



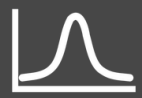
2nd FHE Landscape Survey

FHE community insights and projections

Lattica surveys cryptographers, engineers, and researchers once a year to understand where FHE is headed.

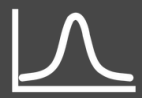
April 2026

www.lattica.ai



Key Takeaways

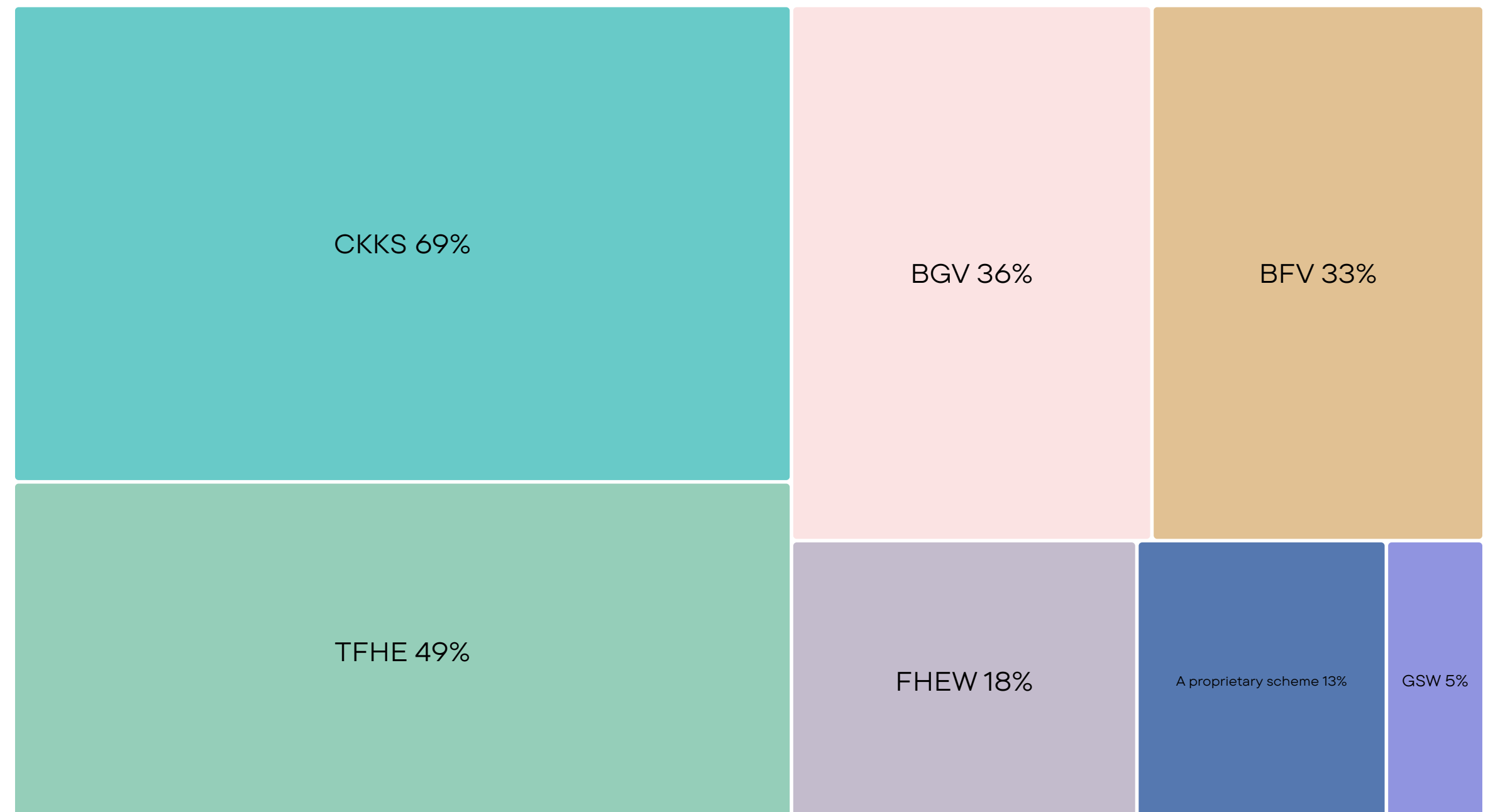
- 1 CKKS is now the leading scheme in today's market. This has changed since last year's survey, where TFHE was #1, and is a reflection of CKKS's strengths when working with machine learning applications.
- 2 The top commercial use cases have also changed from last year's survey, and are:
 - a. Cross-organizational / cross-border collaboration
 - b. "Private LLMs," aka Small Language Models
 - c. Biometric authentication and facial recognition
 - d. Smart contracts
- 3 And finally, most respondents continue to believe FHE adoption will be achieved through a combination of hardware and software.

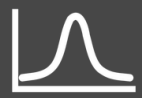


#1 - Which FHE schemes are you currently working with?

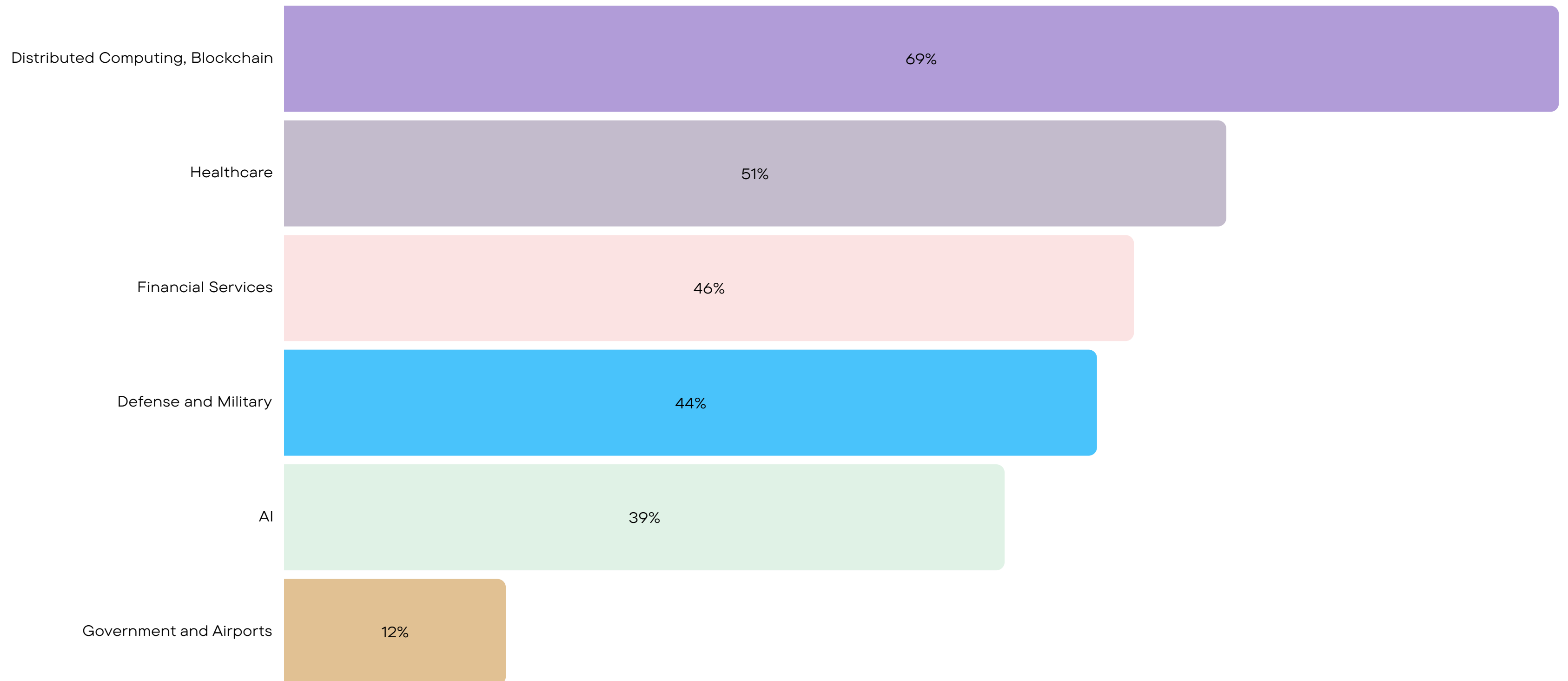
CKKS is now the leading FHE scheme. This has changed since last year's survey, where TFHE was #1, and is a reflection of CKKS's strengths when working with machine learning applications.

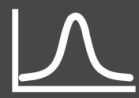
CKKS excels at approximate arithmetic on real numbers for machine learning applications, while TFHE specializes in boolean operations with efficient bootstrapping.



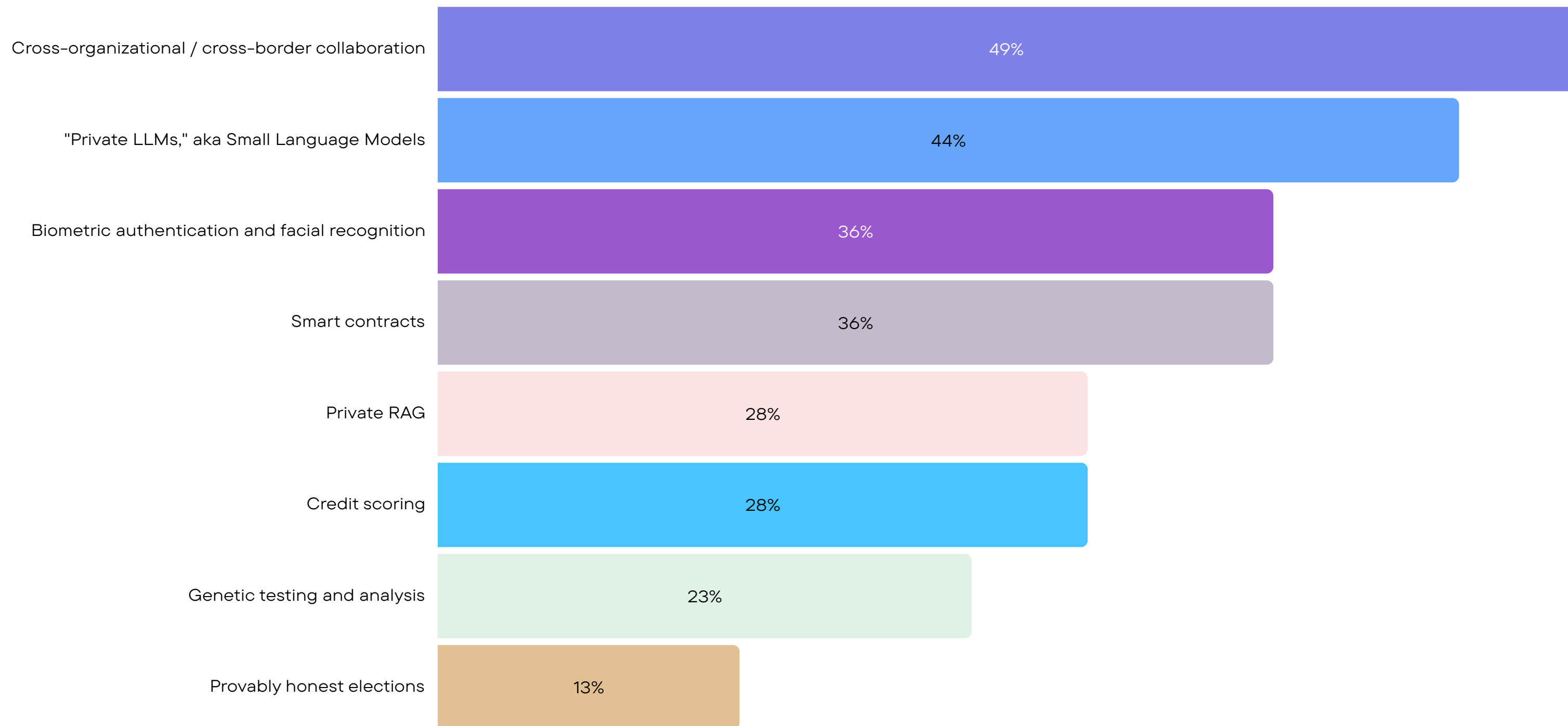


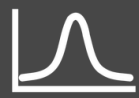
#2 - Which industry sectors will be the first to adopt FHE-based cloud solutions?



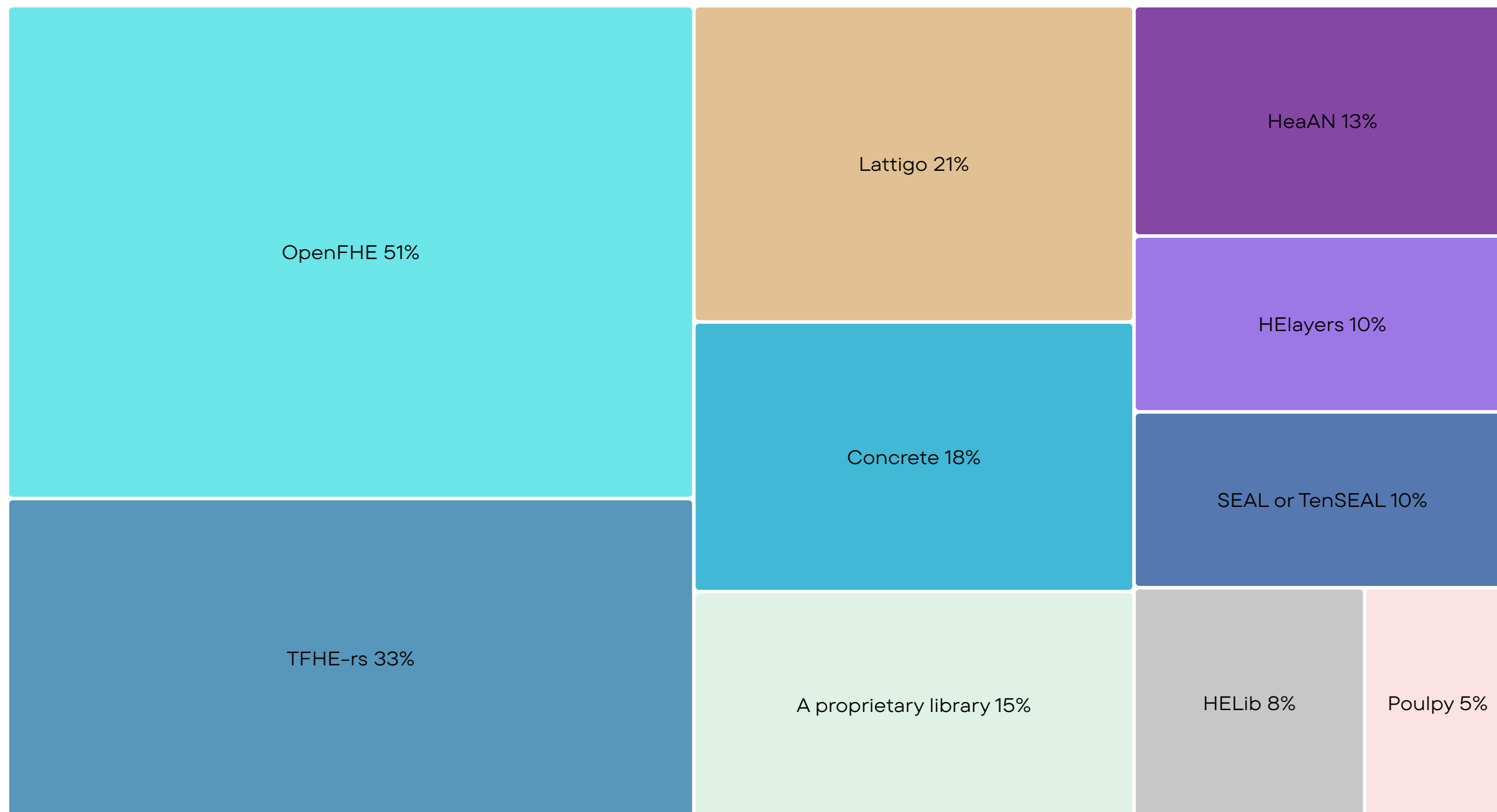


#3 - What do you see as FHE's leading commercial use cases?



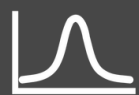


#4 - Which FHE libraries are you working with?



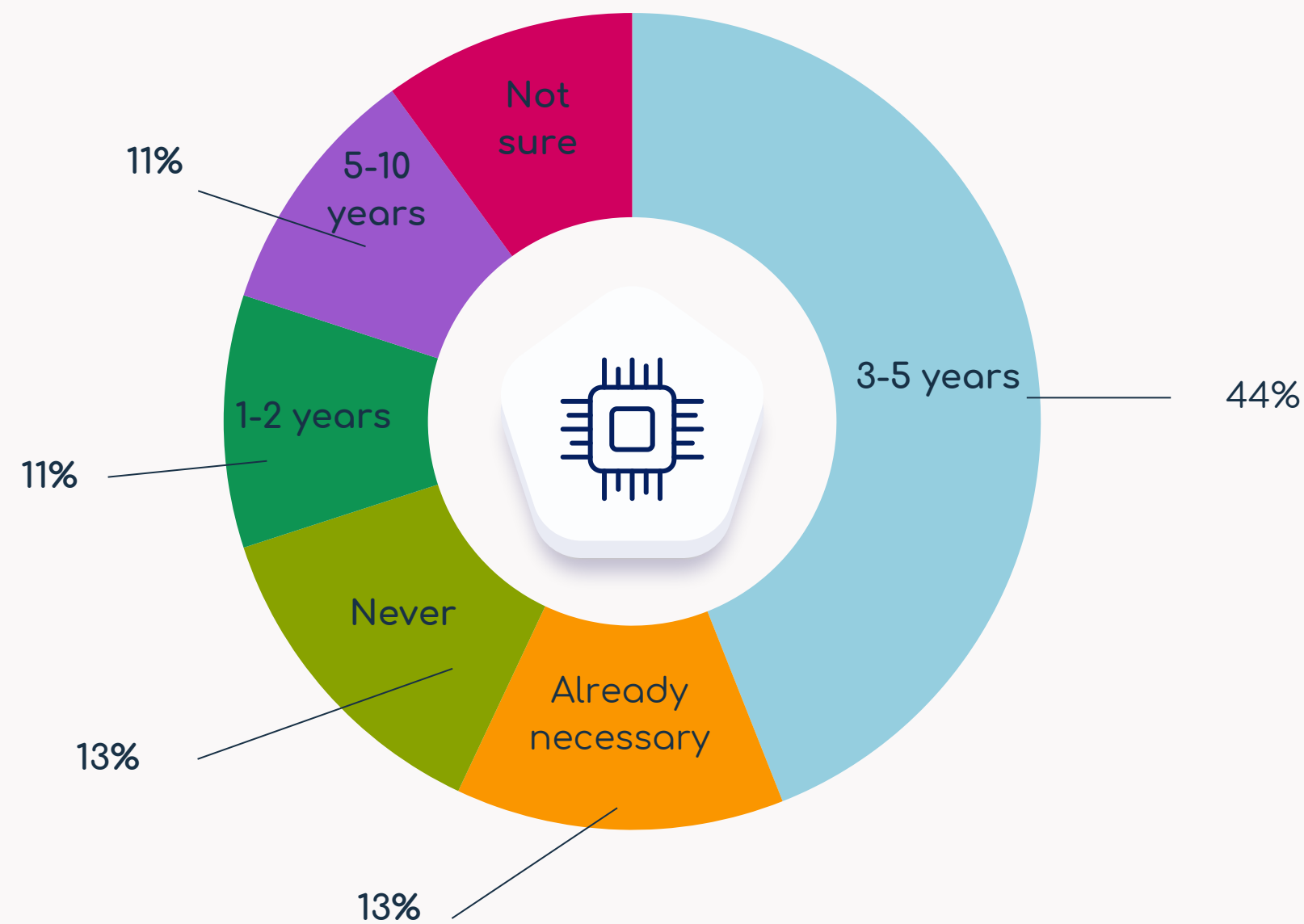
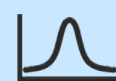
OpenFHE continues to dominate the market, followed by TFHE-rs.

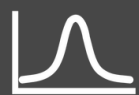
15% of respondents are using proprietary libraries, such as Lattica's. Our implementation of BGV and CKKS is designed for seamless integration with deep learning pipelines, so that developers can leverage FHE without navigating the complexities of cryptographic parameter tuning.



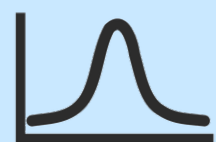
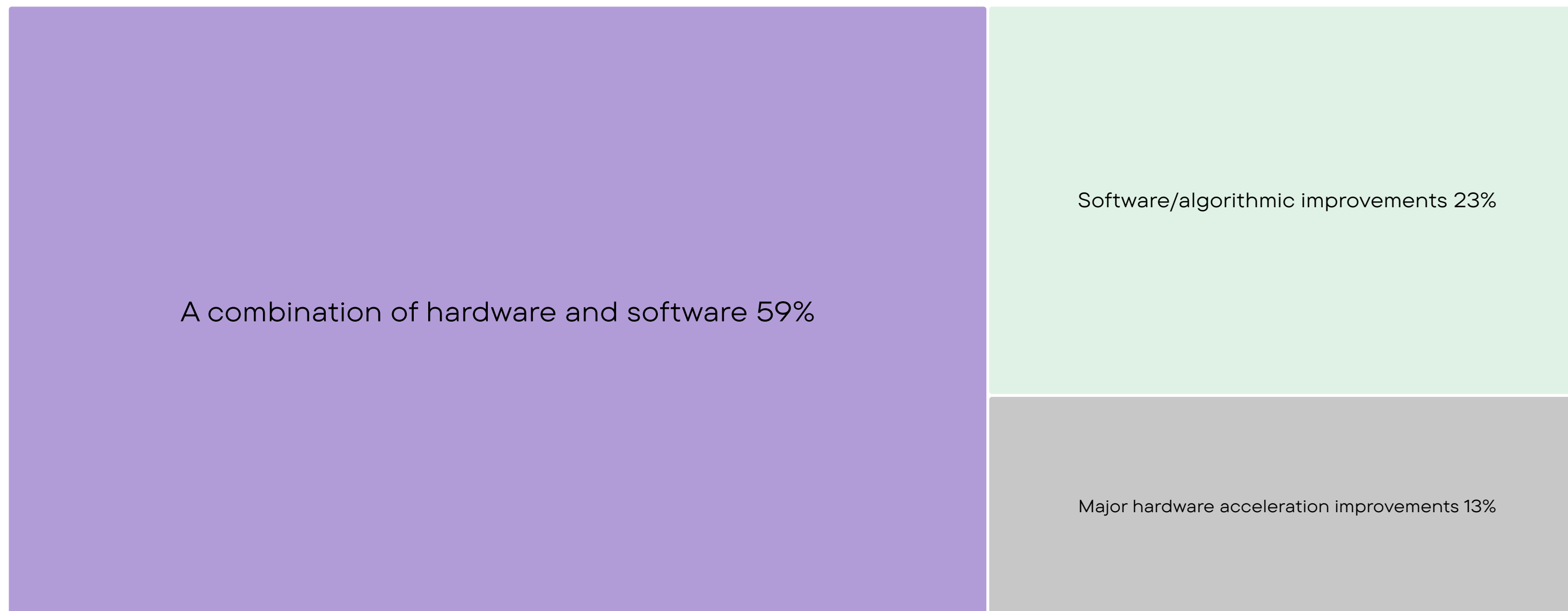
#5 - When do you expect purpose-built FHE acceleration chips to be uniquely advantageous for production-scale deployments?

Most respondents believe FPGAs and ASICs will start making a difference in 3-5 years.

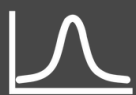




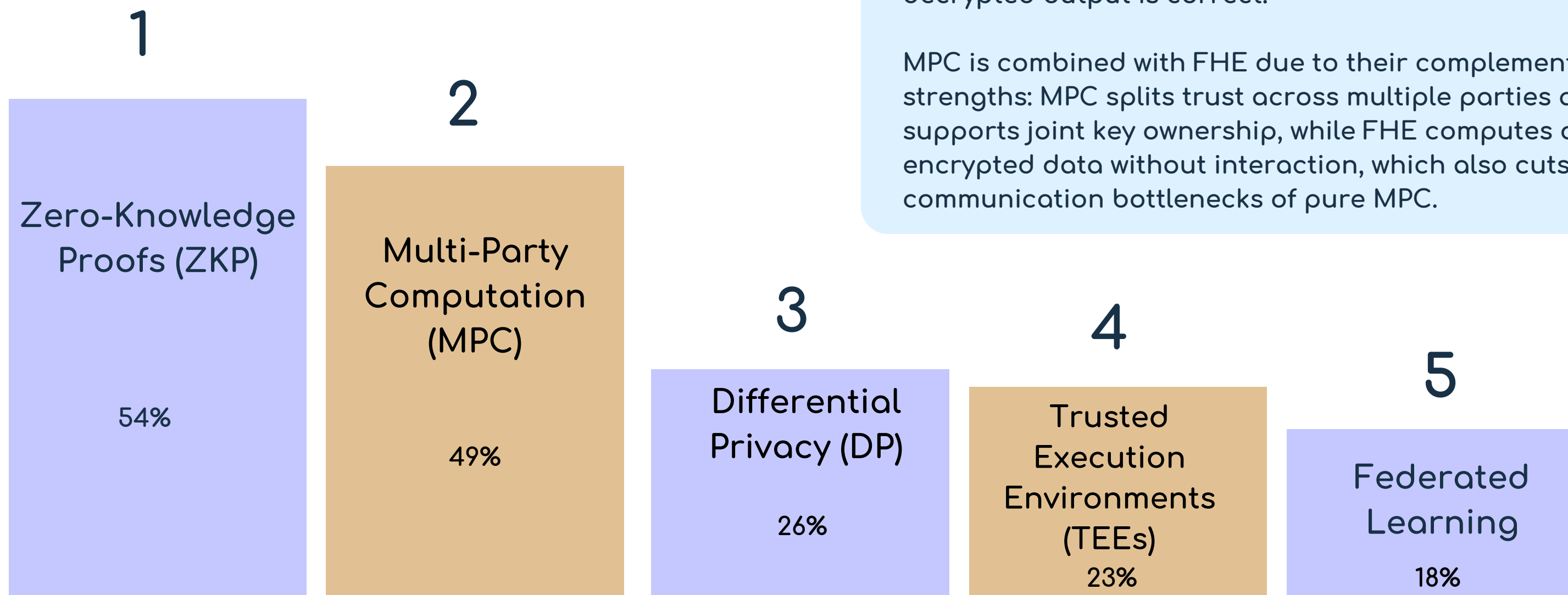
#6 - Which do you believe will be the primary driver of widespread FHE adoption?



Most respondents continue to believe the future is about **hardware-software collaboration**, where startups and research groups work together to optimize FHE performance.



#7 - Which other privacy technologies are you using?



ZKP is often combined with FHE to add verifiability and proof that ciphertexts are well formed, or that the final decrypted output is correct.

MPC is combined with FHE due to their complementary strengths: MPC splits trust across multiple parties and supports joint key ownership, while FHE computes on encrypted data without interaction, which also cuts the communication bottlenecks of pure MPC.



How many FHE PhDs does it take to change a lightbulb?

28%

NONE. The lightbulb is already encrypted, and changing it would leak information.



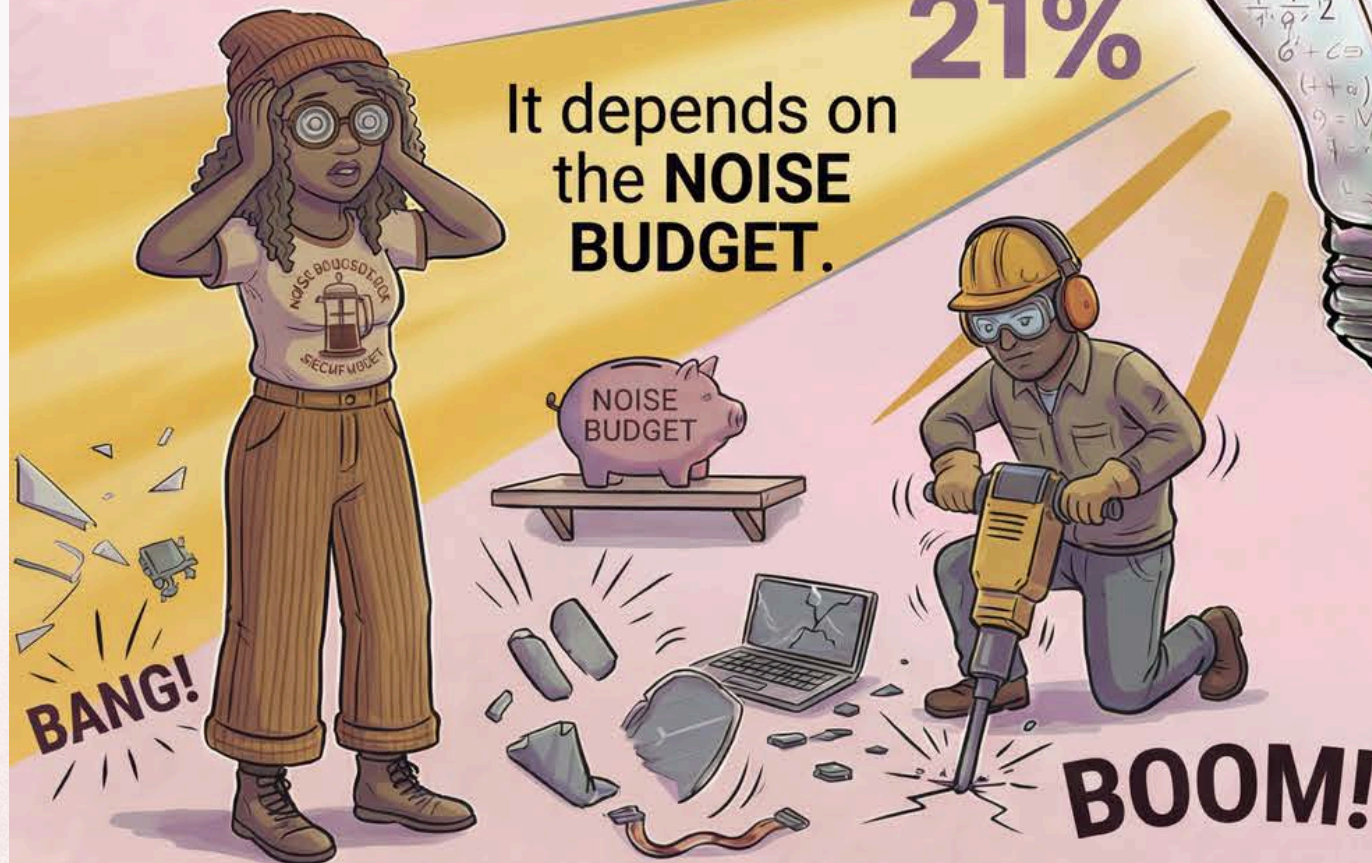
23%

In theory: **ONE.**
In practice, it's still benchmarking.



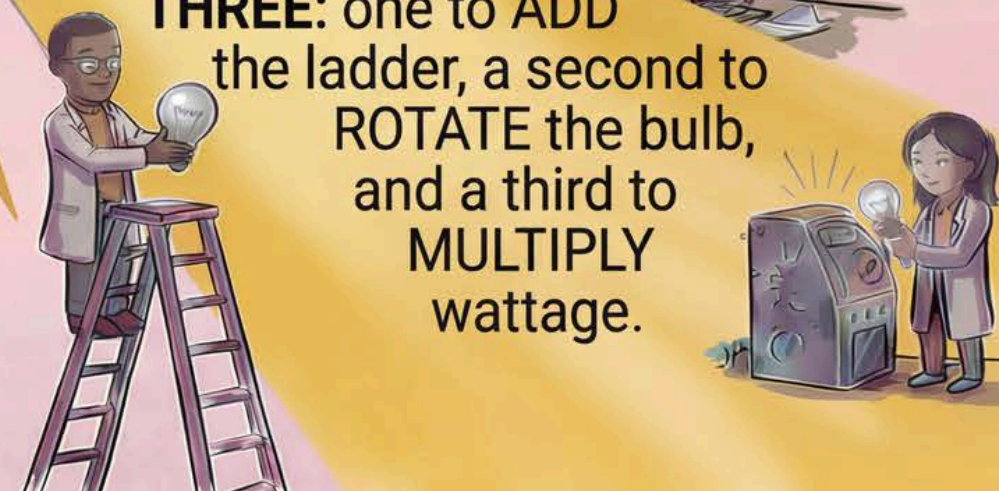
21%

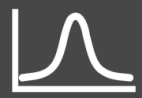
It depends on the **NOISE BUDGET.**



10%

THREE: one to **ADD** the ladder, a second to **ROTATE** the bulb, and a third to **MULTIPLY** wattage.





Lattica's 2nd FHE Landscape Survey

Survey Participants

Education

39% PhD
41% Master's degree

