es Gamification auch in und rund um Spiele geben kann. Dann wenn es Ranklisten, Badges etc. in Spielen gibt, die nichts mit dem Kerninhalt der Spiele zu tun hat. Die Autoren verorten Gamification in konzeptioneller Nähe zu Nudging, unterscheiden Gamification von Nudging jedoch durch ihre systematische, datenbasierte Feedbackstruktur. Diese Daten sowohl für gute Zwecke, als auch für die dunkle Seite von Gamification der „Ludefaction“ oder „Exploitationware“ verwendet werden kann.

Psychologische Grundlagen In seiner Dissertation an der WU-Wien beschreibt Pfeiffer (2018) die psychologischen Grundlagen von Gamification. Man unterscheidet zwischen extrinsischer Motivation (Belohnungen) und intrinsischer Motivation (innere Antriebe). Während extrinsische Belohnungen kurzfristig wirksam sein können, ist das Ziel verantwortungsvoller Gamification, langfristig intrinsische Motivation zu fördern.

Self-Determination Theory (SDT) Die Self-Determination Theory (SDT) von Deci und Ryan ist ein zentrales Framework für das Verständnis intrinsischer Motivation. Sie postuliert drei angeborene psychologische Bedürfnisse:

1. **Autonomie:** Das Bedürfnis, Kontrolle über das eigene Handeln zu haben.
2. **Kompetenz:** Das Bedürfnis, sich als fähig und wirksam zu erleben.
3. **Soziale Eingebundenheit:** Das Bedürfnis, sich mit anderen verbunden zu fühlen.

Gamification-Systeme, die diese drei Bedürfnisse befriedigen, sind besonders effektiv bei der Förderung intrinsischer Motivation.

Octalysis Framework Das Octalysis Framework von Yu-kai Chou ist ein praktisches Design-Tool, das acht Kerntriebe der Motivation identifiziert und die Grundlage für das ZKPG+ Modell:

1. **Epic Meaning & Calling:** Das Gefühl, Teil von etwas Größerem zu sein.
2. **Development & Accomplishment:** Das Gefühl von Fortschritt und Erfolg.
3. **Empowerment of Creativity & Feedback:** Die Möglichkeit, kreativ zu sein und Feedback zu erhalten.
4. **Ownership & Possession:** Das Gefühl, etwas zu besitzen oder zu kontrollieren.
5. **Social Influence & Relatedness:** Soziale Interaktion und Vergleich.
6. **Scarcity & Impatience:** Die Anziehungskraft von Seltenheit und Exklusivität.
7. **Unpredictability & Curiosity:** Die Faszination des Unbekannten.
8. **Loss & Avoidance:** Die Motivation, Verluste zu vermeiden.

Ein gutes Gamification-Design balanciert diese acht Triebe aus, um eine nachhaltige Motivation zu schaffen.

Kritische Perspektiven Pfeiffer (2018) warnt vor den Gefahren der "Pointification" – der reinen Vergabe von Punkten für Aktivitäten, ohne die intrinsische Motivation zu fördern. Er zitiert kritische Stimmen, wie Stampfl, die argumentieren, dass Gamification bestehende organisationale Zwänge verschleiern kann, wenn sie nicht transparent und ethisch gestaltet wird. Eine sorgfältige, ethische Gestaltung ist daher unerlässlich.

Anwendungsbereiche Pfeiffer (2018) dokumentiert eine breite Palette von Anwendungsbereichen für Gamification, darunter Bildung, Gesundheit, Marketing und Umweltschutz. Die empirischen Daten zeigen eine hohe wahrgenommene Relevanz von Gamification, insbesondere im Bildungs- und Gesundheitssektor. Der Umweltschutz wird ebenfalls als relevanter Bereich identifiziert und dies bildet die Grundlage die Verbindung zwischen CSR und Gamification anzudenken.

Konzeptuelle Unterscheidungen Pfeiffer (2018) differenziert klar zwischen verschiedenen Ansätzen:

- **Simulation:** Modellbasierte Nachbildung ohne Spielelemente.
- **Edutainment:** Lernprogramme für die Freizeit, oft mit geringerer Qualität.
- **Serious Games:** Das Spiel steht im Vordergrund, der Lerneffekt ist unterschwellig.
- **Gamifizierte Simulation:** Simulationen, die mit Spielmechaniken angereichert werden.
- **Game Based Assessment:** Spiele, die zur Leistungsbeurteilung eingesetzt werden.

Gamification-Elemente Gamification nutzt eine Vielzahl von Spielelementen:

- **Punkte** bieten unmittelbares Feedback und ein Gefühl des Fortschritts. Sie sind die grundlegendste Form der Gamification und können für verschiedene Aktivitäten vergeben werden.
- **Abzeichen (Badges)** erkennen Erfolge und Meilensteine an. Sie dienen als visuelle Darstellung von Errungenschaften und können Sammelwert haben.
- **Ranglisten (Leaderboards)** fördern Wettbewerb und sozialen Vergleich. Sie können motivierend sein, aber auch demotivierend für diejenigen am unteren Ende.
- **Herausforderungen** bieten klare Ziele und ein Gefühl der Zielsetzung. Sie können zeitlich begrenzt sein, um Dringlichkeit zu erzeugen.
- **Narrative** schaffen eine fesselnde Geschichte, die Aktionen Kontext und Bedeutung verleiht. Sie können besonders effektiv sein, um Epic Meaning & Calling zu aktivieren.

Enterprise Gamification In der Unternehmenswelt wird Gamification eingesetzt, um verschiedene Geschäftsziele zu erreichen:

- **Mitarbeiter_innen-Onboarding und Training:** Gamification macht Lernprozesse ansprechender und effektiver. Interaktive Lernerfahrungen mit Fortschrittsverfolgung und Belohnungen erhöhen die Abschlussraten und die Wissensretention.

- **Performance Management:** Gamifizierte Dashboards visualisieren den Fortschritt bei Zielen und bieten Echtzeit-Feedback. Dies kann die Motivation und das Engagement der Mitarbeiter_innen steigern.
- **Vertriebsmotivation:** Ranglisten und Erfolgssysteme fördern einen gesunden Wettbewerb und erkennen Top-Performer_innen an.
- **Wissensmanagement:** Gamification kann das Teilen von Informationen und Expertise incentivieren, indem Beiträge belohnt werden.

Gamification-Fallstricke und Best Practices Bei der Implementierung von Gamification können verschiedene Fehler auftreten, die den Erfolg gefährden:

Häufige Fehler

- **Übermäßige Abhängigkeit von extrinsischen Belohnungen:** Wenn Nutzer_innen nur für Punkte und Abzeichen arbeiten, kann die intrinsische Motivation untergraben werden. Sobald die Belohnungen entfernt werden, sinkt das Engagement.
- **Unfaire Ranglisten:** Wenn Ranglisten von einer kleinen Gruppe dominiert werden, können sie demotivierend für die Mehrheit sein.
- **Mangelnde Relevanz:** Gamification-Elemente müssen mit den tatsächlichen Zielen und Werten der Nutzer_innen übereinstimmen.
- **Komplizierte Mechaniken:** Übermäßig komplexe Systeme können Nutzer_innen verwirren und abschrecken.

Best Practices

- **Fokus auf intrinsische Motivation:** Gestalten Sie Systeme, die Autonomie, Kompetenz und Verbundenheit fördern.
- **Personalisierung:** Ermöglichen Sie es Nutzer_innen, ihre Erfahrung anzupassen. Aber Achtung – ohne Datenkrake der HR Abteilungen.
- **Klares Feedback:** Geben Sie sofortiges und verständliches Feedback zu Aktionen.
- **Progressive Herausforderungen:** Steigern Sie die Schwierigkeit schrittweise, um Nutzer_innen im "Flow" zu halten.
- **Soziale Elemente:** Fördern Sie Zusammenarbeit und Community-Bildung.

Design für nachhaltige Verhaltensänderung Um langfristige Verhaltensänderungen zu erreichen, muss Gamification über einfache Punkte und Abzeichen hinausgehen. Sie sollte sich auf die Förderung intrinsischer Motivation konzentrieren durch:

Die Schaffung bedeutungsvoller Narrative, die Aktionen mit einem größeren Zweck verbinden. Die Förderung eines Gemeinschaftsgefühls und sozialer Unterstützung. Die Bereitstellung von Möglichkeiten für Autonomie und kreativen Ausdruck. Das schrittweise Reduzieren externer Belohnungen, wenn die intrinsische Motivation greift.

Entscheidend ist auch Transparenz und Fairness, wenn es um etwas geht muss das System überprüfbar glaubwürdig sein.

Zero-Knowledge Proofs (ZKP)

In seiner zweiten Dissertation bietet Pfeiffer (2025) eine Übersicht über verschiedene ZKP-Protokolle. Die beiden prominentesten Typen sind:

- **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):** Diese Protokolle zeichnen sich durch sehr kleine Beweisgrößen und schnelle Verifizierungszeiten aus. Sie erfordern jedoch eine vertrauenswürdige Setup-Zeremonie.
- **zk-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge):** Diese Protokolle benötigen keine vertrauenswürdige Setup-Zeremonie und sind quantenresistent. Sie haben jedoch größere Beweisgrößen.

Für die meisten CSR-Gamification-Anwendungen sind zk-SNARKs aufgrund ihrer Effizienz die bevorzugte Wahl, wie im ZKPG+ Modell nachher erläutert wird.

Quantenresistenz Ein wichtiger Aspekt, der von Pfeiffer (2025) hervorgehoben wird, ist die Bedrohung durch Quantencomputer. Aktuelle kryptografische Systeme sind anfällig für Quantenangriffe. Post-Quantum Cryptography (PQC) entwickelt neue Algorithmen, die diesen Bedrohungen standhalten. Die Integration von PQC in Blockchain-Systeme ist ein aktives Forschungsfeld und für die langfristige Sicherheit von CSR-Anwendungen von entscheidender Bedeutung.

Definition und Konzept Zero-Knowledge Proofs (ZKPs) sind eine kryptographische Technik, die es einer Partei (dem Beweiser oder der Beweiserin) ermöglicht, einer anderen Partei (dem Verifizierer oder der Verifiziererin) zu beweisen, dass eine Aussage wahr ist, ohne dabei zusätzliche Informationen über die Gültigkeit der Aussage hinaus preiszugeben. Diese scheinbar magische Eigenschaft hat tiefgreifende Auswirkungen auf Privatsphäre, Sicherheit und Vertrauen in der digitalen Welt.

Historischer Hintergrund Zero-Knowledge Proofs wurden erstmals 1985 in einem Paper von Shafi Goldwasser und Silvio Micali mit dem Titel “The Knowledge Complexity of Interactive Proof-Systems” beschrieben. Ursprünglich für die theoretische Kryptographie entwickelt, finden ZKPs heute breite Anwendung in Blockchain, Identitätsverifizierung und datenschutzwahrenden Anwendungen.

Die drei fundamentalen Eigenschaften Jedes ZKP-System basiert auf drei grundlegenden Eigenschaften:

- **Vollständigkeit (Completeness):** Wenn die Aussage wahr ist, kann ein_e ehrliche_r Beweiser_in eine_n ehrliche_n Verifizierer_in immer überzeugen.
- **Korrektheit (Soundness):** Wenn die Aussage falsch ist, kann ein_e unehrliche_r Beweiser_in eine_n ehrliche_n Verifizierer_in nicht überzeugen (außer mit einer sehr kleinen, vernachlässigbaren Wahrscheinlichkeit).
- **Zero-Knowledge:** Der oder die Verifizierer_in lernt nichts anderes als die Tatsache, dass die Aussage wahr ist. Keine Informationen über das geheime Wissen des Beweisers oder der Beweiserin werden preisgegeben.

Das Höhlenbeispiel (Ali Babas Höhle) Ein klassisches Beispiel zur Veranschaulichung von ZKPs ist das Höhlenbeispiel:

Eine visuelle Darstellung findet sich hier:

https://www.ffe.de/veroeffentlichungen/beitragsreihe-blockchain-deep-dives-zero-knowledge-proofs/

Man stelle sich eine ringförmige Höhle mit einem einzigen Eingang vor. Am entfernten Ende der Höhle befindet sich eine magische Tür, die sich nur bei Benutzung des richtigen Passworts öffnet. Peggy (P) ist im Besitz des Passworts und möchte Victor (V) ihre Kenntnis beweisen, ohne ihm das Passwort selbst zu verraten.

Hierzu verschließt V zunächst die Augen und P wählt zufällig einen der beiden Pfade zur Tür (1). Nun öffnet V die Augen wieder und wählt ebenfalls zufällig einen der beiden Pfade. Diesen teilt er P per Zuruf mit (2). P trifft nun die nötigen Vorkehrungen, um auf dem von V gewählten Pfad zum Eingang zurückzukehren. Ist sie bereits auf demselben Pfad in die Höhle gelangt, so kehrt sie einfach um. Wurde der andere Pfad gewählt, so tritt sie mithilfe des Passworts durch die magische Tür und setzt den Weg bis zum Eingang fort (3). Auf diese Weise gelingt es P in jedem Fall, auf dem von V gewählten Pfad die Höhle zu verlassen.

Wird dieses Experiment wiederholt, so halbiert sich die Wahrscheinlichkeit, dass P anfangs denselben Pfad einschlägt, den später auch V wählen wird, mit jeder erneuten Durchführung. Sollte P also tatsächlich nicht im Besitz des Passworts sein, so verdoppelt sich die Chance, dass sie nicht in der Lage ist, die Tür zu öffnen und auf dem falschen Weg die Höhle verlassen muss. Bei ausreichend häufiger Durchführung des Experiments entsteht bei V demnach eine statistische Sicherheit, dass P das Passwort kennt oder eben nicht.

Arten von Zero-Knowledge Proofs Interaktive vs. Nicht-interaktive ZKPs

- **Interaktive ZKPs** erfordern eine Hin-und-Her-Kommunikation zwischen Beweiser_in und Verifizierer_in.

- **Nicht-interaktive ZKPs** ermöglichen es dem Beweiser oder der Beweiserin, einen Beweis zu generieren, der von jedem und jeder ohne Interaktion verifiziert werden kann.

zk-SNARKs vs. zk-STARKs

Dies sind wie bereits erwähnt die beiden prominentesten ZKP-Implementierungen:

Aspekt	zk-SNARKs	zk-STARKs
Vollständiger Name	Succinct Non-interactive Argument of Knowledge	Scalable Transparent Argument of Knowledge
Beweisgröße	In vielen Benchmark-Szenarien deutlich kleiner (Größenordnungen abhängig von Implementierung und Circuit)	Größer
Beweisgeschwindigkeit	In vielen Anwendungsfällen schneller, abhängig von Protokoll, Hardware und Circuit-Design	Langsamer
Verifizierungsgeschwindigkeit	Langsamer	Schneller
Trusted Setup	Erforderlich	Nicht erforderlich (transparent)
Quantenresistenz	Nein	Ja
Beste Anwendung	Blockchain, Skalierbarkeit, Finanzsysteme	langfristige Sicherheit

Vorteile von Zero-Knowledge Proofs

- **Privatsphäre:** Informationen verifizieren, ohne die zugrunde liegenden Daten preiszugeben.
- **Sicherheit:** Kryptographisch sichere Verifizierung.
- **Skalierbarkeit:** Komplexe Berechnungen können in kleine Beweise komprimiert werden.
- **Vertrauenslosigkeit:** Kein Vertrauen in den Beweiser oder die Beweiserin mit sensiblen Daten erforderlich.
- **Compliance:** Regulatorische Anforderungen erfüllen und gleichzeitig die Privatsphäre schützen.

Anwendungsfälle

- **Blockchain und Kryptowährung:** Privacy Coins wie Zcash nutzen zk-SNARKs für private Transaktionen. ZK-Rollups (StarkNet, ZKsync, Loopring) ermöglichen die Skalierung von Ethereum.
- **Identitätsverifizierung:** ZKPs ermöglichen es, das Alter zu beweisen, ohne das Geburtsdatum zu verraten, oder die Kreditwürdigkeit zu beweisen, ohne finanzielle Details offenzulegen.
- **Abstimmungssysteme:** ZKPs können sicherstellen, dass Stimmen korrekt gezählt werden, ohne einzelne Stimmen preiszugeben.
- **Lieferkette:** ZKPs können ethische Beschaffung verifizieren, ohne Lieferantendetails zu enthüllen.

Technische Komponenten

- **Circuits:** ZKPs verwenden Rechenschaltkreise (Circuits), um die zu beweisende Aussage zu kodieren. Circuits nehmen Eingaben entgegen und erzeugen Ausgaben durch eine Reihe von Gattern. Der Beweiser oder die Beweiserin demonstriert Kenntnis von Eingaben, die den Circuit erfüllen.
- **Commitment Schemes:** Ermöglichen es dem Beweiser oder der Beweiserin, sich auf einen Wert festzulegen, ohne ihn zu enthüllen. Später kann der Beweiser oder die Beweiserin den Wert offenlegen und beweisen, dass er mit dem Commitment übereinstimmt.

Blockchain und Need to Know

Blockchain: Das dezentrale Vertrauensnetzwerk Wie Pfeiffer, Wernbacher und Vella (2024) in ihrem Kapitel "Blockchain in der schulischen Bildung" argumentieren, bieten Blockchain-Technologien eine robuste Antwort auf die Herausforderungen der Datenintegrität in digitalen Umgebungen. Als dezentrale Systeme bieten Blockchains wenig Möglichkeiten für Manipulationsversuche. Sobald Informationen auf der Blockchain gespeichert sind, können sie nicht rückwirkend geändert werden. Diese Unveränderbarkeit macht Blockchain-Systeme zu einer leistungsfähigen Technologie zur Sicherung der Integrität kritischer Informationen, sofern Governance, Datenquellen und Konsensmechanismen geeignet gestaltet sind.

Blockchain-Grundlagen Eine Blockchain ist im Optimalfall ein verteilter, unveränderlicher Ledger, welcher Transaktionen über ein Netzwerk von Computern aufzeichnet. Jeder Block enthält einen kryptographischen Hash des vorherigen Blocks, einen Zeitstempel und Transaktionsdaten.

Kernmerkmale

- **Dezentralisierung:** Keine zentrale Autorität kontrolliert das Netzwerk.
- **Unveränderlichkeit:** Einmal aufgezeichnete Daten können nicht geändert werden. Es können maximal zusätzliche Daten hinzugefügt werden mit einer neuen Transaktion, welche über die TransaktionsID und/oder TokenID mit der Transaktion davor verbunden ist. (Beispielsweise für Updates)

- **Transparenz:** Alle Transaktionen sind für Netzwerkteilnehmer_innen sichtbar. Zumindest, dass sie stattgefunden haben. Natürlich können und müssen Datensätze darüber hinaus auch verschlüsselt werden können.
- **Konsens:** Netzwerkteilnehmer_innen einigen sich auf den Zustand des Ledgers.

Blockchain und CSR Blockchain-Technologie bietet mehrere Vorteile für CSR:

- **Lieferkettentransparenz:** Blockchain kann die Herkunft von Produkten verfolgen und ethische Beschaffung verifizieren.
- **Unveränderliche Aufzeichnungen:** CSR-Berichte und Zertifizierungen können auf der Blockchain gespeichert werden, um Manipulationen zu verhindern.
- **Smart Contracts:** Automatisierte Verträge können CSR-Verpflichtungen durchsetzen.

Das Need to Know-Prinzip Das Need to Know-Prinzip ist ein Grundsatz der Informationssicherheit, der besagt, dass Personen nur Zugang zu den Informationen haben sollten, die sie für die Erfüllung ihrer Aufgaben benötigen. Dieses Prinzip ist zentral für Datenschutz und Sicherheit.

Anwendung in der Datenarchitektur

In einer Need to Know-Datenarchitektur werden Daten so strukturiert und zugänglich gemacht, dass folgende Aspekte zutreffen:

- **Minimale Offenlegung:** Nur die absolut notwendigen Daten werden geteilt.
- **Rollenbasierter Zugang:** Zugang wird basierend auf der Rolle und den Aufgaben einer Person gewährt.
- **Datensegmentierung:** Daten werden in Segmente unterteilt, um den Zugang zu kontrollieren.

Zero-Knowledge Proofs sind eine mögliche technologische Verkörperung des Need to Know-Prinzips. Sie ermöglichen es, die Wahrheit einer Aussage zu beweisen, ohne mehr Informationen preiszugeben als unbedingt notwendig. Diese Kombination ist besonders wertvoll für CSR-Anwendungen, bei denen Unternehmen Compliance nachweisen müssen, ohne sensible Geschäftsdaten zu enthüllen.

Die Verbindungen der Konzepte

Gamification bietet eine kraftvolle Brücke, um Mitarbeiter_innen und Kund_innen mit den CSR-Zielen eines Unternehmens zu verbinden. Durch die Anwendung von Spielmechaniken können Organisationen abstrakte Nachhaltigkeitsziele in ansprechende, messbare und belohnende Erfahrungen verwandeln.

Mechanismen der gamifizierten CSR

Mechanismus	Beschreibung	CSR-Anwendung
Punkte & Abzeichen	Belohnungssysteme für gewünschte Verhaltensweisen	Anerkennung für nachhaltige Aktionen
Ranglisten	Wettbewerbsorientierte Rankings	Verfolgung der Nachhaltigkeitsleistung von Teams
Herausforderungen	Zeitgebundene Ziele	Monatliche Recycling- oder Energiespar-Challenges
Fortschrittsbalken	Visuelle Darstellung des Fortschritts	Anzeige des Fortschritts bei CSR-Zielen
Narrative	Story-getriebenes Engagement	CSR als kollektive Mission rahmen

Vorteile gamifizierter CSR

- **Erhöhtes Engagement:** Gamification macht CSR-Aktivitäten attraktiver und belohnender. Mitarbeiter_innen, die sonst passiv bleiben würden, werden aktiv in Nachhaltigkeitsinitiativen einbezogen.
- **Messbare Wirkung:** Gamifizierte Systeme generieren Daten über Teilnahme und Leistung. Dies ermöglicht es Unternehmen, den Erfolg ihrer CSR-Initiativen zu quantifizieren.
- **Markenloyalität:** Die Demonstration des Engagements für verantwortungsvolles Handeln stärkt die Bindung von Kund_innen und Mitarbeiter_innen.
- **Kostenreduktion:** Gamifizierte Ansätze sind oft effizienter als traditionelle Methoden wie Umfragen oder Interviews.
- **Kultur der Verantwortlichkeit:** Gamification kann – gut implementiert – dafür sorgen eine Kultur der Verantwortung zu etablieren.

Praxisbeispiele

- **Mitarbeiter_innen-Engagement** Ein Unternehmen führt eine "Green Challenge" ein, bei der Mitarbeiter_innen Punkte und Abzeichen für die Reduzierung ihres Energieverbrauchs verdienen. Echtzeit-Ranglisten fördern einen freundlichen Wettbewerb zwischen Abteilungen.
- **Kunden-Engagement** Ein Einzelhändler oder eine Einzelhändlerin implementiert ein Treueprogramm, das mit nachhaltigen Produktentscheidungen verknüpft ist. Kund_innen erhalten Punkte für den Kauf von Produkten mit geringerem ökologischen Fußabdruck. Diese Punkte können gegen Rabatte oder Spenden an Umweltorganisationen eingelöst werden.

Implementierungsüberlegungen

Bei der Implementierung gamifizierter CSR sollten Unternehmen folgende Aspekte berücksichtigen:

- **Zielgruppenverständnis:** Entwickeln Sie Verhaltensmodelle für spezifische Gruppen. Nicht alle Mitarbeiter_innen werden durch die gleichen Mechanismen motiviert.
- **Klare Ziele:** Etablieren Sie messbare CSR-Ziele, die mit den Gamification-Mechanismen verknüpft sind.
- **Faire Belohnungssysteme:** Schaffen Sie gerechte und motivierende Anreizstrukturen, die nicht zu unbeabsichtigten Verhaltensweisen führen.
- **Datengetriebene Erkenntnisse:** Verfolgen Sie den Fortschritt und passen Sie Strategien basierend auf den gesammelten Daten an. Bei voller Datenkontrolle der einzelnen Nutzer_innen.

Potenzielle Risiken

Gamification in CSR birgt auch Risiken:

- **Wahrnehmung als manipulativ:** Wenn Gamification als Versuch wahrgenommen wird, Mitarbeiter_innen zu manipulieren, kann dies zu Widerstand führen.
- **Druck auf Mitarbeiter_innen:** Wenn Gamification-Ergebnisse mit Leistungsbewertungen verknüpft werden, kann dies zu ungesundem Druck führen.
- **Trivialisierung:** Schlecht gestaltete Gamification kann ernste CSR-Themen trivialisieren.
- **Datenschutzbedenken:** Die Erfassung von Daten für Gamification kann Datenschutzbedenken aufwerfen.

CSR und Zero-Knowledge Proofs

Zero-Knowledge Proofs adressieren eine der größten Herausforderungen in der CSR: das Vertrauensdefizit. Unternehmen machen oft kühne Behauptungen über ihre Nachhaltigkeitsbemühungen, aber Stakeholder_innen haben wenig Möglichkeiten, diese ohne aufdringliche Audits zu verifizieren. ZKPs ermöglichen ein neues Paradigma: “Beweise, behaupte nicht nur.”

Anwendungsbereiche

CSR-Bereich	ZKP-Anwendung	Was bewiesen wird	Was privat bleibt
Faire Löhne	Gehaltsverifizierung	Löhne erfüllen Mindeststandards	Genaue Gehaltsbeträge
Lieferkette	Ethische Beschaffung	Lieferant_innen erfüllen Kriterien	Lieferantenidentitäten

CSR-Bereich	ZKP-Anwendung	Was bewiesen wird	Was privat bleibt
Emissionen	CO2-Berichterstattung	Emissionen unter Schwellenwert	Betriebliche Details
Diversität	Belegschaftszusammensetzung	Diversitätsziele erreicht	Individuelle Demografien
Compliance	Regulatorische Einhaltung	Standards werden erfüllt	Interne Prozesse

Kurzfallstudien (zum besseren Verständnis): Faire-Lohn-Verifizierung

- **Traditioneller Ansatz** Im traditionellen Ansatz behauptet ein Unternehmen, faire Löhne zu zahlen. Auditor_innen benötigen Zugang zu allen Gehaltsdaten. Dies wirft Datenschutzbedenken für Mitarbeiter_innen auf und birgt das Risiko von Datenlecks.
- **ZKP-Ansatz** Mit ZKPs generiert das Unternehmen einen Beweis, dass alle Löhne einen Mindestschwellenwert überschreiten. Der oder die Verifizierer_in bestätigt die Gültigkeit des Beweises. Keine individuellen Gehaltsdaten werden preisgegeben. Es besteht mathematische Gewissheit der Compliance.

Fallstudie: Lieferkettentransparenz

- **Herausforderung** Ein Unternehmen möchte ethische Beschaffung nachweisen, ohne sein Lieferantennetzwerk preiszugeben.
- **ZKP-Lösung** Jeder Lieferant oder jede Lieferantin generiert einen Beweis der Compliance (Arbeitsstandards, Umweltpraktiken). Die Beweise werden aggregiert, ohne einzelne Lieferant_innen zu enthüllen. Der finale Beweis demonstriert, dass die gesamte Lieferkette die Standards erfüllt. Wettbewerber_innen können die Lieferantenbeziehungen nicht identifizieren.

Vorteile für CSR

- **Verifizierbare Behauptungen:** Stakeholder_innen können CSR-Berichten vertrauen, ohne blind glauben zu müssen.
- **Wettbewerbsschutz:** Compliance nachweisen, ohne Geschäftsgeheimnisse preiszugeben.
- **Reduziertes Greenwashing:** Kryptographische Verifizierung verhindert falsche Behauptungen.
- **Stakeholder-Vertrauen:** Vertrauen durch mathematischen Beweis aufbauen.
- **Regulatorische Compliance:** Offenlegungsanforderungen erfüllen und gleichzeitig Daten schützen.

Gamification und Zero-Knowledge Proofs

Die Kombination von Gamification und ZKP schafft Systeme, in denen Teilnehmer_innen Belohnungen und Anerkennung für ihre Leistungen verdienen können, ohne persönliche Daten oder sensible Informationen preiszugeben.

Gamification-Element	ZKP-Verbesserung
Erfolgsabzeichen	Erfolg beweisen, ohne zu enthüllen wie
Ranglisten	Teilnehmer_innen ranken, ohne Punktzahlen offenzulegen
Fortschrittsverfolgung	Fortschritt verifizieren, ohne Details preiszugeben
Belohnungen	Belohnungen beanspruchen ohne Identitätsoffenlegung
Wettbewerbe	Fairer Wettbewerb mit privaten Strategien

Datenschutzwahrende Gamification-Features

- **Anonyme Ranglisten:** Teilnehmer_innen beweisen, dass sie zu einer Ranking-Stufe gehören, ohne ihre genauen Punktzahlen preiszugeben. Man selbst, weiß wo man steht.
- **Verifizierbare Erfolge:** Abzeichen repräsentieren kryptographisch verifizierte Errungenschaften. Zusätzlich Abzeichen auf einer PoS Blockchain als NFT/Singleton Token speichern und ins Wallet der Nutzer_innen übertragen.
- **Privater Fortschritt:** Persönlicher Fortschritt wird verfolgt, ohne zentrale Datenerfassung.
- **Faire Belohnungen:** Belohnungen werden basierend auf verifizierten Kriterien verteilt, ohne Teilnehmerdaten offenzulegen.

Beweisgenerierung Der oder die Nutzer_in führt eine gamifizierte Aktion aus (z.B. reduziert Energieverbrauch). Das System generiert einen ZKP, dass die Aktion die Kriterien erfüllt. Der Beweis wird zur Verifizierung und Belohnung eingereicht.

Verifizierung Der oder die Verifizierer_in bestätigt die Gültigkeit des Beweises. Die Belohnung wird basierend auf dem verifizierten Beweis ausgegeben. Keine zugrunde liegenden Daten werden gespeichert oder übertragen.

Implementierungsbeispiel: Datenschutzwahrende Nachhaltigkeits-App

Ein konkretes Beispiel für die Integration von Gamification und ZKP ist eine mobile Nachhaltigkeits-App für Unternehmen. Die App ermöglicht es Mitarbeiter_innen, nachhaltige Verhaltensweisen zu dokumentieren und dafür Belohnungen zu erhalten, ohne dass das Unternehmen Zugang zu den persönlichen Daten der Mitarbeiter_innen hat.

Funktionsweise

Der oder die Mitarbeiter_in dokumentiert eine nachhaltige Aktion in der App, beispielsweise die Nutzung öffentlicher Verkehrsmittel statt des Autos. Die App generiert lokal auf dem Gerät des oder der Mitarbeiter_in einen Zero-Knowledge Proof, der bestätigt, dass die Aktion die definierten Kriterien erfüllt. Dieser Beweis wird an den Server des Unternehmens übermittelt, wo er verifiziert wird. Bei erfolgreicher Verifizierung werden dem oder der Mitarbeiter_in Punkte gutgeschrieben, die gegen Belohnungen eingetauscht werden können.

Datenschutzgarantien

Das Unternehmen erfährt zu keinem Zeitpunkt, welche spezifischen Aktionen der oder die Mitarbeiter_in durchgeführt hat. Es weiß nur, dass der oder die Mitarbeiter_in Aktionen durchgeführt hat, die die Nachhaltigkeitskriterien erfüllen. Die Standortdaten, Bewegungsprofile und anderen sensiblen Informationen verlassen niemals das Gerät des oder der Mitarbeiter_in.

Gamification-Elemente

Die App nutzt verschiedene Gamification-Elemente, um das Engagement zu fördern. Punkte werden für jede verifizierte nachhaltige Aktion vergeben. Abzeichen erkennen besondere Meilensteine an, wie "100 nachhaltige Aktionen" oder "1 Jahr Streak". Ranglisten zeigen die Leistung von Teams (nicht Einzelpersonen), um den Wettbewerb zu fördern, ohne die Privatsphäre zu gefährden. Herausforderungen bieten zeitlich begrenzte Ziele, die zusätzliche Belohnungen freischalten.

Das ZKPG+ Modell

Kernprinzipien

Das ZKPG+ Modell integriert die Konzepte von CSR, Gamification und ZKP in ein einheitliches Framework. Es wird durch das Konzept der Self-Sovereign Identity (SSI) ergänzt, wie es in der Dissertation von Pfeiffer (2025) beschrieben wird. Das SSI eID-Wallet ermöglicht es Nutzer_innen, ihre digitalen Identitäten und Nachweise selbst zu verwalten.

Die Kernprinzipien des Modells sind:

- **Ethische Grundlage (CSR):** Alle Aktivitäten sind in echten Nachhaltigkeits- und sozialen Verantwortungszielen verankert.
- **Engagierende Mechaniken (Gamification):** Teilnahme wird durch gut gestaltete Spielelemente und Belohnungen motiviert.
- **Privatsphäre-Wahrung (ZKP):** Verifizierung von Aktionen und Behauptungen erfolgt ohne Kompromittierung der individuellen oder organisatorischen Privatsphäre.
- **Nutzer_innen-Souveränität (SSI):** Nutzer_innen behalten weitgehende Kontrolle über ihre Daten und kryptographischen Nachweise.

Das ZKPG+ Modell ist ein Framework, das CSR, Gamification und Zero-Knowledge Proofs integriert. Es basiert auf drei Kernprinzipien:

- **Ethische Grundlage (CSR):** Alle Aktivitäten sind in echten Nachhaltigkeits- und sozialen Verantwortungszielen verankert.
- **Engagierende Mechaniken (Gamification):** Teilnahme wird durch gut gestaltete Spielelemente und Belohnungen motiviert.
- **Privatsphäre-Wahrung (ZKP):** Verifizierung von Aktionen und Behauptungen erfolgt ohne Kompromittierung der individuellen oder organisatorischen Privatsphäre.

Die Drei-Schichten-Architektur

Das Modell kann als Drei-Schichten-Architektur konzeptualisiert werden:

- **Schicht 1: CSR-Ziele** Diese Schicht definiert die Nachhaltigkeitsziele, ethischen Standards und Compliance-Anforderungen, die das System adressieren soll. Sie bildet das Fundament und den Zweck des gesamten Systems.
- **Schicht 2: Gamification-Engine** Diese Schicht bietet die nutzerorientierte Erfahrung, einschließlich Punkte, Abzeichen, Ranglisten, Herausforderungen und Narrative. Sie ist verantwortlich für das Engagement und die Motivation der Teilnehmer_innen.
- **Schicht 3: ZKP-Verifizierung** Diese Schicht handhabt die kryptographische Beweisgenerierung und -verifizierung. Sie stellt die Integrität des Systems sicher, ohne die Privatsphäre zu kompromittieren.

Datenflussmodell

Der Datenfluss im ZKPG+ Modell folgt einem klaren Muster:

- **Datenerfassung:** Sensible Daten werden lokal beim Nutzer oder bei der Nutzerin erfasst.
- **Beweisgenerierung:** Ein ZKP wird generiert, der die Erfüllung der CSR-Kriterien bestätigt.
- **Verifizierung:** Der Beweis wird von der Gamification-Engine verifiziert.
- **Belohnung:** Bei erfolgreicher Verifizierung werden Gamification-Belohnungen vergeben (via einer klassischen Datenbank, oder via

Blockchain oder einer Kombination)
- **Aggregation:** Verifizierte Beweise werden aggregiert, um organisationsweite CSR-Metriken zu generieren.

Vorteile des integrierten Modells

Das ZKPG+ Modell bietet zahlreiche Vorteile für alle Stakeholder_innen:

- **Für Unternehmen** Unternehmen profitieren von erhöhtem Engagement ihrer Mitarbeiter_innen und Kund_innen bei CSR-Initiativen. Die kryptographische Verifizierung ihrer CSR-Behauptungen stärkt ihre Glaubwürdigkeit und differenziert sie im Markt. Gleichzeitig schützen sie sensible Geschäftsdaten und erfüllen Datenschutzanforderungen.
- **Für Mitarbeiter_innen** Mitarbeiter_innen erleben CSR-Initiativen als engagierend und belohnend statt als Pflichtübung. Ihre Privatsphäre wird geschützt, da keine persönlichen Daten zentral gespeichert werden. Sie können ihre Beiträge zur Nachhaltigkeit nachweisen, ohne sensible Informationen preiszugeben.
- **Für Stakeholder_innen** Investor_innen, Kund_innen und Regulierungsbehörden können CSR-Berichten vertrauen, da sie kryptographisch verifiziert sind. Sie erhalten Transparenz über die Nachhaltigkeitsleistung, ohne dass sensible Unternehmensdaten offengelegt werden müssen.
- **Für die Gesellschaft** Das Modell fördert echte Nachhaltigkeit statt Greenwashing. Es schafft Anreize für verantwortungsvolles Unternehmenshandeln und trägt zur Lösung gesellschaftlicher Herausforderungen bei.

Technische Spezifikation

Empfohlenes Protokoll: zk-SNARKs

Für die meisten CSR-Gamification-Anwendungen empfehlen wir zk-SNARKs aufgrund ihrer:

- **Schnellen Verifizierungszeit:** Kritisch für Gamification-Anwendungen mit niedriger Latenz.
- **Kleinen Beweisgröße:** Ermöglicht effiziente Speicherung und Übertragung.
- **Reife Tooling-Landschaft:** Bibliotheken wie Circom, snarkjs und ZoKrates erleichtern die Implementierung.
- **Circuit-Design:** Für jeden CSR-Anwendungsfall muss ein spezifischer Circuit entworfen werden. Ein Beispiel für einen CO2-Reduktions-Circuit:
  - **Private Eingaben:** Tatsächliche CO2-Emissionen, Basiswert, Reduktionsprozentsatz.
  - **Öffentliche Eingaben:** Mindest-Reduktionsziel, Commitment zum Basiswert.
  - **Ausgabe:** Boolescher Wert (Ziel erreicht/nicht erreicht).

Schlussfolgerung

Das ZKPG+ Modell repräsentiert einen bedeutenden Fortschritt in der Evolution der Corporate Social Responsibility. Durch die Kombination der motivierenden Kraft der Gamification mit den vertrauensermöglichenden Fähigkeiten von Zero-Knowledge Proofs können Organisationen CSR-Initiativen schaffen, die nicht nur engagierender und effektiver sind, sondern auch transparenter und datenschutzwahrend.

Dieser integrierte Ansatz bietet einen Weg in eine Zukunft, in der unternehmerische Nachhaltigkeit nicht nur eine Behauptung, sondern eine verifizierbare Realität ist. Er fördert eine neue Ära des Vertrauens und der Verantwortlichkeit zwischen Unternehmen und ihren Stakeholder_innen.

Ausblick

Die Technologien, die dem ZKPG+ Modell zugrunde liegen, entwickeln sich rasant weiter.

Empfehlungen für die Implementierung

Für Unternehmen, die das ZKPG+ Modell implementieren möchten, empfehlen wir einen schrittweisen Ansatz:

Phase 1: Awareness und Bildung

Bevor technische Systeme implementiert werden, sollten Mitarbeiter_innen und Stakeholder_innen über die Konzepte von CSR, Gamification und Zero-Knowledge Proofs informiert werden. Das begleitende Kartenspiel “The Ethical Enabler” kann als effektives Schulungsinstrument dienen, um das Verständnis für diese komplexen Themen zu fördern.

Phase 2: Pilotprojekt

Beginnen Sie mit einem begrenzten Pilotprojekt, das einen spezifischen CSR-Anwendungsfall adressiert. Wählen Sie einen Bereich, in dem der Nutzen von Datenschutz und Verifizierung besonders offensichtlich ist, wie beispielsweise die Verifizierung fairer Löhne oder die Messung von CO2-Reduktionen.

Phase 3: Skalierung

Nach erfolgreicher Pilotierung kann das System schrittweise auf weitere Anwendungsbereiche ausgeweitet werden. Sammeln Sie kontinuierlich Feedback von Nutzer_innen und passen Sie die Gamification-Mechaniken entsprechend an.

Phase 4: Integration

Integrieren Sie das ZKPG+ System in bestehende CSR-Berichterstattungsprozesse und ESG-Frameworks. Nutzen Sie die verifizierten Daten für externe Kommunikation und Stakeholder-Engagement.

Herausforderungen und Lösungen

Bei der Implementierung des ZKPG+ Modells können verschiedene Herausforderungen auftreten:

- **Technische Komplexität** Zero-Knowledge Proofs sind technisch komplex. Lösung: Nutzen Sie bestehende Bibliotheken und Frameworks wie Circom, snarkjs oder ZoKrates, die die Implementierung vereinfachen.
- **Benutzerakzeptanz** Mitarbeiter_innen könnten skeptisch gegenüber neuen Systemen sein. Lösung: Betonen Sie die Datenschutzvorteile und gestalten Sie die Gamification-Elemente ansprechend und belohnend.
- **Skalierbarkeit** ZKP-Systeme können bei großen Datenmengen langsam werden. Lösung: Wählen Sie das richtige Protokoll (zk-SNARKs für schnelle Verifizierung, zk-STARKs für Skalierbarkeit) und optimieren Sie die Circuit-Designs.
- **Regulatorische Unsicherheit** Die regulatorische Anerkennung von ZKP-Beweisen ist noch nicht überall etabliert. Lösung: Arbeiten Sie proaktiv mit Regulierungsbehörden zusammen und dokumentieren Sie die Integrität Ihrer Systeme.

Das begleitende Kartenspiel "The Ethical Enabler" dient als wichtige Brücke zwischen Theorie und Praxis. Es ermöglicht es Teilnehmer_innen, die komplexen Konzepte des ZKPG+ Modells spielerisch zu erlernen und zu verinnerlichen. Das Spiel kann in verschiedenen Kontexten eingesetzt werden:

- **Mitarbeiter_innen-Schulungen:** Als interaktives Lerninstrument in Workshops und Seminaren.
- **Stakeholder-Engagement:** Um Investor_innen und Partner_innen die Konzepte zu vermitteln.
- **Universitäre Lehre:** Als Lehrmaterial in Kursen zu CSR, Kryptographie oder Gamification.
- **Team-Building:** Als kooperatives Spiel, das Zusammenarbeit und gemeinsames Lernen fördert. Mit der zunehmenden Reife von ZKP-Protokollen und der wachsenden Akzeptanz von Gamification in Unternehmenskontexten erwarten wir eine breitere Adoption dieses integrierten Ansatzes.

Zukünftige Entwicklungen könnten umfassen:

- **Standardisierung:** Die Entwicklung von Industriestandards für ZKP-basierte CSR-Verifizierung.
- **Interoperabilität:** Systeme, die es ermöglichen, ZKP-Beweise über Organisationsgrenzen hinweg zu verifizieren.
- **Regulatorische Integration:** Die Anerkennung von ZKP-Beweisen durch Regulierungsbehörden als gültige Form der Compliance-Dokumentation.
- **Erweiterte Gamification:** Fortgeschrittenere Gamification-Mechaniken, die tiefere Verhaltensänderungen fördern.

Das ZKPG+ ist nicht nur ein theoretisches Konzept, sondern ein praktischer Rahmen, der bereits heute implementiert werden kann. Wir laden Unternehmen,

Forscher_innen und Entwickler_innen ein, diesen Ansatz zu erkunden und zur Weiterentwicklung beizutragen.

Wir freuen uns unter Feedback an: office@limesoda.com und/oder alexander.pfeiffer@donau-uni.ac.at

Literatur

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. (2014). Succinct non-interactive zero- knowledge for a von Neumann architecture. In Proceedings of the 23rd USENIX Security Symposium.

Bogensperger, A., & Zeiselmeier, A. (n.d.). Blockchain deep dives: Zero-knowledge proofs. Forschungsstelle für Energiewirtschaft.

https://www.ffe.de/veroeffentlichungen/beitragsreihe-blockchain-deep-dives-zero-knowledge-proofs/

Bowen, H. R. (1953). Social responsibilities of the businessman. Harper & Row.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. Business Horizons, 34(4), 39–48.

https://doi.org/10.1016/0007-6813(91)90005-G

Chainlink. (2024). Zero-knowledge proof (ZKP) — explained.

https://chain.link/education/zero-knowledge-proof-zkp

Chou, Y.-k. (2016). Actionable gamification: Beyond points, badges, and leaderboards. Octalysis Media.

Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. Psychological Inquiry, 11(4), 227–268.

https://doi.org/10.1207/S15327965PLI1104_01

Elkington, J. (1997). Cannibals with forks: The triple bottom line of 21st century business. Capstone.

Global Reporting Initiative. (2021). GRI 1: Foundation 2021.

https://globalreporting.org/standards/

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 186–208.

https://doi.org/10.1137/0218012

Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does gamification work? A literature review of empirical studies on gamification. In Proceedings of the 47th Hawaii International Conference on System Sciences (pp. 3025–3034). IEEE.

https://doi.org/10.1109/HICSS.2014.377

KPMG. (2024). Survey of sustainability reporting 2024: The move to mandatory reporting.

https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2024/11/the-move-to-mandatory-reporting-report.pdf

Mayo, M. J. (2009). Video games: A route to large-scale STEM education? Science, 323(5910), 79–82.

https://doi.org/10.1126/science.1166900

Pfeiffer, A. (2018). Auf dem Weg zur ludischen Gesellschaft: Über den Stellenwert von Spiel und spielähnlichen Prozessen (Doctoral dissertation, Wirtschaftsuniversität Wien).

Pfeiffer, A. (2025). Blockchain technologies and their impact on game-based education and learning assessment (Doctoral dissertation, University of Malta). University of Malta Open Access Repository.

https://www.um.edu.mt/library/oar/handle/123456789/140713

Pfeiffer, A., Wernbacher, T., & Vella, V. (2024). Blockchain in der schulischen Bildung als Teil des Bildungswesens: Einsatz von Blockchain-Technologien in Gamification und Serious Games. In W. Becker & M. Metz (Eds.), Serious games und gamification in der schulischen Bildung. Springer VS.

https://doi.org/10.1007/978-3-658-44317-7_4

Quisquater, J.-J., Quisquater, M., Quisquater, M., Quisquater, M., Guillou, L., Guillou, M. A., Guillou, S. (1989). How to explain zero-knowledge protocols to your children. In G. Brassard (Ed.), Advances in cryptology — CRYPTO '89 proceedings (Lecture Notes in Computer Science, Vol. 435, pp. 628–631). Springer.

https://doi.org/10.1007/0-387-34805-0_60

Smartico.ai. (2025). Gamification in corporate social responsibility.

https://www.smartico.ai/blog-post/gamification-in-corporate-social-responsibility

The Satell Institute. (2025, October 20). A history of corporate social responsibility: Concepts and practices.

https://www.satellinstitute.org/whitepapers/a-history-of-corporate-social-responsibility-concepts-and-practices

Werbach, K., & Hunter, D. (2012). For the win: How game thinking can revolutionize your business. Wharton Digital Press.

Wouters, P., van Nimwegen, C., van der Spek, E. D., & van Oostendorp, H. (2013). A meta- analysis of the cognitive and motivational effects of serious games. Journal of Educational Psychology, 105(2), 249–265.

https://doi.org/10.1037/a0031311

Yee, N. (2006). The demographics, motivations, and derived experiences of users of massively multi-user online graphical environments. Presence: Teleoperators and Virtual Environments, 15(3), 309–329.

https://doi.org/10.1162/pres.15.3.309

Anhang: Das Kartenspiel (zur eigenen Verwendung)

Siehe: www.zkp-gamification.com

CSR-Herausforderungskarten (Challenge Cards)

Nr.	Fokus	Titel	Herausforderung
C-01	Sozial	Gleiche Bezahlung beweisen	Das Unternehmen möchte öffentlich beweisen, dass es die Gender-Pay-Gap geschlossen hat, ohne die individuellen Gehälter der Mitarbeiter_innen offenzulegen.
C-02	Umwelt	Fälschungssichere CO2-Bilanz	Ein Zulieferer behauptet, seine Produktion sei CO2-neutral. Wie kann das Unternehmen diese Behauptung lückenlos, transparent und manipulation-ssicher in seine eigene Bilanz übernehmen?

Nr.	Fokus	Titel	Herausforderung
C-03	Governance	Mitarbeiter_innen-Engagement für Nachhaltigkeit	Das Unternehmen möchte seine Mitarbeiter_innen spielerisch dazu motivieren, den Energieverbrauch im Büro zu senken. Wie kann dieses Engagement gemessen und belohnt werden, ohne die Privatsphäre der Einzelnen zu verletzen?
C-04	Sozial	Transparente Spendenkette	Ein Unternehmen möchte eine Spendenaktion durchführen und den Spender_innen garantieren, dass 100% der Gelder den Endempfänger oder die Endempfängerin erreichen und der Prozess manipulationssicher ist.
C-05	Umwelt	Ethische Rohstoffherkunft	Wie kann ein Unternehmen die Herkunft von seltenen Erden in seinen Produkten belegen, um Kinderarbeit auszuschließen, ohne sensible Lieferanten-verträge offenzulegen?

Nr.	Fokus	Titel	Herausforderung
C-06	Governance	Whistleblower-Schutz	Wie kann ein internes System eingerichtet werden, das Mitarbeiter_innen ermöglicht, Missstände anonym zu melden, wobei die Gültigkeit der Meldung verifiziert werden kann?
C-07	Sozial	Mitarbeiter_innen-Weiterbildung	Wie motiviert man Mitarbeiter_innen spielerisch, sich in Nachhaltigkeits-themen weiterzubilden, und wie kann der Lernerfolg daten-schutzkonform nachgewiesen werden?
C-08	Umwelt	Reduzierung des Wasserverbrauchs	Ein Produktionsbe-trieb möchte den Wasserverbrauch durch Gamification senken. Wie kann der Erfolg gemessen werden, ohne die detaillierten Produktionsdaten der einzelnen Abteilungen zu zentralisieren?

Nr.	Fokus	Titel	Herausforderung
C-09	Governance	Audit-Nachweis	Ein externer Auditor oder eine externe Auditorin verlangt den Nachweis, dass alle Datenzugriffe im letzten Quartal dem “Need to Know”-Prinzip entsprachen.
C-10	Sozial	Altersverifikation ohne ID	Ein Online-Dienst möchte sicherstellen, dass seine Nutzer_innen volljährig sind, ohne eine Kopie des Personalausweises zu speichern.
C-11	Umwelt	Grünes Investment-Tracking	Wie kann ein Investor oder eine Investorin die Einhaltung von ESG-Kriterien in seinem oder ihrem Portfolio transparent und unveränderlich nachverfolgen?
C-12	Governance	Dezentrale Entscheidungsfindung	Ein Unternehmen möchte seine Mitarbeiter_innen in CSR-Entscheidungen einbinden, wobei die Abstimmungsergebnisse transparent und fälschungssicher sein müssen.

Nr.	Fokus	Titel	Herausforderung
C-13	Sozial	Gesundheitsdaten-Sharing	Ein Forschungsprojekt benötigt aggregierte Gesundheitsdaten zur Analyse von Umwelteinflüssen, aber die individuellen Daten müssen geschützt bleiben.
C-14	Umwelt	Recycling-Anreize	Wie kann ein Belohnungssystem für das korrekte Recycling von Verpackungen implementiert werden, das die Menge des recycelten Materials fälschungssicher erfasst?
C-15	Governance	Compliance-Training	Wie kann ein Compliance-Training gamifiziert werden, um die Teilnahmequote zu erhöhen, und wie wird der erfolgreiche Abschluss fälschungssicher dokumentiert?

Nr.	Fokus	Titel	Herausforderung
C-16	Sozial	Fair-Trade-Zertifizierung	Ein kleines Unternehmen möchte seine Fair-Trade-Zertifizierung beweisen, ohne seine gesamte Kundenliste oder seine Einkaufspreise offenzulegen.
C-17	Umwelt	Energieeffizienz-Wettbewerb	Wie kann ein Wettbewerb zwischen verschiedenen Standorten zur Energieeinsparung durchgeführt werden, bei dem die Verbrauchsdaten nur minimal offengelegt werden?
C-18	Governance	Zugriffskontrolle	Wie wird sichergestellt, dass nur die IT-Sicherheitsabteilung Zugriff auf die vollständigen Protokolle der Datenzugriffe hat, aber die Compliance-Abteilung die Einhaltung des Need-to-Know-Prinzips prüfen kann?

Nr.	Fokus	Titel	Herausforderung
C-19	Sozial	Anonyme Feedback-Kultur	Wie kann ein System für anonymes Mitarbeiter_innen-Feedback implementiert werden, das die Echtheit der Person verifiziert, ohne die Identität preiszugeben?
C-20	Umwelt	Nachhaltige Beschaffung	Wie kann ein Unternehmen beweisen, dass 80% seiner Beschaffung von nachhaltig zertifizierten Lieferant_innen stammt, ohne die Zertifikate jedes einzelnen Lieferanten oder jeder einzelnen Lieferantin zu veröffentlichen?

Technologie-Karten (Solution Cards)

Technologie	Titel	Konzept	Nutzen für CSR
Blockchain	Unveränderliches Register	Ein dezentrales, verteiltes und kryptografisch gesichertes Register, das Transaktionen in Blöcken speichert.	**Transparenz & Vertrauen:** Ermöglicht die fälschungssichere Dokumentation von Lieferketten oder Spendenzwecken.

Technologie	Titel	Konzept	Nutzen für CSR
Zero Knowledge Proofs	Beweisen ohne Wissen	Ein kryptografisches Protokoll, das die Gültigkeit einer Aussage beweist, ohne die zugrundeliegenden Daten preiszugeben.	**Datenschutz & Verifizierung:** Ermöglicht die datenschutzkonforme Offenlegung von sensiblen Daten.
Need to Know	Datenminimierung	Ein Architekturprinzip, das den Datenzugriff auf das absolute Minimum beschränkt, das zur Aufgabenerfüllung notwendig ist.	**Datensicherheit:** Reduziert das Risiko von Datenlecks und Missbrauch.
Gamification	Spielerische Motivation	Anwendung von Spielelementen (Punkte, Badges, Leaderboards) in spielfremden Kontexten zur Förderung von Engagement und Verhaltensänderung.	**Engagement:** Erhöht die Beteiligung an CSR-Initiativen.

Schnittstellenkarten (Quiz Cards) - Auszug

Nr.	Frage	Antwort
Q-01	Wie kann Gamification CSR-Initiativen unterstützen?	Gamification kann CSR-Initiativen unterstützen, indem sie Nachhaltigkeitsziele in ansprechende, messbare und belohnende Erfahrungen verwandelt.

Nr.	Frage	Antwort
Q-02	Was ist der Hauptvorteil von Zero-Knowledge Proofs für CSR?	ZKPs ermöglichen es, die Wahrheit einer Aussage zu beweisen, ohne sensible Daten preiszugeben – ideal für Compliance-Nachweise.
Q-03	Wie unterstützt Blockchain die Transparenz in der Lieferkette?	Blockchain ermöglicht die unveränderliche Aufzeichnung aller Transaktionen und Zertifizierungen entlang der Lieferkette.
Q-04	Was ist das Need to Know-Prinzip?	Das Need to Know-Prinzip besagt, dass Personen nur Zugang zu den Informationen haben sollten, die sie für ihre Aufgaben benötigen.
Q-05	Welche Gamification-Elemente fördern intrinsische Motivation?	Narrative, Autonomie, Kompetenzentwicklung und soziale Verbundenheit fördern intrinsische Motivation.

Lernkarten (Flashcards) - Auszug

Nr.	Frage (Vorderseite)	Antwort (Rückseite)
L-01	Was ist Corporate Social Responsibility (CSR)?	CSR ist die Verantwortung von Unternehmen, über ihre wirtschaftlichen und rechtlichen Pflichten hinaus einen positiven Beitrag zur Gesellschaft und Umwelt zu leisten.
L-02	Was ist die Triple Bottom Line?	Ein Konzept, das argumentiert, dass Unternehmen ihren Erfolg an Profit, People und Planet messen sollten.

Nr.	Frage (Vorderseite)	Antwort (Rückseite)
L-03	Was ist Gamification?	Die Anwendung von Spieldesign-Elementen in zumeist spielfremden Kontexten zur Förderung von Engagement und Motivation.
L-04	Was sind die drei Grundbedürfnisse nach SDT?	Autonomie, Kompetenz und Verbundenheit.
L-05	Was ist ein Zero-Knowledge Proof?	Eine kryptographische Technik, die es ermöglicht, die Wahrheit einer Aussage zu beweisen, ohne dabei zusätzliche Informationen preiszugeben.
L-06	Was sind zk-SNARKs?	Succinct Non-interactive Argument of Knowledge – eine ZKP-Implementierung mit kleinen Beweisgrößen.
L-07	Was ist eine Blockchain?	Ein verteiltes, unveränderliches Ledger, das Transaktionen über ein Netzwerk von Computern aufzeichnet.
L-08	Was ist das Need to Know-Prinzip?	Ein Grundsatz der Informationssicherheit, der besagt, dass Personen nur Zugang zu notwendigen Informationen haben sollten.