LatticaAI

April 2025

# The FHE Landscape

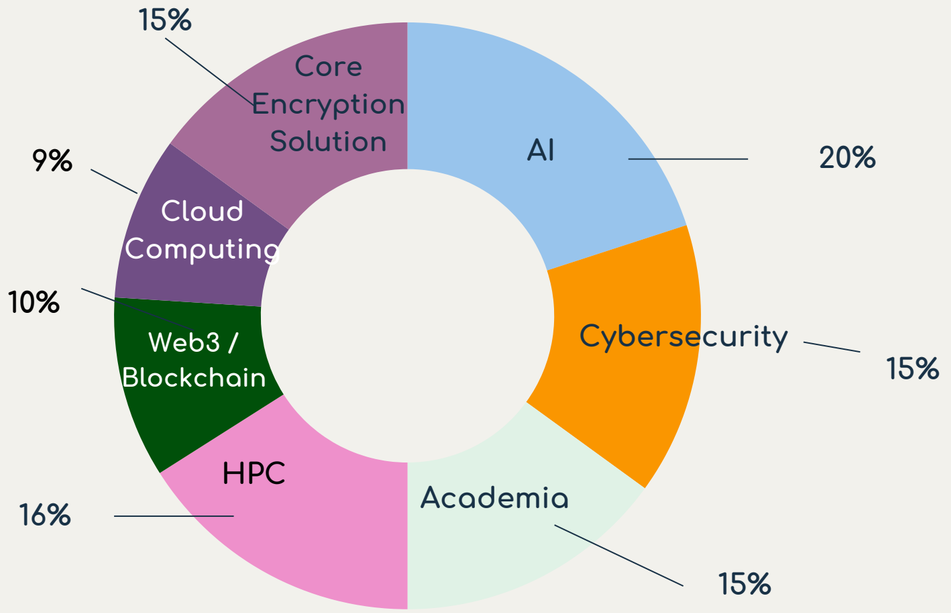
Lattica surveyed cryptographers, engineers, and researchers to understand where FHE is headed. Responses reveal a mix of optimism and skepticism – progress is happening, but challenges remain.

Here's what the FHE community thinks.

## Survey Participants

**Education**
44% PhD
37% Master's degree

**Industry**



The FHE Landscape - 2025

# Key Takeaways

1. Most respondents (41%) believe we will see FHE in production in 3-5 years. Healthcare and financial services will be first to adopt the cloud once FHE becomes mainstream.
2. Leading commercial use cases are:
    a. Database operations
    b. Cryptocurrency marketplaces
    c. Private inference for ML models
3. TFHE is the leading scheme in today's market, followed by CKKS and BFV. CKKS excels at approximate arithmetic on real numbers for machine learning applications, while TFHE specializes in boolean operations with efficient bootstrapping.
4. Most respondents (71%) believe FHE adoption will be achieved through a combination of hardware and software.
5. Most respondents (62%) would like to see updated standardization of FHE security parameters.
6. Most respondents (90%) see FHE as intersecting with other PETs, especially ZKPs and MPC.

LatticaAI

# FHE

Fully Homomorphic Encryption (FHE) is an advanced cryptographic technique that enables computations on encrypted data without ever decrypting it.

This means that even when data is processed by AI models, cloud services, or third parties - its confidentiality remains intact.

Step 1

### ENCRYPT ON DEVICE

A query is encrypted directly in your browser using FHE.

This ensures that Lattica never sees or stores your raw data, only its encrypted form.

Step 2

### COMPUTE ON CLOUD

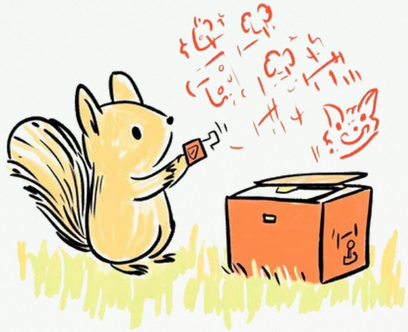
The AI model runs directly on the encrypted query without first decrypting it.

Lattica cannot see your input, output, or intermediate results during computation.

Step 3

### RECEIVE ENCRYPTED RESULT

The model returns an encrypted prediction.



Step 4

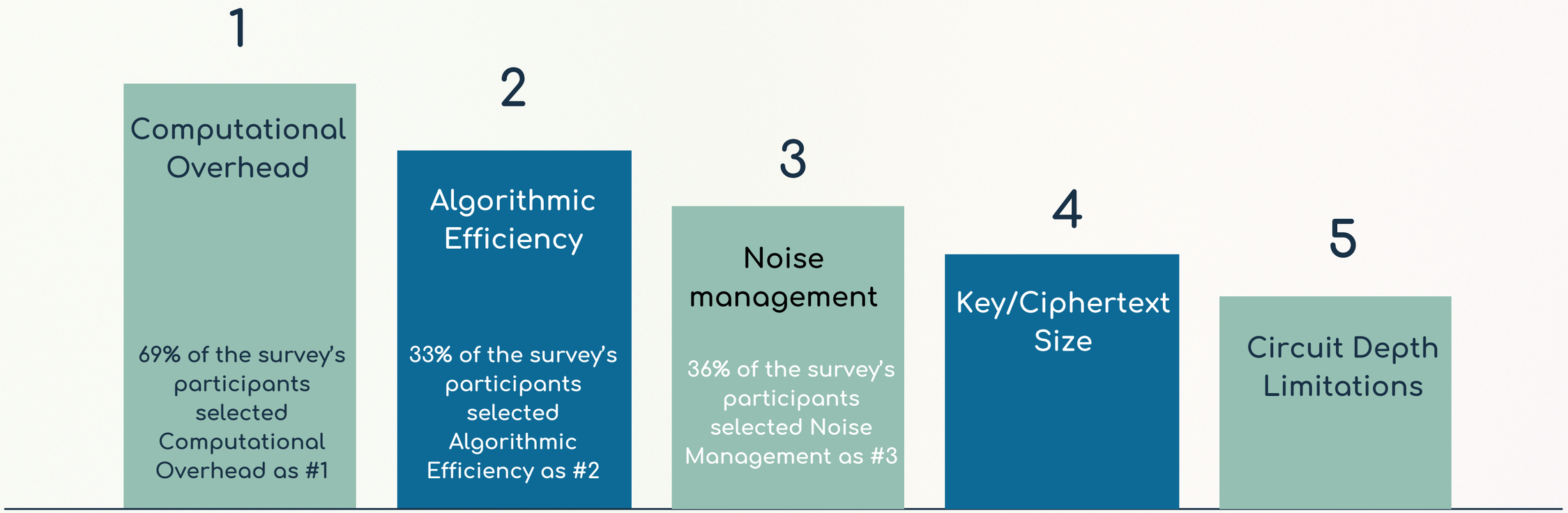
### DECRYPT ON DEVICE

Decrypt and view the final prediction on your browser.

LatticaAI

# #1 - Which aspect of FHE has the most potential to improve?

(Rank from 1-5, 1 being most critical)

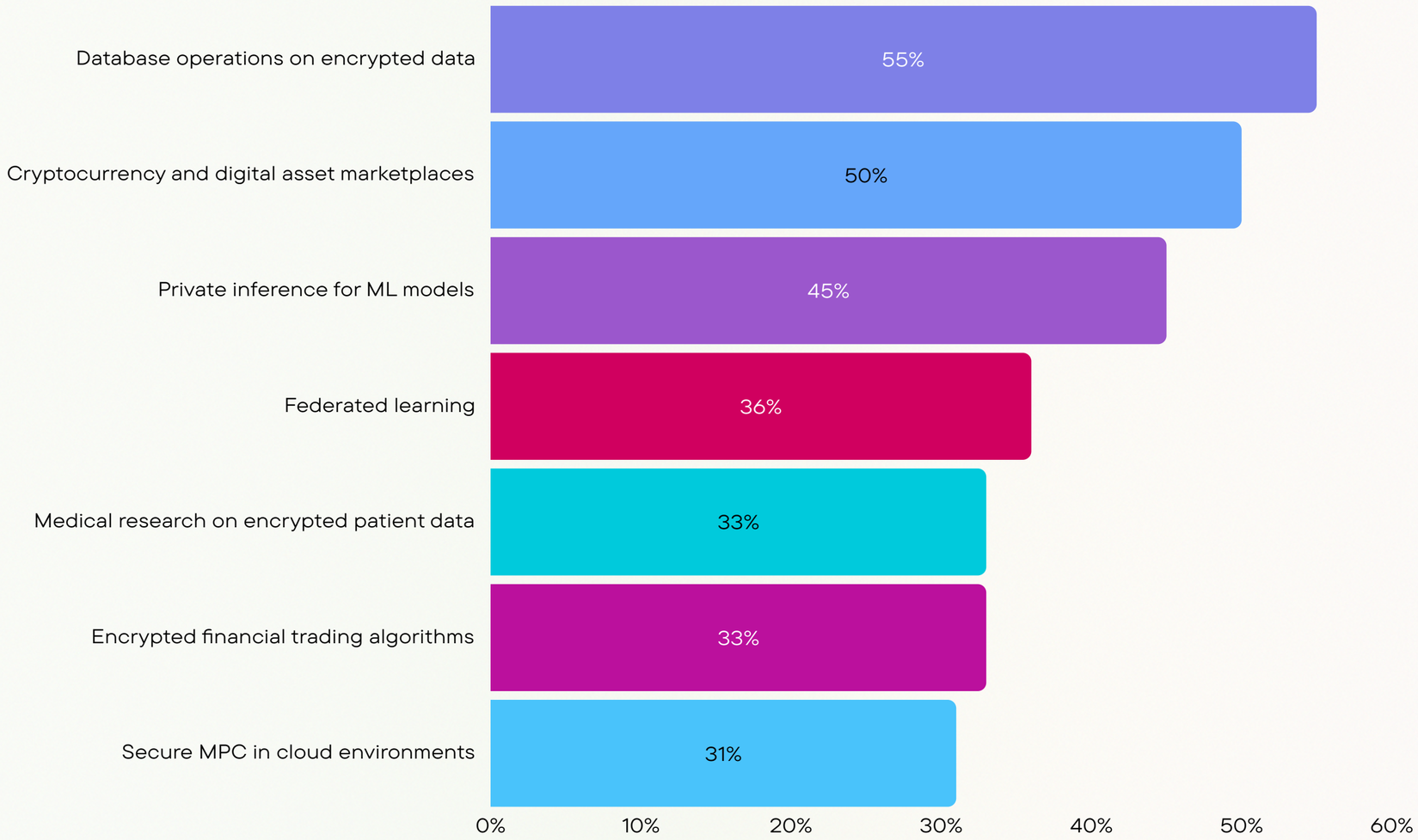



**Computational Overhead** is the dominant concern for FHE, followed by **Algorithmic Efficiency** and **Noise Management**. These results highlight that despite FHE's promise, significant performance challenges remain the primary barrier to widespread adoption.

LatticaAI

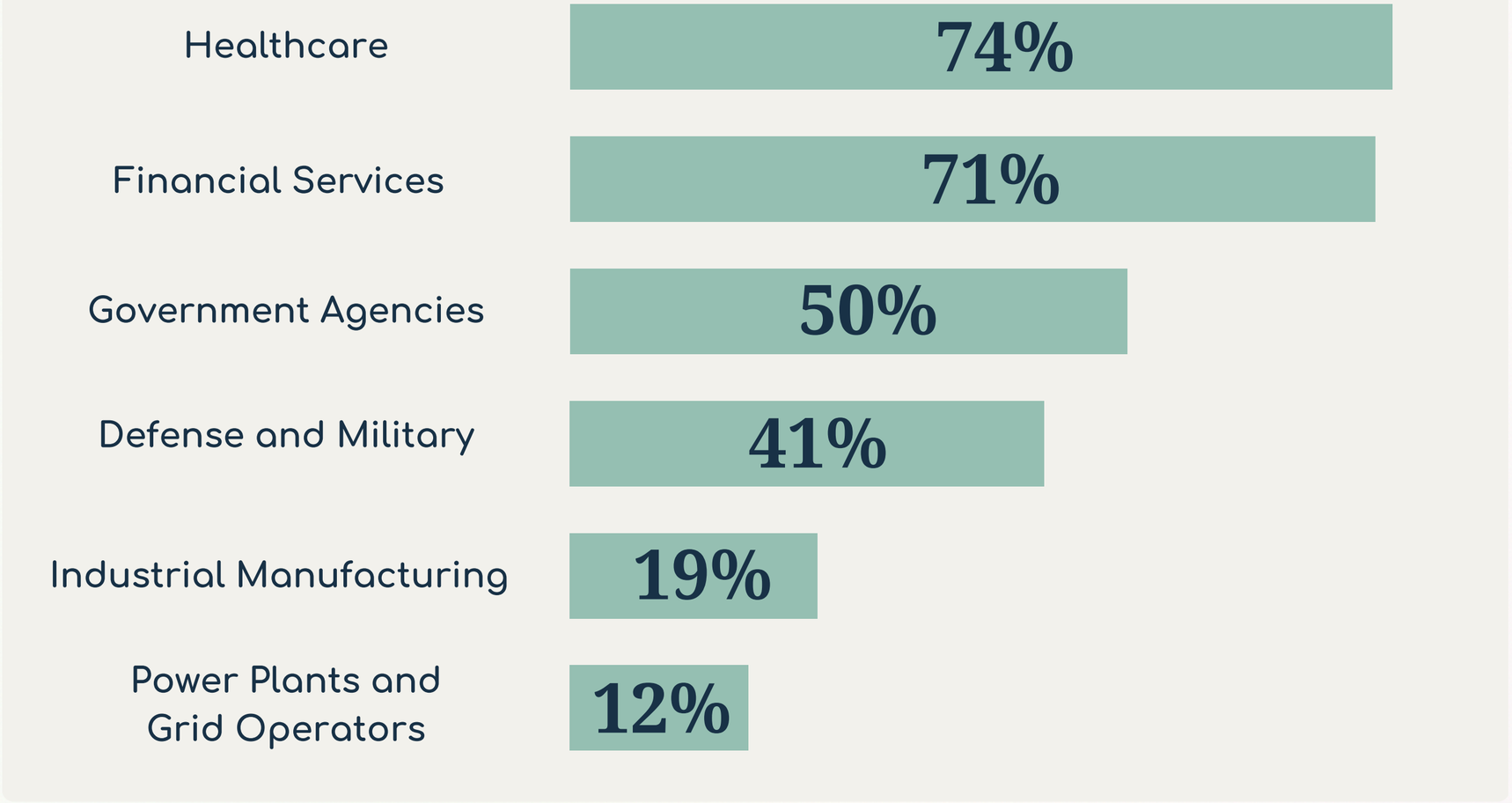
# #2 - What do you see as FHE's leading commercial use cases?

(Select all that apply)



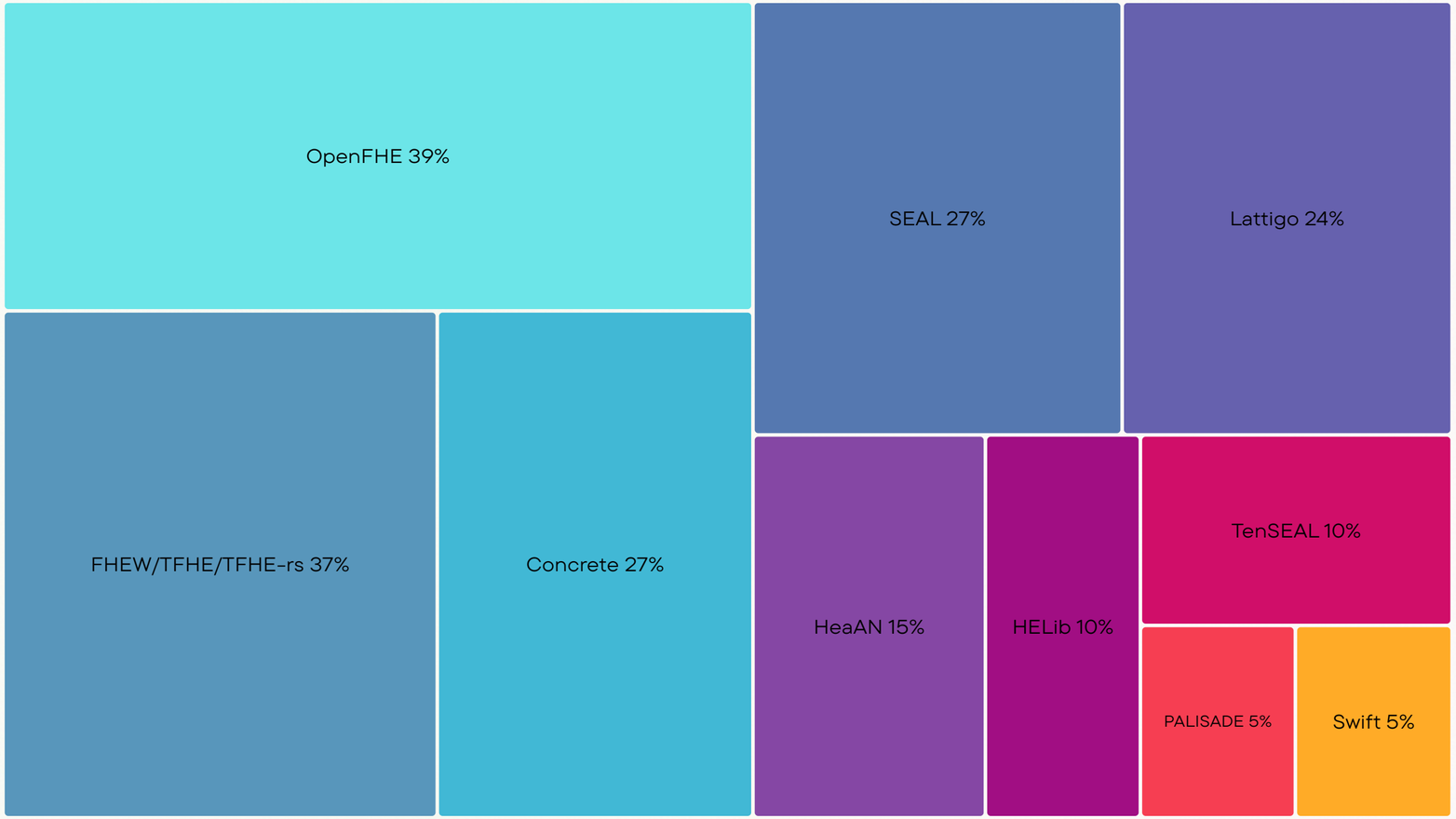
# #3 - Which industry sectors do you believe are likely to adopt the cloud once FHE is a mainstream, financially viable solution?

(Select all that apply)



# #4 - Which FHE libraries are you currently working with?

(Select all that apply)

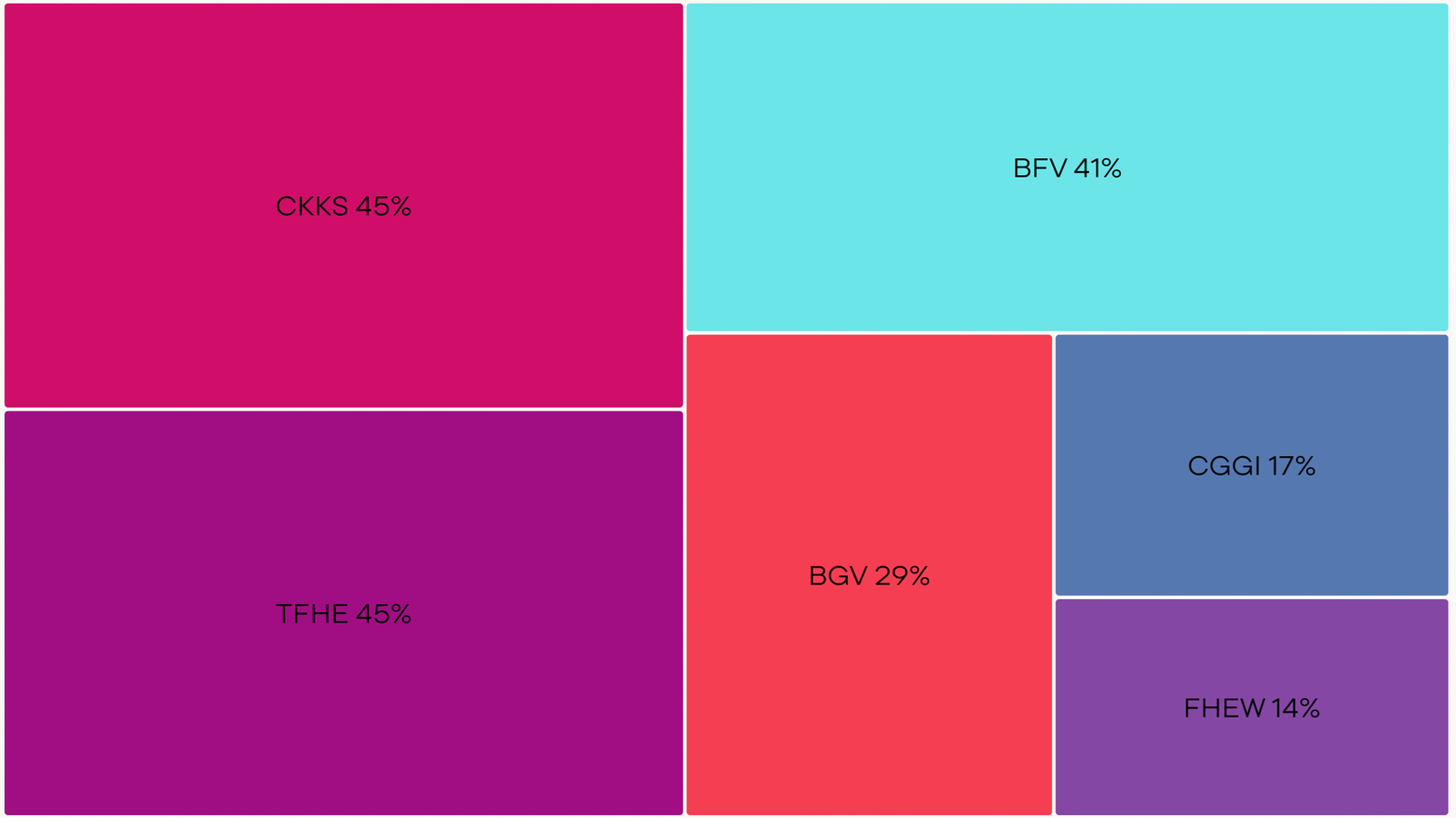



Instead of adding another general-purpose FHE library, Lattica focuses on removing complexity for AI applications. Our implementation of BGV and CKKS is designed for seamless integration with deep learning pipelines, ensuring that developers can leverage FHE without navigating the complexities of cryptographic parameter tuning.

LatticaAI

# #5 - Which FHE schemes are you currently working with?

(Select all that apply)

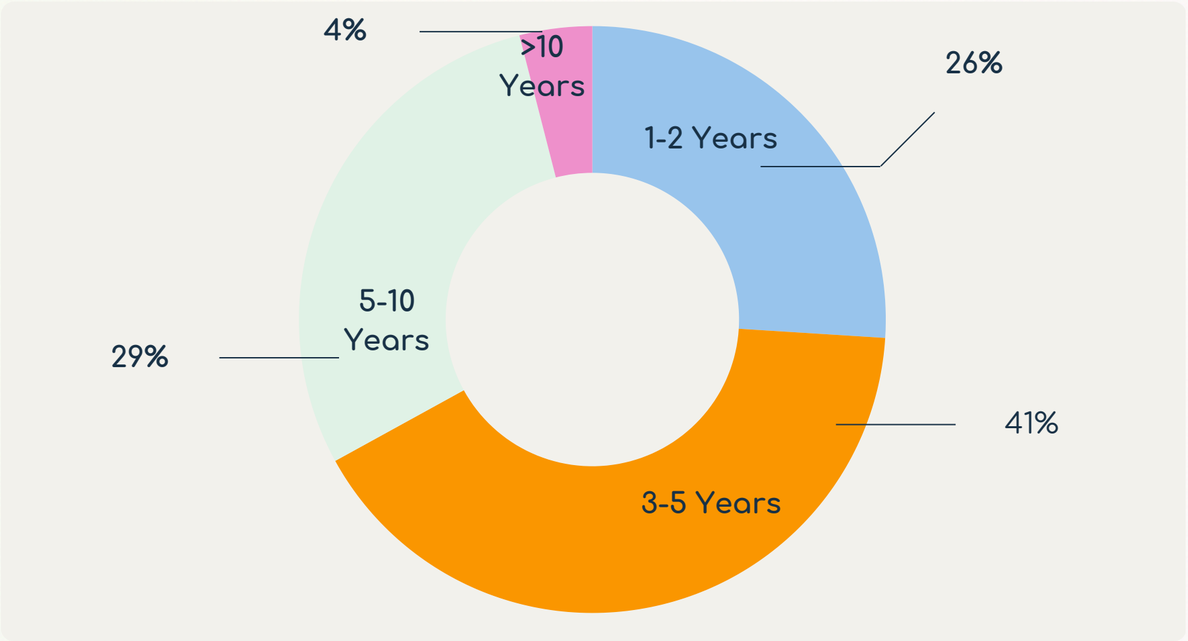


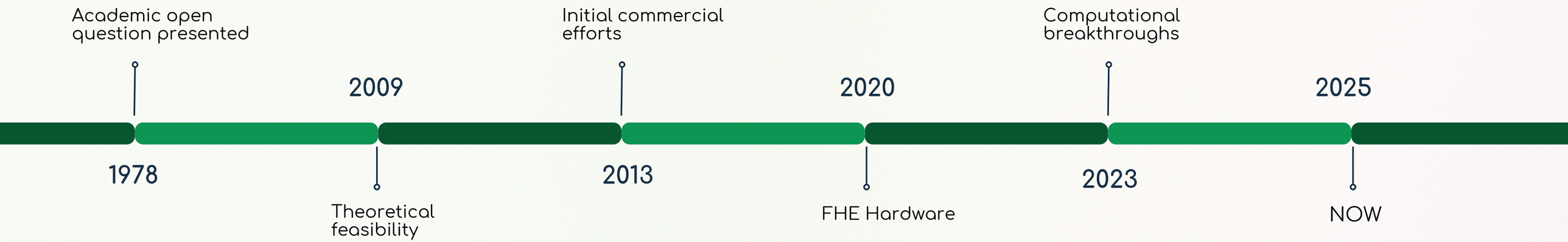

CKKS and TFHE lead as the most widely used FHE schemes due to their complementary strengths. CKKS excels at approximate arithmetic on real numbers for machine learning applications, while TFHE specializes in boolean operations with efficient bootstrapping. This reflects how practitioners select different schemes based on their specific computational requirements.

LatticaAI

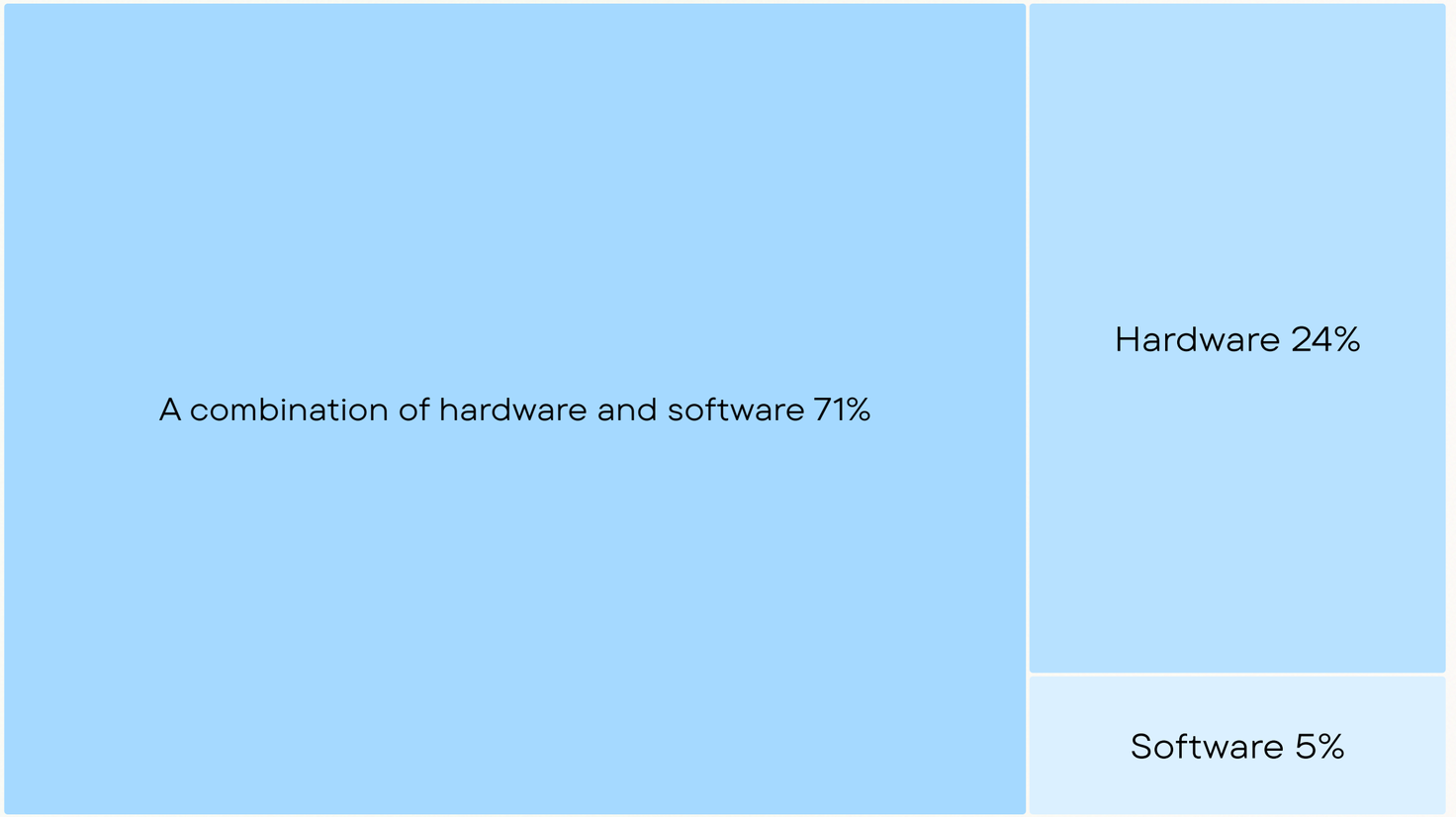
# #6 - What timeline do you predict for FHE adoption in production systems?

**Predictions varied**: some expect mainstream adoption in 1-2 years, driven by improved tooling and specialized hardware; others believe we're still 5-10 years away due to computational overhead and lack of standardization.



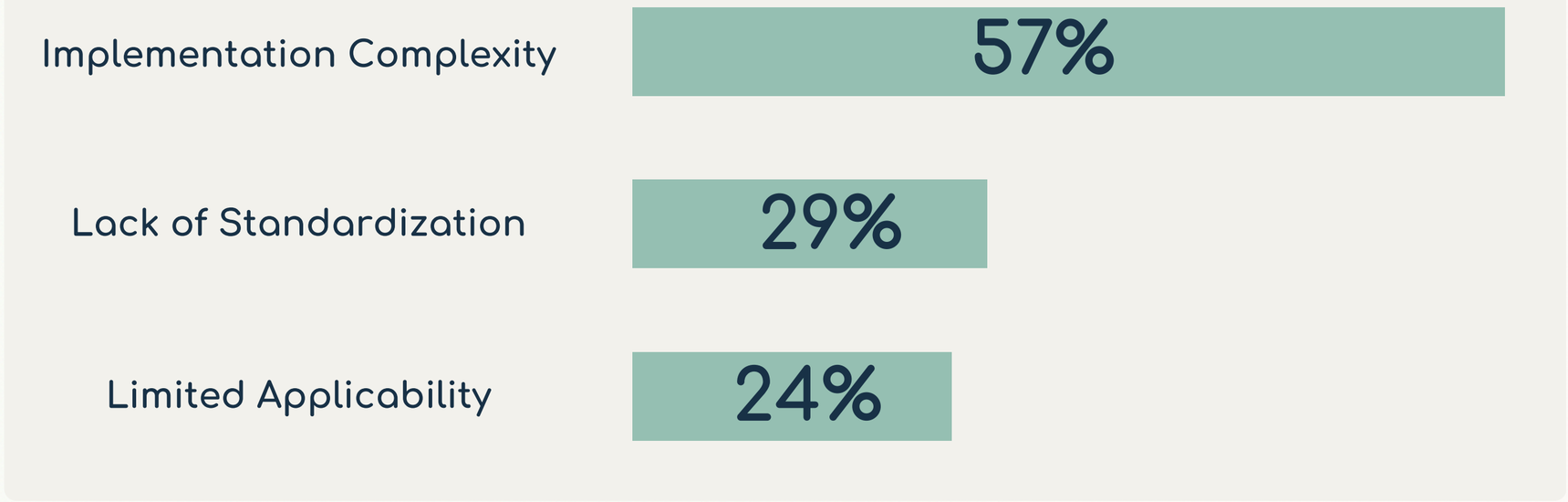
# #7 - What will ultimately lead to FHE adoption: game changing computational acceleration, or software promoting algorithmic efficiency?




Many respondents agreed that both hardware acceleration and better software optimizations are needed for FHE to scale. **We observe a growing number of hardware-software collaborations in the community**, where startups and research groups are working together to optimize FHE performance.

# #8 - Other than computational overhead and complexity, what do you believe is the main challenge in FHE adoption?

(Select all that apply)




Most respondents are highly familiar with FHE, but even experts highlight the difficulty of implementing FHE efficiently.

# #9 - Do you see FHE intersecting with other PETs (MPC, ZKP, etc.)?

> ZKP for verifiability

-Cryptography Researcher

> MPC & ZKP are complementary to FHE

-Engineer

> FHE and ZKP can solve related real-world problems.

-Cryptography Researcher

> MPC for key management, ZKPs for (mostly) decentralized applications

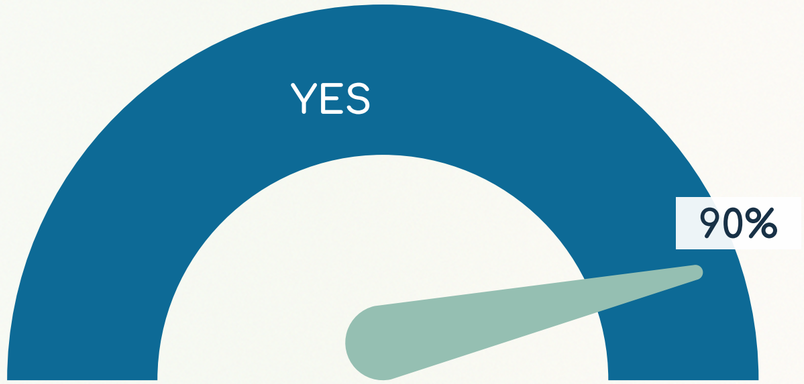
-Technical Lead

> Yes. Solutions will be a mix. For example, the cloud side will be required to prove it performed the correct computation.

-Engineer

> Yes MPC, ZKP, Oblivious transfer - ZKP for verifiability, MPC for protection of algorithms, oblivious transfer for protecting server only secrets.

-Engineer




> The recent work by Apple in their "Wally" private search model is a good example of a case where FHE and differential privacy are both required.

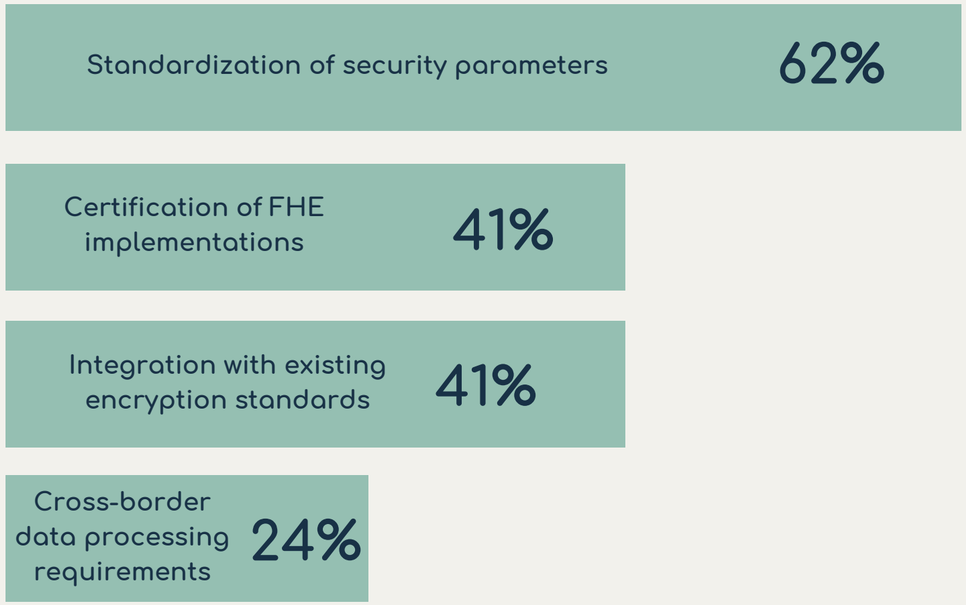
-Engineer

Most respondents see FHE as part of a broader privacy stack, often used alongside MPC, ZKPs, and Secure Enclaves. Some noted that FHE can reduce reliance on vendor-trusted hardware, while others pointed to hybrid models for balancing tradeoffs.

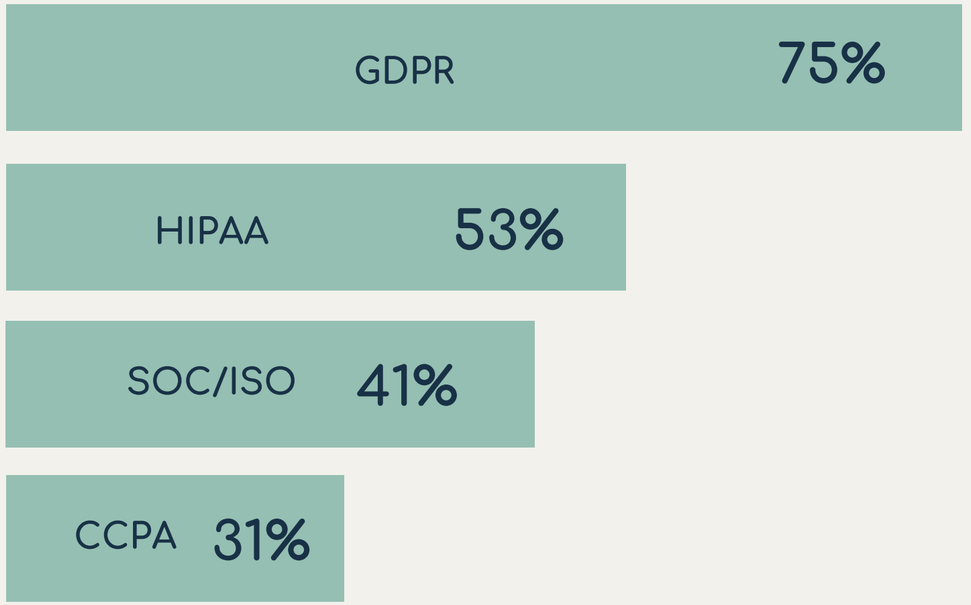
# #10 - Regulatory frameworks and Standards

(Select all that apply)

Which aspects of FHE require new or updated regulatory frameworks?




Which regulations or standards will be most relevant to FHE implementations? (Select all that apply)



Lattica's FHE Survey - 2025

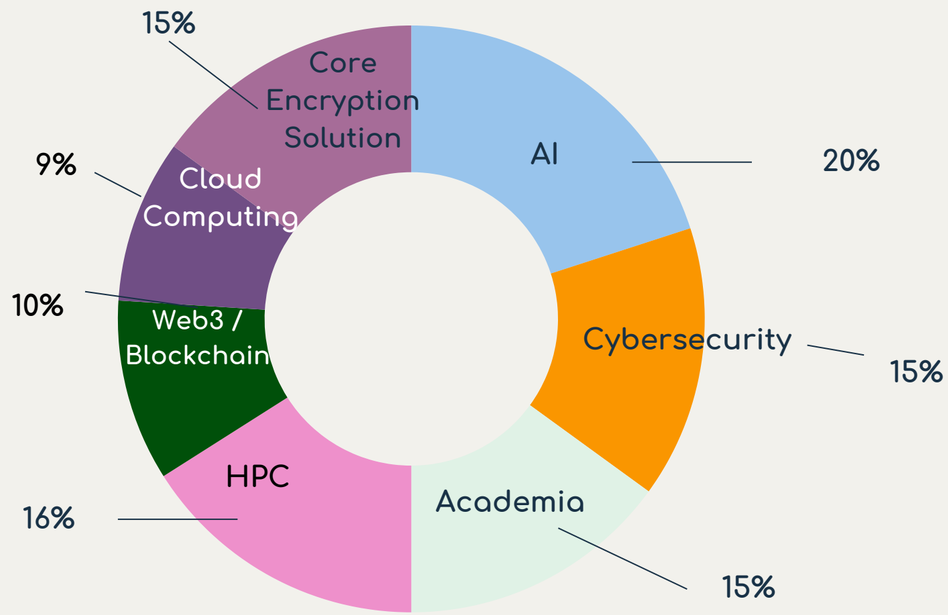
# Appendix

FHE doesn't have to be a distant vision. The key to adoption is making it work in specific, high-value applications today, while also building the foundations for broader adoption as the technology and ecosystem evolve.

## Survey Participants

**Education**
44% PhD
37% Master's degree

**Industry**




hello@lattica.ai

LatticaAI

Lattica was founded on a simple yet radical idea: FHE could be made practical by leveraging the same acceleration techniques that power modern machine learning.

FHE makes it possible to compute on encrypted data, but its real-world adoption has been limited by performance bottlenecks and complex implementations. We realized that by applying the optimization strategies used in modern ML, such as parallel computation, tensor operations and hardware acceleration, we could unlock FHE's potential for AI.

With deep expertise in cryptography, neural networks and AI infrastructure, we built a developer-friendly platform that integrates privacy-preserving AI seamlessly into existing workflows.

To reach out to us with feedback and comments, please email hello@lattica.ai.


LatticaAI