
HÄRTING

Der CISO im Metaverse

RAin lic. iur. Nicole Beranek Zanon, Exec. MBA HSG, CIPE/E



AGENDA

1. Metaverse + Stakeholder
2. Blockchain + NFT
3. Kauf von Land im Metaverse
4. Allg. Hacking auf der Blockchain
5. Hacking von Wallets
6. Blockchain Domain-Namen und Cybersquatting
7. Rechtliche Themen
8. Rechtsdurchsetzung

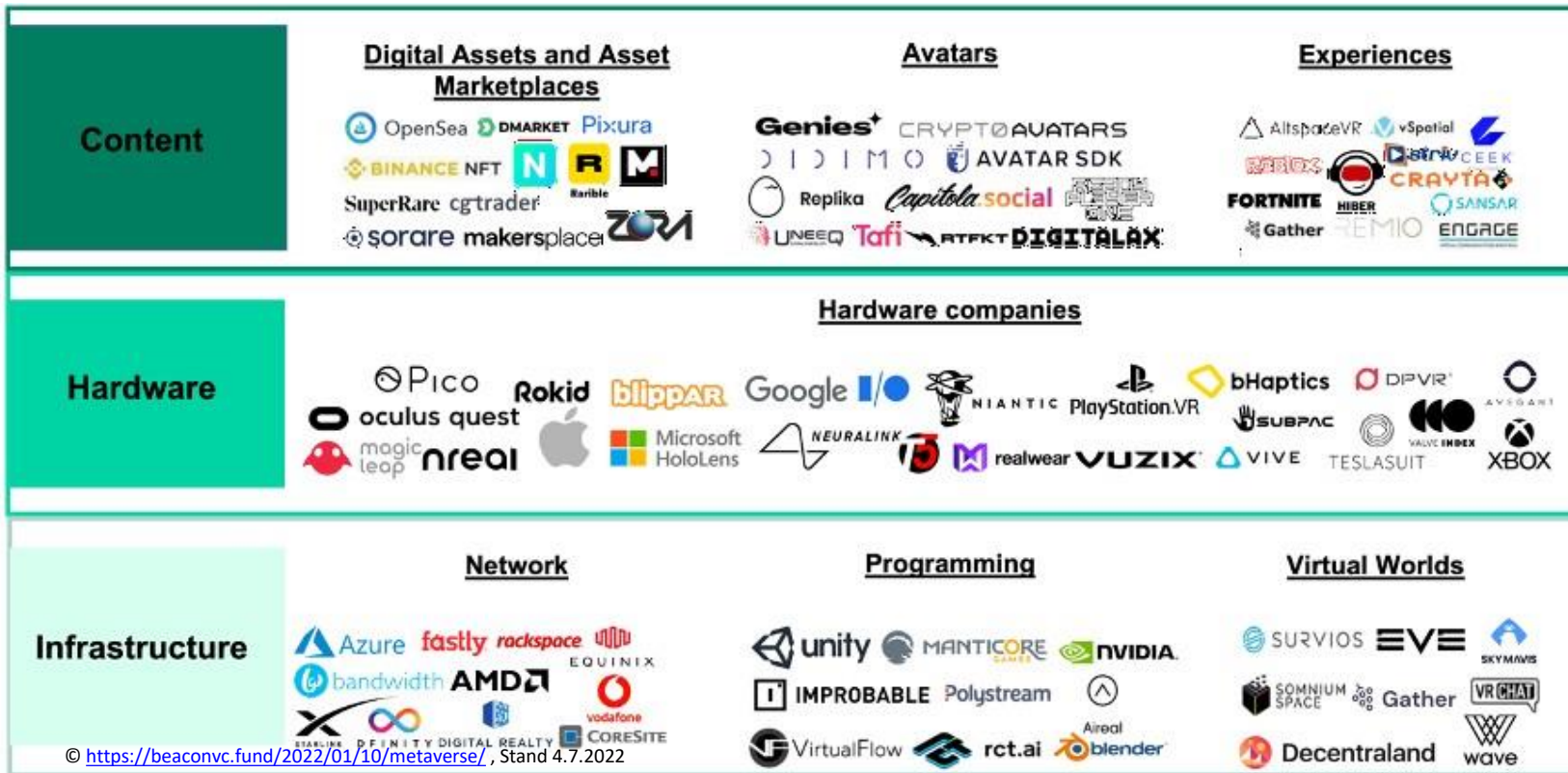
1. Metaverse + Stakeholder



WAS IST DAS METAVERSE?

- Verknüpfung von realem Leben mit mehr Technologie
- Digitale Welt, die von uns als echte Individuen kontrolliert und geformt wird
- Dazu gehören:
 - Virtuelle Welten (wo gearbeitet und gespielt werden kann)
 - Technologien wie VR-Headsets und Kryptowährungen
- Hat seine eigene Wirtschaft, Firmen und Individuen können investieren, kaufen und verkaufen
- Kann nicht beendet oder pausiert werden

STAKEHOLDER DES METAVERSE



© <https://beaconvc.fund/2022/01/10/metaverse/>, Stand 4.7.2022

2. Blockchain + NFT's



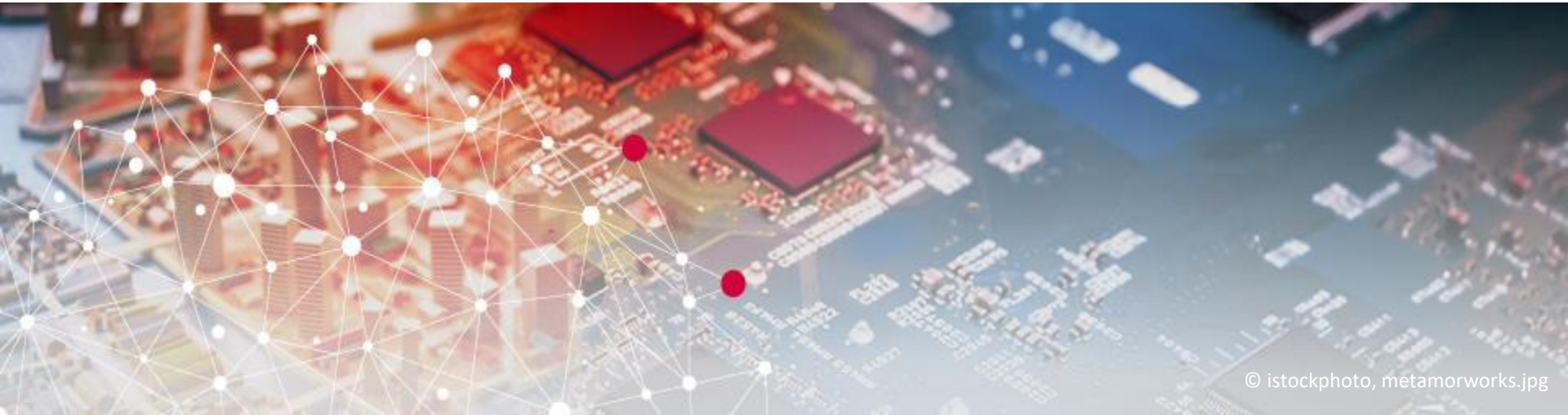
BLOCKCHAIN + NFT'S

- Dezentrale Datenbank in einzelne Blöcke gegliedert – Blöcke nach Konsensverfahren erstellt und an Kette angehängt
- Informationen werden fälschungssicher übermittelt
- Non Fungible Tokens (NFT`s) werden dabei als Vermögenswerte genutzt
- Ein Token repräsentiert ein Vermögensgegenstand oder Wirtschaftsgut
- Er ist einzigartig

NFT'S - ANWENDUNGSBEREICHE

- digitale Sammelkarten
- Spielecharaktere
- virtuelle Landstriche in virtuellen Welten
- Krypto-Kunst
- Personalausweise
- Impfpässe
- Andere wichtige Dokumente
- Echtheitszertifikat für physisches Gut

3. Kauf von Land im Metaverse



IDENTIFIKATION

- Mehrere Webseiten bieten den Verkauf von Land an (beispielsweise Plattformen wie Decentraland und Sandbox)
- Abwicklung des Kaufes unterscheidet sich nur minimal von Anbieter zu Anbieter
- Meistens Erstellung eines Accounts notwendig
- Metaverse-Landparzellen sind technisch gesehen NFT`s, welche auf der Blockchain vermerkt werden

IDENTIFIKATION

- Für den Kauf von Land im Metaverse braucht es:
 1. Crypto-Wallet: muss mit dem Account verbunden sein
 2. Passende Kryptowährung
- Bei gehosteten Wallets müssen für die Erstellung des Kontos persönliche Angaben eingegeben werden (Custodial Wallets)
- Bei Self-Custody Wallets sind keine persönlichen Angaben erforderlich (nicht mal eine Mailadresse)
- Jedes Wallet besitzt **einen individuellen privaten und öffentlichen Schlüssel**, der zur Identifikation auf der Blockchain dient, dies bezieht sich auch auf den Kauf von Land im Metaverse

IDENTIFIKATION

- Während der Wahl einer Parzelle im Metaverse, ist der Preis, Gesamtgrösse und Besitzer ersichtlich
- Nach dem Kauf wird die **Eigentumsurkunde** als solche auf einer Blockchain vermerkt
- Die Blockchain wird mit gültigen digitalen Schlüsseln erzeugt
- Der öffentliche Schlüssel gleicht einer Bankkontonummer und der private Schlüssel einem geheimen Pin
- Die Schlüssel werden in der Wallet-Datei gespeichert und von der Bitcoin-Wallet-Software verwaltet

4. Allgemeines zu Hacking von Blockchains



METHODEN VON HACKERN

- **Phishing:** betrügerischer Versuch, um an Anmeldeinformationen von Benutzer zu kommen mittels Sendung von E-Mails
- **Routing:** Hacker fangen Daten ab, während der Übertragung an Internet-Service-Provider, vertrauliche Daten oder Währungen werden extrahiert, ohne dass Blockchain-Teilnehmer etwas merkt
- **Sybil-Angriffe:** viele falsche Netzidentitäten werden erstellt und verwendet mit dem Ziel, das System zum Absturz zu bringen.
- **51%-Angriffe:** Miner sammelt genügend Ressourcen, erreicht mehr als 50% der Mining-Leistung eines Blockchain-Netzes und hat so die Kontrolle über das Ledger, kann es auch manipulieren, keine Gefahr besteht hierbei für private Blockchains

HACKER ANGRIFF AUF NFT-CLUB

- Durch fortschreitende Technologie und Digitalisierung, immer mehr Betrüger
- Auch in Bereich von NFT können sich Hacker durch Phishing Zugang zu Daten verschaffen, auch durch Ausfindig machen von Sicherheitslücken
- Hacker erlangte kürzlich Zugriff auf BAYCs (Bored Ape Yacht Club) Instagram Account → Schutz der Blockchain konnte so umgangen werden Hacker postete auf Instagram Links, die zu einem gefälschten Airdrop führten, wo Nutzer ihre Daten preisgegeben haben → Zugriff auf Wallets und Entnahme von NFTs im Wert von mehreren Millionen

5. Hacking von Wallets



HACKING VON WALLETS

- Sicherheitsmassnahmen sind nicht dem neuesten Stand der Technik angepasst → Diebstahl von Kryptowährung wird begünstigt
- Dabei geht es oft um immense Summen z.B. Hack des Poly-Netzwerks, wo 600 Millionen Dollar gestohlen wurden
- Hacker können dabei mit internen Tools und Phishing-Versuche vorgehen z.B Hackerattacke auf Plattform MailChimp
- Hacker nutzen dabei erhaltene Infos um gefälschte Mails zu versenden → Benutzer mussten persönliche Informationen angeben, haben Schadsoftware heruntergeladen und Vermögenswerte wurden gestohlen

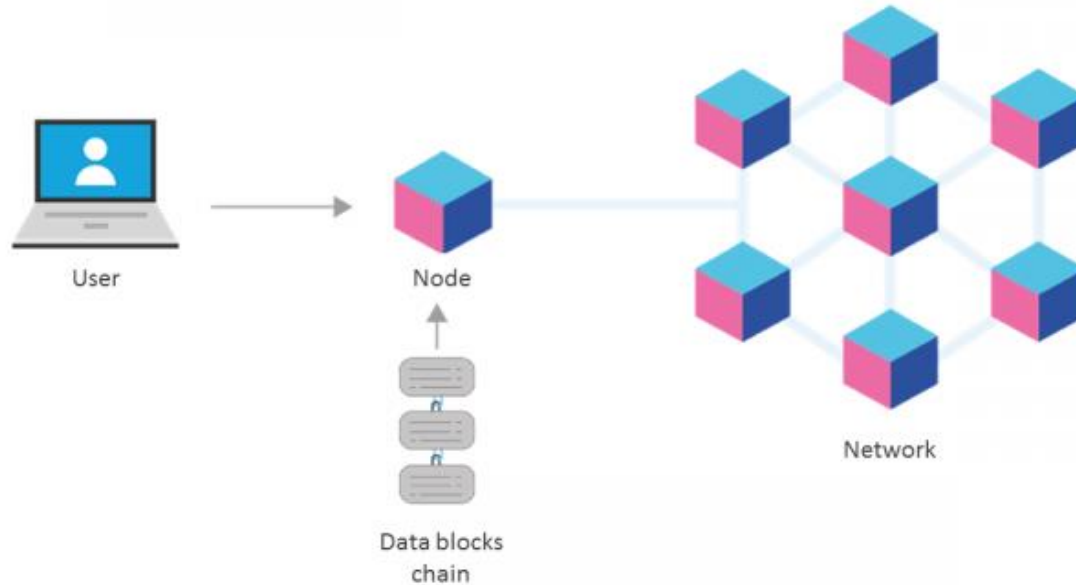
MASSNAHMEN NACH EINER HACKING-ATTACKE

- Änderung der Anmeldedaten: Passwort und andere Sicherheitsdetails sind zurückzusetzen, falls noch ins Konto eingeloggt werden kann
- Wallet-Anbieter benachrichtigen: sofern Token auf online-Plattform gespeichert sind
 - Nach dem Hack: hilft bei den Ermittlungen indem betrügerische Transaktionen aufgedeckt werden
 - Während dem Hack: Aktion kann gestoppt werden und Geldanteile können zurückgewonnen werden
- Neue Wallet erstellen: einzelner Hack macht Wallet anfällig für zukünftige Angriffe → Entsorgung der alten Wallet und Erstellung einer Neuen

6. Blockchain Domain-Names Cybersquatting



FUNKTIONSWEISE/ NUTZEN DER BLOCKCHAIN-DOMAIN



CYBERSQUATTING

- Durch Cybersquatting wird eine Person oder Firma imitiert und deren Name als Domäne verwendet
- Der verletzte Name wird verwendet, um beispielsweise Kunden zu verwirren, zu fälschen oder zu betrügen

7.

Rechtliche Themen



RECHTLICHE THEMEN

Beispiel: Im Metaverse baut x eine Bank y. Die y ist eine Weltweit tätige Bank. Die y Bank tauscht NFT's im Metaverse gegen Cryptocurrencies oder allg. Digitale Assets

Quid?

- Nationale Gesetzte
- Keine Monitoring-Dienste im Metaverse, keine Governance, wenig Self Regulation (via z.T. DAO's)
- Identität von x als Landerwerber oder Wallet-Inhaber oft nicht möglich, da fehlende KYC
- Firmenrechtsverletzung
- Design-Verletzung

DATENSCHUTZ

- Metaverse sorgt für Herausforderung für Datenschutz, weil umfassende Sammlung verschiedener personenbezogener Daten
- Institutionen erhalten neue Arten von Informationen über Einzelpersonen wie z. B. ihre Bewegungen, Handlungen oder Gewohnheiten
- Konsumverhalten kann tiefer analysiert werden

IMMATERIALGÜTERRECHTE

- Im Metaverse werden neue Dinge geschaffen (meist im Kollektivum)
- gemeinsame Inhaberschaft erweist sich als kompliziert
- Wem gehören die geschaffenen Rechte z.B ein Patentrecht?
- Europäische Kommission strebt Reform in Bezug auf gemeinsam geschaffenes geistiges Eigentum in Verbindung mit neuen Technologien an
- Wie wird eine Marke in virtueller Umgebung geschützt?
- Kann ein Möbelhersteller seine Designrechte auch im Metaverse geltend machen? erste namhafte Modebrands haben ihr Schutz auf digitale Güter erweitert oder verkaufen digitale Güter z.B. Sneaker werden im Metaverse als 3D-Objekte modelliert und virtuell getragen

FIRMENRECHT / PERSÖNLICHKEITSSCHUTZ

- Können Unternehmen den von ihnen für den Handelsverkehr gewählten Name im Metaverse schützen lassen?
- Beim Handel mit NFT kommt die Frage auf, ob es Erlaubnis- und Prospektpflichten für den Handel von digitalen Gütern gibt
- ob blockchainbasierte Token wie NFT tatsächlich Eigentum im Sinne des Rechts sein können, darüber wird allerdings noch immer diskutiert
- Können berühmte Personen im Metaverse eine Persönlichkeitsverletzung geltend machen, falls Avatare ihren Namen tragen oder ähnlich aussehen?

WETTBEWERBSRECHT

- Metaverse muss nahtlos gestaltet werden → verschiedene Unternehmen müssen kommunizieren, zusammenarbeiten und sicherstellen, dass die Plattformen kompatibel sind → kartellrechtlichen Probleme
- Preisgestaltung oder Vereinbarung über Entwicklung bestimmter Bereiche führen zu Wettbewerbsverstöße
- Lösung: Richtlinien, Schulungsprogramme sowie Kontrollmechanismen sind von Nöten

8. Rechtsdurchsetzung im Metaverse



RECHTSDURCHSETZUNG

- Wallet-Inhaber bei Self-Custodian fast nicht ermittelbar
- Kaskadenhaftung von Providern: keine ausdrückliche Regelung im StGB
- Content-Provider (Anbieter der Medieninhalten (Universum) wie z.B. meta oder decentraland) bei Haftung im Fokus, Haftung von Access-Provider (Browseranbieter) zweitrangig
- Bei Kenntnisnahme (z.B. wegen Hinweis von Strafverfolgungsbehörde) ist Zusammenarbeit mit Strafverfolgungsbehörden notwendig

RECHTSDURCHSETZUNG

- Hoster: Hosting der Websites auf IPFS -> Protocol Labs
<https://protocol.ai/about/>
- «Registry»
 - ENS: Registrierung von Domain-Namen -> Fehlender Schutz von Namensrechten
 - Untoppable domains: Registrierung von Domain-Namen -> Namensschutz für Marken, Organisationen oder bekannte Persönlichkeiten durch Liste mit „protected domains“
 - Handshake: Registrierung von Domains -> Namensschutz durch Ausschluss der 1500 DNS TLD's und der 100'000 meistbesuchten Domain-Namen

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT



© Alle Rechte an dieser Präsentation gehören der HÄRTING Rechtsanwälte AG. Jegliche Nutzung dieser Präsentation ohne unsere Zustimmung ist nicht gestattet. Dies gilt insbesondere für Vervielfältigungen (grafisch, technisch, elektronisch und/oder digital, einschliesslich Fotokopien, Down- und Uploads), Übersetzungen und die Speicherung und Verarbeitung in und mit elektronischen Systemen. Jede Verwendung in den vorgenannten Fällen oder in anderen als den gesetzlich zulässigen Fällen bedarf der vorherigen schriftlichen Zustimmung der HÄRTING Rechtsanwälte AG. Diese Präsentation ist keine Rechtsberatung und ersetzt eine solche in keinem Fall.



Nicole Beranek Zanon

Partnerin | Notarin | Exec. MBA HSG



Paula Zimmermann

Rechtsanwältin



Roman Rey

Rechtsanwalt | Musiker



Ursina Eichenberger

Juristin



Olivia Boccali

Juristin



Dominic Grunder

Studentischer Mitarbeiter



Cedric Bamert

Studentischer Mitarbeiter



Christine Grass

Zentrale

HÄRTING 

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1

6300 Zug

Switzerland

Tel. +41 41 710 28 50

www.haerting.ch

beranek@haerting.ch

Agenda

- 14:30 *Eintreffen der Teilnehmer/innen*
- 15:15 **Begrüssung**
Michel Geelhaar (Moderator) & Arié Malz (ISSS-Präsidium)
- 15:25 **Security als Gemeinschaftswerk – wie man zukünftige Bedrohungen dezentral mitigieren kann**
Raphael Marques, Head Security Management, Migros-Genossenschafts-Bund
- 15:50 **Vom Backup zum Digitalen Leader – Die Zukunft der CISO Rolle**
Reto Zeidler, Head of Information and Cyber Security, Pragmatica
- 16:15 **Lights and Shadows in Deep Learning**
Alessandro Antonucci, Senior Lecturer-Researcher, IDSIA Dalle Molle Institute for AI, USI-SUPSI
- 16:40 **Digital Ethics: Who, What, Where, How – Why?"**
Yanya Viskovich, Chair of the Cyber Law and Governance Workgroup of the Swiss Cyber Institute
- 17:20 *Pause & Networking*
- 17:50 **Der CISO im Metaverse**
Nicole Beranek Zanon, Managing Partnerin HÄRTING Rechtsanwälte AG
- 18:10 Podiums Diskussion – moderiert von Michael Geelhaar**
- 18.45 *Apéro & Networking*

Podiumsdiskussion



Michel Geelhaar (Moderator)
Strategie- und Organisations-
entwickler



Nicole Beranek Zanon
Managing Partnerin
HÄRTING Rechtsanwälte AG



Raphael Marques
Head Security Management
Migros-Genossenschafts-Bund



Alessandro Antonucci
Senior Lecturer-Researcher
IDSIA Institute for Artificial
Intelligence, USI-SUPSI



Yanya Viskovich
Chair of the Cyber Law and
Governance Workgroup of the
Swiss Cyber Institute



Reto Zeidler
Head of Information and Cyber
Security Pragmatica

Agenda

- 14:30 *Eintreffen der Teilnehmer/innen*
- 15:15 **Begrüssung**
Michel Geelhaar (Moderator) & Arié Malz (ISSS-Präsidium)
- 15:25 **Security als Gemeinschaftswerk – wie man zukünftige Bedrohungen dezentral mitigieren kann**
Raphael Marques, Head Security Management, Migros-Genossenschafts-Bund
- 15:50 **Vom Backup zum Digitalen Leader – Die Zukunft der CISO Rolle**
Reto Zeidler, Head of Information and Cyber Security, Pragmatica
- 16:15 **Lights and Shadows in Deep Learning**
Alessandro Antonucci, Senior Lecturer-Researcher, IDSIA Dalle Molle Institute for AI, USI-SUPSI
- 16:40 **Digital Ethics: Who, What, Where, How – Why?"**
Yanya Viskovich, Chair of the Cyber Law and Governance Workgroup of the Swiss Cyber Institute
- 17:20 *Pause & Networking*
- 17:50 **Der CISO im Metaverse**
Nicole Beranek Zanon, Managing Partnerin HÄRTING Rechtsanwälte AG
- 18:10 **Podiums Diskussion – moderiert von Michael Geelhaar**
- 18.45 *Apéro & Networking***

**Herzlichen Dank
für Ihre Teilnahme!**



22