

Introduction to pq signature schemes for ethereum

Options, tradeoffs

Pierre Daix-Moreux

PSE



Context



Peter Shor

What quantum computers do

Quantum computers are very good at exploring large search spaces.

Shor's algorithm: can solve the DLP very efficiently, ECDLP and pairings break catastrophically.

Hashing is SAFU.

What it means for ethereum

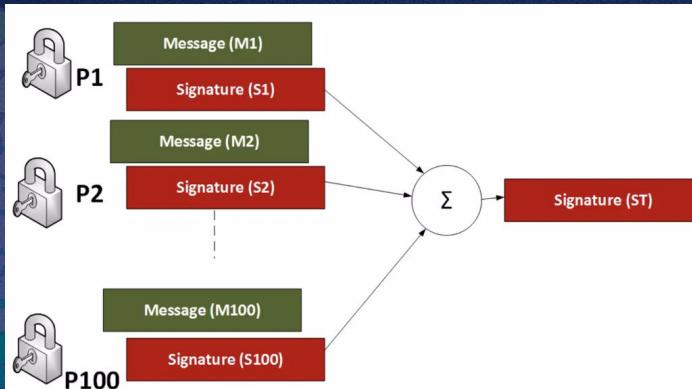
The constraint space

For the consensus layer:

Keep aggregation schemes and generally avoid too high hardware requirements on nodes.

For the execution layer:

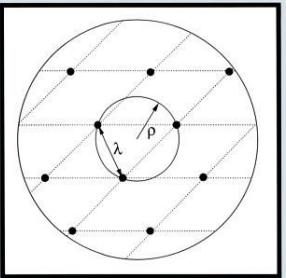
Keep the account based model and minimize requirement updates from wallet teams.



The toolbox

**COMPLEXITY OF
LATTICE PROBLEMS**
A Cryptographic
Perspective

Daniele Micciancio
Shafi Goldwasser



The toolbox

Crypto that runs on classical computers but remains secure against quantum adversaries.

Among others, 3 pq cryptography tools:

1. Hash functions (no changes)
2. Lattices (large sigs, but fast)
3. Isogenies (small sigs, but slow + no aggregation yet)

For instance::

- ML-DSA: Module lattice based signatures (NIST standard)
- Winternitz signatures (hash based)
- Use STARK based aggregation + some pq resistant signature scheme



What's next?

What's next

Very hard to predict.

Some think that QC's are not even physically realizable.

Yet, Scott Aaronson: "*either there are useful fault-tolerant QC's in the next decade or else something surprising happens to stop that*" (sept. 24)

Meta calculus probability density has pretty fat tails.

Use quantum canaries?



Thanks!

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

**Enter your main point /
statement here.**

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

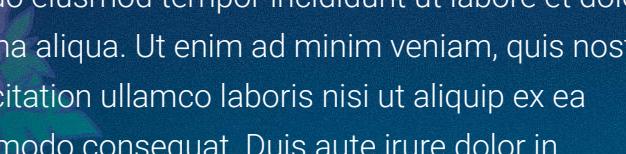
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

Section 2 details with an image. Enter title here.

Lore ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Section 3

Section 3 title here.

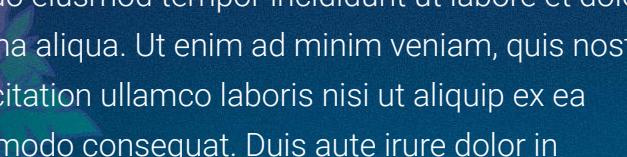
Enter your main point / statement here.

Section 3 details with a main point. Enter title here.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

**Enter your main point /
statement here.**

Here's the timeline.

Event 1



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
— Pythagoras

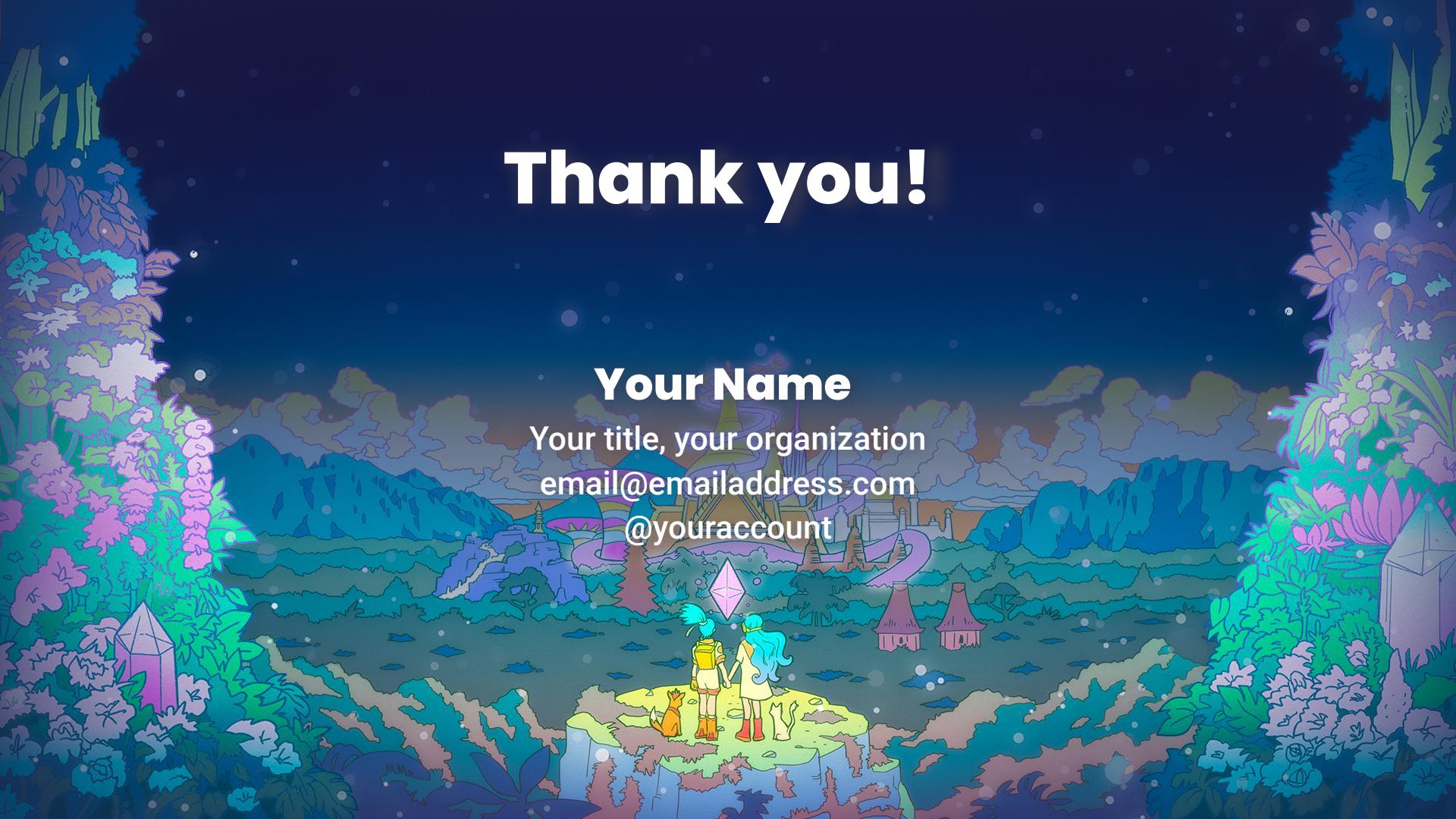
Thank you!

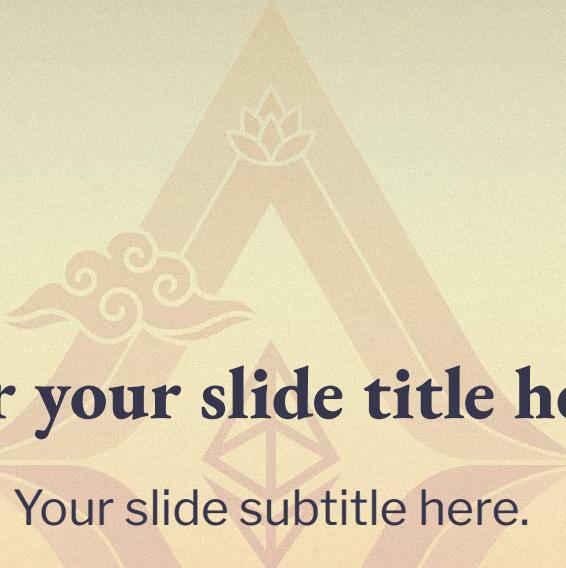
Your Name

Your title, your organization

email@emailaddress.com

@youraccount





Enter your slide title here

Your slide subtitle here.

Your Name

Your title, your organization





Section 1 title here.



Section 1 details with an image. Enter title here.

Consectetur adipisci ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.



Section 1 title here.

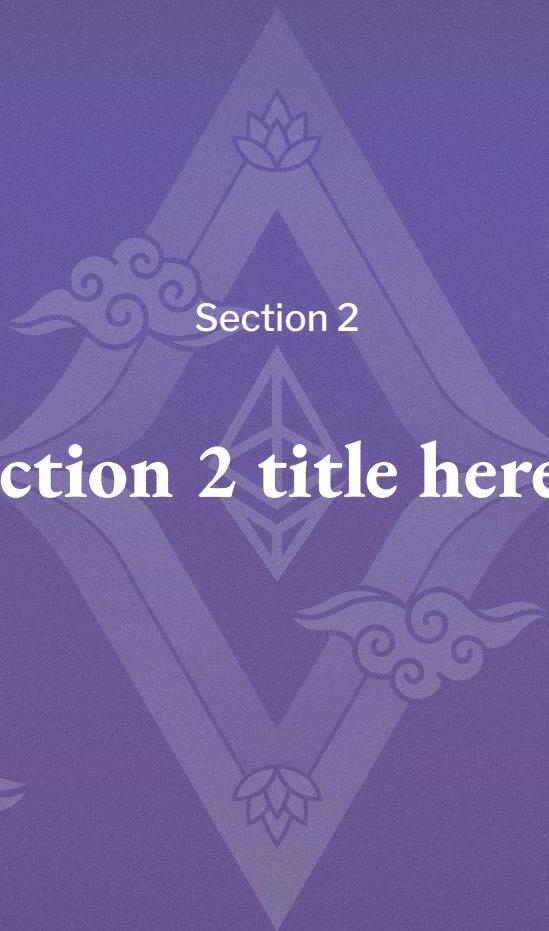
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula



Enter your main point /
statement here.

Section 1 details with a main point. Enter title here.



Section 2

Section 2 title here.





Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula





Section 2 details with an image. Enter title here.

 Lorem ipsum dolor sit amet, consectetur
 adipiscing elit, sed do eiusmod tempor incididunt
 ut labore et dolore magna aliqua. Ut enim ad
 minim veniam, quis nostrud exercitation ullamco
 laboris nisi ut aliquip ex ea commodo consequat.
 Duis aute irure dolor in reprehenderit in voluptate
 velit esse cillum dolore eu fugiat nulla pariatur.

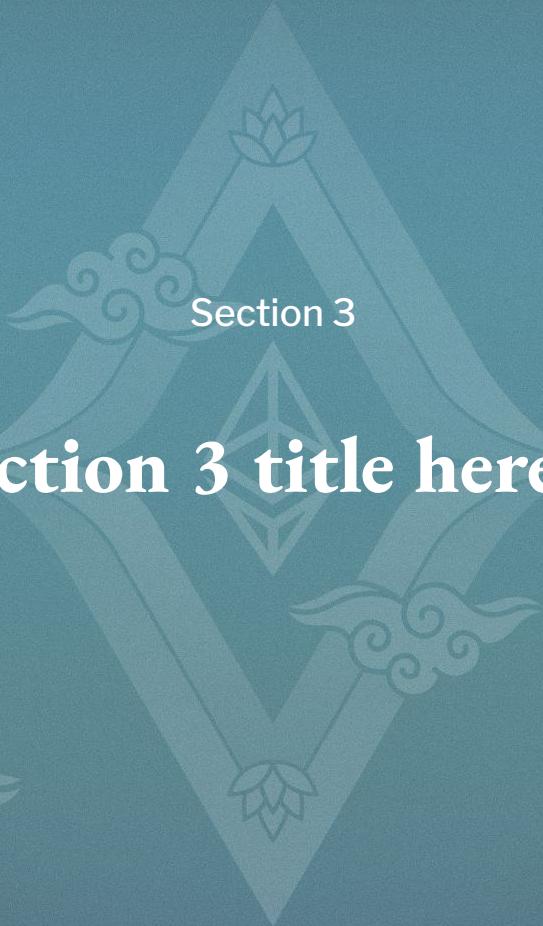




Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.



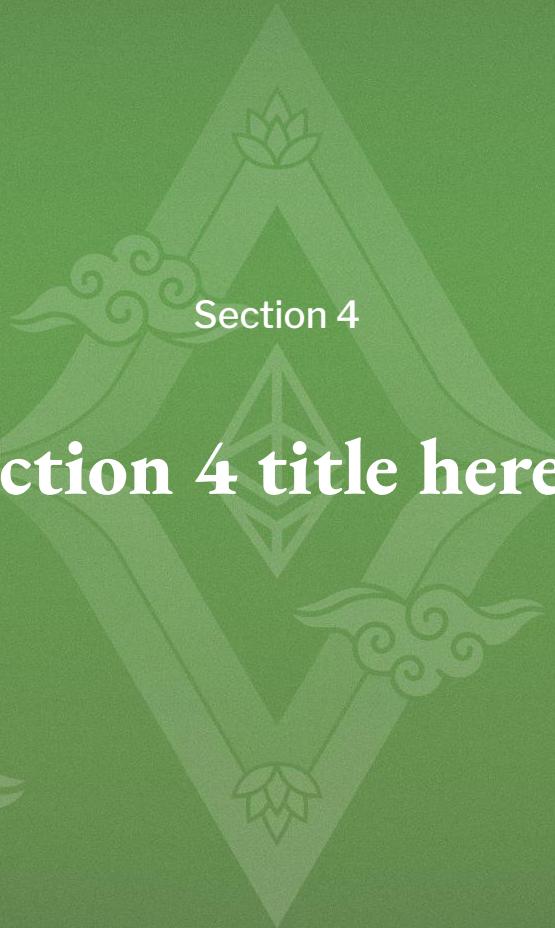
Section 3

Section 3 title here.



Enter your main point / statement here.

Section 3 details with a main point. Enter title here.



Section 4 title here.



Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.



Enter your main point / statement here.



Enter your main point / statement here.





Here's the timeline.

Event 1



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.



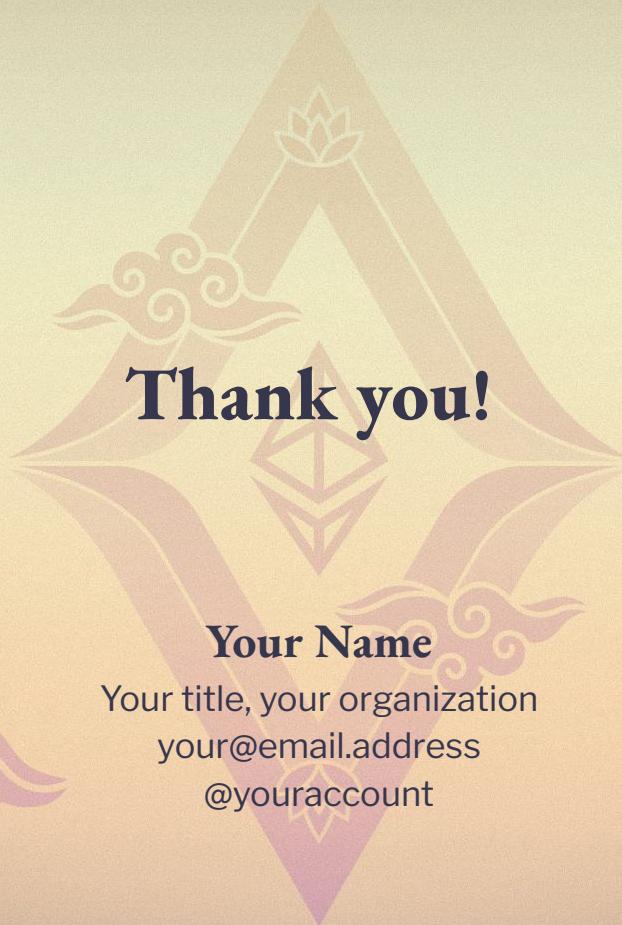


99.99%

“Number rules the universe.”

— Pythagoras





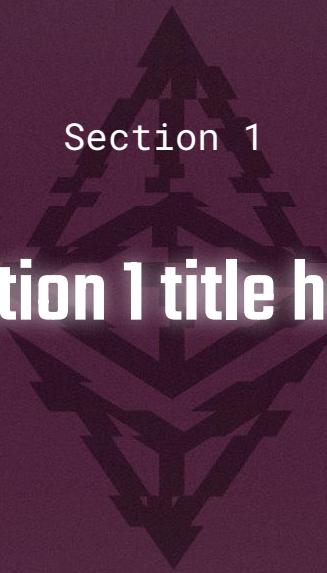


Enter your slide title here

Your slide subtitle here.

Your Name

Your title, your organization



Section 1

Section 1 title here.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
 - Condimentum
 - Magna
 - Ligula

Section 1 details with an image.

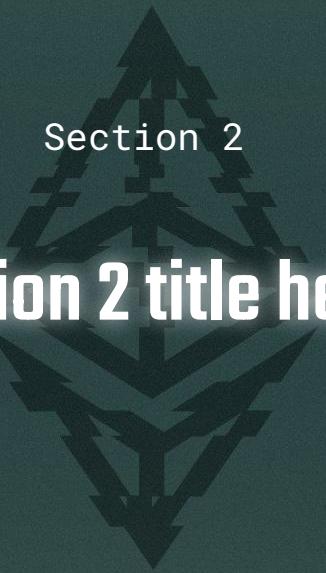
Enter title here.

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in
voluptate velit esse cillum dolore eu
fugiat nulla pariatur.

**Enter your main point /
statement here.**

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in
voluptate velit esse cillum dolore eu
fugiat nulla pariatur.



Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet,
 consectetur adipiscing elit, sed do
 eiusmod tempor incididunt ut labore et
 dolore magna aliqua.

- Sollicitudin
 - Consectetur
 - Condimentum
 - Magna
 - Ligula

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore et
dolore magna aliqua.

- Sollicitudin
 - Consectetur
 - Condimentum
 - Magna
 - Ligula

Section 2 details with an image.

Enter title here.

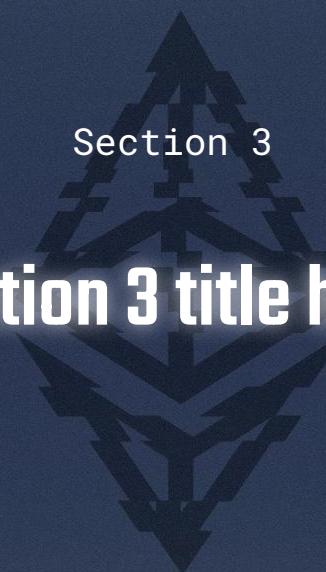
 Lorem ipsum dolor sit amet,
 consectetur adipiscing elit, sed do
 eiusmod tempor incididunt ut labore
 et dolore magna aliqua. Ut enim ad
 minim veniam, quis nostrud
 exercitation ullamco laboris nisi ut
 aliquip ex ea commodo consequat. Duis
 aute irure dolor in reprehenderit in
 voluptate velit esse cillum dolore eu
 fugiat nulla pariatur.

Section 2 details with a main point. Enter title here.

 Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in
voluptate velit esse cillum dolore eu
fugiat nulla pariatur.



**Enter your main point /
statement here.**



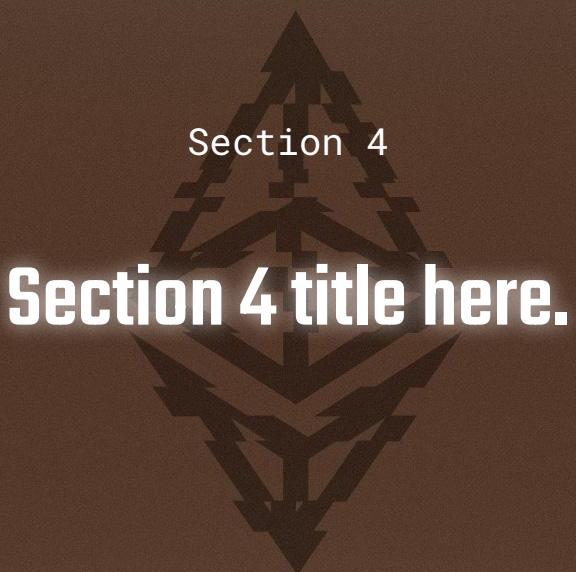
Section 3

Section 3 title here.

**Enter your main point /
statement here.**

Section 3 details with a main point. Enter title here.

Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in
voluptate velit esse cillum dolore eu
fugiat nulla pariatur.



Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

 Lorem ipsum dolor sit amet,
consectetur adipiscing elit, sed do
eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad
minim veniam, quis nostrud
exercitation ullamco laboris nisi ut
aliquip ex ea commodo consequat. Duis
aute irure dolor in reprehenderit in
voluptate velit esse cillum dolore eu
fugiat nulla pariatur.



**Enter your main point /
statement here.**

Enter your main point / statement here.

Here's the timeline.

Event 1



A horizontal timeline is shown with three circular markers. From left to right, the markers are purple, blue, and brown. Below each marker is a block of placeholder text.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
– Pythagoras



Your title, your organization
your@email.address
@youraccount