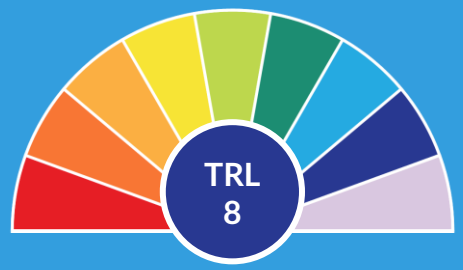
Feynic TECHNOLOGY

FINOS

Artificial Intelligence

Zenith Special Interest Group

Executive Primer



Artificial Intelligence

3 Types of Artificial Intelligence:

Weak AI

- Limited by programming – won't develop new skills
- Analyses preferences and improves over time

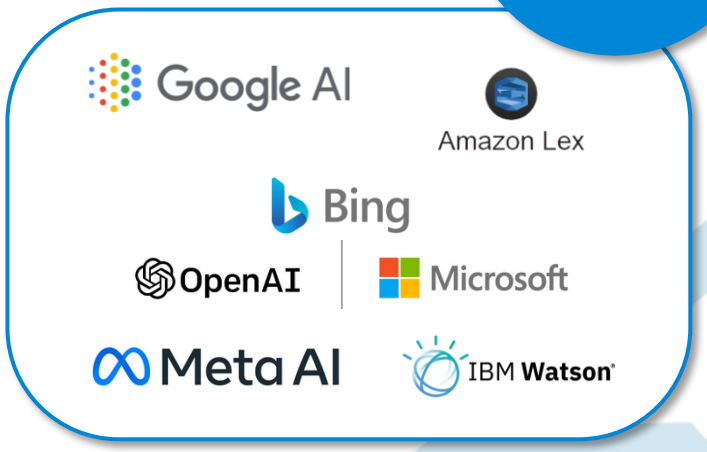
Strong AI

- Learns new skills through contextualisation
- Applies knowledge to plan ahead
- Can adapt as changes occur

Superintelligence

- Self-aware
- Surpasses human intelligence
- Only exists in science fiction

AI Industry $190bn (by 2025)



Artificial Intelligence is revolutionizing the financial technology (fintech) industry, offering unprecedented opportunities and challenges alike. As a rapidly advancing branch of computer science, AI enables the simulation of human thought and language through code, with recent breakthroughs in machine learning and deep learning propelling the field's growth.

For fintech companies, embracing AI presents a pathway to stay competitive amid the increasing investments in AI innovation by big tech firms. However, alongside these opportunities, several critical challenges arise, demanding careful attention.

In this executive briefing, we will explore the key challenges facing the fintech industry as it harnesses the potential of AI. Specifically, we will examine the issues of bias in AI systems, the ethical implications of AI adoption, and the importance of addressing security and maintenance concerns for AI systems.

By addressing these challenges, fintech companies can pave the way for widespread and responsible adoption of AI tools, ensuring a safe, secure, and sustainable transformation of the financial services industry.

In the following sections, we will delve deeper into each challenge, highlighting the Zenith program's opportunities to assist fintech and financial services firms in overcoming these hurdles and unlocking the full potential of AI technology. In our appendices, we will brief you on the landscape of each underlying technology.

Biases in AI Systems

Key Highlights

- AI algorithms can inherit biases from the data they are trained on, leading to unfair and discriminatory outcomes.
- Identifying and mitigating bias in AI systems is crucial to building trust and ensuring ethical AI adoption.
- Biases in AI can have significant consequences in sensitive domains such as finance, impacting customer satisfaction and regulatory compliance.

Artificial Intelligence (AI) systems are prone to inheriting biases present in the data used for their training. Technologies such as **Data Annotation** and **Data Quality & Observability** play vital roles in identifying potential biases and ensuring that training data is diverse and representative. By incorporating these technologies, fintech companies can reduce the risk of biased AI outcomes and promote fairness in their algorithms.

By adopting **Synthetic Data** generating practices, fintech companies can broaden the training data sets to include more diverse demographics in their customer data to improve the quality of the data in.

To ensure ethical AI adoption, fintech companies should also invest in technologies that relate to **Model Validation & Monitoring**. These technologies help in understanding how AI models arrive at decisions, making the decision-making process more transparent and interpretable for customers and regulators.

To tackle biases effectively, fintech firms should adopt strategies such as **diverse and representative data collection**, **regular audits**, and **fairness-aware machine learning algorithms**. Transparency in AI decision-making can also aid in identifying potential biases and gaining customer trust.

Ethical Implications of AI Adoption

Key Highlights

- Ethical considerations in AI adoption involve privacy, transparency, fairness, and accountability.
- Fintech companies must balance AI-driven innovation with societal and ethical responsibilities.
- Responsible AI practices enhance brand reputation and foster long-term customer loyalty.

As fintech companies embrace AI-driven innovation, they must navigate the ethical implications associated with its adoption. Ethical considerations involve ensuring customer privacy, maintaining transparency in AI decision-making, promoting fairness in algorithms, and being accountable for AI-driven outcomes.

To address ethical concerns related to data privacy, fintech companies should implement **Data De-Identification** techniques. These technologies protect sensitive customer information while still allowing AI models to derive valuable insights.

Transparency and explain-ability are vital to address ethical concerns in AI adoption. Consumers and regulators are increasingly demanding explanations for AI-driven decisions. To enhance transparency, fintech firms should adopt **Interpretable AI** models and establish clear communication channels to explain the logic behind AI recommendations.

Fintech companies should acknowledge their responsibility for AI-driven outcomes and establish mechanisms to rectify errors and address customer complaints. Being accountable for AI systems' behaviour fosters trust and loyalty among customers and stakeholders.

Responsible AI practices not only align with societal values but also enhance the reputation of fintech companies. Customers are more likely to engage with companies that demonstrate a commitment to ethical AI practices, leading to long-term customer loyalty and sustainable growth.

Interpretable AI	Explainable AI
Small models that are inherently interpretable e.g. Small decision trees or linear models with a small number of input variables	The process of applying a method that models the output of a more complex model This is performed after model training has been completed

Feynic TECHNOLOGY

Key Highlights

- The integration of AI in fintech increases cybersecurity risks and potential vulnerabilities.
- Continuous monitoring and updates are essential to ensure the robustness and reliability of AI systems.
- Investing in AI security and maintenance is a proactive approach to safeguarding financial data and operations.

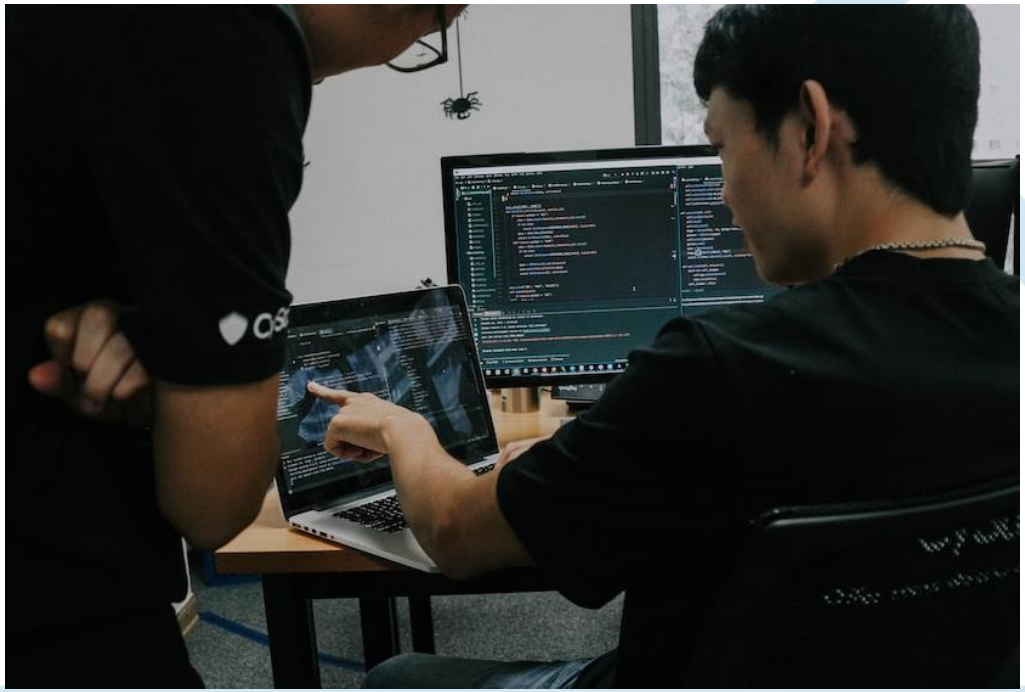
Security & Maintenance Concerns of Artificial Intelligence

While AI offers transformative opportunities for fintech, it also introduces new cybersecurity risks and vulnerabilities. The integration of AI in financial services creates potential entry points for cyber threats, necessitating a proactive approach to security and maintenance.

Technologies like **Resource Optimisation** and **Machine Learning Deployment** are essential in enhancing AI system robustness. These technologies ensure that AI models are efficiently deployed and managed, minimizing potential vulnerabilities and optimizing real-time resource usage.

AI can also play a pivotal role in fraud prevention and risk mitigation within fintech. Implementing **AI-driven Fraud Detection** systems enhances the security of financial transactions and improves overall risk management.

Considering the rapid evolution of cyber threats, fintech companies must stay informed about emerging security challenges and invest in state-of-the-art AI security technologies. Collaborating with industry experts and sharing insights on security best practices can further fortify fintech systems against potential threats.



Zenith Opportunities

Benefits of Exploration Through Zenith

1. Common frameworks for adoption can be crowdsourced
2. Reduce internal expertise limitations through community engagement
3. Time-to-market of exploration in innovation labs reduced
4. Reserve resources for high-value development
5. Interoperability improves adoption across the industry
6. Keep in step with security, standards, and new feature development
7. Benefit from community contributions across key themes
8. Empower, retain, and attract innovators and developers

12 Identified AI Themes

In the Appendix, we have outlined 12 key themes that serve as innovation verticals within the Zenith program.

These themes encompass cutting-edge technologies and trends in Artificial Intelligence.

Embracing these themes will drive transformative advancements in fintech, fostering collaboration, and collective innovation within our foundation.

26 Identified Blockers

We have identified 26 crucial blockers impeding the widespread adoption of AI technologies in the fintech industry. These will be posted on the Zenith site and repository.

To address these challenges, we call upon the wider development community to propose open source solutions through the Zenith program.

Together, we can leverage the power of collective expertise to overcome these obstacles and shape the future of AI-powered fintech solutions.

Join us in our mission to create secure, transparent, and ethical AI applications that redefine the financial services landscape.

- AI Chipsets
- AI-Driven Fraud Detection
- Computer Vision
- Data Annotation
- Data De-Identification
- Data Quality & Observability
- Machine Learning Platforms & Deployment
- Model Validation & Monitoring
- Natural Language Processing
- Resource Optimisation
- Synthetic Data
- Version Control & Experiment Tracking

Appendices

Data Sheets

This report uses Technology Readiness Levels. For more information as to this classification system, please refer to ***https://zenith.finos.org/docs/roadmap/TRL***

Feynic TECHNOLOGY

AI Chipsets

Specialized processors designed to accelerate AI computations, enabling faster and more efficient AI model training and inference.

In fintech, AI chipsets drive groundbreaking advancements, powering complex algorithms for fraud detection, risk assessment, and personalized financial recommendations.

The high-performance computing capabilities of AI chipsets empower fintech companies to deliver real-time, data-intensive services, transforming the way financial institutions operate and serve their customers.

You can find out more about this subject in our AI Chipset Primer on the Zenith GitHub.

OPPORTUNITY

Trigger
- Surging Demand for applications
- Need for fast/efficient data processing
- Deep learning advancements

Players
NVIDIA, intel, AMD, IBM, Alphabet Google

Drivers
- Regulatory pressure to improve fraud detection
- Cost savings through AI-driven automation

IMPACT

Macro

Network Effects & Interactions
- Integration across multiple processes
- AI-powered data analytics
- Desire to enhance financial inclusivity & accessibility

Distruptees
- Legacy hardware manufacturers
- Traditional financial services requiring adaptation
- Skill shifts in job market as AI impacts workforce

Micro

Competitive Advantage
- Faster & more accurate decision making
- Risk mgmt. & fraud detection capabilities
- Real-time data processing for insights

Financial Benefits
- Optimised AI model training on chipsets
- AI-powers Fintech expands market reach
- Increased investment for innovative startups

Supply Chain
- Data storage and integration chipsets
- Collaboration with data/chipset manufacturers
- Disruption to trad. hardware supply chains

TECHNICAL FEASIBILITY

Technical Merit
- Success of accelerated AI model training
- Scalability of AI chipsets for high volume data
- Need for continuous upskilling to ensure workforce proficiency

Tools, Ecosystem & Skills
- Growing ecosystem of service providers
- Availability of dev tools & frameworks
- Need for continuous upskilling to ensure chipsets are implemented correctly

Friction
- Data privacy concerns
- Integration challenges with legacy hardware
- Regulatory compliance complexities

FUTURE

Timeline
- **Short term** Initial adoption and integration of chipsets
- **Medium term** Widespread deployment in financial services
- **Long term** Evolution of chipsets for autonomous solutions

Risks
- Potential delays in advancements and innovations
- Market resistance and scepticism in AI-decision making
- Ethical considerations surrounding responsible use

SUMMARY

AI chipsets offer a compelling opportunity for fintech, revolutionizing financial services through accelerated AI computations. Advancements in specialized hardware enable groundbreaking applications in fraud detection, risk assessment, and personalized financial recommendations. The high-performance computing capabilities of AI chipsets empower real-time, data-intensive financial services, transforming traditional banking and ushering in a new era of customer-centric financial experiences. Despite technical feasibility and potential financial benefits, challenges like data privacy, regulatory compliance, and integration frictions require careful navigation. With a promising future outlook, early adoption and collaboration between fintech players and AI chipset manufacturers will play a crucial role in shaping the trajectory of AI-driven fintech innovation.

Feynic TECHNOLOGY

AI-Driven Fraud Detection

This leverages advanced machine learning algorithms to detect and prevent fraudulent activities in real-time.

In fintech, this technology acts as a vigilant security layer, continuously analysing vast volumes of financial data to identify suspicious patterns and transactions.

By swiftly detecting and mitigating fraud, AI-driven systems protect financial assets, preserve customer trust, and enhance overall cybersecurity in the rapidly evolving digital financial landscape.

You can find out more about this subject in our AI Chipset Primer on the Zenith GitHub.

OPPORTUNITY

Trigger
- Escalating cyber threats
- Growing adoption of digital financial services
- AI advancements increase accuracy & efficiency

Players
feedzai, FORTER, Kount (An Equifax Company), sift, F5 Distributed Cloud Services, FEATURE SPACE, PayPal, Ravelin

Drivers
- Regulatory mandates & compliance reqs.
- Brand reputation & Consumer trust
- Significant cost saving through loss prevention

IMPACT

Macro

Network Effects & Interactions
- Widespread adoption leads to collective intelligence
- Collaborative Industry-wide defence strategy
- Increased trust in FS promotes further adoption

Distruptees
- Cybercriminals facing more evolved systems
- Legacy fraud detection losing competitiveness
- Shift in the dynamics of financial crime investigation toward automation

Micro

Competitive Advantage
- Superior fraud detection & reduced losses
- Enhanced customer trust & loyalty
- Real-time response capabilities to incidents

Financial Benefits
- Cost savings & less post-fraud investigations
- Customer retention through reputation
- Investments & partnerships for potential applications following successful tests

Supply Chain
- Integration of AI-driven solutions to core infra
- Collaboration between AI solution providers, data aggregators & financial entities
- Potential changes in risk assessment and underwriting of Financial Services

TECHNICAL FEASIBILITY

Technical Merit
- Demonstrable success in real world scenarios
- Scalability of AI models to process vast volumes of data
- Continuous improvement and refinement of ML models to adapt to evolving threat landscape

Tools, Ecosystem & Skills
- Readily available dev. frameworks
- Growing ecosystem of talent working with AI tools
- Need for continuous upskilling to keep up with emerging fraud techniques

Friction
- Data privacy concerns
- Over-reliance on AI models leading to blind spots
- Regulatory compliance complexities in explainability of models

FUTURE

Timeline
- **Short term** Integration efforts into security infrastructure
- **Medium term** **Industry-wide adoption & increased reliance**
- **Long term** Evolution of AI-driven responses to emerging fraud techniques

Risks
- False negatives where AI fails to detect new or adaptive fraud patterns
- Adversarial attacks targeting AI models to manipulate outcomes
- Potential overfitting or bias in AI models affecting accuracy and/or fairness of detection

SUMMARY

AI-driven fraud detection represents a significant opportunity in fintech, providing real-time protection against sophisticated cyber threats. Advanced machine learning algorithms analyse vast financial data to swiftly identify and prevent fraudulent activities, safeguarding financial assets and customer trust. Collaboration between fintech companies, financial institutions, and cybersecurity experts is driving the development and adoption of robust fraud prevention solutions. The technology's impact is far-reaching, with macro network effects and improved cybersecurity across the digital financial landscape. While the potential for financial benefits and competitive advantages is substantial, the implementation of AI-driven fraud detection requires careful consideration of technical feasibility, frictions, and risks. By striking the right balance between innovation and responsible use, AI-driven fraud detection will continue to transform the way financial entities combat financial crime, contributing to a more secure and trusted financial ecosystem.