swiss financial
innovation desk

Pathway 2035 for Financial Innovation

Your Navigator

Version 1.0.2 | January 2025

Publisher
Swiss Financial Innovation Desk (FIND)

Concept
Eva Selamlar-Leuthold

Content
FIND, authors and contributors as listed in each chapter

Review Board
Claudia Grisard Barbour
Johs. Hoehener
Eva Selamlar-Leuthold

Layout
André Lergier

Illustration
imavox

Cover Image
Augstmatthorn (Switzerland) by Kimon Maritz

Proofreading
Vénusia Bertin

Contact
info@find.swiss

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

FIND promotes financial innovation in Switzerland and thus contributes to strengthening Switzerland as one of the world's leading financial centres. It operates as an independent unit within the State Secretariat for International Finance of the Federal Department of Finance.

Setting the Scene

Switzerland's legacy of neutrality, innovation and international dialogue plays a pivotal role in driving inclusive, cross-border opportunities and partnerships that foster financial transformation. On 5 November 2024, the *Redesigning Financial Innovation* event and working sessions were hosted by the Swiss Embassy in Singapore and curated by the Swiss Financial Innovation Desk (FIND). A group of remarkable global leaders from finance, technology, academia and policymakers met and committed to exploring the anticipated key markers reshaping the financial landscape in the next decade. "Thank You" to the originators, hosts, curators, supporters, contributors and participants whose efforts made possible the "Pathway 2035 for Financial Innovation - Your Navigator".

Looking forward to 2035, the financial landscape will continue to be shaped by megatrends such as technological advancements, demographic shifts, geopolitical changes and climate demands. Breakthroughs in artificial intelligence, digital trust, digital assets and quantum-safe technologies will be key drivers of collaboration, growth and innovation. However, addressing challenges such as geopolitical tensions, economic disputes and uncertainties from pivotal elections or policy disputes shifts will require careful decision-making. Striking the right balance between the outstanding risks and the pursuit of inclusive prosperity, growth and innovation will be crucial. Understanding both current and emerging challenges, while timely leveraging the opportunities within these key trend advancements will be essential for building a sustainable, secure and interoperable financial ecosystem.

It is a central theme that sustainable progress for financial innovation relies on individual leadership, shared responsibility and cross-disciplinary collaboration. While challenges often stem from a variety of reasons including expertise gaps, disparate perspectives, policy and technology misalignments, it is through open dialogue, shared understanding and coordinated action that we can bridge divides and create pathways toward innovation and growth.

As you explore the "Pathway 2035 for Financial Innovation - Your Navigator," I encourage you to approach it with an open mind and enthusiasm. Let's maintain constructive dialogues, rooted on shared experiences, practical insights and extended feedbacks in order to refine our evolving roadmap. Together, we can seize this opportunity to shape a prosperous, inclusive and resilient financial future by forging new pathways through vision and collaboration.

Claudia Grisard Barbour
Review Board Member, Institute of International Finance Member and Bretton Woods Committee Individual Member

---

Pathway 2035 serves as a high-level navigator for decision-makers in the financial and fintech sectors, guiding those who wish to shape the journey toward 2035. Through bold, honest and at times provocative theses, this paper aims to spark critical dialogue around the strategic choices ahead. Covering core themes — artificial intelligence, digital assets, digital trust and quantum technology — it highlights Switzerland's strengths, as valuable insights for building resilient, secure financial systems. The discussions underscore that as these technologies advance, regulatory frameworks must balance innovation with stability, ensuring trust and security in a digitally interconnected world. As the first in a series, this study invites ongoing challenge, review and adaptation to stay aligned with the pace of change. My thanks go to the FIND Team and all authors whose contributions have made this visionary guide possible.

Johs. Hoehener
Johs. Hoehener, Review Board Member and Swiss Fintech Influencer of the Year 2024

As we chart the pathway to 2035, the Finternet vision imagines a future where individuals and businesses can securely manage their financial interactions with greater autonomy and efficiency. Switzerland, with its ecosystem of innovation, regulatory foresight and trust stands as a leader in integrating traditional finance with cutting-edge technologies. This report serves as a call to action: to responsibly harness these advancements, creating digital ecosystems that balance resilience, opportunity and accessibility, while fostering trust and stability across financial services.

Siddharth Shetty
Co-Creator of the Finternet

Prologue

This paper builds on the "Finternet: The Financial System for the Future", a working paper of A. Carstens and N. Nilekani, published in April 2024 by the Bank of International Settlement (BIS). Therein, the authors propose the concept of the "Finternet" as a vision for the future financial system through multiple financial ecosystems interconnected with eachother. They envision empowered individuals and businesses placed at the very center of their financial lives. The Finternet publication identified three necessary components: an efficient economic and financial architecture, the application of cutting-edge digital technology and a robust legal and governance framework.

Together with a global group of visionaries, futurists and thought leaders, FIND took elements of the Finternet vision and expanded on them, not without critical review and debate. Those elements were discussed and validated with international peers in four different working sessions on 5 November 2024 at the Swiss Club in Singapore on the eve of the Singapore Fintech Festival and subsequently endorsed for publication.

We would like to thank the authors and contributors for their invaluable assistance in the preparation of the content and the session guests for their engagement and contributions in the working sessions, all as listed at the beginning of each of the four chapters. In particular, I would like to express my gratitude to Claudia Grisard Barbour and Johs. Hoehener for immensely helpful guidance and discussions throughout the process, Justin Friedrich and Vénusia Bertin for consolidation work and communication, Andrea Weber for post-editorial review as well as André Lergier for layout and design. A special shout-out goes to Drew Propson of the World Economic Forum (WEF) who supported from the outset in many different ways.

Eva Selamlar-Leuthold
Head of FIND

01.

Introduction

1.1. From (Finternet) Vision to Action

This publication builds and expands on the "Finternet: The Financial System for the Future" (Finternet), a working paper of A. Carstens and N. Nilekani, published in April 2024 by BIS. Therein, the authors propose the concept of the "Finternet" as a vision for the future financial system through multiple financial ecosystems interconnected with eachother. They envision **empowered individuals and businesses placed at the very center of their financial lives**. The Finternet publication identified three necessary components: an efficient economic and financial architecture, the application of cutting-edge digital technology and a robust legal and governance framework. The Finternet publication is flanked by a white paper called "Finternet: Technology Vision and Architecture" by N. Nilekani, P. Varma and S. Shetty, also published in April 2024.

Both Finternet papers served as starting point and reference for the present "Pathway 2035 for Financial Innovation – Your Navigator" (Pathway 2035 for Financial Innovation) in so far as **FIND picked four technological developments** which in its view are crucial building blocks to operationalize and further expand on the Finternet vision. The latter being an intriguing starting point and one vision, naturally, many other visions exist and many other building blocks are just as important. FIND is keen to dive into them at a later point with relevant national and international experts.

1.2. A Pathway 2035 for Financial Innovation

The goal of launching Pathway 2035 for Financial Innovation was to kick-start an open-minded discussion amongst experts within the Swiss financial ecosystem, factoring in the valuable expertise of further international thoughtleaders as learning from and collaborating with each other across borders and across sectors is and always will be key for financial innovation to scale in a digital and data-driven economy. In fact, the financial sector is undergoing a transformative period marked by the convergence of multiple innovations. Looking toward 2035, the development and deployment of these emerging technologies are reshaping the foundations of the digital world. This convergence enhances operational efficiency and enables greater personalization of financial services. However, it also introduces significant challenges, adding layers of complexity to financial systems that must be carefully managed.

In a first step towards 2035 and considering global reports on financial innovation trends such as "The Future of Global Fintech: Towards Resilient and Inclusive Growth", a collaborative report by the World Economic Forum and the Cambridge Center of for Alternative Finance, FIND has pinpointed four key areas as critical to the financial sector's future: artificial intelligence (AI), digital assets, digital trust and quantum-safe technology. Further key areas exist as mentioned and ought to be addressed at a later point in time. In the following individual chapters, each of the mentioned key areas has been collaboratively analyzed and introduced by the individual authors and contributors with a particular view on opportunities and challenges for the financial sector by means of thesis statements and discussions under the Finternet north star to navigate the *Pathway 2035 for Financial Innovation*.

The potential of these technologies to reshape the financial landscape is immense. By 2035, we anticipate a radically changed financial ecosystem where, due to the rapid adoption of new digital technologies, a significant part of the financial service industry will have moved to the virtual domain and where most of the financial experts' knowledge has been democratized. This will not only result in unprecedented security, efficiency and personalization in financial services; but, even more importantly, affect how societies define the role, value and function of financial intermediaries, services and institutions.

There is no single path to 2035. Policymakers and all other ecosystem actors will face many choices, including those relating to politicial strategy, technology scope, access and ownership. Jurisdictions will naturally differ in their approaches, reflecting their own unique circumstances. Smart governance will, however, always be key. Jurisdictions will "walk" along their own trail, some tend to lean more toward the regulatory path, others on the (market-driven) innovation path, some seeking a balanced middle ground.

The overarching Finternet vision can serve as a guiding north star for an open infrastructure that centers on the needs of users – both individuals and businesses. To support this journey, the following checklist may provide a helpful compass for navigating strategies in AI, digital assets, digital trust and quantum-safe technologies:

#	As a user I …	Examples
1	Could be any natural person or legal person	Individuals and legal persons (eg corporations, governments, non-profits, trusts, partnerships)
2	Could use my electronically verifiable identities and verifiable attestations to participate in the ecosystem	*Identities*: Passport, national (digital) ID card, driver's licence, birth certificate, social security number/card, bank cards, etc *Attestations*: Investor accreditation, educational degrees, employment history, professional licences/certifications, health/financial records, criminal background checks, social media, etc
3	Could authenticate myself and authorise transactions on any ledger of my choice	PIN, biometric verification, hardware token, SMS/email-based, authorisation chains, etc
4	Could create personalised integrated financial workflows	Rule-based transactions (eg predefined limits/caps on the amount/volume), transaction interlinking, delegation, etc
5	Could choose what data to reveal, how and to whom	Virtual addresses, aliases based on time/payee/amount, zero knowledge proofs of personal data, etc
6	Could use any device for authorising transactions	Mobile phone, laptop, desktop, mixed reality headset, internet-of-things device, NFC tag and other form factors
7	Could send and receive anything of value in any unit, any amount, to anyone, anywhere	Any asset (registered/unregistered, regulated/unregulated, attested/unattested), any amount, anyone (any natural or legal person), anywhere
8	Could manage my assets with any asset manager of my choice	Banks, brokers, asset management companies, depositories, etc
9	Should be protected from fraud, abuse and bad actors	Know-your-customer and anti-money laundering, fraud monitoring/alerts, encryption and other secure cryptographic mechanisms, two-factor authentication, regulatory compliance checks, sanctions checks
10	Should be able to adhere to established legal norms	Banking law, securities law, taxation law, dispute resolution mechanisms, etc

Table: Key characteristics of a user-centric Finternet

Source: Carstens, A., & Nilekani, N. 2024, Table 1, p. 19

Table of Contents

02.

Artificial Intelligence (AI)

Authors and Contributors

Name	Level of Contribution	Association
Prof. Dr. Posth, Jan-Alexander	Co-Thematic Lead & Co-Lead Author	Zurich University of Applied Sciences (ZHAW)
Prof. Dr. Farkas, Walter	Co-Thematic Lead & Co-Lead Author	University of Zurich (UZH)
Dr. Wulfmeyer, Sina	Co-Session Lead & Co-Lead Author	Unique AG
Chan, Jonathan	Co-Session Lead & Co-Lead Author	Bank Julius Bär AG
Perrelet, Simon	Co-Academic Lead & Author	University of Bern
Hostettler, Fabian	Co-Academic Lead & Author	University of Bern
Gramke, Kai	Author	EconSight AG
Goh, Wee Kiat	Author	Bank Julius Bär AG
Andermatt, Silvan	Contributor	Sielva Management AG
Dr. Böckenfeld, Martha	Contributor	FIND Innovation Sounding Board member
Lu, Minwen	Contributor	Unique AG
Niklowitz, Matthias	Contributor	e-foresight Digital Banking Trendscout by Swisscom AG
Ben Hattar, Ariel	Contributor	The Capital Markets and Technology Association (CMTA) / Lenz & Staehelin
Iffland, Jacques	Contributor	CMTA
Mogicato, Ralph	Contributor	SICTIC
Petric, Marko Nanut	Contributor	Bank for International Settlements (BIS)
Rouam, Sigrid	Contributor	EFG Bank AG
Selamlar, Eva PATHWAY 2035 TEAM	Contributor	Swiss Financial Innovation Desk (FIND)

Unlike previous waves of digitalization and automation, AI has the potential to be the biggest technological shift for the decade to come, with major impact how we do business and serve clients. It is comparable to the introduction of the iPhone and Apple's App Store which sparked the mobile revolution for a broader, less tech-savvy user community. AI applications such as ChatGPT have introduced a whole new approach, and tools previously used only by experts can now be used by many more. The rapid pace of AI advancement places immense pressure on companies, states and societies to adapt. In different countries, the focus tends to vary between the opportunities AI presents and the risks it poses, largely influenced by the prevailing societal and political mindset.

FINMA polled 100 insurers in 2021 and approximately 70 banks and asset managers in 2022. The 2022 survey revealed that around half the polled institutions make use of AI or are specifically planning to do so. The fields of use were mainly in the front office area (e.g., generating investment ideas and marketing), process optimisation (e.g., categorizing documents), compliance and conduct (e.g. know your customer), financial risk management (e.g. risk analyses), system monitoring (e.g., monitoring IT security perimeters) and many more (e.g., translations). Compared to the survey among insurers in 2021, it became apparent that depending on the business area, different applications were pursued. Similarities were observed in the predominant use of existing structures and processes for AI applications and the focus on applications in the front office area and process optimisation[1].

As seen in Switzerland and abroad, financial service organizations have long used AI in particular fields of their business, e.g., in transaction monitoring, the output being subject to stringent model risk assessments. However, the recent wave of new GenAI applications calls for companies to navigate a complex landscape of increasing state regulation, voluntary self-regulation and competitive pressure. This competitive environment can push firms to launch AI applications that are not fully developed, resulting in potentially misleading or harmful outcomes. As AI technology becomes more sophisticated, the risks associated with misaligned usage increase. AI that fails to align with ethical standards, shared societal values or the objectives set by developers poses significant dangers.

1 FINMA Annual Report 2021 (p. 20 et seq. and p. 43) and FINMA Annual Report 2022 (p. 22 and 25), see finma.ch/en, visited in January 2025.

A brief history of AI

In 1956, the Dartmouth Conference established AI as a field of study and set a research agenda for **natural language processing (NLP)**. The first successful chatbot was Eliza in 1964, followed by symbolic and statistical NLP developments until about 2010. Google changed the standard of NLP from statistical models to **machine learning (ML)** in 2014. The well-known general-purpose models by OpenAI became apparent in 2018 and were released to the public as ChatGPT in 2022. In the meantime, other models appeared and the adoption of technology and development massively accelerated.

AI in Switzerland

A study by the Innovate Switzerland Community[1], conducted with the support of the ETH Zurich AI Center and Microsoft Switzerland, reveals that AI has significant potential to boost economic growth in Switzerland through productivity gains and enhanced innovation. Most respondents expect noticeable productivity increases within the next five years, with 86 percent believing AI will significantly enhance innovative capacity and 73 percent anticipating increased profitability. The study also highlights AI's versatile applications, including strengthening research excellence, mitigating skilled worker shortages and addressing pressures to innovate and grow, alongside other areas like education quality and climate change.

A study by Implement Consulting Group commissioned by Google expects **a 11% increase in the Swiss Gross Domestic Product (GDP), which corresponds to CHF 80–85 billion**, if all industry verticals start implementing and using AI now. Waiting five years could lead to a substantially lower increase in the Swiss GDP of 3%, which corresponds to CHF 20–25 billion. According to this study, 66% of jobs are expected to work together with generative AI, 26% of jobs are likely to remain unaffected by generative AI and **only 8% of jobs are deemed highly exposed to generative AI**, leading to some job closures. New jobs in the AI-powered economy are expected to replace those lost due to automation, **resulting in unchanged employment levels**.

1 Merluzzi, R., Hoffet, I., Sigrist S., 2024.

Switzerland as Leading Tech Hub

According to Forbes, Switzerland is Europe's leading tech hub, driven by its top-tier technical universities, a growing number of successful start-ups and significant venture capital investments, despite broader European challenges in venture funding[1]. This status is further validated by recent announcements from major AI companies like OpenAI and Anthropic, which are establishing offices in Zurich. Switzerland excels in AI research and the education of AI talent, making it an attractive destination for international tech players. However, for Switzerland to maintain and enhance its leadership position, significant investments in local AI infrastructure are essential. This includes bolstering computing power and developing locally hosted and trained large language models (LLMs), supported by governmental initiatives and regulations that promote a go-local approach.

1 Prosser, D., 2024.

Singapore's strategy is one of government co-investment in AI companies, which aims to position Singapore as a global AI leader and leverage AI for public good. Key initiatives include a USD 20 million investment in AI scholarships and internships and up to USD 500 million for high-performance computing resources to drive AI innovation.

A first step into the right direction has been made: the Swiss AI Initiative[1] has recently launched "The Alps", a supercomputer at the National Supercomputing Center (CSCS) which is the world's first national research infrastructure equipped with over 10,000 Nvidia Grace Hopper GPUs, supporting the Swiss AI Initiative. This initiative, now operated by the Swiss National AI Institute (SNAI), aims to advance AI research, education and innovation in Switzerland, leveraging the expertise of over 70 AI-focused professors from multiple academic institutions.

To secure long-term success in the AI sector, it is crucial for major Swiss corporations, including all big players in the banking and in (re-)insurance industry, to also invest in local AI infrastructure. Relying on large US hyperscalers could undermine Switzerland's competitive edge. By fostering a robust local AI ecosystem, Switzerland can ensure sustained growth, innovation and national independence in the Swiss tech industry.

1 swiss-ai.org, visited on 10 December 2024.

Sustainable AI: Powering the Future with Green Energy by 2035

Energy consumption is a growing topic when speaking about the future of AI-powered solutions. For example, the Nvidia H100 GPU, designed for intense AI programs, is projected to consume as much energy as the entire nation of Guatemala in 2024[1]. By 2035, the energy consumption of (generative) AI applications will be a critical factor in the global push for sustainable technology. Training and deploying large GenAI models will require advanced, energy-efficient algorithms and hardware to mitigate their substantial power demands. The environmental impact, particularly the carbon footprint of AI, will drive the adoption of renewable energy sources and stricter regulatory measures. Economic pressures will incentivize companies to innovate in reducing operational costs through energy-efficient AI solutions. Social and corporate responsibility will further propel the shift towards greener AI practices, ensuring that technological advancements align with global sustainability goals. In this regard financial service providers show increased interest in "Small Language Models" to tackle the mentioned challenges.

1 statista.com/statistics/1446532/energy-consumption-nvidia-microchip/, visited on 10 December 2024.

2.1. The AI Race to the Top: Progress, Regulation and Mindset

Thesis 2.1

There is a race to the top. The United States (US) and China will significantly shape the future of AI among other competitive powers. The future of global markets including that of the European Union (EU) are all being affected with certain limits and opportunities based on their technological, regulatory and political expertise.

Discussion

The debate surrounding AI regulation has intensified in recent years, reflecting the challenges of navigating this rapidly evolving landscape. First, the continuously advancing technology raises complex and nuanced questions about what can and should be regulated in a dynamic and fast progressive environment. Second, regulation methodologies are equally contentious. Without a global framework, regulatory efforts will inevitably reflect the diverse socio-political values and ethical principles that vary widely across countries. This situation leads to regulatory competition and fragmentation among differing social and economic systems.

Currently, we see three distinct regulatory approaches:

1. **US Approach**: Emphasizing innovation, the US adopts a market-oriented stance with limited regulation, fostering a climate conducive to technological advancement[1].
2. **EU Approach**: The EU prioritizes the protection of human rights, implementing risk-based regulations that focus on ethical considerations and accountability[2].
3. **Chinese Approach**: China seeks to balance AI development with stringent state control, emphasizing national security and social stability[3].

As these approaches evolve, all other countries face the challenge of choosing which regulatory model to adopt while navigating the complexities of innovation, ethics and governance in a competitive global environment. This boundary pushing landscape calls for strategic decisions driven by collaboration to effectively align regulations and build long-term trust in AI technologies.

The graph [Image 2.1] shows global AI activity by patenting, highlighting countries with the most active AI and applied AI developments. Patents, especially groundbreaking and highly-relevant ones in areas like deep learning, neural networks and generative AI, offer a forward-looking measure of technological progress. These high-quality patents are expected to drive major AI advancements in the years ahead.

Leveling the Race: The International Computation and AI Network (ICAIN)

ICAIN is a Swiss initiative with a global focus on broadening access to AI resources for sustainable development research. The organization connects AI capabilities (computing power, data and expertise) with research projects aligned with the UN Sustainable Development Goals. With its current members (both Swiss Federal Institutes of Technology, Swiss National Computing Center, European Laboratory for Learning and Intelligent Systems, Data Science Africa, Finnish IT Center for Science) and under the patronage of the Swiss Federal Department of Foreign Affairs, ICAIN not only draws on the expertise of experienced policy-makers and some of the best AI researchers in Europe and Africa, but also has two of the most advanced and powerful supercomputers in the world at its disposal. ICAIN is currently transitioning into its operational pilot phase, scheduled for 2025–2026 and is looking for additional members and donors.

Source: Information received from Federal Department of Foreign Affairs FDFA in late 2024, see also icain.org

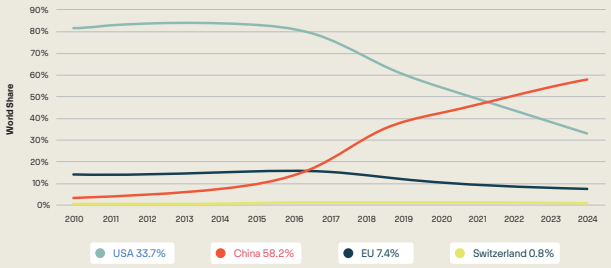


Image 2.1: Country Share in Deep Learning/Neural Networks/Generative AI World Class Patents, 2010–2024

Source: EconSight 2024

High-quality research and development (R&D) in AI is increasingly concentrated in just a few countries. The number of world-class AI patents has tripled since 2020, from 21'000 to 63'000. China owns 58% of all currently active world-class patents in deep learning/neural networks technologies. The US share has more than halved in the last six years to just under 34%. The EU accounts for only 7%.

In addition to advanced AI, applying AI in other technologies is also becoming increasingly important. AI is accelerating development in different technologies, leading to new products, processes, structural change and societal challenges. The following chart highlights this as it shows the application of AI to selected cutting-edge technologies.

1 White House, 2023.
2 EU AI Act: First Regulation on Artificial Intelligence | Topics | European Parliament, see europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence, visited in January 2025.
3 cset.georgetown.edu/publication/china-ai-law-draft/ and AI Watch: Global regulatory tracker - China | White & Case LLP, see whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china, visited in January 2025.

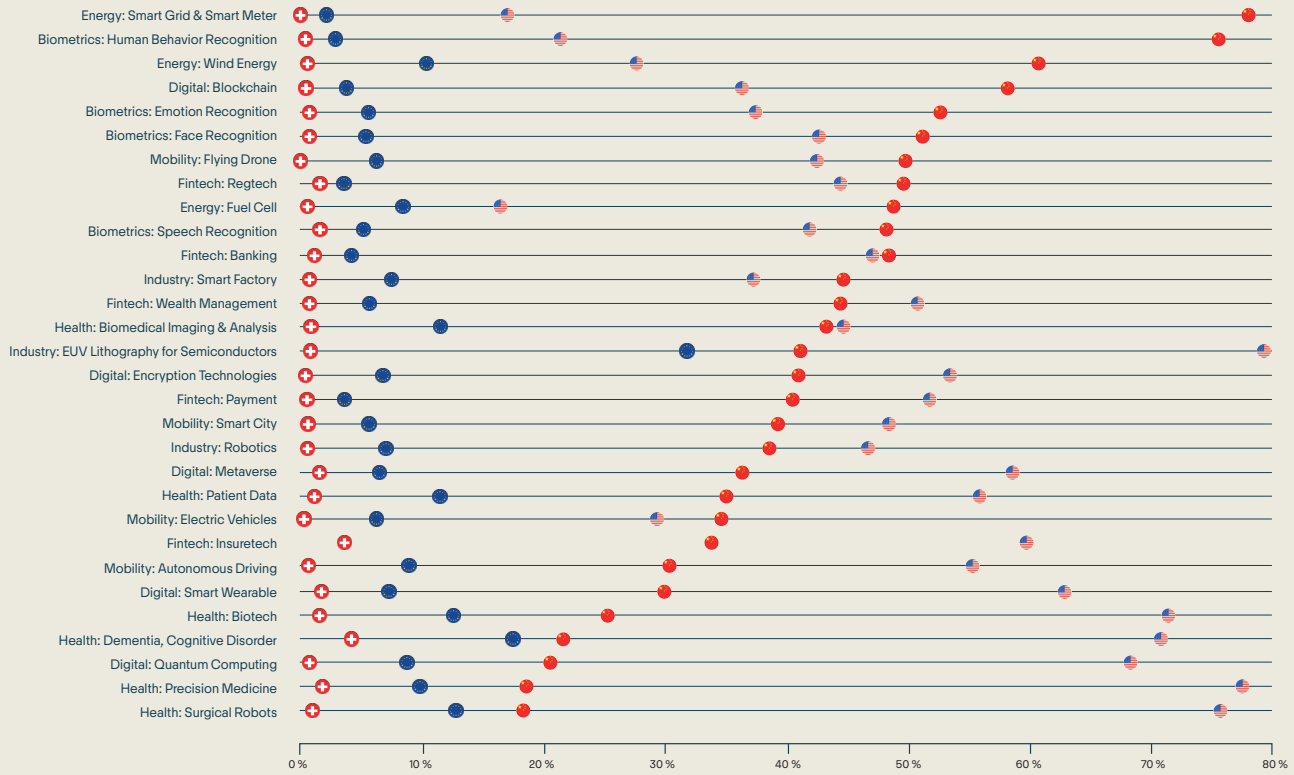


Image 2.1: **Country Share in Application of Advanced AI in Selected Cutting-Edge Technologies, 2024**
Patents that are assigned to both AI and an application technology. Many patents are the result of international research collaborations. Consequently, aggregated world shares per technology may add up to more than 100%.
Source: EconSight 2024

The analysis shows that China is competing with the US for leadership in a large proportion of the most critical application technologies in energy, industry, fintech, health, biometrics and mobility. The EU is lagging behind in most technologies. Although the US is still leading in some areas, particularly in health tech, the trend and momentum are in favor of China. Particularly in the case of potential surveillance technologies, the gap between the different regional regulatory approaches is becoming apparent: while China, for example, can further develop its social credit system because of less-restricted access to personal data, AI-based social scoring systems are an unacceptable risk in the EU's AI Act.

Conclusion and Outlook

From a purely technological standpoint, the regulatory competition between the US, the EU and China currently represents a race between two primary systems. While the EU, leveraging its economic influence, extends the reach of its regulations to impact third-country players seeking to enter the EU market, the US and China understand regulation as a necessity that must not limit progress – be it with a technological focus as for the US or a focus on national security and social stability as for China.

Applied AI – Focus Switzerland

Switzerland is well positioned in the application of AI in insurtech (3.6% world share) and in selected health technologies such as dementia and Alzheimer's research (4.2% world share). This puts Switzerland on par with the EU in insurtech. Swiss Re is the leading company in insurtech in Switzerland, while Roche is at the forefront of dementia research. Across all technologies, Roche leads in the application of AI in Switzerland with 27% of all AI world-class patents filed, followed by Swiss Re (11%), UBS (9%), ABB (8%) and ETH Zurich with 6%. Switzerland's Federal Council has mandated the Federal Department of the Environment, Transport, Energy and Communications (DETEC) with exploring the existing regulatory framework to balance innovation with societal risk management in relation to AI matters. This assessment is flanked and supported by a sector-specific analysis conducted e.g. by SIF with regard to financial markets regulation. Given DETEC's assessment of AI frameworks of 18 countries, the proposed path forward will need to navigate between legal, economic and other implications. The report is expected for early 2025.

Source: EconSight 2024 / DETEC information as of December 2024.

Although the EU's significant economic size provides a solid stepping-stone, its influence may be constrained by a relative lack of technological expertise compared to its counterparts. The EU must strengthen its technological capabilities; plus, it must identify and capitalize on opportunities for innovation and strategic partnerships to enhance its position. By focusing on collaboration and targeted investments, the EU could compete in the regulatory race, ensuring that its financial infrastructure supports innovation and growth while fostering a secure environment for technological advancements.

2.2. Navigating AI Limitations: Call for Smart Policy Setting & Regulation

Thesis 2.2.
To achieve social acceptance of AI, policy makers must find a balance between mitigating risks and fostering innovation. Smart regulations are needed to ensure the balance between innovation and responsible use of AI technologies.

Discussion
Although AI offers various advancements to the way we work and live, there is growing concern about negative and unintended consequences, such as negative bias, discrimination, lack of transparency and limited human agency[1]. These issues necessitate a policy and regulatory environment that governs AI technologies' ethical and responsible use.

AI systems have already demonstrated their ability to impact essential aspects of society and that corresponding challenges and risks accompany their use. Therefore, mechanisms to mitigate these risks and the use of responsible AI are indispensable[2]. A growing consensus supports the idea that Responsible AI is a set of principles ensuring ethical, transparent and responsible use of AI technologies in alignment with user expectations, organizational values and societal laws and norms.

Smart policymakers and regulators, which are comfortable with technology, forward-thinking and foster collaboration with industry, are crucial for ensuring that AI remains both innovative and safe. A policymaker or regulator should not impede the ability to innovate but rather create and implement a framework in which AI can develop responsibly. A policymaker or regulator can support the industry to prevent harmful or unintended outcomes by enshrining and implementing various principles that ensure ethical, transparent, fair and responsible policies and regulation.

Early and proactive engagement by policymakers and regulators is central to addressing potential risks and societal impacts before they become deeply rooted in technology and its applications. To this end, they should draw on the findings of leading research and exchange practical experiences with the industry. This exchange aims to build a knowledge base that expands technical expertise and oversight experience. In addition, a growth mindset and continuous training of policymakers' and regulator's staff is required to keep up with the speed of new advancement in the AI space. Through joint initiatives and cooperation of different policymakers and regulators, information can be better shared, allowing the necessary information for quicker access in decision-making and for immediate respond to events.

MindForge: Singapore's Blueprint for Ethical AI in Financial Services

In 2023, the Monetary Authority of Singapore (MAS) launched Project MindForge as a continuation of the Veritas initiative, which started in 2019 to establish the Fairness, Ethics, Accountability and Transparency (FEAT) Principles for AI in financial services. Project MindForge, involving MAS, major banks and tech companies, focuses on responsible generative AI use in finance. Its primary goal is to create an industry-led whitepaper detailing best practices and risk management strategies for generative AI. The project addresses new challenges, examining risks in areas like governance, transparency and data security. Generative AI's potential in finance includes enhancing customer service, boosting productivity and reducing costs. Project MindForge emphasizes the need for frameworks that address emerging risks to ensure AI is deployed ethically and securely.

Source: mas.gov.sg/schemes-and-initiatives/project-mindforge

Switzerland's AI Monitor

In 2024, FIND entered into a collaboration with academia and the industry to gather intel about the best path forward for the Swiss financial industry to use AI in a bold yet responsible manner. The AI Monitor, led by ETH Zurich and N9 House of Innovation, will provide clear, research-driven insights that empower businesses to make informed, strategic decisions. It will track AI development over the years, set industry standards and offer clear, data-driven overview of AI adoption in the Swiss economy. By combining AI technology, practical implementation and close government engagement, the AI Monitor will drive sustainable growth and societal impact through AI and provide the regulator – through FIND – with valuable insights for smart regulation.

Source: ai-monitor.ch

1 Mirzadeh et al., 2023; UK Government, 2023; Kordzadeh & Ghasemaghaei, 2021.
2 Mikalef, Conboy, Lundström, & Popovič, 2022.

Conclusion

Proactive and effective policymakers and regulators play a crucial role in managing potential risks and societal impacts of AI, fostering public trust and providing clear guidance and stability to the industry. By acting thoughtfully, they can help minimize the risk of social division and ensure that AI systems are developed in alignment with societal values. Important elements of smart regulation include a high level of AI literacy among policymakers' and regulators' staff including technical skills as well as the willingness to deal with ongoing development of new AI applications.

2.3. The Inevitable Integration of AI into the Global Financial Ecosystem

Thesis 2.3.

The envisioned Finternet by A. Carstens and N. Nilekani and AI will work symbiotically, enabling a financial system that is faster, safer and far more adaptable to the needs of a digital-first, highly interconnected global economy. One important condition is the need to facilitate efficient data sharing across organizations and countries to be able to build this decentralised but interoperable and unified digital highway.

Discussion

AI is transforming global finance by enabling faster, more secure transactions, automating compliance and providing hyper-personalized financial services. However, we are only at the beginning of this journey. Over the next decade, AI will evolve from a tool for efficiency into a foundational layer that redefines global financial infrastructure and integrated into the very fabric of our financial ecosystem.

AI without data is like a fish out of water. For the Finternet to thrive, it is essential to **facilitate data sharing** across organizations (not just financial institutions) and countries, creating an interconnected system. The value of data, especially proprietary data from banks like client insights, is continuously rising. To unlock this value and foster collaboration, a secure data-sharing approach must be developed. This approach should define data access levels, duration and purpose. Solving the data-sharing challenge can lead to new interconnected systems and innovative business models. AI will be pivotal in this ecosystem, helping to analyze data, simulate scenarios and identify new value streams. AI can enhance decision-making and personalize customer experiences[1]. Leading companies and disruptors have already embarked on this path. Additionally, fostering trust and collaboration among stakeholders is vital to foster an open data-sharing culture and willingness to share. This includes establishing standardized data exchange protocols, promoting system interoperability and encouraging open innovation. By addressing these factors, the Finternet can drive financial innovation and global economic growth.

1 ey.com/en_ca/insights/open-banking/how-hyper-personalization-helps-fis-boost-open-banking-potential, visited December 2024.

Following the Finternet's call to action, AI also plays its part to mitigate security breaches in decentralized finance, underpinned by blockchain technology, leading to billions of USD in annual losses[2]. AI techniques help to fortify such blockchain-based applications by using LLMs to conduct thorough security audits on smart contracts through advanced prompt engineering. "BlockGPT" is a pioneering tool that produces intricate tracing representations of blockchain activity. The tool is designed to train an LLM from the ground up, enabling it to function as a real-time Intrusion Detection System[3].

2 Feng, D., Hitsch, R., Qin, K., Gervais, A., Wattenhofer, R., Yao, Y., Wang Y. 2023.
3 blockchain.uzh.ch/events/ai-enhanced-security-in-defi-leveraging-llms-for-proactive-defense/, visited December 2024.

Increased Competition and Financial Health through Agentic Customer Bots

Mike Kelly built a plug-in to link ChatGPT to his bank account using the UK's open banking Application Programming Interfaces (APIs). The plug-in, called "BankGPT", can tell the balance, find transactions, discuss budgeting and make payments. This experiment shows that AI and open finance will change financial services beyond measure[1]. As the author aptly puts it, in the not-too-distant future, consumer's financial decisions, transactions and analysis will be performed by bots operating under relevant duty of care legislation with the co-ordinated goal of delivering financial health. Financial health is defined as the extent to which a person or a family (or a business, for that matter) can successfully manage their financial obligations and have confidence in their financial future[2].

1 Birch, D., 2024.
2 Carstens, A., & Nilekani, N., 2024.

Open Finance and Open Data as Imperative Building Blocks for the Finternet

Open Finance and Open Data is key to realize the vision of the Finternet[1] as standardized APIs or other technological means to ensure interoperability enable seamless, interoperable financial and non-financial services by providing access to data and fostering competition and innovation across platforms. The Global Open Data Tracker includes an Innovation Atlas with an overview of open banking/finance/data initiatives, the innovation taking place and progress towards financial inclusion[2].

1 Carstens, A., & Nilekani, N., 2024.
2 ozoneapi.com/the-global-open-data-tracker/atlas/list/

To better allow for **data sharing and collaboration** across organizations and countries, besides the pertinent policies and regulation, more community building initiatives are needed that allow corporates, start-ups, students, venture capitalists can connect and collaborate.

Currently, AI operates largely in a reactive capacity, detecting fraud, automating tasks and analyzing large data sets. In areas like lending and risk management, AI-driven credit scoring is improving access to finance, though legacy systems and regulatory constraints still pose challenges. The forthcoming transformation will shift AI's role from reactive to proactive, with predictive models that continuously learn from real-time financial activity. This evolution will enable AI to forecast market trends and anticipate systemic risks before they arise, while also providing alerts to regulators as a safeguard. Ultimately, AI will move beyond merely optimizing processes to become the orchestrator of financial ecosystems.

This shift will converge with the concept of the Finternet, an interconnected, tokenized financial network[1]. By 2035, AI will no longer operate in silos but will be integrated into unified ledgers where tokenized assets, including central bank digital currencies (CBDC), securities and digital identity systems seamlessly interact. The intelligence of AI will power this infrastructure, enabling real-time settlement and programmable money across borders without the inefficiencies of current correspondent banking systems. The Finternet will democratize access to financial services, driven by AI-enabled interoperability, breaking down barriers between traditional banks, fintechs and decentralized finance platforms.

AI will further transform risk management. Instead of detecting fraud ex-post, AI systems will proactively mitigate risk by dynamically adjusting transaction thresholds, liquidity allocations and even trade executions. This transformation is critical in the complex world where tokenized assets and smart contracts autonomously execute countless mini-transactions.

Conclusion

AI's integration into an evolved Global Financial Ecosystem and Finternet is an eventuality; the immense benefits it brings will forever change the way our financial system operates. AI will break down traditional barriers like geography, credit history and collateral, promoting global financial inclusion. By leveraging alternative data - from social interactions to digital footprints - creating highly personalized financial profiles for the underbanked. Enabling real-time microcredit, dynamic savings tools and AI-powered financial planning accessible to anyone with a mobile device. AI will further drive hyper-personalization in financial services, transforming how individuals engage with their institutions. AI will change the way consumers and businesses are protected from financial fraud and help ensure a more resilient banking ecosystem.

However, for this Finternet future to thrive, secure and efficient data sharing across organizations and countries is essential. An AI-powered Finternet will continue to fundamentally change the way financial companies interact, driving a significant industry shift by leveraging AI to unlock value, enhance privacy and promote innovation and collaboration.

1 Carstens & Nilekani, 2024.

Ecosystem Collaboration in Switzerland through Hackathon SwissHacks

In Switzerland, FIND initiated the hackathon premiere "SwissHacks" in close collaboration with the Federal Chancellery, Tenity, Innovation Zurich and the industry such as Ripple, Microsoft/Unique, Postfinance, Julius Baer and the Swiss Stock Exchange. The participants - within 48h - developed GenAI applications for the financial services industry. The challenge attracted tech enthusiasts and innovators from around the globe. The hackathon saw a diverse range of participants, including students, professionals and start-ups, all aiming to showcase their skills to leverage AI to solve some real-world problem statements from supporting organisations. The outcomes included several projects, with Microsoft/Unique teams standing out for their creative approach and technical prowess and Julius Baer's team being brought to the bank to share their approach towards identifying AI deepfakes overall. The success led to a second edition in the run-up of the Point Zero Forum 2025, fostering collaboration and highlighting cutting-edge technological advancements.

Source: swisshacks.com, pointzeroforum.com

03.

Digital Assets

Authors and Contributors

Name	Level of Contribution	Association
Dr. Veprek, Ratko G.	Co-Thematic Lead & Co-Lead Author	Digital Asset Holdings LLC
Pilav, Darko	Co-Thematic Lead & Co-Lead Author	Digital Asset Holdings LLC
Dr. Glarner, Andreas	Practice Lead and Author	MME Compliance AG
Prof. Dr. Affolter, Beat	Academic Lead & Author	Zurich University of Applied Sciences (ZHAW)
Stuedlein, Max	Session Lead and Contributor	Sygnum Bank AG
Eberle, Pascal	Author	Sygnum Bank AG
Andermatt, Silvan	Author	Sielva Management AG
Langer, René	Author	Luzerner Kantonalbank AG
Kaulitz, Serge	Author	Luzerner Kantonalbank AG
Bianchi, Raphael	Contributor	OpenWealth Association / Synpulse
Eroglu, Hakan	Contributor	Bank of International Settlement Innovation Hub (BISIH), Hong Kong Center
Lai, Ryann	Contributor	UN Refugee Agency (UNHCR)
Ro, Sandra	Contributor	Global Blockchain Business Council (GBBC)
Rooz, Yuval	Contributor	Digital Asset Holdings LLC
Wolf, Stephan	Contributor	Global Legal Entity Identifier Foundation (GLEIF)
Grisard Barbour, Claudia PATHWAY 2035 TEAM	Contributor	Bretton Woods Committee individual member, Aker International AG and Pathway 2035 Review Board member

Providing financial services, a core economic activity contributing around 20–25% of the global GDP[1] has undergone significant transformations. The 19th and 20th centuries saw the introduction of real-time communication and electronic record-keeping, which together with the rise of financial regulation established the globally interconnected financial markets we have today.

Most financial assets are currently recorded in centralized databases, with message-based systems or APIs used for communication[2]. Digital assets leveraging distributed ledgers are increasingly seen as being the next step towards an ever more connected and integrated market, driven by the need for increased asset utility, operational efficiency and lower management cost.

1 Financial Services: Sizing the Sector in the Global Economy (investopedia.com).
2 Messaging and Standards | Swift & What is FIX? – FIX Trading Community v2.0 & ISO 20022 | ISO20022

Digital Asset Definition

A digital asset is generally considered anything that is created, transferred or stored digitally. It is identifiable and discoverable and has or provides value. Within this paper, we specifically define digital assets as being dependant on cryptography and distributed ledger technologies (DLTs) in their use for payments, investment purposes or access to goods or services[1].

1 This narrow definition is also termed crypto assets. SCO60 - Cryptoasset exposures.

Distributed Ledger

A distributed ledger is a system for securely managing, replicating and sharing digital data across geographically distributed participants without a central party controlling data and infrastructure. It effectively represents the opposite of a centralized database[1].

1 World Bank, 2017.

Momentum has been created with the invention of Bitcoin in 2009 based on the Bitcoin whitepaper published in 2008[3]. Since then, many traditional organizations have recognized the potential of digital assets and have been exploring ways to capitalize on the opportunities they offer. Bitcoin has become one of the ten largest assets globally and is one of most frequently traded assets of the world. The last decade has seen growing interest in harvesting the benefits of digital assets. Nevertheless, significant challenges related to regulation and implementation, along with the network effects inherent in existing markets persist. However, emerging frameworks and technologies present promising opportunities for the future development of digital assets.

As policymakers and regulators update their frameworks to accommodate technological advancements, the fundamental necessity of regulations to ensure financial system stability remains paramount. The “move fast and break things” Mark Zuckerberg approach to innovation that encourages rapid experimentation, risk-taking and disruption, even at the cost of potentially causing damage or unintended consequences is not tenable in capital markets. They involve complex financial systems, regulations and stakeholder interests. The risks of “breaking things” (such as causing instability, financial loss, or regulatory violations) are much higher.

3 Nakamoto, 2008; ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf.

In this context, a cautious, thoughtful and collaborative approach is needed, one that balances innovation with the stability and trust required for the functioning of financial markets. Stakeholders including both **decentralized finance (DeFi) and traditional finance (TradFi) need to work together to identify and implement structural changes that facilitate interoperability, privacy and governance**, paving the way for widespread adoption of the new technology.

Successfully navigating this complex landscape will enable the introduction of innovative technologies and operational models into the financial industry, unlocking significant cost savings, new business opportunities and enhanced supervisory capabilities. The evolution of financial ecosystems will enhance efficiency and transparency and pave the way for a more inclusive and sustainable financial future. The progress we make at this critical juncture will determine the scale of value we can create, transforming how digital capital flows and is managed across the globe.

3.1. The Significance of Digital Assets

Thesis 3.1.
Atomic composability (see knowledge box) and real-time shared truth[1] provided by digital assets on blockchains will unlock a new era of streamlined finance by removing inherent inefficiencies in the financial markets.

Discussion
Many financial markets and processes operate on outdated legacy infrastructure and siloed data systems, leading to inefficiencies. Adoption of technologies allowing a switch to digital assets in the financial industry will increase rapidly as they reduce the cost of existing business and enable new business models.

With distributed ledgers underlying digital assets, participants automatically share the same implementation and the same data record, observing consistent updates in **real-time**. This eliminates the need for redundant reconciliation processes and enables **industry-wide straight-through processing.**

In traditional finance, ensuring atomicity[2] and composition[3] around assets and transactions is complex and costly. This is typically achieved by transferring the assets into the custody of a trusted service provider, operating a specific financial workflow. Digital assets on digital ledgers are different: An application developer can define a series of steps to be performed as part of an **atomic** transaction, such that either all steps are committed or none. Another developer may extend the system by adding another application that **composes** several transactions to be committed together as one with **atomicity**. This allows distributed applications to replace the role of trusted service providers and thereby not only technically mitigate the risk of partial delivery, but also – depending on the chosen settlement workflow, remove transactional counterparty risks.

A key property for capital markets is guaranteeing **finality** of transactions, the irreversible assurance that a transaction has succeeded. Some distributed ledgers provide strict finality, while others support only weaker finality guarantees, which are undesired from a financial market perspective.

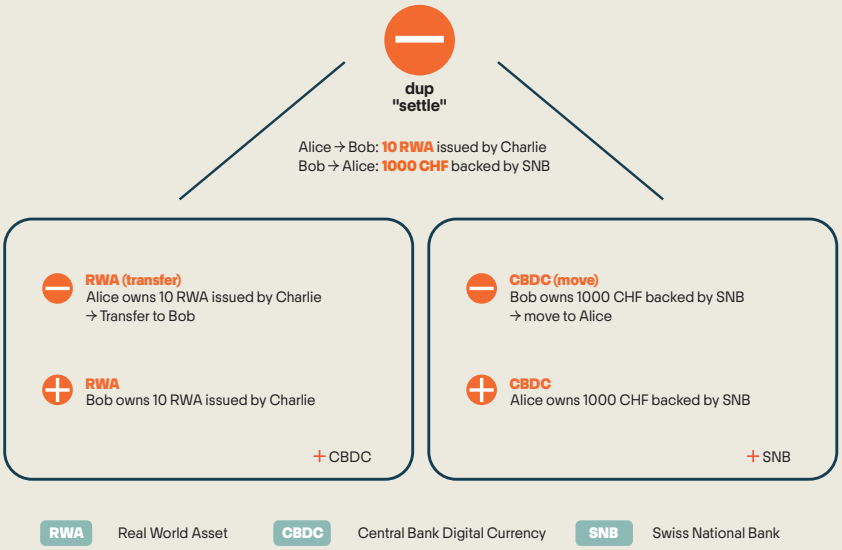
1 Real-time shared truth refers to a state where all participants in a network have guaranteed access to consistent and up-to-date shared data, along with the ability to selectively perform authorized changes. This eliminates the need for participants to reconcile their individual data as the system ensures consistency across the network.

2 Atomicity refers to the ability to ensure all parts of a transaction happen inseparably and with strict conditionality (either all or nothing).

3 Composition or Composability in digital assets refers to the ability of combining various blockchain-based assets and protocols to create new, more complex applications.

Composed Atomic Transactions

Transaction composition is the ability to combine two or more separate transactions from different applications into one atomic transaction, such that either all the (sub-)transactions succeed or none. A classic example of this is delivery versus payment (DvP), where two individual asset transfer transactions are composed into one single atomic transaction that forms the DvP. The DvP itself is represented as an on-ledger obligation, which is settled together conditionally when both transfers succeed, but none of the sub-transactions can be committed to the ledger in isolation. If such a DvP is settled on a ledger with strong finality guarantees, the risk of partial delivery is removed.



- **Decentralized Finance (DeFi)**
  DeFi refers to open, permissionless and composable applications built on public smart contract platforms. It re-imagines existing financial services in a more open and transparent way[1], but often lacks the privacy expected by traditional financial markets. Also, more recently the term is being used for a wide range of blockchain-based financial applications, some of which with centralized dependencies.

- **Smart Contract**
  A deterministic software program, running on a distributed interpreter to compute and validate authorized state progression of a distributed ledger.

- **Crypto Currency**
  A digital asset issued by a decentralized process not tied to real-world obligations.

- **Real World Tokenized Asset (RWA)**
  A digital asset representing a real-world asset, guaranteed by its issuer.

- **Stablecoin**
  A digital asset with the purpose of providing a fungible and stable definition of value on a distributed ledger. Stablecoins can be implemented by an issuer establishing a peg to an underlying (single or basket of fiat or crypto currencies, or real-world assets) or through algorithmic price stabilization means.

- **Central Bank Digital Currency (CBDC)**
  A CBDC is a digital, possibly tokenized, form of a country's national currency, issued and regulated by its central bank, designed to facilitate secure and efficient settlement and cross-border payments.

1 Schär, 2021.

To date, the significance of digital assets and distributed ledgers has been realized in only partially interconnected pockets and by different audiences. These range from cryptocurrencies, DeFi and stablecoins, to enterprise DLT networks and the tokenization of real-world assets (RWAs). But the true global economic potential will be unlocked when the principal value propositions that these pockets of innovation show us can be unified in approaches that deliver on the promise of a more interconnected global economic network.

DeFi demonstrated the power of composed atomic transactions, showing how capital can be unlocked and deployed more rapidly. Yet, while DeFi has shown this fluidity, it has not reached the scale of traditional capital markets. DeFi solutions can introduce new risks that outweigh the benefits and as such be subject to capital charges as per the crypto asset standard of the Bank of International Settlement (BIS SC060)[1] and require off-chain workarounds to accommodate the control, privacy and scaling needs of global financial markets.

Early digital asset projects have created a bifurcated landscape with crypto-native and traditional actors moving at different speeds in different domains, competing with different strategies on how to deliver the promised potential payoff in network effects. Traditional financial institutions initially concentrated on exploratory initiatives, seeking opportunities in areas that would complement rather than compete with established, highly efficient services and markets, to avoid barriers to adoption. Many have recently reached a tipping point[2], moving from pilots to production. Distributed ledger platforms used by financial institutions are now processing trillions of dollars in real-world assets monthly[3].

Similarly, the recent rise in activity and excitement around the potential for the tokenization of RWAs has demonstrated how traditional institutions can boost asset distribution through new networks, such as BlackRock's BUIDL[4] which has further sparked interest and driven institutional adoption. The true transformative potential of such digital assets lies in their ability to unlock utility and mobility across financial markets, creating real positive impact in the process. The next phase of adoption will need to deliver on solutions that inherently address risks around transaction finality, privacy and operational control, while preserving the core value proposition and innovation of composed atomic transactions.

Conclusion

The rapid expansion of the ecosystem has led to fragmentation. Connecting these systems will be instrumental in unlocking and realizing the full global value of digital assets. Unification and interoperability will deliver more than a new investment class, improved distribution or a shared record – it will also create a more efficient and interconnected financial landscape, offering benefits like global value transfer with largely mitigated transactional counterparty risk, 24/7 capital accessibility and reduced operational costs.

1 bis.org/bcbs/publ/d579.pdf, visited December 2024.
2 Tokenized financial assets: From pilot to scale | McKinsey, see mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets, visited December 2024.
3 Tokenization: A digital-asset déjà vu | McKinsey & Distributed Ledger Repo (DLR) for Capital Markets | Broadridge & The Canton Network Series [Part 1 of 5] - The Tie, mckinsey.com/industries/financial-services/our-insights/tokenization-a-digital-asset-deja-vu, visited December 2024.
4 BlackRock (BLK) Unveils Tokenized RWA Fund on Ethereum Network, Invests in Tokenization Platform Securitize, see coindesk.com/markets/2024/03/20/blackrock-enters-asset-tokenization-race-with-new-fund-on-the-ethereum-network, visited December 2024.

3.2. Decentralization and Connectivity without Trade-Offs

Thesis 3.2.
The true potential of digital assets will be unlocked by digital ledger solutions that fundamentally solve privacy, security and accountability concerns while delivering global scalability and connectivity.

Discussion
While digital asset innovation has demonstrated the power of decentralized trust, it also highlighted challenges that must be resolved to unlock value at scale.

One major obstacle to the widespread adoption of digital assets is the complexity of accessing on-chain assets and applications. Handling cryptographic keys, coupled with the wide variety of different solutions and deployments, for example, is challenging. This causes users to access the systems like in the traditional world through intermediaries. Simplifying these processes is essential for broader and direct adoption.

Traditional financial actors are generally avoiding **public-permissionless ledgers**, instead opting for **private ledgers** with restricted access in order to address the necessary privacy, regulatory compliance and scalability needs of larger scale RWA activities. While this approach provides value to the direct participants, it hinders seamless interoperability between the different ledgers, creating new silos within the ecosystem and effectively preventing composability.

There are several methods to connect these different ledgers. Such connections can happen on the application level **through open APIs, token bridges, different locking techniques or more native interoperability protocols**. All these connections have different properties in terms of scalability, trust and expressivity and often limit the type of workflows that can be implemented across ledgers compared to within a single ledger. The resulting interoperability of the systems is defined by the lowest common shared functionality, which often limits the provided utility.

Conclusion
To realise the full value proposition of digital assets, the underlying technology must be able to uniformly connect all networks in a way that combines the openness of public permissionless networks with the security, privacy and control known today in private networks, while maintaining expressivity and composability. Such an infrastructure, also referred to as a unified ledger, should be an integral part of a globally connected financial infrastructure network. Such a vision is currently being conceptualised by various global thought leaders, for example by BIS in its Finternet concept presented in April 2024[1]. While no consensus has yet been reached on the building blocks of such a network, these conceptual approaches can serve as a basis for discussion on how to design the global financial infrastructure of the future.

1 Carstens, A., & Nilekani, N., 2024.

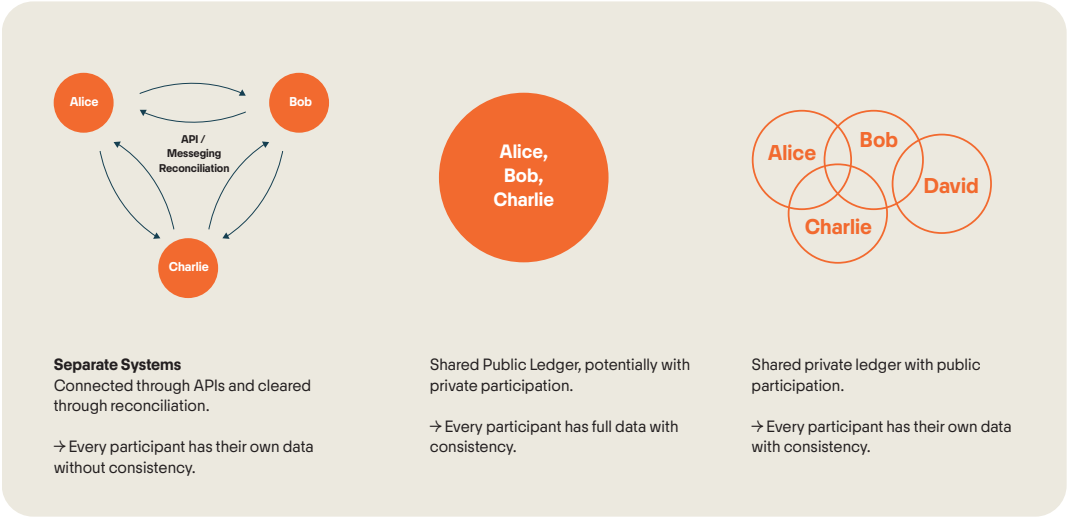
- **Public-Permissionless Ledgers**
  A public-permissionless ledger shares all data publicly and allows everyone to transact on, providing composability and decentralization. As these ledgers are based on public verifiability, they don't provide privacy by default. More advanced cryptographic concepts such as zero-knowledge proofs (ZKP) exist to introduce privacy, but these have not yet found widespread adoption, especially for real world assets. Other solutions combine off-chain and on-chain elements in order to introduce privacy through data segregation. However, currently, possessions on public blockchains are generally known to everyone[1], with only the cryptographic address allowing for pseudonymity.

- **Zero-knowledge proofs (ZKP)**
  A ZKP is a cryptographic technique where one party (the prover) can demonstrate to another party (the verifier) that a statement is true without revealing any additional information beyond the fact that it is true.

- **Private Ledger**
  A private ledger is an isolated deployment with restricted access to a set of users, potentially of an algorithm that is also used to run a public ledger. This allows to limit the control and visibility to a selected set of users, but prevents composability and connectivity.

- **Network of Networks**
  A network of networks is a global ledger that principally allows to connect shared private ledgers with each other with public participation.

1 [BUIDL] BlackRock USD Institutional Digital Liquidity Fund Token - Ethereum contract address 0x7712c34205737192402172409a8F7ccef8aA2AEc, vethplorer.io/address/0x7712c34205737192402172409a8f7ccef8aa2aec#, visited December 2024.



Separate Systems
Connected through APIs and cleared through reconciliation.

→ Every participant has their own data without consistency.

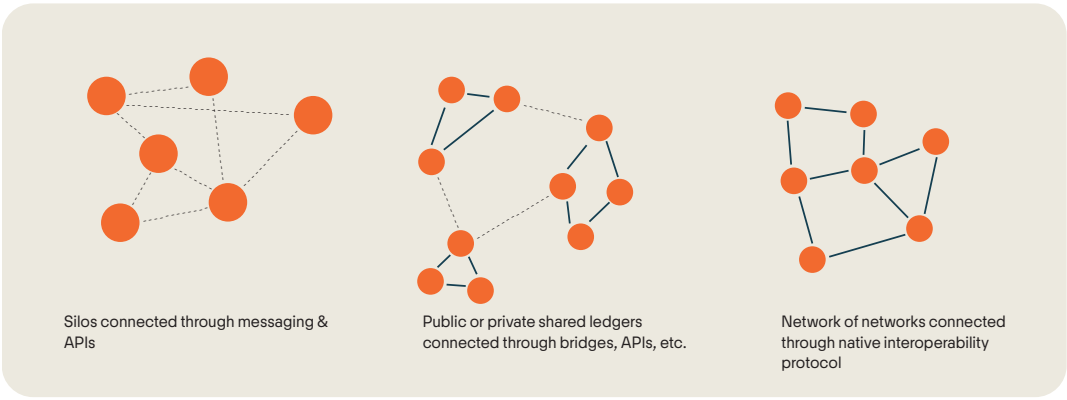
Shared Public Ledger, potentially with private participation.

→ Every participant has full data with consistency.

Shared private ledger with public participation.

→ Every participant has their own data with consistency.

Shared Ledgers



Silos connected through messaging & APIs

Public or private shared ledgers connected through bridges, APIs, etc.

Network of networks connected through native interoperability protocol

Unified Ledger

3.3. Regulatory Challenges for Digital Assets

Thesis 3.3.
To successfully participate in the emerging financial ecosystem, jurisdictions will need regulatory frameworks that accommodate digital assets while maintaining their primary policy objectives of ensuring financial stability and protecting consumers.

Discussion
As digital assets evolve, financial regulators are updating their frameworks. While digital assets technologies and infrastructure eliminate certain risk addressed by existing regulations, new risks and regulatory needs arise. Controls and governance remain crucial in decentralized ecosystems used by traditional financial institutions to ensure financial stability and integrity, ensuring adequate consumer protection. Participants need to understand who manages their applications, assets and networks.

This is especially important when it comes to gaining favorable capital treatment under Basel requirements, which emphasize transparency about transaction validators, which is essential for bridging DeFi and TradFi.

Also, Anti-Money Laundering (AML) regulations, including the Travel Rule, are challenging to implement in the context of the broader adoption of digital assets on public open networks.

Digital ledger solutions capable of bridging the gap provide open access and connectivity, but maintain privacy and control by ensuring that only authorized entities can validate transactions or access certain data, supporting cross-jurisdictional transactions without compromising regulatory compliance.

The internet provides a helpful analogy. It's a public network, globally connected through common standards, yet each organization controls access to its own systems and data. Firewalls, authentication and access controls ensure that only authorized parties can interact with or view sensitive information.

Markets worldwide are adopting digital asset regulations at different paces. Some are moving quickly, leveraging supportive legal frameworks, while others are more cautious, slowing adoption. This multi-speed regulatory landscape presents a challenge - digital asset solutions must be flexible enough to accommodate different jurisdictions without

sacrificing global connectivity and efficient transfer of data across markets. Achieving unified global regulatory standards for digital assets is an unrealistic expectation for adoption, but interoperability across jurisdictions remains crucial. In a globally interconnected financial system, what happens in one market often affects others. As regulations change, these systems must remain agile enough to accommodate shifting requirements without sacrificing stability or security.

Conclusion
To succeed in the evolving digital asset landscape, regulatory frameworks must balance innovation with financial stability and consumer protection. As global uniformity is unlikely, interoperable systems that adapt to diverse regulations are essential. Jurisdictions with flexible, but robust rules will be well-positioned to thrive in the emerging digital asset economy.

3.4. Switzerland as a Financial Market Hub for Digital Assets

Thesis 3.4.
Switzerland has established a strong foundation to position itself as a key player in the emerging financial ecosystem.

Discussion
Historically, Switzerland's limited natural resources have driven a strong emphasis on education and innovation, positioning it as a global leader in both areas[1]. This foundation has enabled Switzerland to develop one of the world's most competitive financial industries, vital to its economy, supported by a technically skilled labor force, top educational institutions, a dynamic, innovation-driven environment, complemented by a stable political system that supports decentralized governance and innovation-friendly regulations.

Switzerland's expertise extends to international collaboration, with many associations facilitating dialogue on topics like AI governance, financial innovation and inclusion. Favorable tax policies, coupled with open trade and foreign policies, attract both domestic and international businesses, fostering a supportive environment for emerging industries, such as digital assets. Regulatory milestones, like the FINMA ICO Guidelines (2018)[2] and the Swiss DLT Framework (2021)[3], establish Switzerland as a pioneer in the regulation of digital assets, setting standards that balance market stability and regulatory clarity for the growing digital asset sector.

1 Switzerland ranking in the QS World University, see Subject Rankings 2024 | Top Universities, and the Global Innovation Index 2024, see wipo.int/gii-ranking/en/switzerland, both visited in January 2025.
2 FINMA ICO Guidelines, see finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/, visited in January 2025.
3 SIF information on blockchain and DLT, see sif.admin.ch/en/blockchain-dlt-en, visited in January 2025.

Further, Switzerland's legal framework, developer hubs, blockchain-focused co-working spaces, knowledgeable regulators and service providers, as well as the foundation model's importance for Layer 1 blockchain projects underscore its distinct position in digital finance. The country hosts crypto banks and specialized financial service providers, as well as traditional banks integrating new technologies. Leading research and educational initiatives at ETHZ Finsuretech hub, EPFL, the University of Zurich's Blockchain Center and the University of Basel Center for Innovative Finance contribute significantly to blockchain advancements[4]. Notably, the University of Lucerne recently established a new research hub focused on this technology. The Swiss National Bank's work on wholesale CBDCs and the crypto-friendly stances of Zug and Lugano reinforce Switzerland's unique role as a center for public blockchain initiatives.

Global Impact through First Live Wholesale CBDC from Swiss National Bank

The Swiss National Bank (SNB) won the Global Impact Award by Central Banking in the latter's seventh annual Fintech and Regtech Global Awards in November 2024 for pioneering – as the world's first central bank – live wholesale CBDC and monetary policy operations on distributed ledger technology[1]. The SNB thereby completed phase III of Project Helvetia, its multiphase investigation on the settlement of tokenised assets using central bank money. The issuance of token-based SNB bills worth CHF 64 million (USD 72 million) on SIX Digital Exchange (SDX), with a one-week term for liquidity absorption, was a success. However, the number of participants and the traded volumes on DLT-based infrastructures are yet to increase. Hence, the question of whether to conduct monetary policy operations on a DLT-based infrastructure is premature. SDX is a stock exchange and central securities depository run on DLT by the same group that runs the Swiss Exchange and Bolsas y Mercados Españoles, the latter of which operates all of Spain's stock markets and financial systems[2].

1 Popowicz, J., 2024.
2 Swiss National Bank, Economic Note, Nr. 4 / 2024.

In addition to Switzerland's regulatory and innovation-driven environment, the country's financial sector has become increasingly integrated with digital asset offerings. SDX established the world's first fully regulated stock exchange

4 European Commission: Directorate-General for Financial Stability, Financial Services and Capital Markets Union and Schär, F., Enhancing financial services with permissionless blockchains, Publications Office of the European Union, 2024, see op.europa.eu/en/publication-detail/-/publication/cab54e8e-ad3b-11ef-acb1-01aa75ed71a1/language-en, visited December 2024.

and central securities depository and they have issued pioneering digital bonds, signalling an important step forward in regulated digital finance. New blockchain enabled platforms like BX Digital are following to establish a market for digital assets. Software providers such as Digital Asset deliver software that underpins such platforms on the global market through the Canton Network, monthly processing USD 3.6 trillion of tokenized RWAs.

Furthermore, approximately 20 Swiss banks now provide custody and trading services for digital assets, reflecting a strong institutional adoption. The crypto native banks Sygnum and Amina are among the first globally to offer comprehensive digital asset services, including custody, trading, staking and tokenized asset management. In addition, various globally active digital asset financial service providers like GenTwo (assetization), 21Shares (crypto ETPs), Scrypt (institutional trading and custody), CryptoFinance (institutional trading and custody) or G-20 (asset management) have setup an operational hub in Switzerland.

The Swiss Crypto Valley region in Zug hosts major organizations behind prominent public blockchain networks like Ethereum, Solana, Tezos, Polkadot, Near, Dfinity, Cardano and Cosmos Interchain, fostering a vibrant ecosystem of innovation. Further south, Lugano's "Plan B" — a collaboration with Tether — aims to establish the city as a blockchain hub by transforming its financial infrastructure with Bitcoin technology. This initiative underscores Switzerland's position as a pioneer in integrating blockchain into urban development. Switzerland is also home to key digital asset custody technology providers, such as Taurus, Ripple (Metaco), Securosys and Bitbox, which play a critical role in supporting the secure handling of digital assets for institutions and private investors alike. Finally, some of the globally most recognized blockchain and DeFi projects like dYdX (perpetual trading), Curve (AMM), 1inch (exchange), Linea (Ethereum L2), Safe (multisig wallet), Liquity (borrowing), Socios (fan token) and many others have built up a presence in Switzerland.

Conclusion

This environment has positioned Switzerland at the forefront of digital transformation, fostering a vibrant and diverse ecosystem. On one hand, the Crypto Valley is home to numerous crypto-native actors, including the foundations behind many leading public blockchains, as well as service providers and crypto-focused banks. On the other hand, traditional organizations are actively investing in technological innovation and adoption, with established banks, digital exchanges and technology providers transforming their business models to leverage the benefits of new technologies. Some traditional banks have already implemented a crypto offering, while others are preparing to launch in the near future.

Switzerland's regulatory framework allows for the natural progression of business while ensuring the stability of the financial systems for which it is entrusted. Moreover, the country offers a strong academic foundation in this realm, with top-rated universities, research institutions and spin-offs driving advancements in finance, technology and digital assets. This holistic approach enhances Switzerland's reputation as a global leader in digital finance, illustrates its commitment to embrace change and its encouragement for innovation throughout the financial ecosystem.

04.

Digital Trust

Authors and Contributors

Name	Level of Contribution	Association
Säuberli, Daniel	Thematic Lead & Lead Author	Digital Identity and Data Sovereignty Association (DIDAS)
Suvorov, Vasily	Author	Accelerate.swiss
Tölke, Andreas	Author and Session Lead	Swisscom AG
Camenisch, Jan	Author	DFINITIY Foundation
Dr. Aad, Imad	Author	École Polytechnique Fédérale de Lausanne (EPFL)
Goldscheider, Daniel	Contributor	OpenWallet Foundation
Schneider, Christoph	Contributor	Global Legal Entity Identifier Foundation (GLEIF)
Tan, Xue	Contributor	GLEIF
Ng, Adrian	Contributor	GLEIF
Dr. Alioth, Simon	Contributor	Synpulse Schweiz AG
Huber, Hans	Contributor	verifiable.trade Foundation
Bühler, Marc	Contributor	TI&M AG
Wolf, Stephan	Contributor	International Chamber of Commerce, DSI IAB
Zuberbühler, Roger	Contributor	TI&M AG
Dr. Rauschenbach, Rolf	Contributor	Federal Office of Justice FOJ, Swiss Confederation
Hett, Carmen	Contributor	UN Refugee Agency (UNHCR)
Kaeppeli, Juerg	Contributor	Noumena Digital
Birch, David	Contributor	Global Thought Leader in Digital Finance, author, writer
Darrell O'Donnell	Contributor	Ayra Association
Trachsler, Tracy	Contributor	DFINITY Foundation
Hoehener, Johs. PATHWAY 2035 TEAM	Contributor	FIND Innovation Sounding Board and Pathway 2035 Review Board member

The digital age has transformed how we live, work and interact. It is challenging individuals' and organizations' control over their data and digital traces as power shifts to centralized platforms and automated systems.

The erosion of sovereignty reflects a broader trend where individuals and organizations struggle to understand risks or to retain control over their personal data, in favor of external actors, often operating with opaque practices. As digital infrastructures evolve, safeguarding autonomy and agency will be key to ensuring that individuals and organizations can continue to operate freely and with trust in increasingly automated and complex digital ecosystems.

This chapter shall increase decision maker's awareness on digital trust and Switzerland's strategic journey towards facilitating robust digital trust ecosystems. A strategic imperative that requires a delicate balance between attracting foreign investment and addressing the diverse requirements of its own economy and society as well as those of its partners.

Digital trust pertains to the confidence individuals, businesses and societies place in the secure and reliable exchange of information and transactions within the digital realm. As digital technologies and automation become increasingly ubiquitous, safeguarding this trust has emerged as a critical challenge[1].

The importance of digital trust cannot be overstated. Failure of digital technology in critical scenarios can lead to significant harm, making it imperative to cultivate user trust in these systems[2]. Moreover, the rapid growth of the internet and the proliferation of digital services have rendered it impractical for entities to have prior offline trust, necessitating the evolution of new approaches to digital trust.

Switzerland, renowned for its innovative spirit and attractiveness to foreign investment, is uniquely positioned to facilitate dialogue and advancements in and around these complexities[3].

The foundational need for trust layers that enable people, organizations and machines to globally verify counterparties and data authenticity can be globally observed in increasing complexity of complying with regulations as well as exploitation by bad actors and fraudsters. While economic incentives have advanced emphasis on building digital public infrastructures, bridging the trust gap is critical to ensure secure interactions in increasingly autonomous digital systems.

This is especially important as IT systems evolve from being primarily human-centric to increasingly machine-driven, with algorithms and automation operating more autonomously. Ensuring human agency and accountability within this shifting digital landscape is essential to maintain trust and governance.

As one of the most innovative and trusted countries in the world[4], Switzerland is uniquely positioned not only as a convener of conversations in and around digital trust, but as a landmark to establish key principles, evolve technology and act as a **key player, contributor and showcase leader** to collaboratively build and demonstrate trust mechanisms in action. As it has done in the past, building and relying on true innovation partnerships.

The aim of this chapter is to define the global role Switzerland must adopt to maintain its digital sovereignty while positioning itself to seize the opportunities created by global digital trust initiatives.

What is Digital Trust?

Digital trust is the foundation determining the confidence in digital ecosystems. It goes beyond integrity, security, authenticity and ethical use of systems and data, to ensure that all participants can interact securely and responsibly. It is ensured by the interplay of the two inseparable parts: Technical Trust and Human Trust.

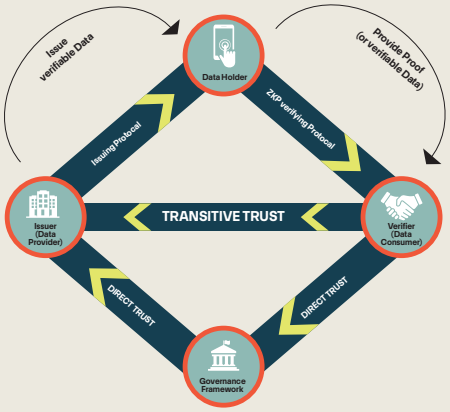
Technical Trust is all the foundational technologies and assurances that go along with them - e.g., cryptography, protocols, data formats. **Human Trust**, however, is all about the governance rules that apply to the norms and usage of technology and determine the roles of various players and how they participate in a given ecosystem. It is very important to understand that no technology alone can ensure trust, only in combination with a proper governance framework it becomes possible to create an ecosystem that builds trust and required liability for all its participants. **Transactional trust** emerges during specific interactions or exchanges between participants in the ecosystem. It is built within the context of a specific use case or interaction and depends on how information is presented, verified and interpreted in real-time interactions.

Complexities in establishing digital trust demand an "act global – think local" approach, rooted in worldwide standards while empowering localized governance. In response, the Digital Identity and Data Sovereignty Association (DIDAS) has been founded in Switzerland, dedicated to fostering inclusive, ongoing dialogue. DIDAS aims to help shape technology, governance and the adoption process, while demystifying the mechanisms at play through real-world use cases and practical showcases.

1 Akram, R. N., & Ko, R. K. L., 2014; Dapp, T. F., 2017.
2 Given-Wilson, T., Baranov, E., & Legay, A., 2020.
3 Tan, K.-L., Chi, C., & Lam, K., 2022; Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M., 2018.
4 WIPO Global Innovation Index, 2024.

The Trust Diamond

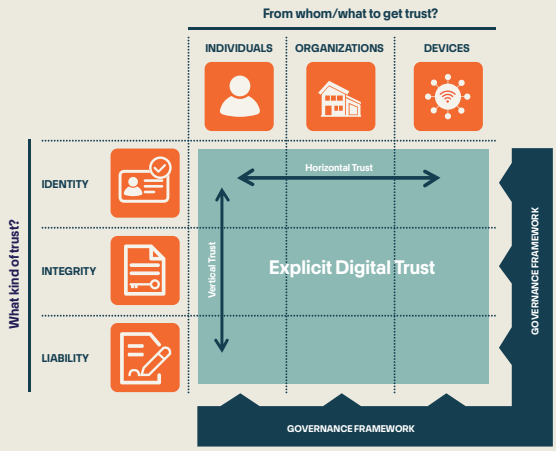
The Trust Diamond as of the Trust over IP's Whitepaper of November 2021 illustrates roles in a digital trust ecosystem: issuers provide data, holders manage credentials, verifiers authenticate them and governing authorities ensure compliance. There is no direct relationship between the issuer and the verifier, ensuring privacy.



Source: trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0–2021–11–17.pdf, visited in December 2024; DIDAS.swiss – Digital Identity and Data Sovereignty Association, derived from Trust Over IP Whitepaper (2021)

Transactional Trust Model

The following Transactional Trust model provides a good foundation and high-level understanding on what is driving the need for digital identities and the interplay with the integrity of information and a required liability of a digital transaction. However, a governance is required as well to define the interplay between human and technical trust and the dynamics between vertical and horizontal trust, incorporating the role of interfaces (like wallet-based applications) in creating human-comprehensible transparency on governance for the user.



Fertile Ground for the future of Financial Services

Source: Andreas Toelke, Swisscom

Furthermore, digital trust is shaped by diverse regional requirements and approaches to privacy, governance and security. While China, the EU and the US each have different models, the core goal of digital trust remains the same: ensuring integrity, security, liability and autonomy in digital ecosystems.

Trust mechanisms can make use of various technological components. E.g., using decentralized identifiers (DIDs) and verifiable credentials (VCs) allows users to securely control their data while interacting in a privacy-preserving manner. Technologies like DLT and their applications such as DeFi play crucial roles in promoting new ways to create transparency and immutability. Critically, however, the success of these systems relies heavily on the combinations in which they are applied to solve problems in use cases, that otherwise would not be solved.

To capitalize on its leadership in innovation and address challenges in digital trust, Switzerland should:

- **Enhance Funding Mechanisms**: Develop and systematically apply strategies to make public funds available and to attract venture capital for start-ups and established economic players specializing in digital trust technologies alike.
- **Promote Public-Private Partnerships**: Leverage collaborations between government entities, private sector companies and academic institutions and society, to foster innovation and advance the impact of adaptable digital trust solutions.
- **Invest in Talent Development**: Focus on education and training programs that equip the workforce with skills pertinent to cybersecurity and digital trust, ensuring a pipeline of qualified professionals.
- **Strengthen Regulatory Frameworks**: Continue to refine and enforce regulations that uphold agility in innovation, digital inclusion, data privacy and security, reinforcing Switzerland's reputation as a trusted digital hub.

Switzerland's Unique Legal Framework for Electronic Signatures

Switzerland stands out for integrating electronic signatures directly into its Code of Obligations (CO)[1], providing a clear and robust legal basis for their use. Under Swiss law, the Qualified Electronic Signature (QES) is **explicitly recognized as equivalent to a handwritten signature**. This alignment ensures that electronic signatures carry the same legal weight as traditional signatures, offering businesses and individuals a secure, efficient and legally binding method for executing agreements in a digital environment. This forward-thinking approach underscores Switzerland's commitment to fostering trust and innovation in digital interactions.

The Legal Entity Identifier: Enabling Global Identification of Entities

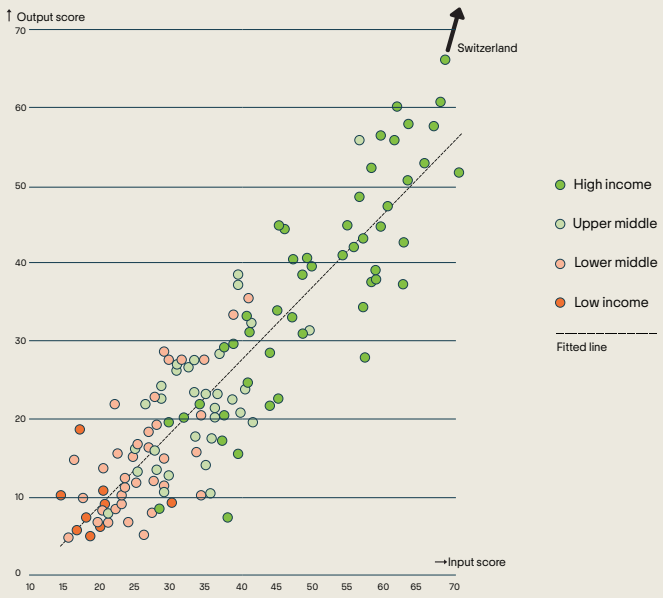
The Legal Entity Identifier (LEI), managed by the Global Legal Entity Identifier Foundation (GLEIF), is a unique, 20-character alphanumeric code used to identify legal entities engaging in financial transactions. Designed to enhance transparency and reduce systemic risk, the LEI provides a standardized reference point for legal entities worldwide, linking key reference data such as ownership and registration details. It is widely used in financial markets for regulatory reporting, compliance and risk management, facilitating seamless cross-border transactions and improving trust in the global financial system. By enabling clear entity identification, the LEI plays a crucial role in fostering accountability and stability across industries. The verifiable Legal Entity Identifier (vLEI) holds immense potential to enable trusted, automated, and cross-border verification of organizations, enhancing transparency, reducing compliance costs, and unlocking new efficiencies in global digital ecosystems.

1 Art. 14 para. 2 CO.

Switzerland Widely Recognized for Leadership in Innovation

The Global Innovation Index 2024 report highlights Switzerland's exceptional performance in innovation outputs, ranking first globally[1]. This indicates proficiency in converting innovation investments into tangible outcomes - a critical factor in developing, implementing and advancing digital trust capabilities. However, the report also notes a decline in venture capital deal values by 43.7% between 2022 and 2023, suggesting potential challenges in funding for emerging ventures.

1 WIPO Global Innovation Index, 2024.



Relationship between innovation inputs and outputs
Source: WIPO Global Innovation Index (2024)

Fertile Ground for the Future of Financial Services

Trust has always been vital in financial services and trade. The future of banking relies not only on navigating regulatory boundaries; but also, on fostering global and local opportunities through dynamic partnerships among regulators, governments, established organizations, startups and society to drive innovation and progress.

Switzerland's political system, which emphasizes consensus, stability and citizen-driven involvement, forms a foundation for such innovation partnerships, as regulations not only reflect the core values; but also, actively help public and private stakeholders to create and capture value in new market domains.

Exceptional opportunities emerge when governments, regulators and businesses collaborate to foster sustainable economic growth with technology playing a central role. Switzerland's history, illustrates the **potential of strategic public-private partnerships**. To illustrate, the Swiss railway system is a historic example of how coordinated efforts in infrastructure have driven significant economic value, showcasing

the power of collaboration across government, industry and innovation.

Albeit every jurisdiction must choose its own path, it seems that public-private collaboration is essential to build robust and **trustworthy "digital rails"** that ensure the digital realm remains secure, trusted and accountable. As societies increasingly depend on complex digital infrastructures and interconnected systems, the digital transformation of global economies highlights the urgent need for these frameworks. They cannot be built effectively by either the public or private sector alone but often require joint efforts with a focus on international cooperation and interoperability.

Shifts toward digital sovereignty, such as Europe's efforts to reduce Big Tech reliance through marketplace guardrails and open protocols, could foster inclusive ecosystems. By empowering individuals to access data traditionally held by banks, the rule offers a pathway to reshape customer interactions and foster greater trust and collaboration.

Where We Are Today?

The foundational internet architecture lacks robust mechanisms to verify the identities of individuals, organizations and controlled machines. Initially designed to facilitate open knowledge sharing, the core internet infrastructure relies on system identifiers such as IP addresses, which do not inherently provide the means to authenticate diverse entities within digital ecosystems.

Today's Solutions: Fight Symptoms

Current IT stacks rely on stop-gap measures - controls, accounts, firewalls - addressing symptoms of the internet's early design choices. These measures, costly and unreliable, fail to curb the rising cost of cybercrime, projected to surge 50% by 2029 reaching USD 16 trillion losses, annually[1].

Public Key Infrastructure (PKI), critical yet insufficient, introduces additional vulnerabilities. Emerging decentralized solutions and post-quantum security initiatives aim to close these gaps. However, end-to-end digitization expectations, heightened during COVID, remain unmet, emphasizing the need for **bridging this gap**. Without **trustworthy infrastructure** enabling global, legally certain transactions, barriers to digital value creation persist. A shift from platform-based models to **protocol-driven infrastructures** is essential to building resilient, interoperable systems that address these challenges at their root.

1 Global Cybercrime Estimated Cost 2029, 2024.

Lessons Learned from the Past

Switzerland's Crypto AG incident[2] highlighted the misuse of trust and underscores the need for verifiability, autonomy and inclusive governance at all levels, from software developers to politicians. Such principles guide efforts to build trust-based digital foundations. Paradoxically, **a key learning is that ensuring sustained sovereignty and innovation requires collaborative, open and privacy-focused infrastructures, instead of attempting to manage security through obfuscation**.

Digital Public Infrastructures (DPI)

DPIs, increasingly vital foundations of the digital fabric serving societal and economic needs, emphasize security, equity and innovation. But unlike the internet's original design, they must embed privacy, transparency and inclusive governance as their trust foundations - key to fostering their adoption and success. They also ensure infrastructure components, our future "digital rails", are invested collaboratively, so economic participants and the economy as a whole is enabled to build and leverage network effects, prospering on top of their foundations.

Trust in Running Code

The concept of "trust in running code" highlights the importance of embedding transparency, security and verifiability into the digital systems and infrastructures. This approach ensures that software, algorithms and systems operate as intended, without hidden biases or vulnerabilities. By emphasizing open-source standards and verifiable execution, it provides a foundation for innovation and resilience of digital ecosystems.

Verifiable execution is particularly crucial as wallets become more prevalent. Ensuring that code executes transparently and can be audited by all stakeholders builds confidence in these systems and prevents misuse or unauthorized alterations. This capability not only strengthens technical trust; but also, empowers individuals and organizations to take control of their digital interactions. Verifiable execution transforms trust from an assumption into a provable reality.

Agents and Agency

Artificial intelligence (AI) systems designed to reduce information asymmetries, democratize access, or even maximize shareholder value - such as wallets or algorithmic tools. These are powerful instruments that facilitate digital transactions and other tasks. However, these tools do not and should not

2 Crypto AG Scandal: Swiss Crypto AG spying scandal shakes reputation for neutrality, see bbc.com/news/world-europe-51487856, visited December 2024.

embody agency. The concept of AI holding agency, or the ability to make autonomous decisions or act with self-direction based on reasoning, is both misplaced and counterproductive at the current state of AI/ML (machine learning) development. Instead, these systems should operate under **verifiable delegation**: acting on behalf of individuals or organizations, with clear control mechanisms in place.

This approach ensures that humans - whether individuals, businesses, or nations - retain **verifiable controllership** over tools and machines. Such a framework reinforces **accountability**. By focusing on verifiable delegation and acting on behalf, we can build trust in digital infrastructures while maintaining human oversight and agency at every level.

The Opportunity

In this context, based on its history of providing the world with trusted services for centuries, Switzerland's role can be significant. Historically, the alpine country of Switzerland has been driven by the core principles of neutrality and self-sovereignty. Its well-functioning direct democracy ensures legislative initiatives reflect the needs, interests and preferences of its citizens. Valuing privacy both online and offline, individual autonomy is central to Swiss values.

Just as Switzerland built its railway systems in the 19th century, which has not only catered to its internal needs, but also created value for its neighbors, significantly enhancing the overall economic and societal impact. Similarly, can the Confederation repeat this success by enabling values-aligned, digital foundations that have impact beyond its sovereign territory?

Switzerland is, as demonstrated by its pioneering DLT framework law and the ongoing e-ID initiative, an **early adoption and showcase leader** and thus attract investments and economic activity that has international impact. **Digital trust capabilities rooted in Switzerland, would be an extremely welcomed and credible proposition for jurisdictions and ecosystems across the globe**. Continuing this approach will enable the country to meet its citizens' needs domestically while supporting its international partners. The future belongs to those who demonstrate action, not just words.

Achieving mature and continuously improving digital trust capabilities requires strategic prioritization and funding of digital trust research and development. These efforts must be integrated into political and economic agendas and aligned across key economic sectors, including telecommunications, trade, energy, healthcare and financial services.

Institutions such as Innosuisse and the Swiss National Science Foundation, in collaboration with international partners from the EU, Asia and the USA should align behind a unified vision for fostering innovation in this space. By investing in research, development and capacity-building initiatives, these organizations would contribute to catalyze the creation of resilient, interoperable infrastructures. This not only positions Switzerland as a global leader in digital trust; but also ensures that its ecosystem benefits from the network effects of collaboration, driving economic growth and reinforcing its role as a trusted partner in the global digital economy.

As individuals take greater control of their digital data and traces by 2035, it is crucial to initiate a meaningful dialogue today to align investments, regulations and innovation. This will enable the creation of a robust, trust-based digital future characterized by seamless, authentic and universally accessible experiences and interactions.

As individuals take greater control of their digital data and traces by 2035, it is crucial to initiate a meaningful dialogue today to align investments, regulations and innovation. This will enable the creation of a robust, trust-based digital future characterized by seamless, authentic and universally accessible experiences and interactions.

4.1. Trend towards Decentralized, Sovereign and User-Centric Service Models

Thesis 4.1.
The shifts towards increasingly decentralized, sovereign and user-centric service models will transform digital channels.

Discussion
Decentralized and self-sovereign identity models offer significant advantages, such as enhanced data privacy control, reduced dependency on centralized providers and improved security through cryptographic methods. They foster trust by enabling users to share their data selectively and transparently. However, these opportunities come with challenges, including the complexity of implementation, the potential burden on users to safeguard digital keys and possible resistance from established institutions. Another risk is the lack of standards, which could lead to interoperability issues. In addition, self-sovereign concepts often trigger resistance, given their radical views of sovereignty and decentralization, while there may be many shades of grey in implementing privacy-by-design and data minimization principles.

Tokenization bridges the real and digital worlds, integrating digital assets and verifiable proofs into essential tools for daily life and wealth management. Language needs to be carefully chosen in describing applied concepts and a wealth of expert dialogue and experimentation is required, enabling usable self-sovereign solutions to be ready for adoption by the mass market. Commitment to key principles enabling users' privacy and increased levels of control is representing the international community's expectation towards future solutions coming from Switzerland.

Increased computing power in personal devices enables privacy-preserving, edge-based processing of complex data,

simplifying user experiences. Users can consent to share information and revoke access at will, with data remaining on their devices or under enhanced control when shared beyond. Tokenization bridges the real and digital worlds, integrating digital assets and verifiable proofs into essential tools for daily life and wealth management. Language needs to be carefully chosen in describing applied concepts and a wealth of expert dialogue and experimentation is required, enabling usable self-sovereign solutions to be ready for adoption by the mass market. Commitment to key principles enabling users' privacy and increased levels of control is representing the international community's expectation towards future solutions coming from Switzerland.

Conclusion

By empowering individuals to securely manage and control their digital assets and data, it reduces reliance on third-party brokers, enabling users to navigate the digital world with greater security and autonomy. Wallets combined with advanced, algorithmic user experience (UX) apps allow users to broker digital services under their sovereign control, supported by standardized protocols for seamless service integration. Increased computing power in personal devices enables privacy-preserving, edge-based processing of complex data, simplifying user experiences. Users can consent to share information and revoke access at will, with data remaining on their devices or under enhanced control when shared beyond. Tokenization bridges the real and digital worlds, integrating digital assets and verifiable proofs into essential tools for daily life and wealth management. Language needs to be carefully chosen in describing applied concepts and a wealth of expert dialogue and experimentation is required, enabling usable self-sovereign solutions to be ready for adoption by the mass market. Commitment to key principles enabling users' privacy and increased levels of control is representing the international community's expectation towards future solutions coming from Switzerland.

4.2. From Trust Fragmentation to Governed, Interoperable Digital Trust Ecosystems

Thesis 4.2.

The Evolution of the Internet - From trust fragmentation to governed, interoperable digital trust ecosystems by 2035.

Discussion

The transition from fragmented trust systems to governed, interoperable digital trust ecosystems by 2035 sparks debates over balancing central governance with decentralization principles. Proponents argue that standardized frameworks can ensure security, interoperability and scalability, fostering global trust. Critics caution that centralized governance could stifle innovation, compromise individual autonomy and introduce new points of failure. The challenge lies in balancing local governance, global standards and the self-sovereign ethos of digital trust.

UK Digital Identity and Attributes Trust Framework Gamma (0.4) Pre-Release

In November 2024, the UK Office for Digital Identities and Attributes (OfDIA) published a pre-release of the latest iteration of the UK digital identity and attributes trust framework In November 2024. It sets the standards that various categories of service provider operating in the digital identity space must meet to achieve certification against the standards, denoting that the organisation is a secure and trusted provider of digital identity products and services[1].

1 gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04/uk-digital-identity-and-attributes-trust-framework-gamma-04-pre-release; twobirds.com/en/insights/2024/uk/version-4-ofdia-announces-the-gamma-trust-framework, both visited in December 2024.

European Digital Identity (EUDI) vs. UK Digital ID: Key Differences

The European Digital Identity (EUDI) is an initiative by the EU aimed at providing secure and universally accepted digital identities for EU citizens, businesses, and public authorities. It is designed to enable access both private and public services across the EU in a secure and trusted manner, with a strong emphasis on privacy and user control. Unlike the UK's digital ID system, which is primarily focused on providing federated authentication services for access to government services, the EUDI seeks to create a pan-European, wallet-based framework, ensuring interoperability across member states. The key difference lies in the EU's vision of a cross-border, harmonized approach to digital identity, enabling the single market, whereas the UK has adopted a more fragmented, national approach, with separate digital identity schemes for various sectors.

Conclusion

In the 2020s, misinformation, deep fakes and unreliable content have undermined trust in the internet, fuelled by social media giants and bad actors. This has created echo chambers and false realities, threatening trust and the internet as we know it.

However, a "rebirth" is emerging through global trust networks using standardized protocols, verifiable identities, data and privacy-enhancing technologies (e.g., ZKPs) as trust anchors. A minimal "digital trust layer" will ensure technical, semantic, organizational and legal interoperability, enabling participants to transparently verify information authenticity. This will restore confidence in automation, make tamper-proof data

The Trust Over IP Foundation (ToIP) / The Ayra Association

The US-based foundation's mission is to align the technology layers with what they term the "human accountability" of business, legal and social layers that make up governance. Combined, these two halves form a complete framework for digital trust infrastructure, known as the ToIP stack. Specifically, the governance stack defines roles, responsibilities and provides a framework to define rules for all participating entities and mechanisms for ensuring compliance with the agreed standards and policies. Importantly it also provides standardised mechanisms for dispute resolution and enforcement[1]. The Zurich-based **Ayra Association** (formerly the Global Acceptance Network) complements ToIP by focusing on real-world adoption and scaling of trust ecosystems across all ecosystems, while ToIP provides the open standards and frameworks for technical and governance interoperability. Ayra ensures practical implementation across borders and industries, turning ToIP's foundational architecture into operational solutions for use cases like onboarding, compliance, and worker mobility.

1 trustoverip.org/, visited in December 2024.

reusable and realize the once-only principle. Services are increasingly built on open, governance-free protocols like Digital Public Infrastructure (DPI), fostering a sovereign, interoperable global ecosystem.

4.3. Consumer Tech's Triumph in Digital Identity by 2035

Thesis 4.3.
Consumer tech's triumph in digital identity as a possible reality by 2035.

Discussion
Experts debated the tension between government-led efforts to address technical debt (also known as code design debt or code debt, i.e., the implied cost of future reworking because a solution prioritizes expedience over long-term design) and interoperability in digital identity and the dominance of closed ecosystems developed by tech giants. While proponents of private-sector solutions highlighted their scalability and adoption, critics argued these ecosystems undermine privacy, autonomy and transparency, leading to "dark patterns" similar to the ones employed in today's cookie practices. Advocates for self-sovereign identity (SSI) emphasized its potential to empower users and ensure trust through decentralized technologies, citing Switzerland's pioneering role in creating an open digital trust ecosystem. The discussion underscored the need for incentives to drive private-sector participation in interoperable, user-centric identity frameworks.

Conclusion
Three key risks must be avoided:

A. Failure to ensure privacy and autonomy in the use of identity attributes.

B. Treating digital identity merely as an isolated identifier instead of recognizing it as a foundational trust anchor to enhance customer experiences, streamline operations and improve compliance.

C. The use of "dark patterns" in consent design and non-transparent governance, similar to the transparency issues seen with current cookie practices.

As noted in the BIS Finternet report[1], the shift toward SSI frameworks is pivotal, where individuals and entities retain full control of their digital identities, verified through decentralized technologies. This will enable seamless, secure interactions across financial ecosystems without reliance on centralized authorities. Switzerland is pioneering the adoption of privacy-by-design, data minimization and portability principles as part of the future Swiss trust infrastructure[2] (SWIYU) and the creation of an open digital trust ecosystem. SWIYU's initial technology decision has been communicated by the Federal Council[3] on 6 December 2024[4] and its public beta[5] will be launched in early 2025. Technology- and product experimentation has been performed in parallel to the law-making process: The e-ID law's passing by the Swiss Parliament on 20 December 2024 is subject to an optional public referendum within 100 days of the official publication of the decree.

Similarly for legal entities: GLEIF's adoption of decentralized PKI protocols for its organisational identity capability - the vLEI – is building on top of its global, G20 backed governance framework. It highlights how innovative application of technologies can help solve global trust and delegation issues.

1 Carstens, A., & Nilekani, N., 2024.
2 Discussion Paper re Swiss Trust Infrastructure, 2023; SWIYU, 2024.
3 admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-102922.html, visited December 2024.
4 eid.admin.ch/en/e-id-technische-umsetzung-in-zwei-schritten-e, visited December 2024.
5 Public Beta Factsheet, available at backend.eid.admin.ch/fileservice/sdweb-docs-prod-eidch-files/files/2024/10/24/fdbcf1fa-7f33-4f27-80d6-44f14d991939.pdf, visited December 2024.

4.4. A New Approach to Design and Develop IT Infrastructure

Thesis 4.4.
A new fabric is underpinning a digital world.

Discussion
The discussion centers around the role of verifiable data-sharing in driving the adoption of embedded finance and personalized wealth management. Proponents argue that privacy-preserving technologies (PETs), such as zero-knowledge proofs (ZKP) and multi-party computation (MPC), are essential for building trust and enabling innovative, data-driven financial services. Critics, however, question whether the complexities and costs of implementing these technologies can be justified, particularly for smaller financial institutions. Others highlight concerns about achieving sufficient collaboration between public and private infrastructures to create scalable, interoperable systems that benefit all stakeholders equally.

The integration of verifiable data-sharing capabilities is pivotal for accelerating innovation in embedded finance and wealth management, enabling secure, privacy-preserving insights and services. As an end effect, trust-enabled, embedded finance and wealth management, rely on three key pillars: verifiable open data and data commons, verifiable proprietary data that makes services unique and verifiable x-party data shared by clients using sovereign control mechanisms to do so. verifiable open data, proprietary data for unique services and client-controlled data sharing. Beyond identifying investment areas, collaborative funding and transformative levers are necessary to ensure the development, adoption and continuous improvement of these technologies. By fostering synergies between digital public and private infrastructures, stakeholders can create scalable solutions with lasting network effects and economies of scale.

Conclusion
Integrating verifiable data-sharing capabilities is essential for driving innovation in embedded finance and wealth management, enabling secure, privacy-preserving insights and services. Trust-enabled embedded finance relies on three pillars: verifiable open data and data commons, proprietary verifiable data that supports unique services and client-controlled data sharing using sovereign control mechanisms.

Beyond identifying investment opportunities, collaborative funding and strategic levers are vital to ensure the development, adoption and continuous improvement of these technologies. By aligning public and private digital infrastructures, stakeholders can create scalable solutions with enduring network effects and economies of scale.

4.5. Opportunities and Challenges for Banks

Thesis 4.5.
Verifiable data-sharing capabilities accelerate the adoption of embedded finance and personalized digital wealth management.

Discussion
Although trust is essential to the finance industry's business, digital trust is not traditionally a core competence for the sector. This is due to several factors: banks[1] have historically focused on trust in financial transactions, risk management and regulatory compliance, rooted in their long-standing role as central trust intermediaries - areas distinct from the digital expertise required to navigate the complexities of today's digital ecosystems.

While used to meeting regulatory requirements, banks often lack the agility, mindset for experimentation and continuous improvement as well as flexibility in existing technological infrastructures needed to swiftly develop or adopt cutting-edge advancements. Banks have historically relied on their reputation and regulatory frameworks to establish trust with customers. Furthermore, the boundaries between the physical world and the digital one are fading away: assets can be physical or digital and are increasingly interchangeable. Customer interactions with their banks are shifting to digital channels, posing new challenges for Know-Your-Customer (KYC) and Anti-Money Laundering (AML) compliance.

Conversely, decentralized finance (DeFi) relies on protocols, algorithms and code to ensure the security and accuracy of transactions, fundamentally changing how trust is established. Although DeFi is still in its early stage, banks will need to rethink their trust models and incorporate digital trust frameworks if they want to compete in a DeFi-driven world[2]. To thrive in this new landscape, banks must evolve beyond their legacy systems and move towards becoming vital parts of protocols-based, open and interoperable ecosystems that enable them to quickly adapt and innovate.

As the financial industry becomes more dependent on external partners to create innovations, banks remain uniquely positioned when it comes to the issuance of verifiable data to reduce friction and to increase regulatory compliance. Next-Gen Financial Services enabled by digital trust - a core prerequisite for the broader adoption of digital assets and algorithmic tools and automation - offer significant strategic opportunities for banks.

Operational Efficiency and Automation: Removing friction within banks' own and commercial customer's operations, through enabling automation based on trustworthy, verifiable data is an exceptional business opportunity.

1 In this paper the focus is on banks, in future editions a broader scope will be applied.
2 Dapp, 2017.

Banks can, for example, issue and charge for digital proofs that will allow a client to complete a certain transaction with a verifying 3rd party, in frictionless ways. In turn, that enables the 3rd party to accelerate their process automation journey with higher assurance. Their ability to assess and certify the value of real-world assets positions them as natural issuers of transaction-enabling certificates, such as bank guarantees or asset-backed verifiable credentials. These certificates add significant value in complex transactions, streamlining processes and enhancing confidence between parties. A further key area of opportunity is to bring industry solutions to the market that embed key financial services in productized and/or tailored ways into economically relevant, industry specific processes.

Banks can leverage their KYC expertise to issue digital identities for organisations, reducing cross-industry, cross-domain frictions. This aligns with GLEIF's governance framework for Legal Entity Identifiers (LEIs) and the digitally verifiable vLEI[1], offering a globally interoperable standard. The vLEI holds enormous potential for establishing a globally interoperable organizational digital identity standard across all sectors and enables chaining of credentials and resulting verifiable delegation of authority, through a decentralized public key infrastructure (DPKIs).

By adopting this approach, banks can not only cut compliance costs but also create new, scalable revenue models, positioning themselves as essential players in a trust-based digital economy. This shift highlights the potential for financial institutions to extend their roles beyond traditional services, reinforcing their relevance in increasingly interconnected and automated ecosystems.

Increasing consumer confidence: Banks can start to experiment with digital wallets and algorithmic tools today. While digital wallets will take time to enable interoperability, Banks can provide their clients with wallets that work in the bank's broader business ecosystem, enabling holders to hold valuable digital credentials and assets. This can be offered to commercial organizations and individuals. This also provides their clients with tools for secure data handling, particularly as AI and open banking technologies become more integrated. By becoming trusted stewards of verifiable data, banks position themselves well in the broader ecosystem of digital interactions and transactions. This not only aligns with consumer expectations for privacy, but also opens new avenues for revenue and customer engagement in a data-driven world. Further, they can transform the channels and experiences in how financial products are consumed. For example, through trustworthy bots or algorithmic tools that help automate the management of their client's financial wealth on their behalf[2]. These channels are business growth opportunities, to increasingly serve their clients with further future financial services products through new channels, at scale.

Embracing Digital Assets and Decentralized Finance (DeFi): Establishing trust and verifiability in legally binding digital information is crucial and forms the starting point for any reliable and secure digital asset infrastructure. This trust can be achieved by securely programming and configuring smart contracts that make use of accurate, cryptographically verifiable off-chain and on-chain information. This allows the potential of the DLT- technology to be realized in practice. The DLT amendments to Swiss federal laws allow for the secure, fully electronic issuance and transfer of ledger-based securities, thereby improving legal certainty with regard to tokenization. As blockchain protocols create fragmentation in the digital asset space, banks can be the integrating "glue" for their clients, offering regulatory compliance services while bridging centralized and decentralized finance.

Project Agorá – A Public-Private Collaboration

Project Agorá (Greek for "marketplace") is structured as a public-private collaboration. It brings together seven central banks: Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England and the Federal Reserve Bank of New York. They will work in partnership with 40 financial sector firms, convened by the Institute of International Finance (IFF) to explore how tokenisation can enhance wholesale cross-border payments. The project builds on the unified ledger concept and transactional trust is a key element: It could enhance the functioning of the monetary system and provide new solutions using smart contracts and programmability, while maintaining its two-tier structure[1].

1 bis.org/about/bisih/topics/fmis/agora.htm, visited December 2024.

Collaboration and Regulatory Support: To establish digital trust, banks must collaborate with a broad set of stakeholders and engage in true innovation partnerships with governments and innovators to enable more trusted ecosystems in which they create value to capture value. Strong regulatory frameworks will be key in ensuring that these systems maintain high ethical standards, protect customer data and support financial inclusion. For example, the DLT amendments to Swiss federal laws allow for the secure, fully electronic issuance and transfer of ledger-based securities, thereby improving legal certainty with regard to tokenization. Furthermore, they are a good example of the agility needed in execution, to enable new business ecosystems and remain a leading hub for financial market institutions and technological innovation against the background of a sound regulatory environment.

1 GLEIF, 2023; Verifiable LEI (vLEI) Ecosystem Governance Framework v2.0.
2 Birch, D. G., & Rutter, K., 2023.

In many jurisdictions banks have played a central role in identity verification, due to their position as trusted institutions and being mandated to comply with strong KYC requirements. As seen in countries like Sweden and Poland for example, banks have been successful in becoming the primary issuers of digital identities. In some cases, wilfully, in others, forced by regulation. However, in Switzerland, the state has taken ownership of digital identity issuance based on the desire of its citizens expressed in a direct democratic process, removing intermediaries and embedding privacy-by-design principles to protect citizen data.

This makes the Swiss approach unique in terms of its ability to cope with the future challenges of the digital world, in which the data economy and AI is increasingly misused by bad actors to engineer fraudulent and manipulative activities, at unprecedented scale.

FINMA and other regulators should continue to adapt their supervisory approaches, as far as provided for by their mandate, to account for the rapid pace of digital innovation in the ecosystem. This way they can effectively oversee the increasing complexity and diversity of financial products and services. For instance, leveraging organizational identity frameworks and verifiable delegation capabilities of systems such as the GLEIF vLEI could enable regulators to issue licenses as verifiable digital credentials. While in turn, these organizations would be able to issue credentials for their approved financial products and services. This shift would not only enhance accountability, trust and efficiency within the financial market infrastructure but also position regulators as enablers of innovation, ensuring they remain effective in a rapidly evolving financial landscape. Without such progress, they risk being outpaced by the very systems and products they aim to oversee.

Conclusion

Digital trust is essential for building an inclusive, secure, resilient and sustainable digital economy. Switzerland, with its long-standing reputation for trust and innovation, is uniquely positioned to lead the advancement of global digital trust frameworks that are the basis thereof.

Initiatives like the OpenWallet Forum, the Ayra Association (formerly GAN), and DIDAS provide strong foundations to enable trust-based ecosystems and facilitate the necessary dialogue to advance technology, governance and value creation, as demonstrated in advancing Switzerland's Swiss e-ID initiative and its underlying trust infrastructure (SWIYU). It exemplifies Switzerland's foresight and leadership, serving as a model for agile, participatory development of important digital public infrastructures. By integrating policymaking- and political consensus, flexibility and openness for economic value creation, maintaining democratic principles and privacy-by-design, the initiative is demonstrating how DPI's can effectively drive innovation and societal inclusion. This is well represented in the Federal Council's greeting in June 2024[1] at the annual Digital Identity unconference Europe (DICE) in Zurich[2].

The country's digital ecosystem thrives through contributions from world-class institutions such as ETH and EPFL and strong engagement of the private industry, e.g., through Swisscom as a certified trust service provider (TSP)[3] or Deep Tech Nation Switzerland Foundation (DTN). The DTN initiative demonstrates how private investment can attract resources to high-impact technologies. This synergy between academia, infrastructure and private capital ensures Switzerland remains an attractive destination for investors.

Switzerland's global influence is further amplified through hosting and partnering with international organizations, including the UN, ITU, WTO, UNICC and BIS. Initiatives such as the OpenWallet Forum, which aim to bridge these partnerships in the context of digital trust, underline Switzerland's role in fostering trust and interoperability at a global level. This diversity of actors, industries, and collaborative efforts creates a foundation for innovation that balances inclusion and openness, safety, and impact, positioning Switzerland as a hub for scalable and future-proof digital solutions.

Its proactive approach and principles-based regulation, its ability to balance it with innovation while staying true to democratic traditions, makes it a global example of how digital trust can drive societal progress and economic prosperity.

A robust, privacy-preserving approach to digital trust, exemplified by Switzerland's SWIYU initiative, offers a blueprint for nations looking to harness the digital revolution while safeguarding citizens' rights. Progress in this area requires a clear agenda that prioritizes digital trust and aligns stakeholders around a shared vision. Looking toward 2035, Switzerland must act decisively by fostering innovation, strategically allocating resources and enabling collaboration across sectors.

Similar to the Swiss railways in the 19th century, digital infrastructures such as the Swiss Trust Infrastructure (SWIYU) will be critical for GDP growth, enabling a wealth of trust-based services for the economy, including simplifying the management of data privacy and compliance, increasing levels of assurance of automation and algorithmic solutions, preventing fraud and information warfare, while unlocking novel business opportunities. Global problems that need to be addressed with urgency. In that context, GLEIF's adoption of decentralized PKI protocols for its organisational identity capability the vLEI, building on top of its global, decentralized system (GLEIS), highlights how innovative application

1 eid.admin.ch/de/grussbotschaft-von-bundesrat-beat-jans-zur-der-digital-identity-unconference-europe-dice, visited December 2024.
2 eid.admin.ch/en/grussbotschaft-von-bundesrat-beat-jans-zur-der-digital-identity-unconference-europe-dice-e, visited December 2024.
3 bit.admin.ch/en/sg-pki-trust-service-provider-tsp-en, visited December 2024.

of technologies can help solve global trust and delegation issues.

SWIYU further serves as a first step in that direction as well as both, a foundation for trust and as a sandbox for further experimentation for its iterative evolution, allowing start-ups and established players to develop and scale novel solutions in areas like verifiable data, wholesale- and retail digital value exchange, Privacy-Enhancing Technologies (PETs) and quantum-safe cryptography. National and international public-private-academia partnerships will need to be formed to advance this ecosystem with a focus on fundamental research and economic value creation, informed by applied science and experimentation.

05.

Quantum-Safe

Authors and Contributors

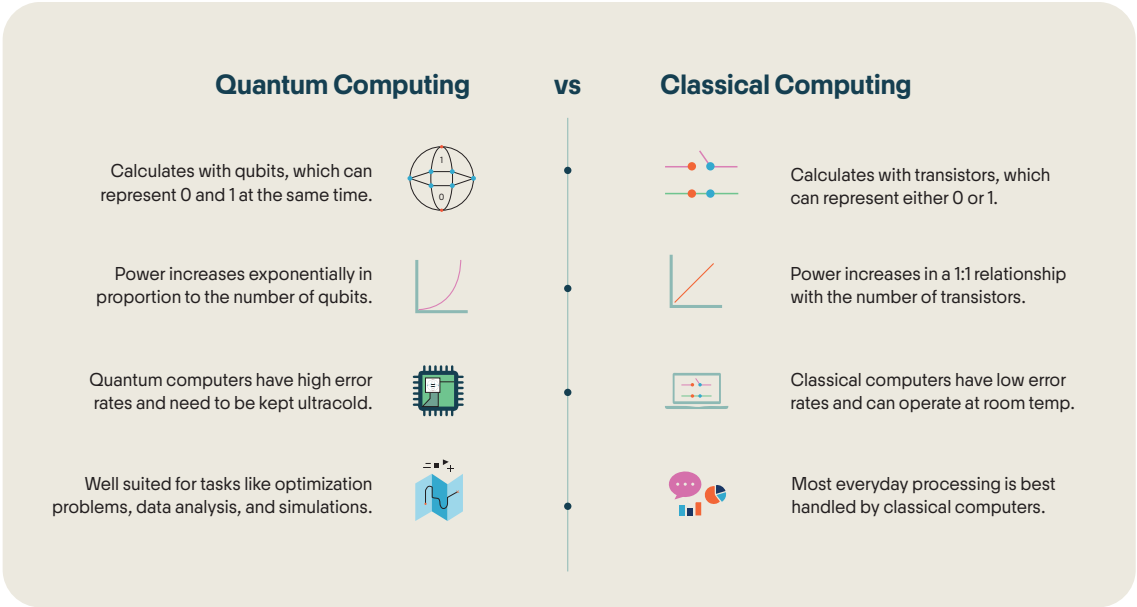
Name	Level of Contribution	Association
Bogdan, Damir	Co-Thematic Lead & Co-Lead Author	QuantumBasel Corp.
Dr. Flöther F., Frederik	Co-Thematic Lead & Co-Lead Author	QuantumBasel Corp.
Comboeuf, Patrick	Contributor	Pixel Plus AG
Gogol, Krzysztof	Contributor	University of Zurich
Niklowitz, Antje	Contributor	Independent
Niklowitz, Matthias	Contributor	Trendscout at e-foresight
Novotny, Pascal	Contributor	Finanz und Wirtschaft Forum
Propson, Drew	Contributor	World Economic Forum
Richard, Johann	Contributor	European Space Deep-Tech Innovation Centre of European Space Agency (ESA)
Suarez, Steve	Contributor	HorizonX Consulting
Tacker, Manoj	Contributor	Ambassador Innovaud Swiss

Quantum technology is experiencing a «2nd revolution» with quantum sensing, communication and computing rapidly developing and making their way from lab to industry. Quantum computing is currently in the **noisy intermediate-scale quantum (NIQS)** era; while the «iPhone moment» has not yet happened, problems are already being mapped to algorithms and use cases are being explored, including applications in chemical simulation, machine learning and optimization. Fully functional (fault-tolerant) quantum computers will become available expectedly in the early 2030s; it is not a question of "if" but "when" quantum computing will be mainstream, with rapid progress being made in hardware as well as algorithms and software.

Although the technology is still nascent and it is important to manage expectations, quantum computing has the potential to solve many challenges in the financial sector and other industries, with hundreds of use cases already identified and billions, if not trillions, in value waiting to be unlocked (Langione, Bobier, Cui, Naudet-Baulieu, & Kumar, 2023). Democratizing access to quantum systems and solutions is of great importance, since there is otherwise a risk of the digital divide widening, as can already be seen in increased export control regulations.

However, quantum computers also pose a significant cybersecurity challenge due to their ability to efficiently solve certain mathematical problems that underlie traditional cryptography. While such decryption will only be possible in a number of years, "harvest now, decrypt later" attacks have likely already started (Vaswani et al., 2019). Hence, all areas of the digital economy, particularly the financial sector, face challenges as a result – and must start planning for migration to quantum-safe cryptography already today, affecting billions of devices across the globe.

To realize the potential of quantum technology, stakeholders must understand its opportunities and risks. Collaboration is key, with organizations seeking partnerships to address the complexities of quantum development. Transition plans and robust security measures are essential. Organizations should prioritize crypto-agility, while regulators should ensure economic resilience.



Source: CB Insights

5.1. The Emergence of Quantum Computing

Thesis 5.1.
Quantum computers will become mainstream in the coming decade and will be used for highly compute-intensive applications by most banks in developed countries.

Discussion
Quantum computing offers a paradigm shift in computing power. Unlike classical computers, which use bits (0 or 1, similar to heads or tails on a coin), quantum computers leverage qubits that can exist in multiple states simultaneously (superposition, similar to a rotating coin). This enables quantum algorithms to solve problems more efficiently, particularly complex simulations, scenarios and data analysis tasks.

However, there are still challenges. For instance, external disturbances can easily disrupt the state of qubits, making calculations unreliable. The first quantum computers are usually set up in particularly stable and heavily cooled environments.

Research is constantly producing new materials, concepts and processes to make these computers more robust and allow them to be installed in conventional data center environments. The advancements will make quantum computing more accessible and practical.

Switzerland is a leader in quantum research, with institutions like Quantum Basel, the Quantum Science and Technology group & Quantum Computing Hub at EPFL and the Quantum Center at ETH driving applied research and development in quantum computing and quantum technologies. On the international stage, governments have been investing heavily in quantum research for years, motivated by the potential for competitive advantages and enhanced cybersecurity (offensively and defensively).

Quantum computers are particularly well suited for a range of applications in finance such as risk management, which involves the complex interdependencies between the interactions of assets and their derivatives. The adjacent field of portfolio management is another promising application area due to the high effort involved and the many compromises inherent in portfolio optimization. Traditional approaches often rely on shortcuts due to limitations in classical computing and quantum computers can provide more accurate and reliable solutions for these complex tasks. The demands on banking IT systems specifically are increasing due to growing data volumes and the rising use of AI, which may soon push these systems to their limits. Consequently, quantum computing is proposing a promising solution[1].

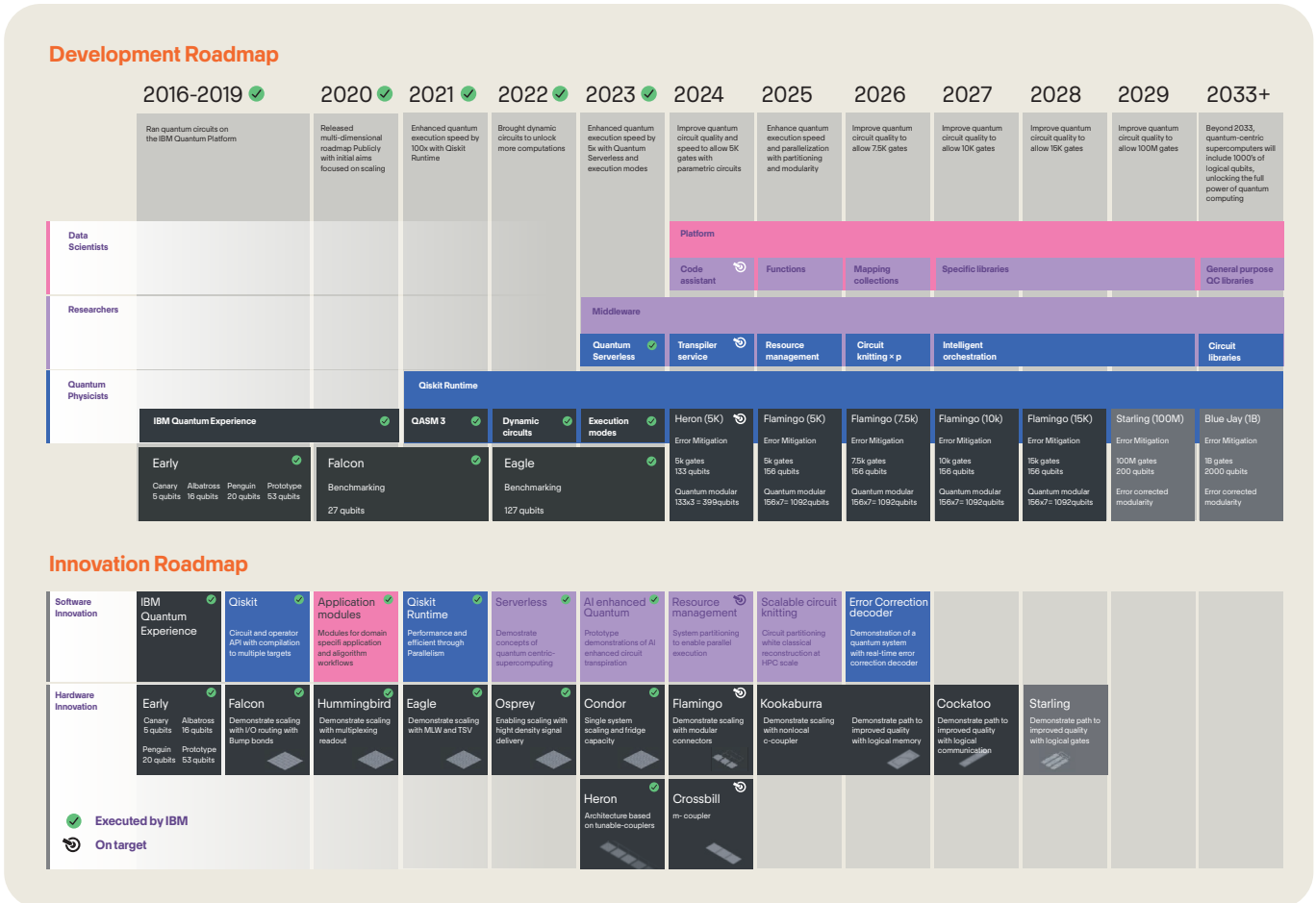
Quantum computers can also be valuable for market monitoring, analyzing complex market interactions and recognizing patterns. Additionally, they can assist supervisory authorities and market participants in their oversight roles. These applications demonstrate the versatility of quantum computing and its potential to transform various aspects of the financial industry.

In recent years, quantum computers have rapidly developed. Quantum supremacy over conventional systems has been achieved, although the tasks solved are often not yet practically relevant. Google solved a very specialized mathematical problem with a proprietary quantum computing system. International companies such as Amazon, Google and IBM are continually publishing and updating their roadmaps for further development in the coming years.

Conclusion

Several technical challenges remain to be overcome before quantum computers can reach their full potential. In the near future, a hybrid approach combining quantum and classical

1 Swiss Banking Association, 2024.



Source: IBM Quantum Roadmap Guide -- Scaling And Expanding The Usefulness of Quantum Computing

computing will likely be the most practical solution. Quantum computers will be used to tackle specific, computationally intensive tasks, while classical computers will handle routine calculations.

5.2. Threats of Quantum Computing

Thesis 5.2.
Quantum computers pose a threat to traditional cryptography in the financial sector and beyond. However, quantum-safe cryptography is expected to safeguard our digital future.

Discussion
Quantum computers will be able to break many of today's encryption methods, which is particularly problematic in our digitalized financial world. They threaten both asymmetric and symmetric cryptography. Shor's algorithm breaks public-key cryptography by efficiently factoring large numbers, compromising authentication methods used in areas such as e-banking. Grover's algorithm speeds up searches quadratically, potentially compromising symmetric-key encryption. While doubling key lengths can mitigate some risks, new quantum algorithms may pose further threats. A key question is when "Y2Q" (when quantum computers are sufficiently powerful to crack current protocols) will happen; many estimates suggest the 2030s, but Y2Q could already happen during the current decade. Therefore, staying updated on the latest developments in quantum computing and cryptography is crucial.

HSBC's recent pilot for quantum-safe cryptography on tokenized gold demonstrates the proactive approach financial institutions take to address quantum computing risks. One the one hand, tokenizing assets on blockchain or DLT platforms offer significant potential for efficiency and innovation. On the other hand, since encryption forms the basis of blockchain and DLT, they are vulnerable to cyber-attacks. The initial results of HSBC's tests indicate that digital assets today can be hacked. However, it is possible to protect the underlying DLT technology without a complete overhaul. This ensures the interoperability of emerging DLT systems and allows for adapting of encryption methods and private keys as needed to address future quantum threats.

As the economy becomes increasingly digital, the threat of quantum computing extends beyond the financial sector. Industries like healthcare and public administration, which are undergoing digital transformation, are also vulnerable. These sectors often rely on outdated encryption methods that quantum computers could compromise. The interconnected nature of modern systems, where numerous databases are linked using traditional encryption, further exacerbates the risk.

Conclusion
The transition to quantum-safe procedures is critical to mitigate the risks of quantum computing. During this transition, compatibility issues and potential security vulnerabilities may arise. Attackers could exploit outdated protocols or standards through downgrade attacks. To address these challenges, one needs to bridge the gap between old and new security standards while minimizing vulnerabilities.

5.3. Quantum-Safe Cryptography

Thesis 5.3.
Quantum-safe approaches such as post-quantum cryptography (PQC) and quantum key distribution (QKD) will be widely deployed in the next decade.

Discussion
The potential of quantum computers to break existing encryption methods necessitates a flexible approach known as cryptoagility. This allows organizations to adapt to evolving threats and adopt new, quantum-resistant cryptographic methods as needed.

Quantum-Save Techniques

- **Post-Quantum Cryptography (PQC)**
  Utilizes new mathematical algorithms (run on classical computers) designed to resist attacks by quantum computers. PQC aims to replace current cryptographic algorithms that will become insecure with the advent of quantum computing. There are generally no guarantees that PQC standards are safe with respect to all future attack possibilities by quantum (and classical) computers.

- **Quantum Key Distribution (QKD)**
  Employs quantum mechanics to create secure communication channels for distributing encryption keys. QKD can work alongside PQC and other cryptographic methods to provide a secure key distribution mechanism in which, at least in theory, no eavesdropping can go undetected.

In August 2024, the National Institute of Standards and Technology (NIST) published the first PQC methods using traditional computers which represents a significant milestone in the development of quantum-resistant cryptography. This, coupled with recommendations from organizations like the G7[1], WEF[2] and the European Union Agency for Cybersecurity (ENISA), underscores the importance of preparing for the quantum era. It is not yet clear how quantum-safe standards will scale; they may be distributed by IT providers through a market-driven approach or they could become a core part of public infrastructure.

1 World Economic Forum & Deloitte, 2022.
2 World Economic Forum, 2023.

While PQC is expected to be the initial solution, QKD offers additional security benefits, particularly in high-security scenarios. The combination of PQC and QKD can provide a robust and layered approach to cybersecurity[1]. Compared to PQC, QKD is currently lacking in certification and standardization, although progress in both areas has recently been made[2]. Additionally, organizations like the World Economic Forum are actively monitoring developments and providing recommendations[3].

Switzerland is at the forefront of quantum technology research and development with initiatives at the level of government, academia and industry[4]. Government initiatives like the Open Quantum Institute (OQI) and the National Cyber Security Centre (NCSC) are working towards the United Nations Sustainable Development Goals (SDGs). Further, leading universities, including ETH Zurich, EPFL, University of Geneva and University of Basel, are pioneering quantum hardware and software. Finally, financial institutions such as UBS, Migros Bank and the BIS are actively exploring quantum technology applications.

Technology companies like IBM and ID Quantique are also driving advancements in quantum-safe cryptography and security, with various pilot projects underway[5]. The Swiss Quantum Initiative (SQI), launched in 2022, aims to strengthen Switzerland's position in quantum technology and foster international collaborations[6].

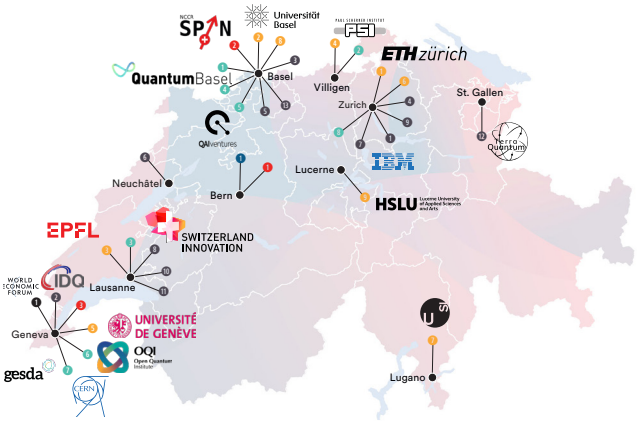


Illustration of quantum computing related endeavours in Switzerland
Source: swissnex.org/boston/news/new-mapping-of-swiss-quantum-ecosystem/

Conclusion

Quantum technologies are here to stay. Quantum computing has not yet become mainstream, but early applications are already being explored. At the same time, there is a need to start planning today for migration to quantum-safe standards as larger quantum computers, which will likely emerge in the 2030s, are expected to threaten many currently employed cryptographic protocols.

1 Quantum Economic Development Consortium, 2022; Quantum Economic Development Consortium 2024a; Quantum Economic Development Consortium, 2024b.
2 Mahon, 2020.
3 G7 Cyber Expert Group, 2024; Bettinger et al., 2024.
4 Mahon, 2020.
5 ID Quantique, 2024a; ID Quantique, 2024b.
6 SERI, 2023.

06.

Conclusion

Embarking on the "Pathway 2035 for Financial Innovation – Your Navigator" is akin to hiking on a complex, ever-changing trail toward a distant summit. The journey is shaped by exploration, collaboration and adaptation through thoughtful preparation and precautions as we navigate key themes defining the future financial system.

Technological megatrends are dominant disruptors shaping finance now and over the next decade. As financial systems evolve, AI, digital trust, digital assets and quantum-safe technologies have emerged as essential building blocks, reflecting financial innovation's intersection with technological change. Within this framework, concepts such as the Finternet — the fusion of finance and interconnected digital ecosystems — represents a parallel, entwined pathway offering both opportunities and challenges. Exploring how these elements align in practical applications has been central to this journey.

The interconnected nature of these building blocks became especially evident on 5 November 2024: Digital assets represent and secure ownership, while digital trust combats threats such as deepfakes and fraud and AI and quantum technologies promise productivity gains and energy efficiencies when applied in tandem. These converged trends highlight the urgency of reaching the summit of 2035 in an inclusive, sustainable and data-driven way without losing assets to cyberattacks or other risks. As we move toward 2035, there is a need to effectively navigate judiciously, balancing options, risks and strategies along the route. Decision-making by the financial ecosystem actors will need to align with these key areas, which are poised to shape the future of finance. This publication aims to spark the dialoque within the ecosystem which is necessary prior to that any informed decision making can take place.

Effectively navigating the future of finance will require adopting AI, digital trust, digital assets and quantum computing with a focus on security, efficiency and strategic impact. Here is why:

- **AI and human oversight balance**: Determining the optimal level of AI autonomy in financial decision-making while maintaining regulatory compliance and ethical standards.
- **AI and blockchain integration**: Leveraging AI for predictive analytics in cryptocurrency markets while using blockchain for transparent and secure transactions.
- **Don't trust, verify**: Implementing trust infrastructures to enable electronic identification and verifiable data exchange ecosystems, fostering users' autonomy and authentic interactions and transactions in an increasingly digital world while addressing fraud, compliance and removing friction in processes across domains and data silos.
- **Quantum-safe cryptography implementation**: Preparing for the post-quantum era by adopting cryptographic algorithms resistant to quantum attacks, ensuring long-term data security and data trust[1].
- **Strategic and timely investments**: Allocating resources to develop quantum machine learning algorithms, quantum enhanced AI, technologies and cross-disciplinary education and regulatory oversight to revolutionize risk assessment and portfolio optimization.

Achieving the above effective navigation requires curated information and the development or enhancement of a framework to guide decision-making and address the trade-offs and uncertainties inherent in adopting these technologies. This framework must balance many considerations to ensure continuity and resilience for a trusted ecosystem. This publication intends to serve that very end by building bridges within the ecosystem, facilitating the flow of information, educate and contribute to the further development or enhancement of the needed framework.

The journey to 2035 will not be straightforward. Like a challenging hike, the Pathway for Financial Innovation can be rocky, foggy and demanding — yet, it is also filled with opportunities for discovery and progress. This collaborative exploration — fuelled by passionate debate, diverse perspectives and mutual learning — mirrors the journey itself. By sharing insights, confronting challenges and remaining open to change, we build clarity, strengthen our collective understanding and pave a more efficient and effective path forward.

1 Mohammed & Abdul, 2024.

References

Akram, R. N., & Ko, R. K. L. (2014). Digital Trust - Trusted Computing and Beyond: A Position Paper (By R. N. Akram & R. K. L. Ko; Vol. 526, p. 884). Available at doi.org/10.1109/trustcom.2014.116.

Bettinger, K., et al. (2024, June). Top 10 emerging technologies of 2024. World Economic Forum. Available at weforum.org/publications/top-10-emerging-technologies-2024/.

Birch, D., & Rutter, K. (2023). Where are the customers' bots? The AI paradigm shift in retail banking. ResearchGate. Available at doi.org/10.13140/RG.2.2.38257.6921.

Birch, D. (2023). The Impact of ChatGPT and Open Banking Cannot be Underestimated, Forbes. Available at The Impact Of ChatGPT And Open Banking Cannot Be Underestimated: forbes.com/sites/davidbirch/2023/05/27/the-impact-of-chatgpt-and-open-banking-cannot-be-underestimated

Carstens, A., & Nilekani, N. (2024). Finternet: The financial system for the future (BIS Working Papers No. 1178). Bank for International Settlements.

Dapp, T. F. (2017). Fintech: The Digital Transformation in the Financial Sector. In T. F. Dapp, CSR, sustainability, ethics & governance (p. 189). Springer International Publishing. Available at doi.org/10.1007/978-3-319-54603-2_16.

Discussion Paper re Swiss Trust Infrastructure (2023). Initial technological basis for the Swiss trust infrastructure github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/discussion-paper-tech-proposal.md.

Feng, D., Hitsch, R., Qin, K., Gervais, A., Wattenhofer, R., Yao, Y., Wang Y. (2023). DeFi Auditing: Mechanisms, Effectiveness and User Perceptions. Available at tik-db.ee.ethz.ch/file/5918406b48ff5e07db534cb4775b6a1c/.

Given-Wilson, T., Baranov, E., & Legay, A. (2020). Building User Trust of Critical Digital Technologies (By T. Given-Wilson, E. Baranov, & A. Legay; Vol. 7, p. 1199). Available at doi.org/10.1109/icit45562.2020.9067154.

GLEIF. (2023). verifiable LEI (vLEI) Ecosystem Governance Framework v2.0.

Global Cybercrime Estimated Cost 2029 (2024). Available at statista.com/forecasts/1280009/cost-cybercrime-worldwide.

G7 Cyber Expert Group (2024). G7 Cyber Expert Group statement on planning for the opportunities and risks of quantum computing. Available at home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf.

G7 Cyber Expert Group (2024). G7 Cyber Expert Group statement on planning for the opportunities and risks of quantum computing. Available at home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf.

ID Quantique (2024a, October 16). IDQ and SK Broadband complete phase one of nation-wide Korean QKD network. Available at idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/.

ID Quantique (2024b, October 16). Singtel to develop Singapore's first nationwide quantum safe network plus for enterprises. Available at idquantique.com/singtel-quantum-safe-network/.

Kordzadeh, N., & Ghasemaghaei, M. (2021). Algorithmic bias: Review, synthesis and future research directions. European Journal of Information Systems, 31(3), 388–409.

Langione, M., Bobier, J.-F., Cui, Z., Naudet-Baulieu, C., & Kumar, A. (2023). Quantum computing is becoming business ready. Boston Consulting Group.

LexisNexis Risk Solutions - Global State of of Fraud and Identity Report (2024). Availalbe at risk.lexisnexis.com/global/en/insights-resources/research/global-state-of-fraud-and-identity.

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. (2018). Governance Strategies for a Sustainable Digital World. In I. Linkov, B. D. Trump, K. Poinsatte-Jones, & M. Florin, Sustainability (Vol. 10, Issue 2, p. 440). Multidisciplinary Digital Publishing Institute. doi.org/10.3390/su10020440.

Mahon, C. J. (2020). Quantentechnologie in der Schweiz: Überlegungen und Empfehlungen des Schweizerischen Wissenschaftsrates SWR. Politische Analyse, 1/2020. Bern: Schweizerischer Wissenschaftsrat.

Merluzzi, R., Hoffet, I., Sigrist S., (2024). Generate AImpact. Available at innovate-switzerland.ch, see Generate-AI-mpact_D.pdf.

Mikalef, P., Conboy, K., Lundström, J. E., & Popovič, A. (2022). Thinking responsibly about responsible AI and the 'dark side' of AI. European Journal of Information Systems, 31(3), 257–268.

Mirzadeh, I., Alizadeh, K., Shahrokhi, H., Tuzel, O., Bengio, S., & Farajtabar, M. (2023). GSM-Symbolic: Understanding the limitations of mathematical reasoning in large language models. Apple. Available at arxiv.org/abs/2304.01927.

Mohammed, S. S., & Abdul, A. (2024). Navigating Blockchain's twin challenges: Scalability and regulatory compliance. Blockchains, 2(3), 265–298.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at bitcoin.org/bitcoin.pdf.

Nilekani, N., Varma P., Shetty S. (2024). Finternet: Technology Vision and Architecture.

Popowicz, J. (2024). The Winners of the 2024 Fintech & RegTech Global Awards, CentralBanking. Available at The winners of the 2024 FinTech & RegTech Global Awards - Central Banking.

Prosser, D. (2024), Switzerland Stakes Its Claim As Europe's Hottest Tech Centre, Forbes. Available at Switzerland Stakes Its Claim As Europe's Hottest Tech Centre.

Quantum Economic Development Consortium (QED-C®) (2022). A guide to a quantum-safe organization: Transitioning from today's cybersecurity to a quantum-resilient environment. Arlington, VA.

Quantum Economic Development Consortium (QED-C®) (2024a, May). QKD: Part of a defense-in-depth security strategy. Available at quantumconsortium.org/qkd-part-of-a-defense-in-depth-security-strategy/.

Quantum Economic Development Consortium (QED-C®) (2024b, May). Quantum technology for securing financial messaging. Available at https://quantumconsortium.org/financial24.

Rödiger, J. (2023). Quantum key distribution. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), Trends in data protection and encryption technologies (pp. 41–45). Cham: Springer Nature Switzerland. doi.org/10.1007/978-3-031-33386-6_9.

SBA (2024). Quantum computing in banking: Funktionsweise, Anwendungsfelder und Handlungsempfehlungen für Schweizer Banken [Expert report]. Available at swissbanking.ch/.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 1–19. doi.org/10.20955/r.103.1-19.

State Secretariat for Education, Research and Innovation (SERI) (2023, April 8). Space research and technology: Establishment of a European space deep-tech innovation centre (ESDI) in Villigen (AG). Available at sbfi.admin.ch/sbfi/en/home/news/press-releases.msg-id-88841.html.

Swiss National Bank, Economic Note, Nr. 4 / 2024, Piloting Monetary Policy Implementation on a DLT-Based Infrastructure – Issuance of Digital SNB Bills.

SWIYU (2024). Notes on the design and name of the e-ID and trust infrastructure. Available at eid.admin.ch/en/swiyu-e.

Tan, K.-L., Chi, C., & Lam, K. (2022). Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization. In K.-L. Tan, C. Chi, & K. Lam, arXiv (Cornell University). Cornell University. Available at doi.org/10.48550/arxiv.2202.10069.

Ting, H. L. J., Kang, X., Li, T., Wang, H., & Chu, C. (2021). On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study. In H. L. J. Ting, X. Kang, T. Li, H. Wang, & C. Chu, IEEE Access (Vol. 9, p. 106743). Institute of Electrical and Electronics Engineers. Available at doi.org/10.1109/access.2021.3100767.

The White House (2023, October 30). Executive Order on the safe, secure and trustworthy development and use of artificial intelligence. Available at whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

UK Government (2023, November 1). The Bletchley Declaration by countries attending the AI Safety Summit. Available at gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

WIPO Global Innovation Index (2024). Available at wipo.int/web-publications/global-innovation-index-2024/en.

World Bank (2017). Distributed Ledger Technology (DLT) and Blockchain. Fintech Note No. 1. Available at documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

World Economic Forum (2023). Quantum security for the financial sector: Informing global regulatory approaches. Available at weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/.

World Economic Forum & Deloitte (2022). Transitioning to a quantum-secure economy. Geneva, Switzerland: World Economic Forum.

Glossary

Abbreviation	Definition
AI	Artificial Intelligence
AML	Anti-Money Laundering
APIs	Application Programming Interfaces
BIS	Bank for International Settlements
BX	BX Swiss AG
CBDC	Central Bank Digital Currency
CSCS	National Supercomputing Center
DeFi	Decentralized Finance
DETEC	Federal Department of the Environment, Transport, Energy and Communications
DID	Decentralized Identifier
DIDAS	Digital Identity and Data Sovereignty Association
DLT	Distributed Ledger Technology
DPI	Digital Public Infrastructure
DPKI	Decentralized Public Key Infrastructures
DTN	Deep Tech Nation Switzerland
DvP	Delivery versus Payment
ENISA	European Union Agency for Cybersecurity
EPFL	École Polytechnique Fédérale de Lausanne
ETH	Swiss Federal Institute of Technology Zurich
ETH	Eidgenössische Technische Hochschule
EU	European Union
EUDI	European Digital Identity
FEAT	Fairness, Ethics, Accountability and Transparency
FHE	Fully Homomorphic Encryption
FIND	Swiss Financial Innovation Desk
GDP	Gross Domestic Product
GLEIF	Global Legal Entity Identifier Foundation
ICAIN	International Computation and AI Network
IT	Information Technology
KYC	Know-Your-Customer
LEI	Legal Entity Identifier
LLM	Large Language Models
MAS	Monetary Authority of Singapore
MIT	Massachusetts Institute of Technology

Abbreviation	Definition
ML	Machine Learning
MPC	Multi-Party Computation
NCSC	National Cyber Security Centre
NIQS	Noisy Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OQI	Open Quantum Institute
PETs	Privacy-Enhancing Technologies
PPTs	Privacy-Preserving Technologies
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QES	Qualified Eletronic Signature
R&D	Research & Development
RWA	Real-World Asset
SDG	Sustainable Development Goals
SDX	Swiss Digital Exchange
SERI	State Secretariat for Education, Research and Innovation
SME	Small and Medium-Sized Enterprises
SNAI	Swiss National AI Institute
SQI	Swiss Quantum Initiative
SSI	Self-Sovereign Identity
SWIYU	Swiss Trust Infrastructure
ToIP	Trust over IP
TradFi	Traditional Finance
TSP	Trust Service Provider
UN	United Nations
US	United States of America
UX	User Experience
VC	Verifiable Credential
vLEI	Verifiable Legal Entity Identifier
WEF	World Economic Forum
ZKP	Zero-Knowledge Proofs