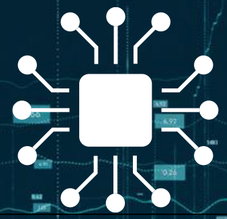


Zero-Knowledge Proofs in Web3

Janno Siim

My background

1

2

3

My background

1. **Full academia**
   Phd, Postdoc, now Lecturer (assistant professor)
2.
3.

My background

1. **Full academia**
   Phd, Postdoc, now Lecturer (assistant professor)
2. **Reseach in (practical) ZKPs and SNARKs**
3.

My background

1

Full academia

Phd, Postdoc, now Lecturer (assistant professor)

2

Reseach in (practical) ZKPs and SNARKs

- Around 10 years

3

My background

1

Full academia

Phd, Postdoc, now Lecturer (assistant professor)

2

Reseach in (practical) ZKPs and SNARKs

- Around 10 years
- **Focus:** security assumptions, security properties, protocol design

3

My background

1

Full academia

Phd, Postdoc, now Lecturer (assistant professor)

2

Reseach in (practical) ZKPs and SNARKs

- Around 10 years
- **Focus:** security assumptions, security properties, protocol design

3

Applications in Web3

My background

1

Full academia

Phd, Postdoc, now Lecturer (assistant professor)

2

Reseach in (practical) ZKPs and SNARKs

- Around 10 years
- **Focus:** security assumptions, security properties, protocol design

3

Applications in Web3

- Never worked in Web3 industry

My background

1

Full academia

Phd, Postdoc, now Lecturer (assistant professor)

2

Reseach in (practical) ZKPs and SNARKs

- Around 10 years
- **Focus:** security assumptions, security properties, protocol design

3

Applications in Web3

- Never worked in Web3 industry
- Important for research relevance

What the heck is Web3?

What the heck is Web3?

Is it just a buzzword?

What the heck is Web3?

Is it just a buzzword?

What the heck is Web3?

Is it just a buzzword?

Partly, yes ☑

What the heck is Web3?

Is it just a buzzword?

Partly, yes ☑

Is there promising tech?

What the heck is Web3?

Is it just a buzzword?

Partly, yes ☑

Is there promising tech?

What the heck is Web3?

Is it just a buzzword?

Partly, yes ☑

Is there promising tech?

Also, yes ☑

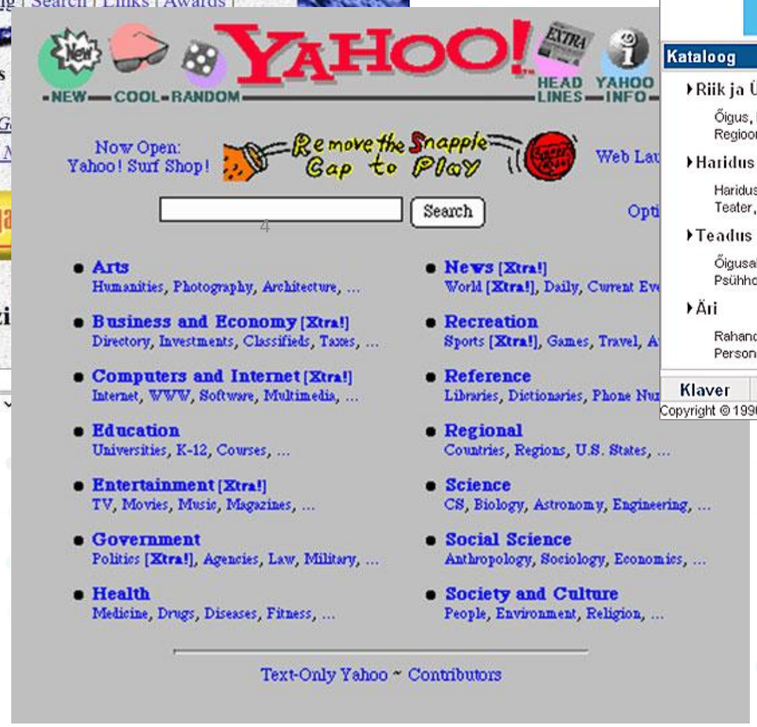
Web 1.0: 90s, early 2000s

Web 1.0: 90s, early 2000s

4

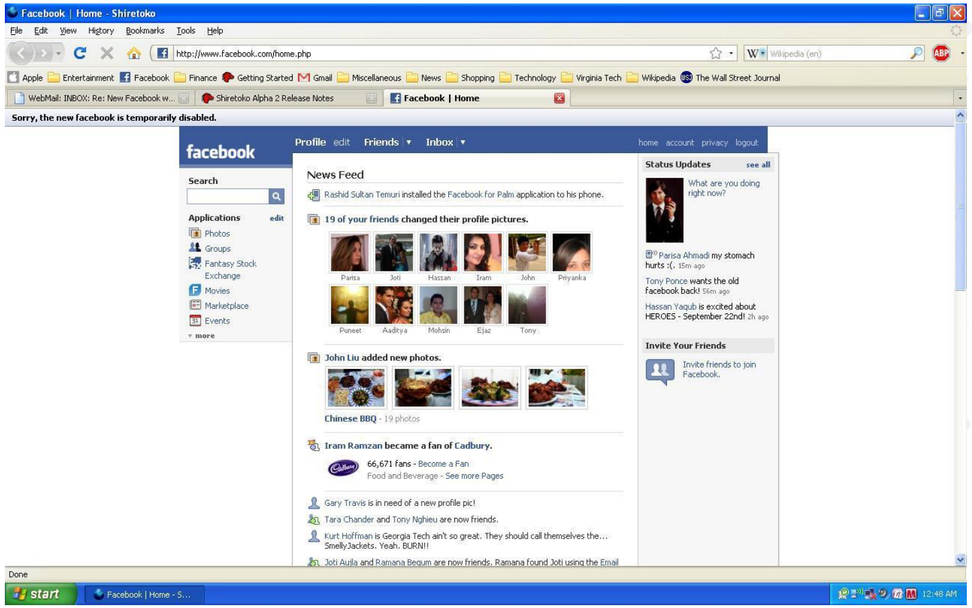
Web 1.0: 90s, early 2000s

Web 1.0: 90s, early 2000s

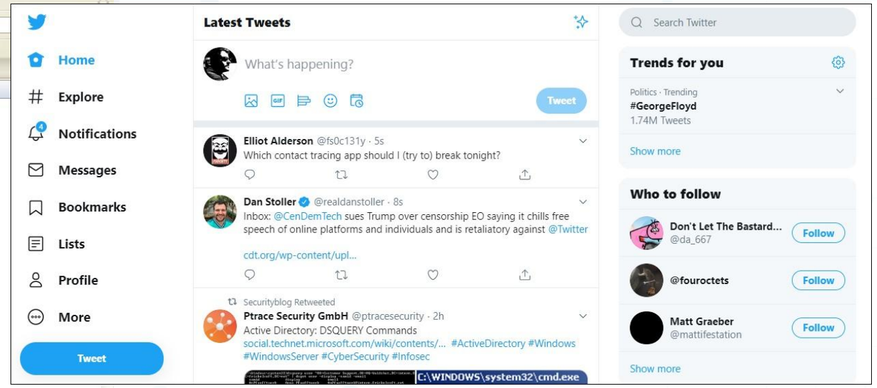


Web 2.0: Mid 2000s to Now

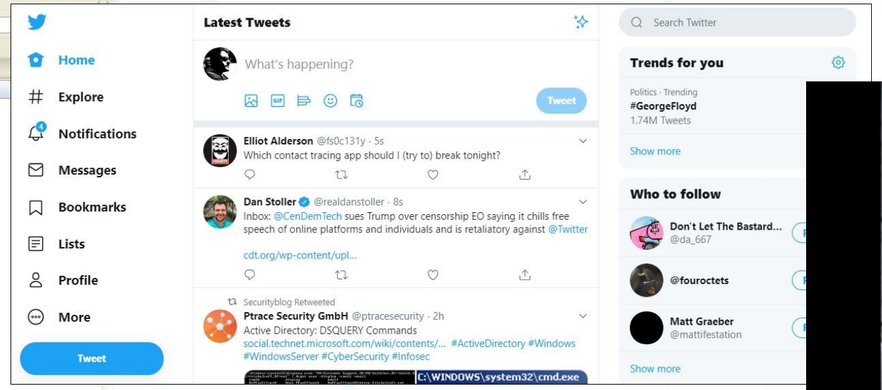
Web 2.0: Mid 2000s to Now

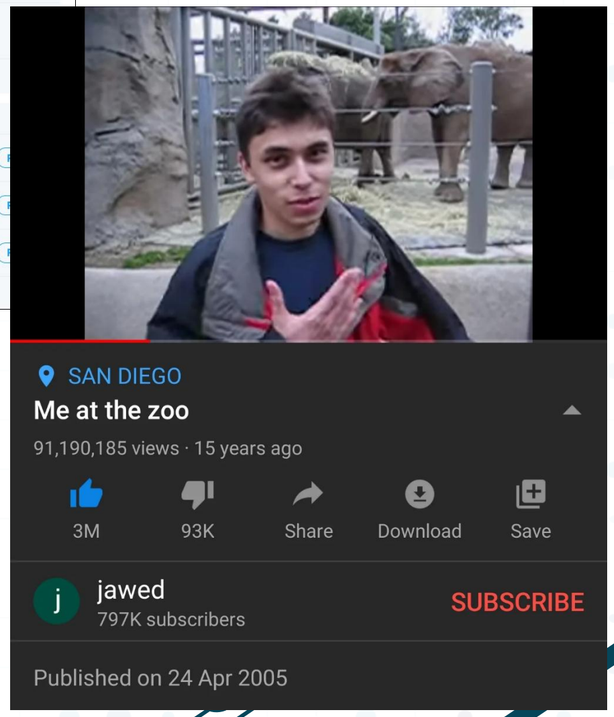


Web 2.0: Mid 2000s to Now

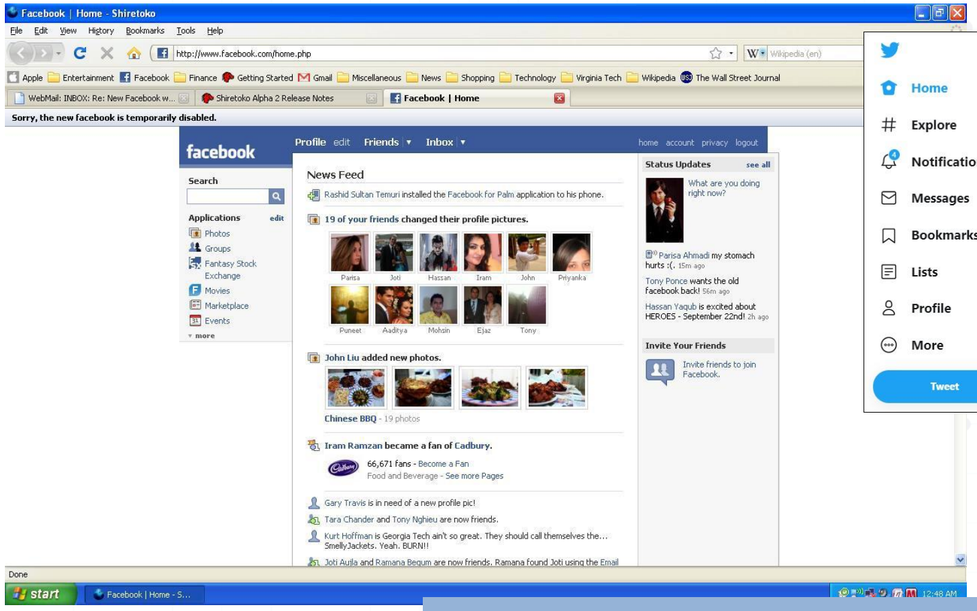


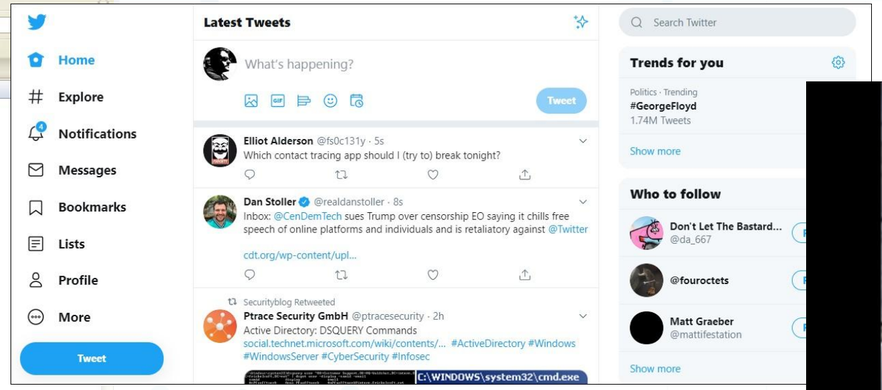
Web 2.0: Mid 2000s to Now

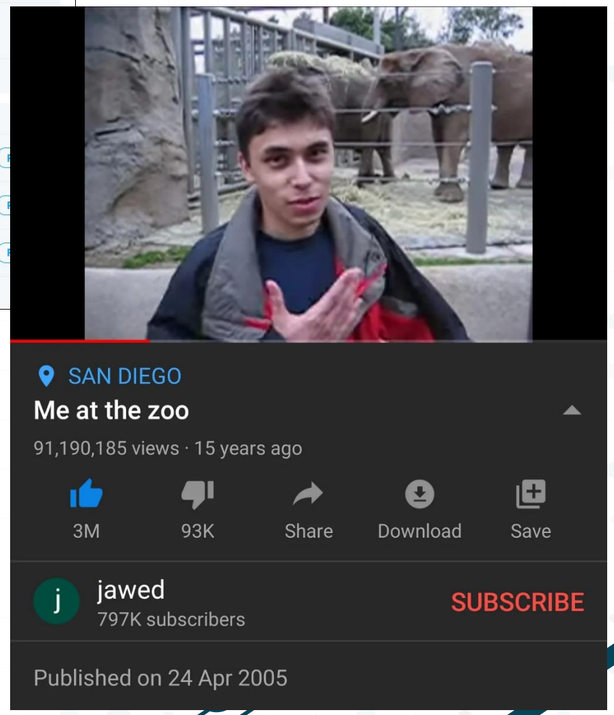




Web 2.0: Mid 2000s to Now



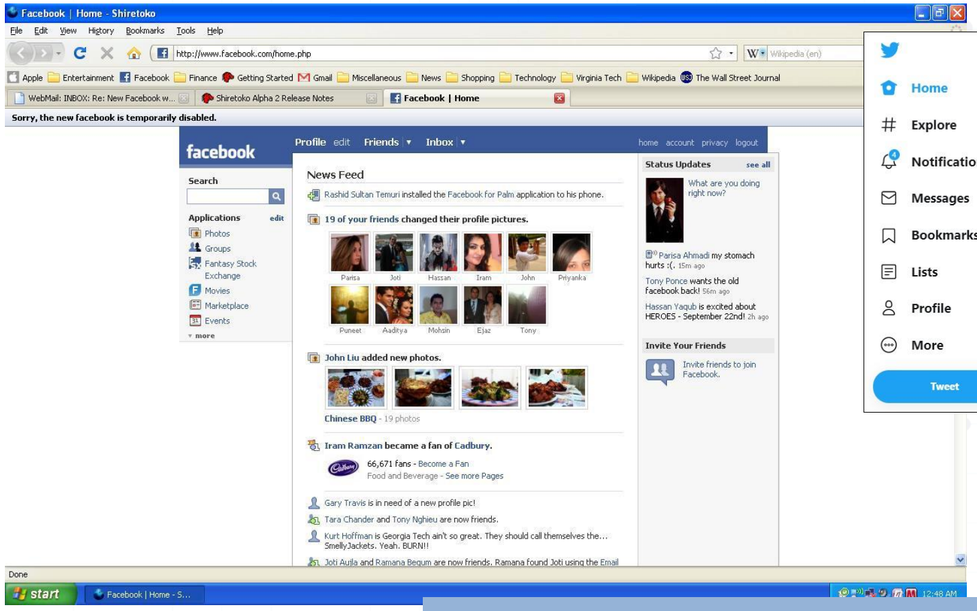


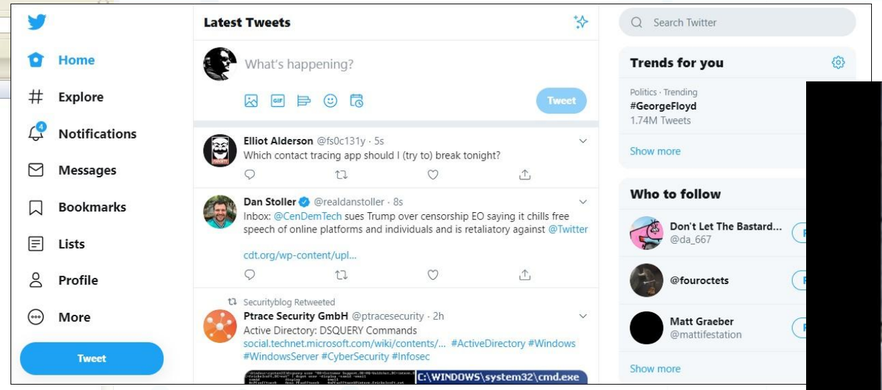


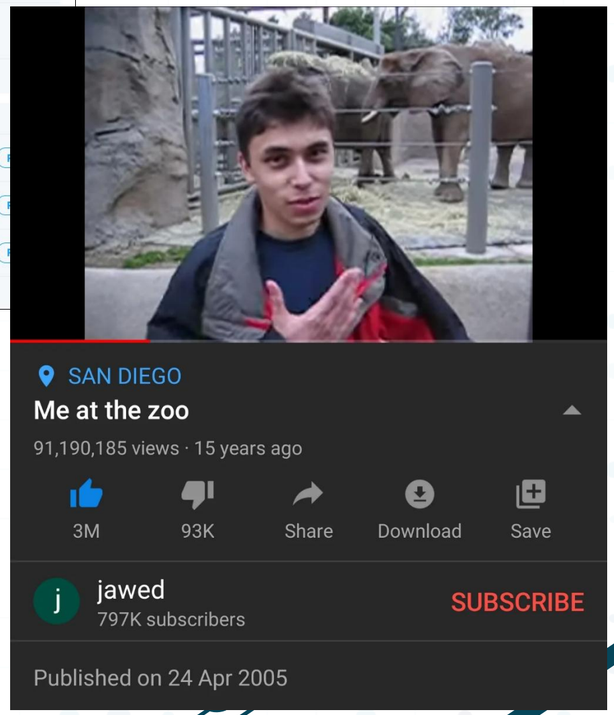
5

CENTRALIZATION:

Web 2.0: Mid 2000s to Now



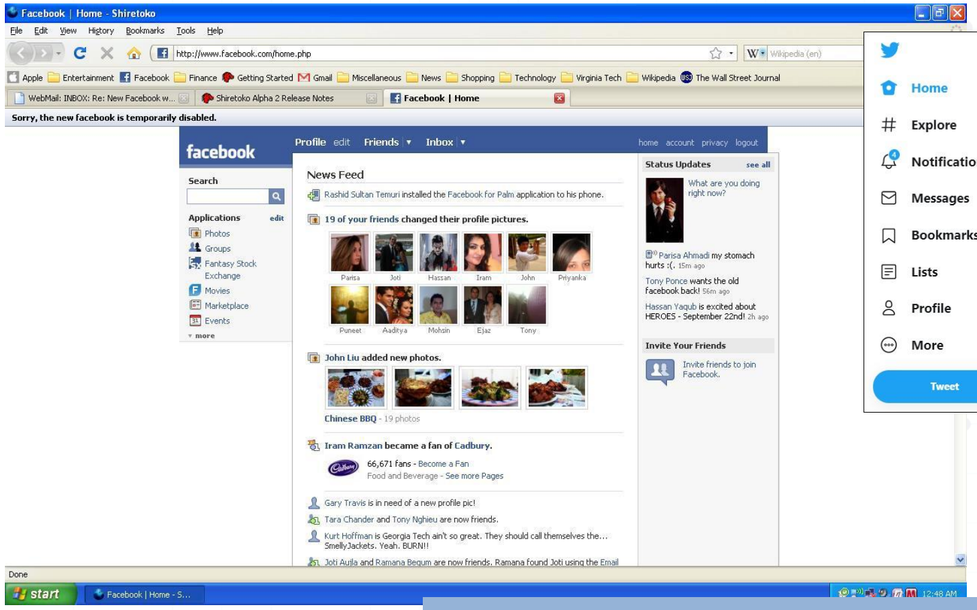


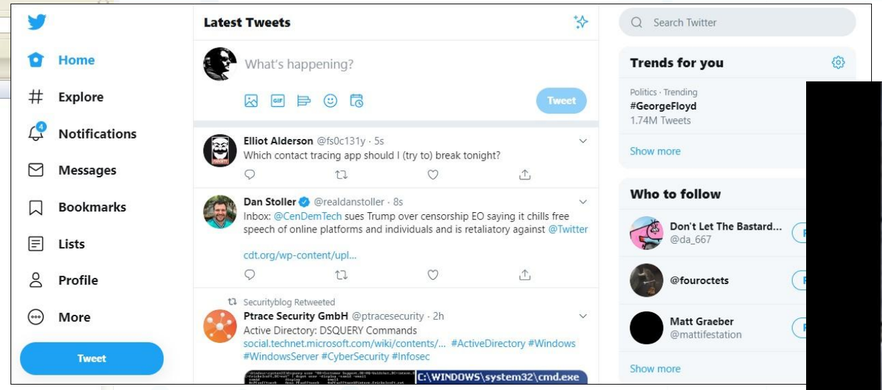


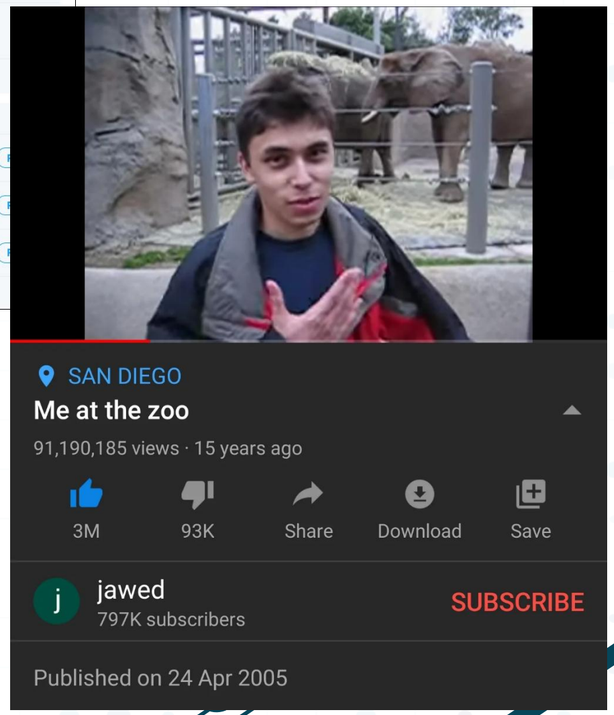
5

CENTRALIZATION: Google

Web 2.0: Mid 2000s to Now







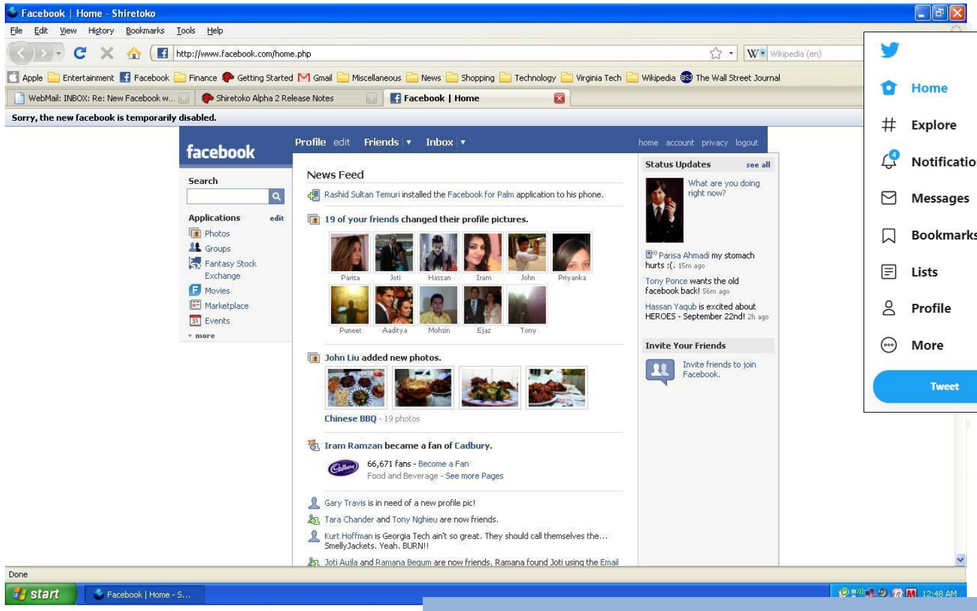
5

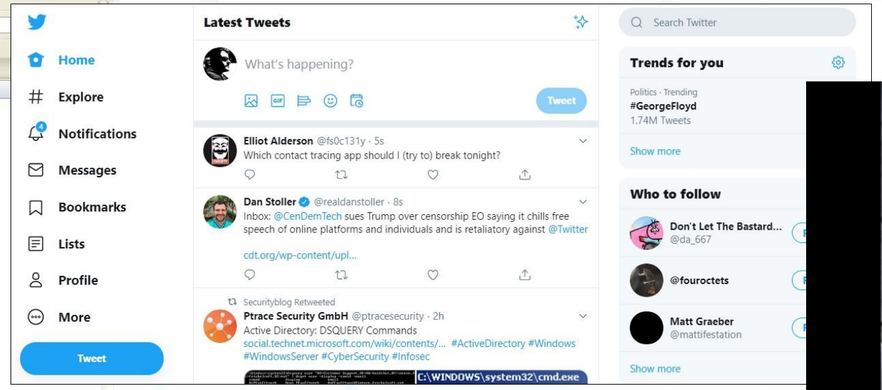
CENTRALIZATION:

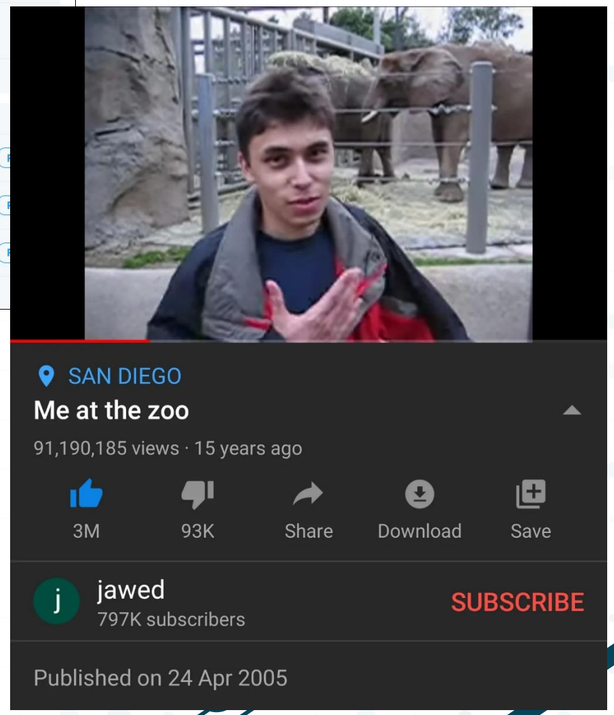
Google

amazon

Web 2.0: Mid 2000s to Now







5

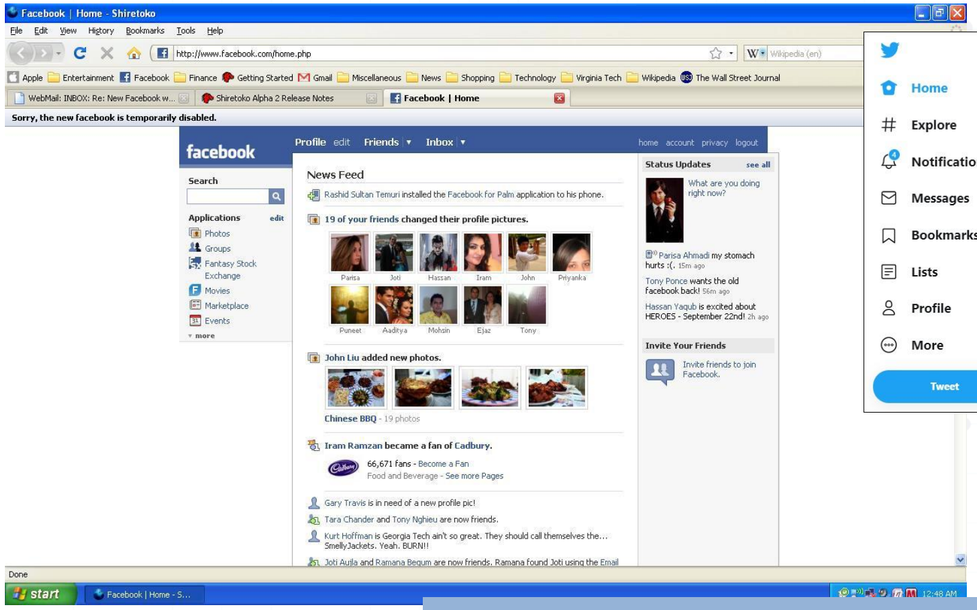
CENTRALIZATION:

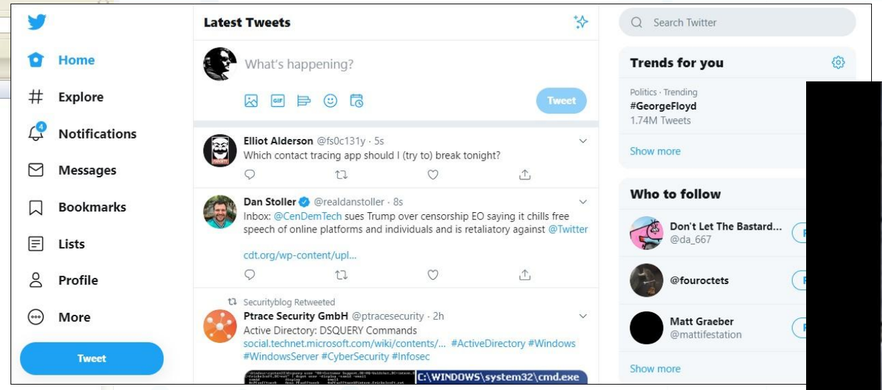
Google

Meta

amazon

Web 2.0: Mid 2000s to Now





5

CENTRALIZATION:

Google

Microsoft

Meta

amazon

Web3: Future?

Distributed Internet

6

Web3: Future?

Distributed Internet

- Decentralization

6

Web3: Future?

Distributed Internet

- Decentralization
- Blockchain technology

Web3: Future?

Distributed Internet

- Decentralization
- Blockchain technology
- Cryptocurrencies

6

Web3: Future?

Distributed Internet

- Decentralization
- Blockchain technology
- Cryptocurrencies
- Smart contracts

Web3: Future?

Distributed Internet

- Decentralization
- Blockchain technology
- Cryptocurrencies
- Smart contracts[6]
- Privacy-preserving cryptography (Zero-knowledge proofs)

Web3: Future?

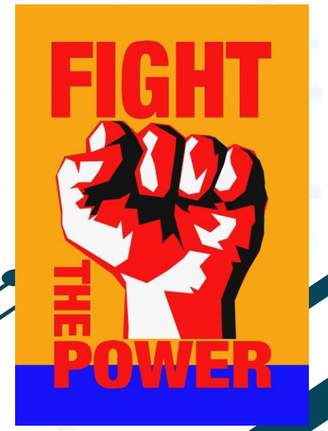
Distributed Internet

- Decentralization
- Blockchain technology
- Cryptocurrencies
- Smart contracts
- Privacy-preserving cryptography (Zero-knowledge proofs)

Web3: Future?

Distributed Internet

- Decentralization
- Blockchain technology
- Cryptocurrencies
- Smart contracts
- Privacy-preserving cryptography (Zero-knowledge proofs)



Core: Blockchain Tech

Immutable database

7

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)

Core: Blockchain Tech

Immutable database

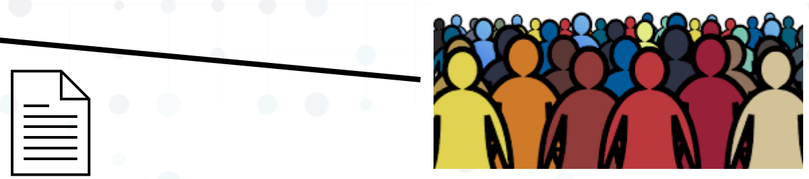
- Add data (under some contraints)
- No removal

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

7



Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

7

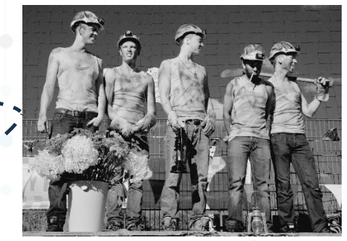
Miners

Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



Miners

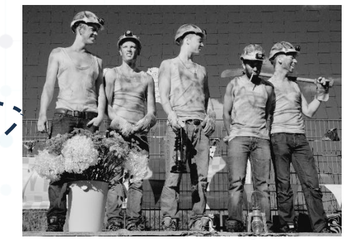
Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

- Check data



Miners

Users

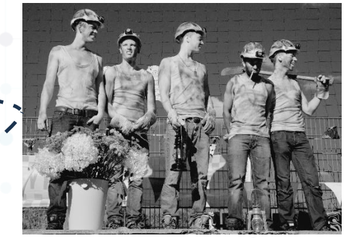
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

7

- Check data
- Mine blocks



Miners

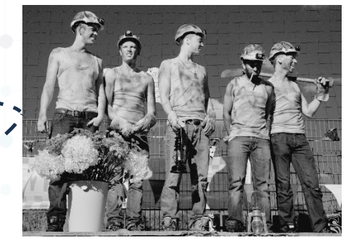
Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

- Check data
- Mine blocks
- Get reward



Miners

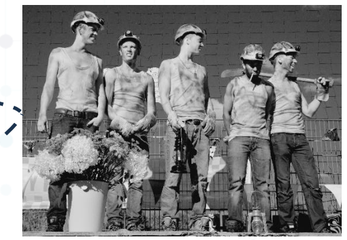
Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

- Check data
- Mine blocks
- Get reward



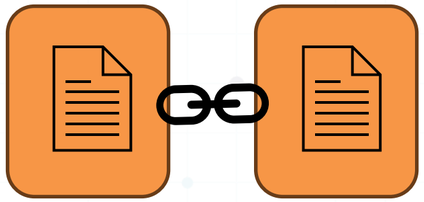
Miners

Users

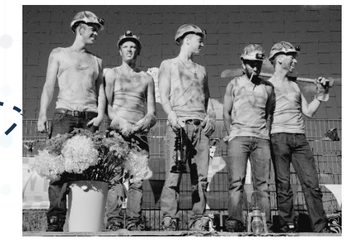
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



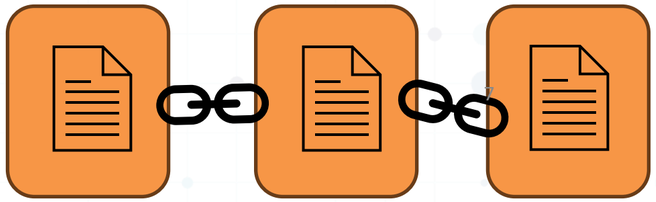
Miners

Users

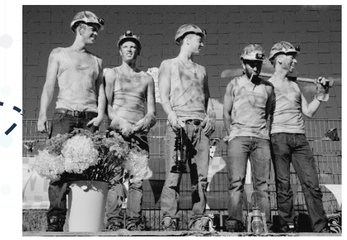
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



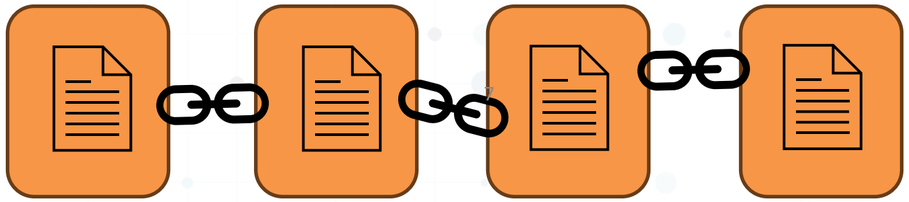
Miners

Users

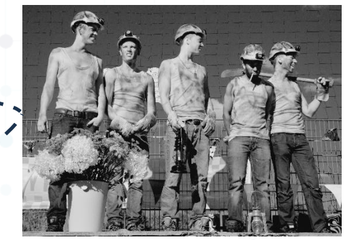
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



Miners

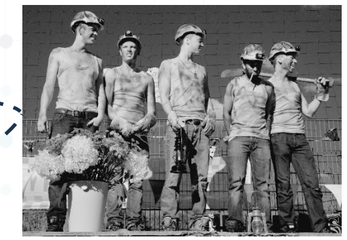
Users

Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal

- Check data
- Mine blocks
- Get reward



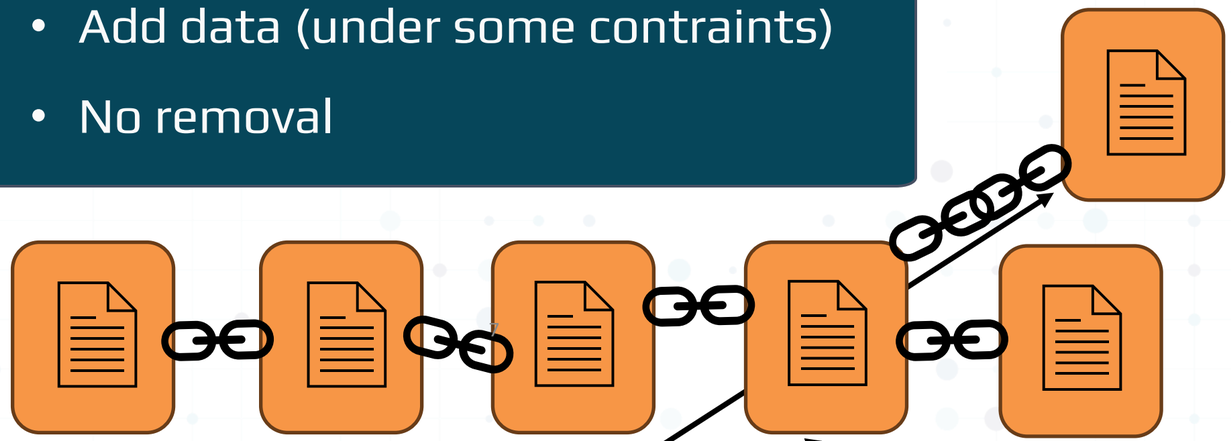
Miners

Users

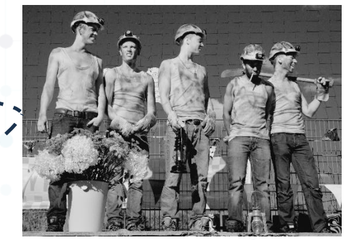
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



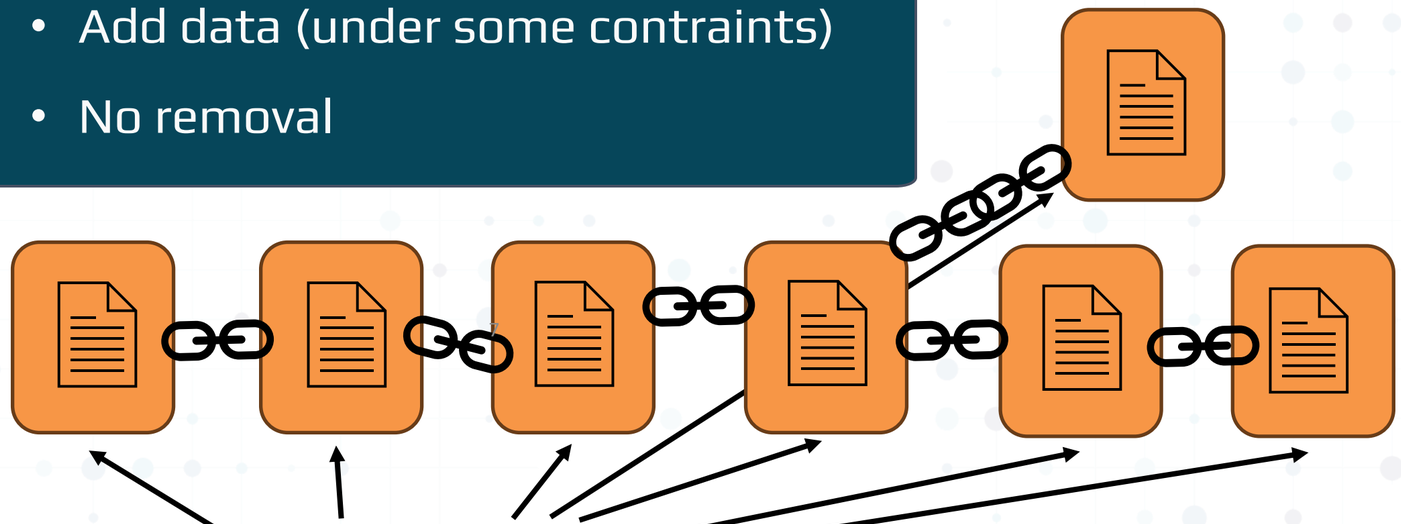
Miners

Users

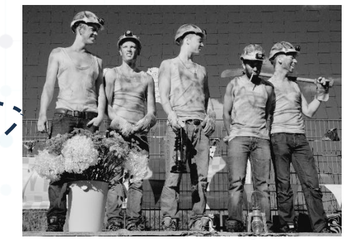
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



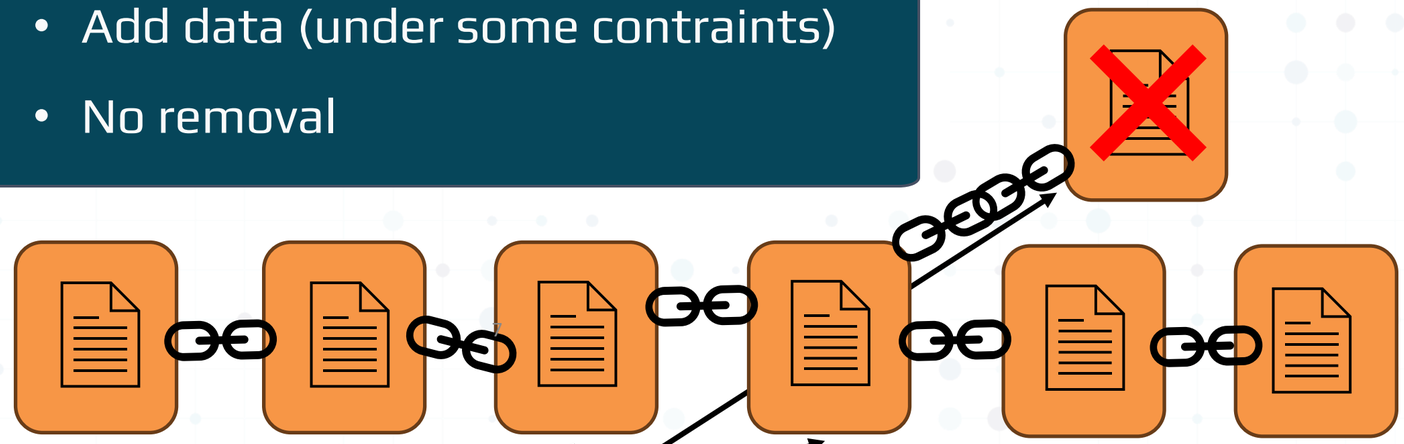
Miners

Users

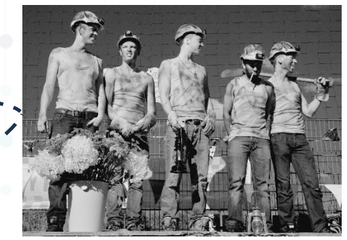
Core: Blockchain Tech

Immutable database

- Add data (under some contraints)
- No removal



- Check data
- Mine blocks
- Get reward



Miners

Users

Crypto Currencies

Immutable database

Miners

Users

Crypto Currencies

Immutable database

From

Miners

Users

Crypto Currencies

Immutable database

From To

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice			

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob		

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby

- Check that no double spending

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby

8

- Check that no double spending
- Siganture valid

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby

8

- Check that no double spending
- Siganture valid

Miners

Users

Crypto Currencies

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby
Alice	Eve	10 euro	Alice

- Check that no double spending
- Siganture valid

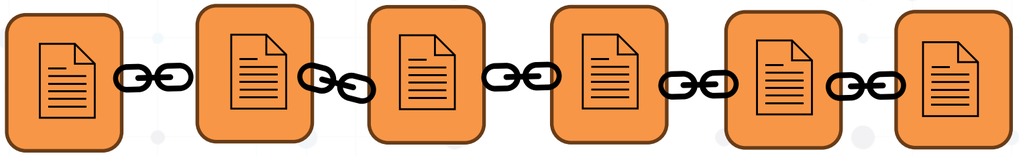
Miners

Users

Smart Contracts

1 **Why just data on blockchain?**

9



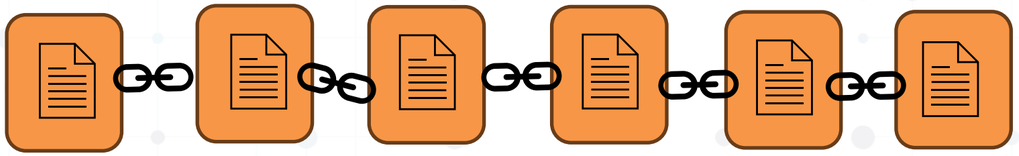
Miners

Users

Smart Contracts

1 **Why just data on blockchain?**

9



Miners

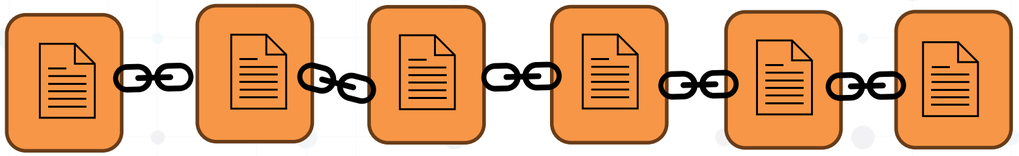
Users

Smart Contracts

1

Why just data on blockchain?

- Let’s run computer programs on blockchain



Miners

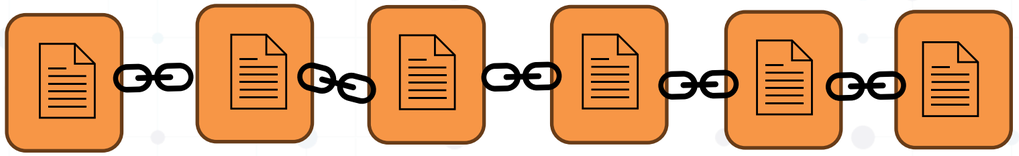
Users

Smart Contracts

1

Why just data on blockchain?

- Let’s run computer programs on blockchain
- On input X do Y



Miners

Users

Smart Contracts

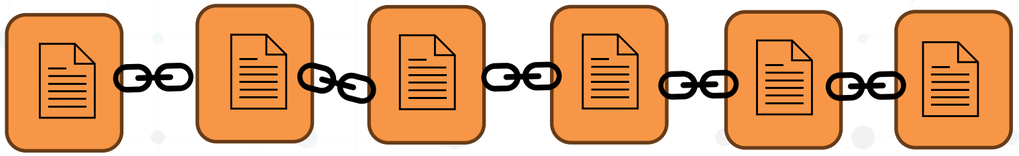
1

Why just data on blockchain?

- Let’s run computer programs on blockchain
- On input X do Y

2

Features:



Miners

Users

Smart Contracts

1

Why just data on blockchain?

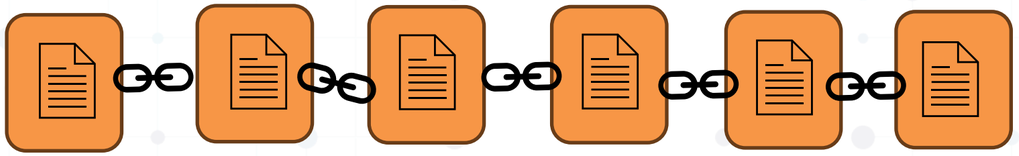
- Let’s run computer programs on blockchain
- On input X do Y

2

Features:

- Automatic execution (no trusted party)

9



Miners

Users

Smart Contracts

1

Why just data on blockchain?

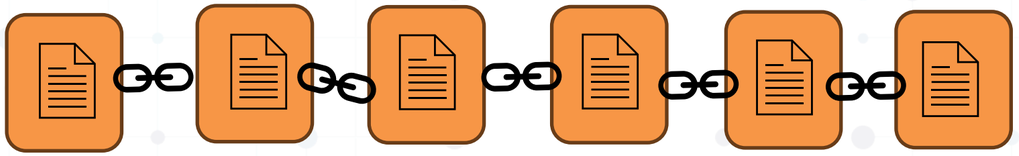
- Let’s run computer programs on blockchain
- On input X do Y

2

Features:

- Automatic execution (no trusted party)
- Transparency (whatever is in contract happens)

9



Miners

Users

Smart Contracts

1

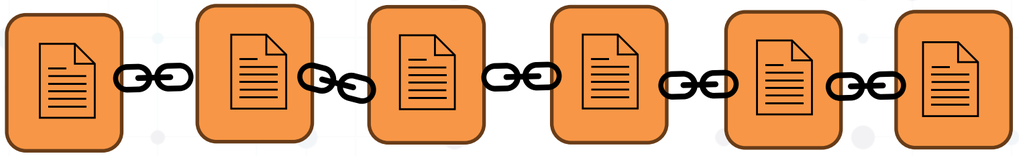
Why just data on blockchain?

- Let’s run computer programs on blockchain
- On input X do Y

2

Features:

- Automatic execution (no trusted party)
- Transparency (whatever is in contract happens)
- Example: supply chain management (truck’s GPS shows location X, release funds)



Miners

Users

Smart Contracts

1

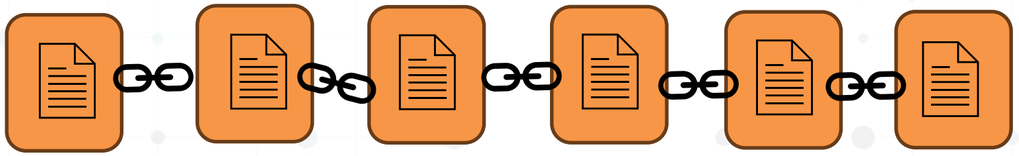
Why just data on blockchain?

- Let's run computer programs on blockchain
- On input X do Y

2

Features:

- Automatic execution (no trusted party)
- Transparency (whatever is in contract happens)
- Example: supply chain management (truck's GPS shows location X, release funds)



Miners

Users

Big Challenges in Blockchain

10

Big Challenges in Blockchain

No Privacy

Transaction are public for everyone.

10

Big Challenges in Blockchain

No Privacy

Transaction are public for everyone.

Scalability

Bitcoin 3-7tx/sec.
Mastercard 5000 tx/sec.

10

Big Challenges in Blockchain

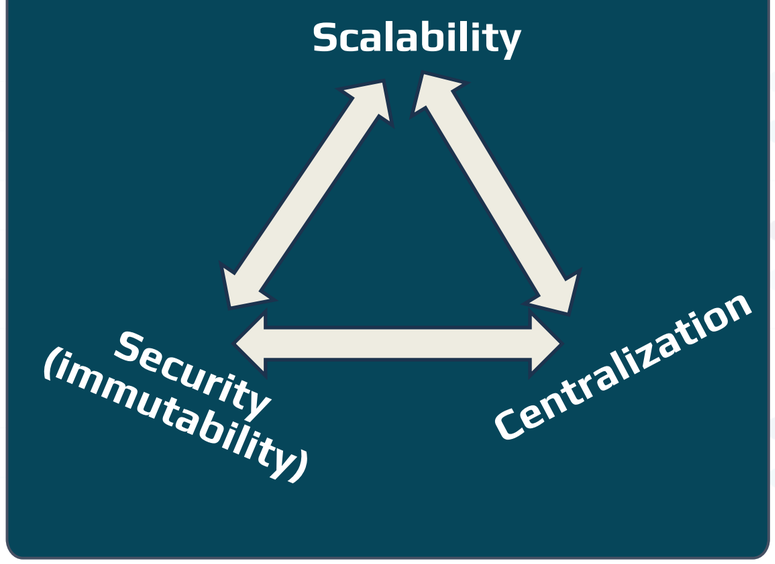
No Privacy

Transaction are public for everyone.

Scalability

Bitcoin 3-7tx/sec.
Mastercard 5000 tx/sec.

Blockchain Trilemma



Zero-Knowledge proof: Perfect tool for both

11

Starkware Valuation Hits $2B After $50M Series C Round

The fresh capital will support the deployment of its StarkNet Layer 2 platform, which will allow anyone to build blockchain applications with its technology.

BY JACQUELYN MELINEK / NOVEMBER 16, 2021 02:24 PM

The Proximity Prize

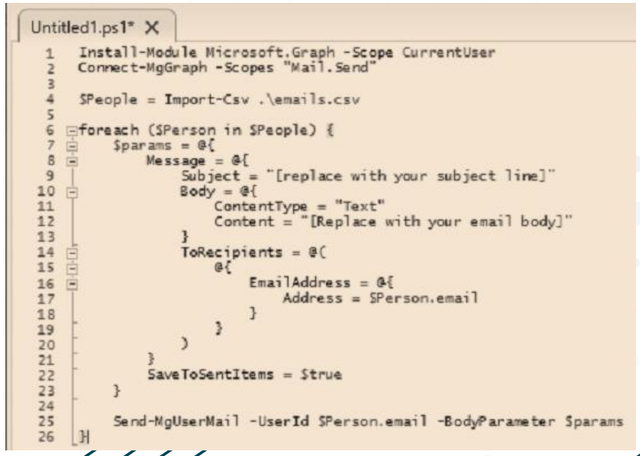
$1,000,000

in prizes to prove (or disprove!) Reed-Solomon proximity gaps conjectures.

An initiative by the Ethereum Foundation to advance the foundations of modern zkVMs.

Zero-Knowledge Virtual Machine

Zero-Knowledge Virtual Machine



ZKVM

12

ZK Prover

Zero-Knowledge Virtual Machine

Public data

Untitled1.ps1*

```
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

ZKVM

12

ZK Prover

Zero-Knowledge Virtual Machine

Public data 

Private data 

Untitled1.ps1*

```
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

ZKVM

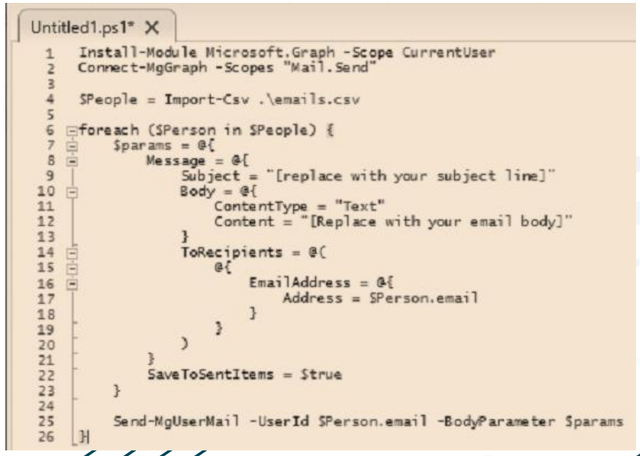
ZK Prover

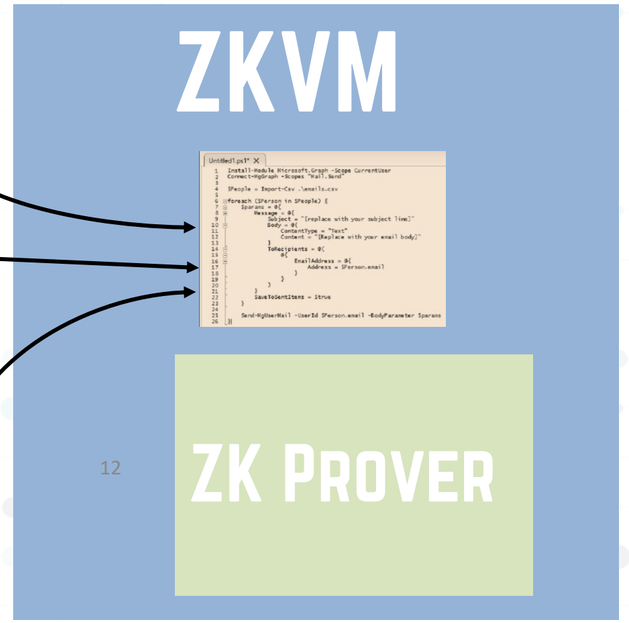
12

Zero-Knowledge Virtual Machine

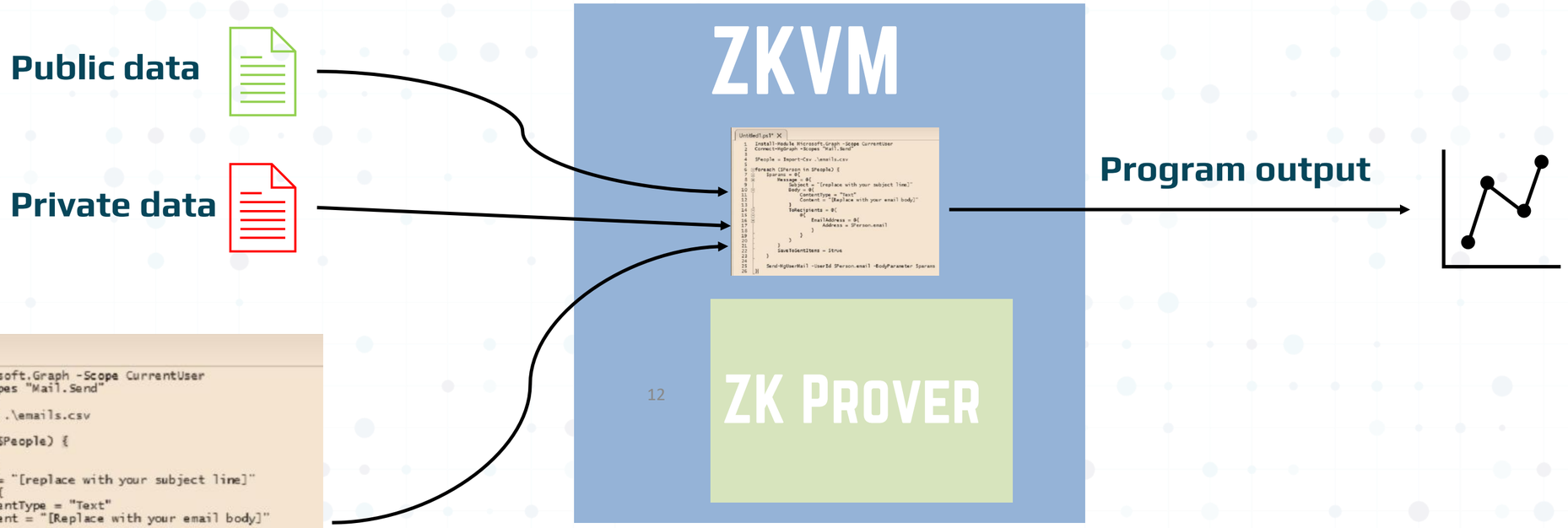
Public data

Private data





Zero-Knowledge Virtual Machine

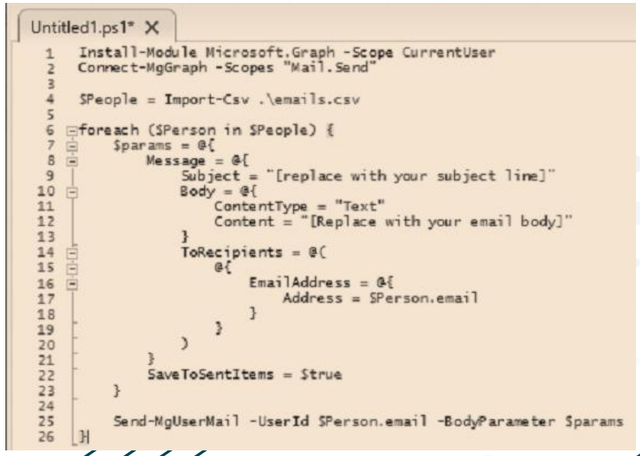



```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

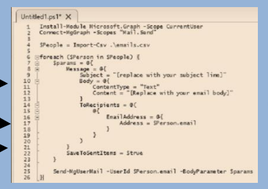
Zero-Knowledge Virtual Machine

Public data

Private data

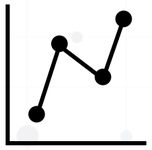


ZKVM



ZK Prover

Program output



ZK proof

12

Verification

ZK Verifier

13

Verification

Public data

ZK Verifier

13

Verification

Public data

ZK Verifier

Untitled1.ps1*

```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

Verification

Public data

ZK Verifier

Untitled1.ps1*

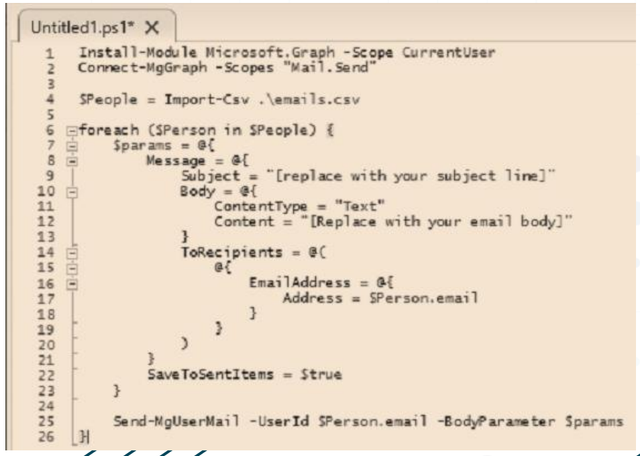
```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

13

ZK Proof

Verification

Public data



ZK Verifier

13

ZK Proof

Program output

Verification

Public data

ZK Verifier

Output correct

Untitled1.ps1*

```
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

13

ZK Proof

Program output

Verification

Public data

Private data

ZK Verifier

Output correct

Untitled1.ps1*

```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

ZK Proof

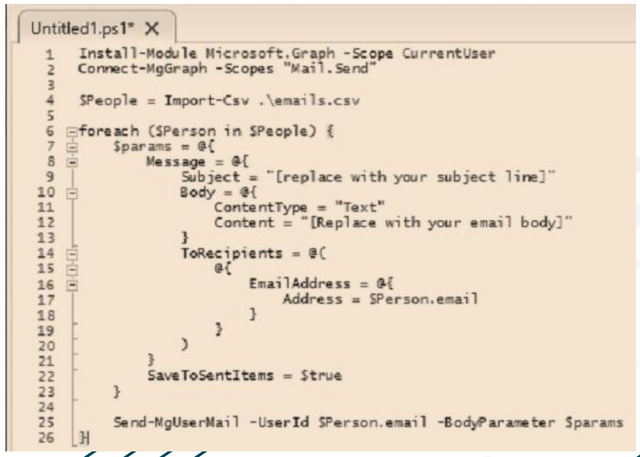
Program output

Verification

Public data

Private data

ZK Verifier



ZK Proof

Wrong output

Verification

Public data

Private data

ZK Verifier

Output incorrect

Untitled1.ps1*

```powershell
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Mail.Send"

$People = Import-Csv .\emails.csv

foreach ($Person in $People) {
    $params = @{
        Message = @{
            Subject = "[replace with your subject line]"
            Body = @{
                ContentType = "Text"
                Content = "[Replace with your email body]"
            }
            ToRecipients = @(
                @{
                    EmailAddress = @{
                        Address = $Person.email
                    }
                }
            )
        }
        SaveToSentItems = $true
    }

    Send-MgUserMail -UserId $Person.email -BodyParameter $params
}
```

ZK Proof

Wrong output

Why care?

Privacy

Why care?

Privacy

- Private data stays private.

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Succinctness (SNARK)

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Succinctness (SNARK)

- Private data >> proof size

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Succinctness (SNARK)

- Private data >> proof size
  - 1GB private data → Few KB proof size

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Succinctness (SNARK)

- Private data >> proof size
  - 1GB private data → Few KB proof size
- Slow program, fast proof verification

Why care?

Privacy

- Private data stays private.
- Proof leaks **ZERO** unnecessary information

15

Succinctness (SNARK)

- Private data >> proof size
  - 1GB private data → Few KB proof size
- Slow program, fast proof verification
  - 1 hour -> less than 1 second

Intuition

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

16

Intuition

Slow to Solve

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

16

Intuition

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

17

Intuition

Fast to verify

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

17

Intuition

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Fast to verify

Non-Succint Proof

17

Intuition

Succinct proof

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

18

Intuition

Succinct proof

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

How is it even possible?

19

How is it even possible?

19

Firstly, if $K \leq n+d+1$, then $\deg(L) \leq K-1 \leq n+d$, contradicting the claim that $\deg(L) > n+d$. Thus, we assume in the following that $K \geq n+d+2$.

Let $S_1 = \{\alpha_i\}_{i=1}^{n+d+1}$ and $L_1(X) := \mathsf{Inter}(\{\alpha_i, y_i\}_{i=1}^{n+d+1})$ be the interpolation polynomial over the respective points. Then, L_1 is a unique polynomial of degree at most $n+d$ such that $L_1(\alpha_i) = y_i$ for all $i \in [1..n+d+1]$. There exists j^* such that $L(\alpha_{j^*}) \neq L_1(\alpha_{j^*})$ (otherwise $L = L_1$ and $\deg(L) \leq n+d$). Let $L_2(X) := \mathsf{Inter}(\{(\alpha_i, y_i)\}_{i=1}^{n+d} \cup \{(\alpha_{j^*}, y_{j^*})\})$. It also holds that $L_1(X) \neq L_2(X)$ because $L_1(\alpha_{j^*}) \neq L_2(\alpha_{j^*})$.

Let $\ell_i^{S_1}(X) \in \mathbb{F}^{\leq n+d}[X]$ be the ith Lagrange polynomial over the set S_1 (see Eq. (1)) for $i \in [1..n+d+1]$. Then, $L_1(X) = \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(X)$. Recall also that

$$\ell_i^{S_1}(X) = d_i^{S_1} \mathsf{Z}_{S_1}(X)/(X-\alpha_i) \ , \tag{3}$$

where $d_i^{S_1} = 1/\prod_{j \in [1..n+d+1]\setminus\{i\}}(\alpha_i - \alpha_j)$. Now, observe that

$$\begin{aligned}
&\textstyle\sum_{j=1}^{m} g_j(x)c_j - L_1(x) = \\
&\textstyle\sum_{j=1}^{m} \left(\sum_{i=1}^{n+d+1} g_j(\alpha_i)\ell_i^{S_1}(x)\right) c_j - \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(x) = \\
&\textstyle\sum_{i=1}^{n+d+1} \ell_i^{S_1}(x) \left(\sum_{j=1}^{m} g_j(\alpha_i)c_j - y_i\right) \overset{(2)}{=} \sum_{i=1}^{n+d+1} \ell_i^{S_1}(x)\pi_i(x-\alpha_i) \overset{(3)}{=} \\
&\textstyle\left(\sum_{i=1}^{n+d+1} d_i^{S_1}\pi_i\right) \mathsf{Z}_{S_1}(x) = \hat{\pi}_1 \mathsf{Z}_{S_1}(x) \ .
\end{aligned}$$

where $\hat{\pi}_1 = \sum_{i=1}^{n+d+1} d_i^{S_1}\pi_i$. On the first step, we used that $\deg(g_j) \leq d$ and thus $g_j(X) = \sum_{i=1}^{n+d+1} g_j(\alpha_i)\ell_i^{S_1}(X)$ and similarly $L_1(X) = \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(X)$.

By defining $S_2 = \{\alpha_i\}_{i=1}^{n+d} \cup \{\alpha_{j^*}\}$, we can apply the same derivations to S_2 and $L_2(X)$. Thus, we obtain that for $b \in \{1,2\}$,

$$\textstyle\sum_{j=1}^{m} g_j(x)c_j - L_b(x) = \hat{\pi}_b \mathsf{Z}_{S_b}(x) \ . \tag{4}$$

Lot of complicated math

How is it even possible?

Unimportant to understand Applications

19

18 Janno Siim

Firstly, if $K \leq n+d+1$, then $\deg(L) \leq K-1 \leq n+d$, contradicting the claim that $\deg(L) > n+d$. Thus, we assume in the following that $K \geq n+d+2$.

Let $S_1 = \{\alpha_i\}_{i=1}^{n+d+1}$ and $L_1(X) := \mathsf{Inter}(\{\alpha_i, y_i\}_{i=1}^{n+d+1})$ be the interpolation polynomial over the respective points. Then, L_1 is a unique polynomial of degree at most $n+d$ such that $L_1(\alpha_i) = y_i$ for all $i \in [1..n+d+1]$. There exists j^* such that $L(\alpha_{j^*}) \neq L_1(\alpha_{j^*})$ (otherwise $L = L_1$ and $\deg(L) \leq n+d$). Let $L_2(X) := \mathsf{Inter}(\{(\alpha_i, y_i)\}_{i=1}^{n+d} \cup \{(\alpha_{j^*}, y_{j^*})\})$. It also holds that $L_1(X) \neq L_2(X)$ because $L_1(\alpha_{j^*}) \neq L_2(\alpha_{j^*})$.

Let $\ell_i^{S_1}(X) \in \mathbb{F}^{\leq n+d}[X]$ be the ith Lagrange polynomial over the set S_1 (see Eq. (1)) for $i \in [1..n+d+1]$. Then, $L_1(X) = \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(X)$. Recall also that

$$\ell_i^{S_1}(X) = d_i^{S_1} \mathsf{Z}_{S_1}(X)/(X-\alpha_i) \ , \tag{3}$$

where $d_i^{S_1} = 1/\prod_{j \in [1..n+d+1]\setminus\{i\}}(\alpha_i - \alpha_j)$. Now, observe that

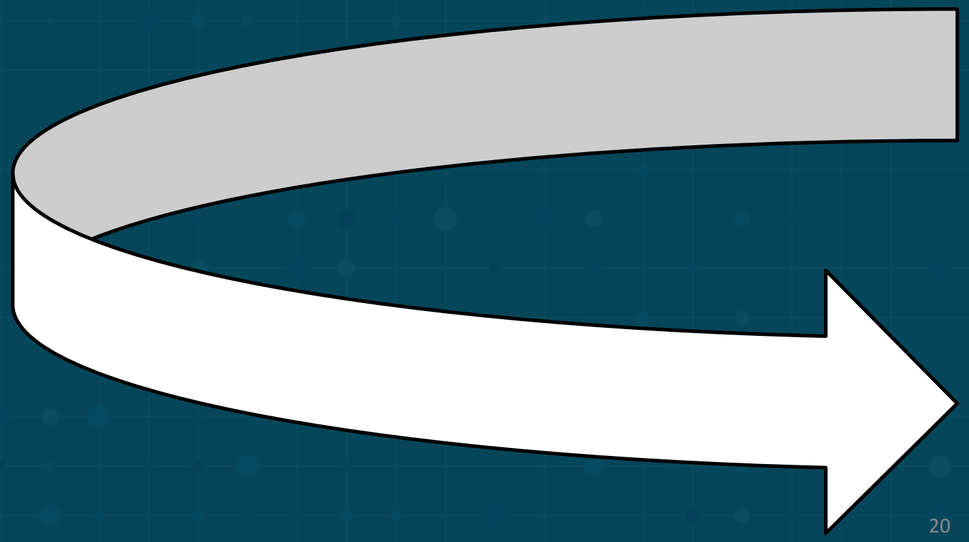
$$\begin{aligned}
&\textstyle\sum_{j=1}^{m} g_j(x)c_j - L_1(x) = \\
&\textstyle\sum_{j=1}^{m} \left(\sum_{i=1}^{n+d+1} g_j(\alpha_i)\ell_i^{S_1}(x)\right) c_j - \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(x) = \\
&\textstyle\sum_{i=1}^{n+d+1} \ell_i^{S_1}(x) \left(\sum_{j=1}^{m} g_j(\alpha_i)c_j - y_i\right) \overset{(2)}{=} \sum_{i=1}^{n+d+1} \ell_i^{S_1}(x)\pi_i(x-\alpha_i) \overset{(3)}{=} \\
&\left(\textstyle\sum_{i=1}^{n+d+1} d_i^{S_1}\pi_i\right) \mathsf{Z}_{S_1}(x) = \hat{\pi}_1 \mathsf{Z}_{S_1}(x) \ .
\end{aligned}$$

where $\hat{\pi}_1 = \sum_{i=1}^{n+d+1} d_i^{S_1}\pi_i$. On the first step, we used that $\deg(g_j) \leq d$ and thus $g_j(X) = \sum_{i=1}^{n+d+1} g_j(\alpha_i)\ell_i^{S_1}(X)$ and similarly $L_1(X) = \sum_{i=1}^{n+d+1} y_i \ell_i^{S_1}(X)$.

By defining $S_2 = \{\alpha_i\}_{i=1}^{n+d} \cup \{\alpha_{j^*}\}$, we can apply the same derivations to S_2 and $L_2(X)$. Thus, we obtain that for $b \in \{1,2\}$,

$$\textstyle\sum_{j=1}^{m} g_j(x)c_j - L_b(x) = \hat{\pi}_b \mathsf{Z}_{S_b}(x) \ . \tag{4}$$

Lot of complicated math



20

Back to blockchain

ZCash

21

ZCash

ZCash

Cryptocurrency launched in 2016

ZCash

ZCash

Cryptocurrency launched in 2016

Private transaction

Transaction are encrypted

21

ZCash

ZCash

Cryptocurrency launched in 2016

Private transaction

Transaction are encrypted

21

Zero-knowledge proofs

Main tool to avoid double spending

ZCash

ZCash

Cryptocurrency launched in 2016

Private transaction

Transaction are encrypted

21

Zero-knowledge proofs

Main tool to avoid double spending

Success

Still one of the top cryptocurrencies

Main Intuition

Immutable database

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby
Alice	Eve	10 euro	Alice

- Check that no double spending
- Siganture valid

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

23

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

23

How to avoid double spending?

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

24

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

24

Enc (tx) + ZK proof of correctness

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

24

Verify proof

Enc (tx) + ZK proof of correctness

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1

24

Verify proof

Enc (tx) + ZK proof of correctness

Miners

Users

Main Intuition

Immutable database

From	To	Amount	Signature
0x43F453	0x23BA2	0xFF231	0xBF9A1
0x1F271	0xF8231	0x5F231	0x4F9A3
0xAF2A1	0xBF9A1	0x3F3A1	0xBD9A1
0x2F241	0xA8331	0x6F331	0x1A9A3

24

Verify proof

Enc (tx) + ZK proof of correctness

Miners

Users

Main motivators

25

Main motivators

1 **Privacy is important**

25

Main motivators

1. **Privacy is important**
2. **Scalability is importanter**

25

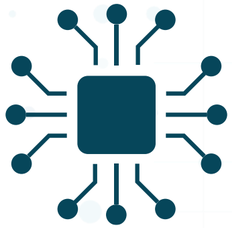
Main motivators

1. Privacy is important
2. Scalability is importanter
3. Scalability is main reason for ZK hype nowadays

Blockchain Layers

Layer 1 blockchains

26



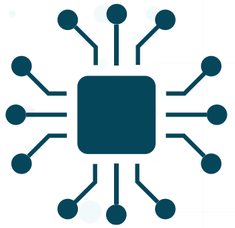
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism



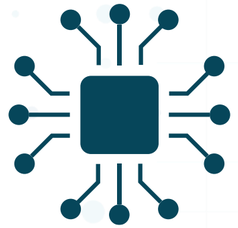
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure



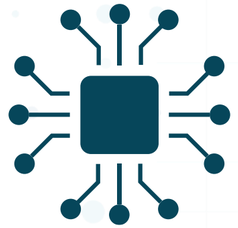
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized



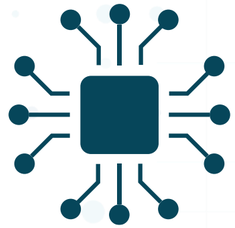
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



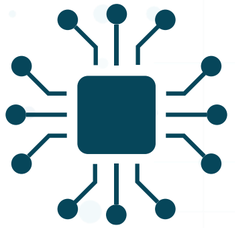
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



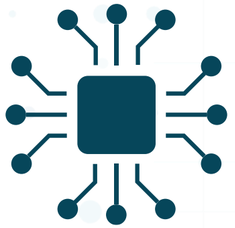
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



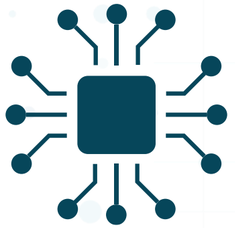
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



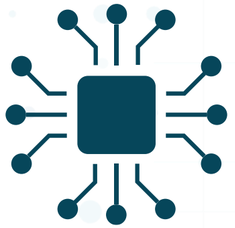
Layer 2 blockchains

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



Layer 2 blockchains

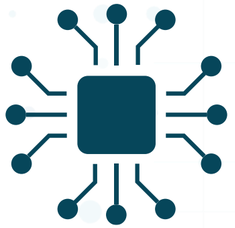
- Depend on layer 1 for security

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



Layer 2 blockchains

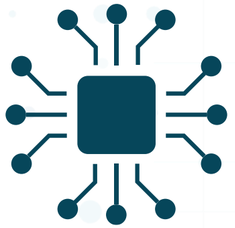
- Depend on layer 1 for security
- Much faster

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



Layer 2 blockchains

- Depend on layer 1 for security
- Much faster

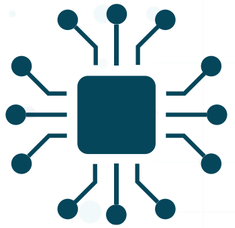
Lightning Network®

Blockchain Layers

Layer 1 blockchains

26

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



Layer 2 blockchains

- Depend on layer 1 for security
- Much faster

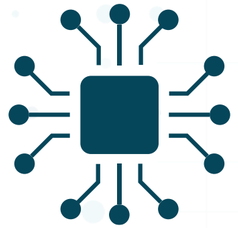
Lightning Network

OP OPTIMISM

Blockchain Layers

Layer 1 blockchains

- Actual concencus mechanism
- Secure
- Decentalized
- Slow



Layer 2 blockchains

- Depend on layer 1 for security
- Much faster

Lightning Network

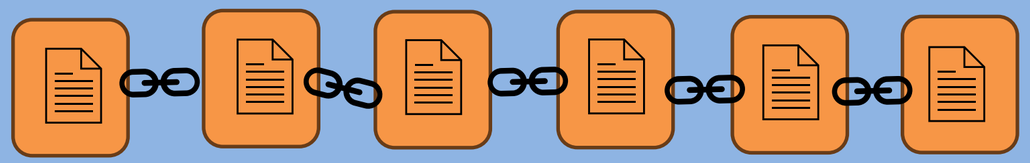
OP OPTIMISM

ZK-Rollup

Layer 2 blockchain

27

Layer 1 blockchain



ethereum

ZK-Rollup

Layer 2
blockchain

Super Node

27

Layer 1
blockchain

ethereum

ZK-Rollup

Layer 2
blockchain

Super Node

27

Layer 1
blockchain

New cryptocurrency
smart contract

STATE

ethereum

ZK-Rollup

Layer 2 blockchain

Users

Super Node

27

Layer 1 blockchain

New cryptocurrency smart contract

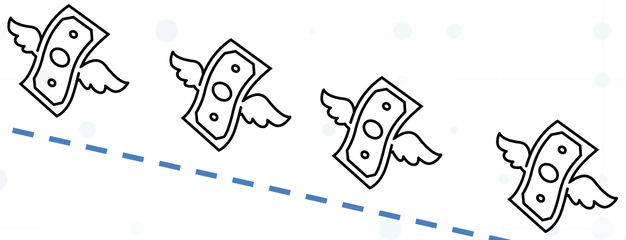
STATE

ethereum

ZK-Rollup

Layer 2 blockchain

Users



Super Node

27

Layer 1 blockchain

New cryptocurrency smart contract

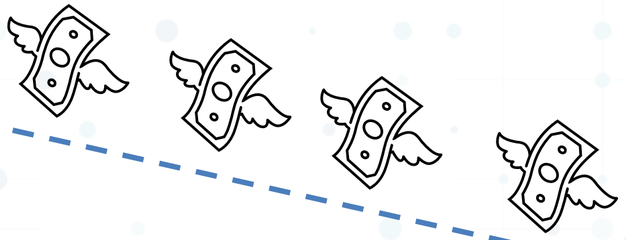
STATE

ethereum

ZK-Rollup

Layer 2 blockchain

Users



Verify/execute tx-s

Super Node

27

Layer 1 blockchain

New cryptocurrency smart contract

STATE

ethereum

ZK-Rollup

Layer 2 blockchain

Users

Compressed tx-s + Succinct Proof

Verify/execute tx-s

Super Node

27

Layer 1 blockchain

New cryptocurrency smart contract

STATE

ethereum

Compression: easy example

From	To	Amount	Signature
Alice	Bob	50 euro	Alice
Bob	Eve	20 euros	Bobby
Alice	Eve	10 euro	Alice

Super Node

Compression: easy example

From	To	Amount	Signature
Alice	Bob	50 euro	
Bob	Eve	20 euros	
Alice	Eve	10 euro	

Super Node

Compression: easy example

From	To	Amount	Signature
Alice	Bob	50 euro	
Bob	Eve	20 euros	
Alice	Eve	10 euro	

Super Node

Succinct proof that signatures verified

Advantages

29

Advantages

1. Transactions now take much less space on Layer 1

29

Advantages

1. Transactions now take much less space on Layer 1
2. Layer 1 only verifies proof (fast!)

Advantages

1. Transactions now take much less space on Layer 1
2. Layer 1 only verifies proof (fast!)
3. More tricks (blobs, external storage)

29

Advantages

1. Transactions now take much less space on Layer 1
2. Layer 1 only verifies proof (fast!)
3. More tricks (blobs, external storage)
4. 10tx/sec ⟶ 3000+ tx/sec

More applications: Proof of Solvency

Customers

Crypto bank

30

More applications: Proof of Solvency

Customers

€

Crypto bank

30

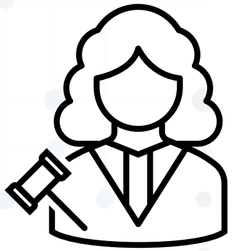
More applications: Proof of Solvency

More applications: Proof of Solvency

Customers

€

Crypto bank



Auditor

More applications: Proof of Solvency

Customers

€

Crypto bank

30

Are you solvent?

Auditor

More applications: Proof of Solvency

Customers

€

Crypto bank

30

ZK proof of solvency

Are you solvent?

Auditor

More applications: Proof of Solvency

Customers

€

Crypto bank

30

ZK proof of solvency

Are you solvent?

Missing Bitcoins: Inside the Mt. Gox Crypto Heist

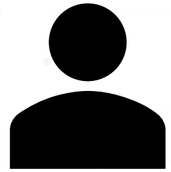
In 2014, Bitcoins worth 470 million USD vanished from an exchange in Tokyo. Where did they go?

Auditor

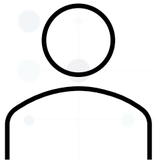
More applications: ZK Machine Learning

ML Model

31

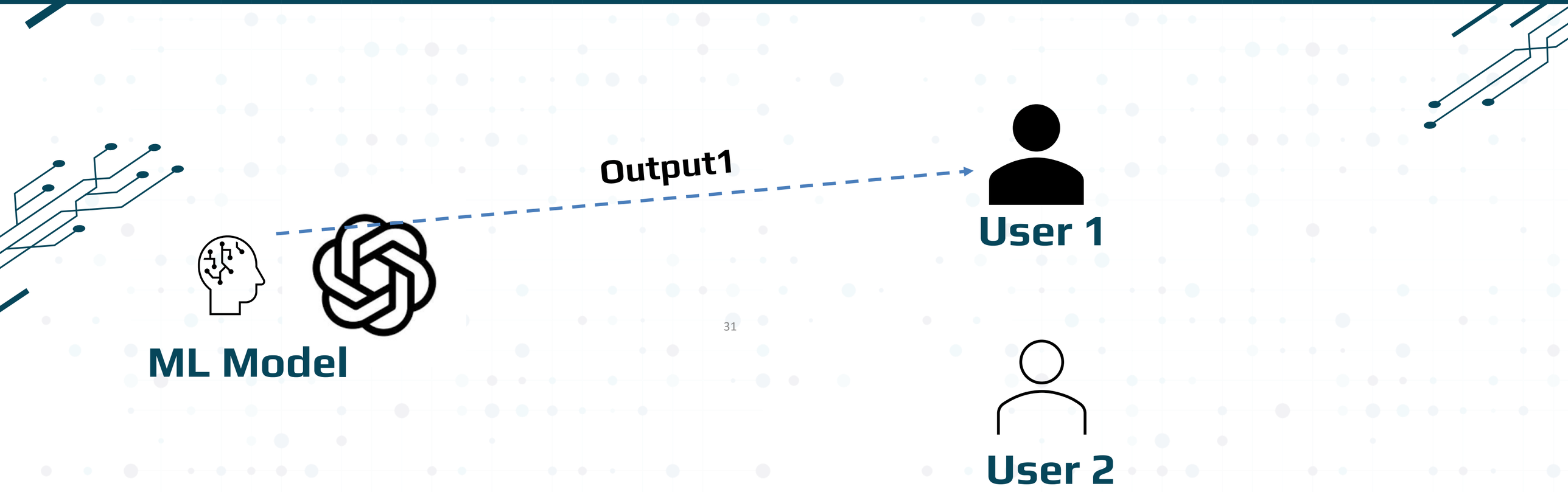


User 1

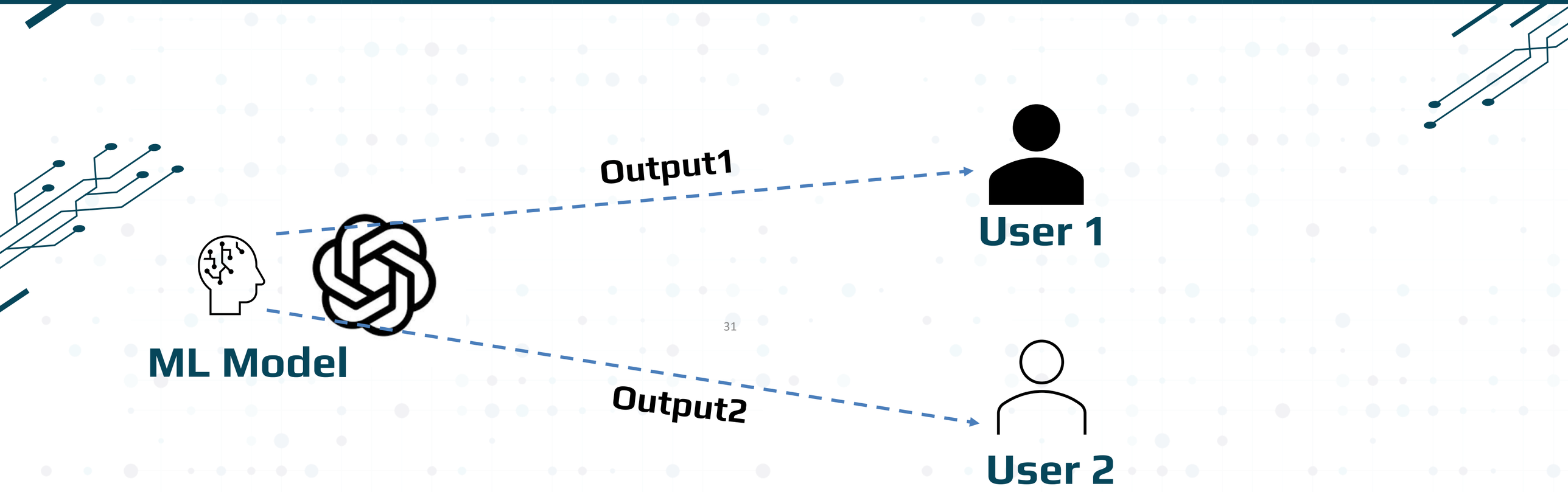


User 2

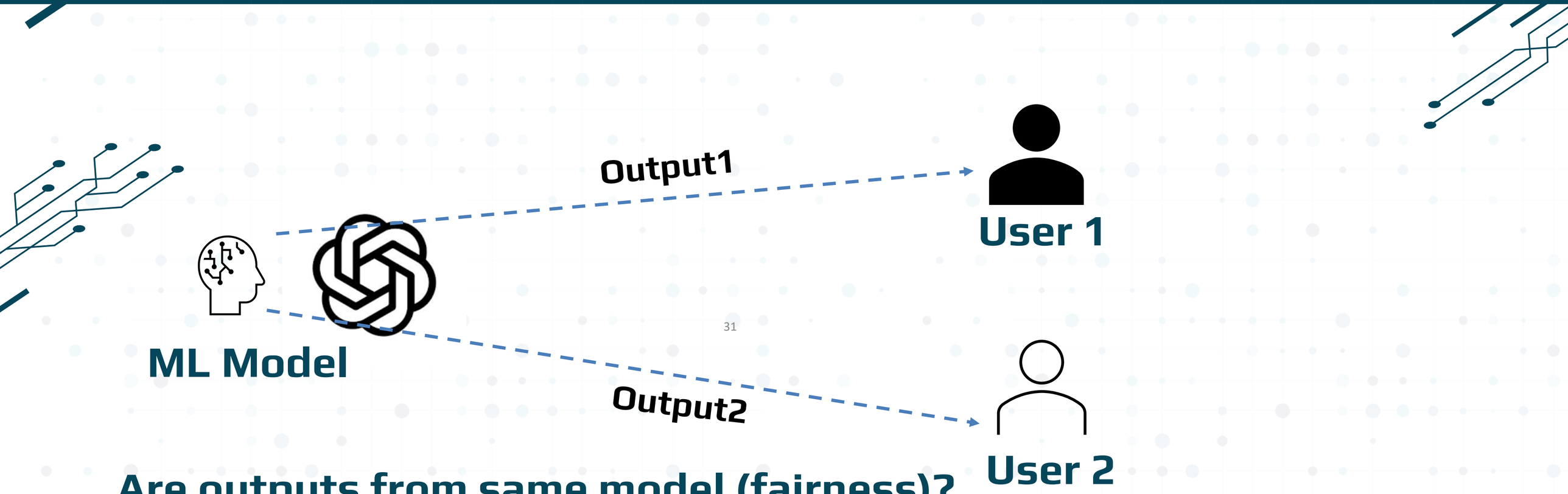
More applications: ZK Machine Learning



More applications: ZK Machine Learning



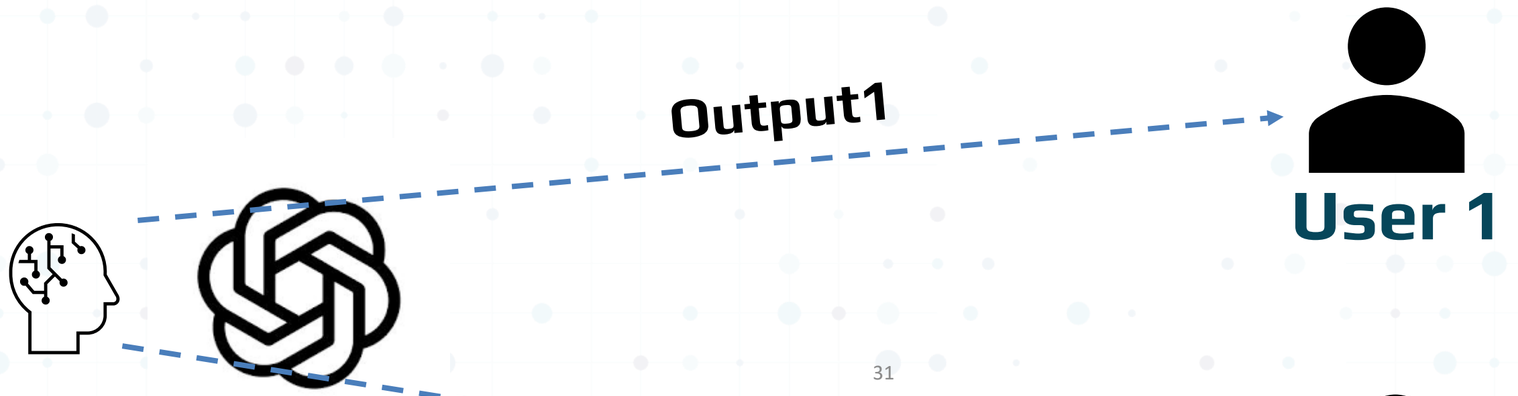
More applications: ZK Machine Learning



31

Are outputs from <u>same</u> model (fairness)?

More applications: ZK Machine Learning

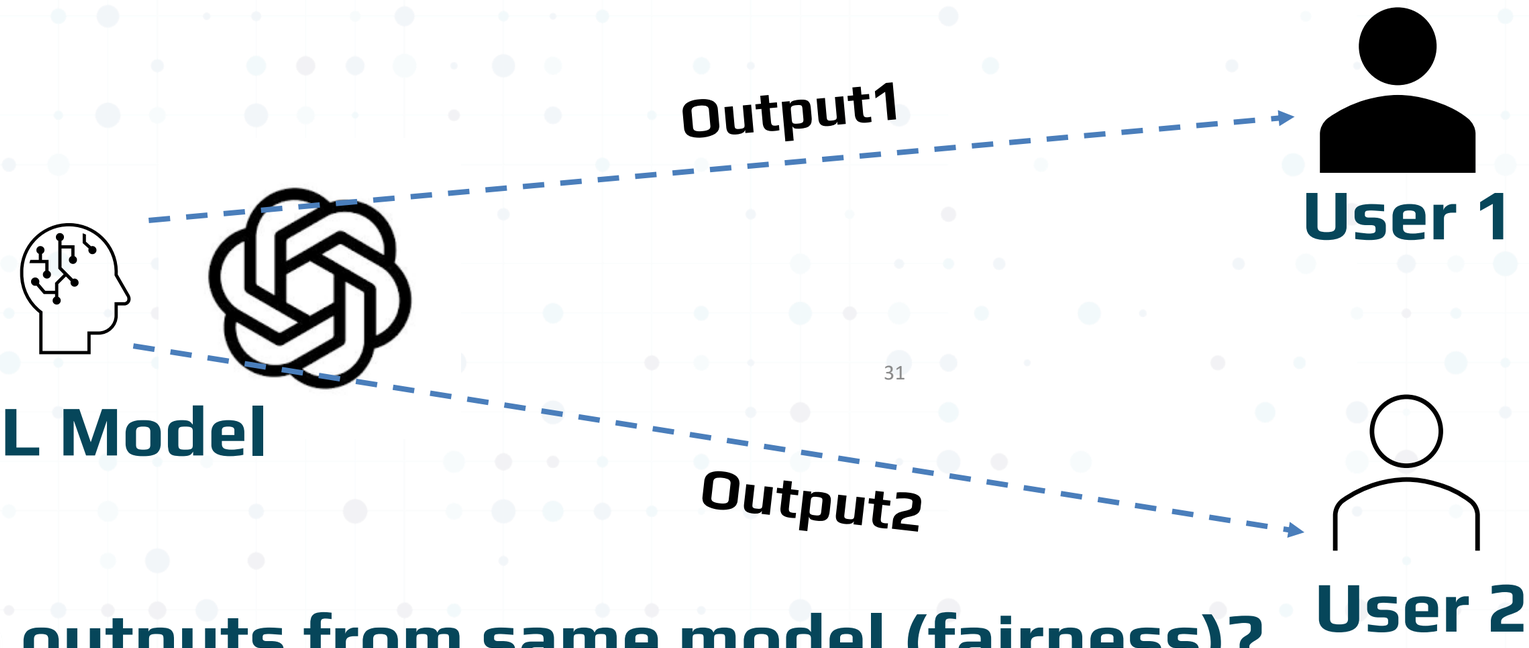


31

Are outputs from <u>same</u> model (fairness)?

- fair loans, fair prices, correct model,...

More applications: ZK Machine Learning



31

Are outputs from <u>same</u> model (fairness)?

- fair loans, fair prices, correct model,...
- give a ZK proof

More applications: fighting fake news

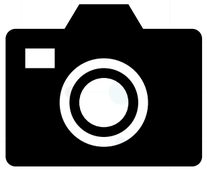
More applications: fighting fake news

How check that photo is authentic?

32

More applications: fighting fake news

How check that photo is authentic?



32

More applications: fighting fake news

How check that photo is authentic?

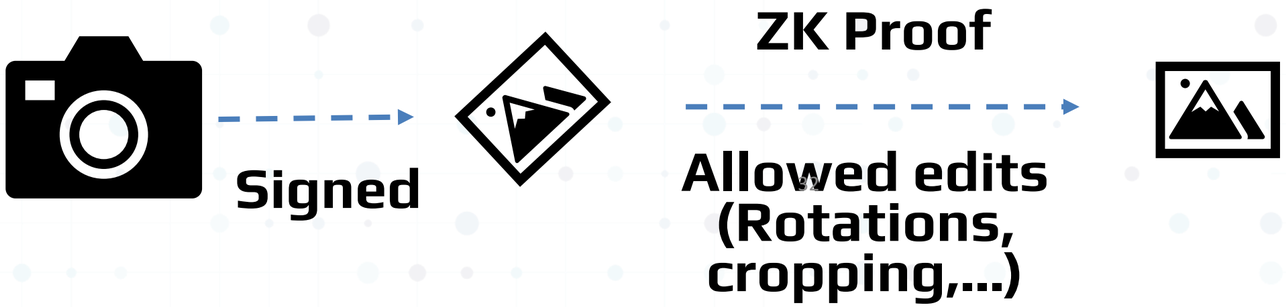
32

More applications: fighting fake news

How check that photo is authentic?

More applications: fighting fake news

How check that photo is authentic?



Vision of Future

33

Real World

Vision of Future

33

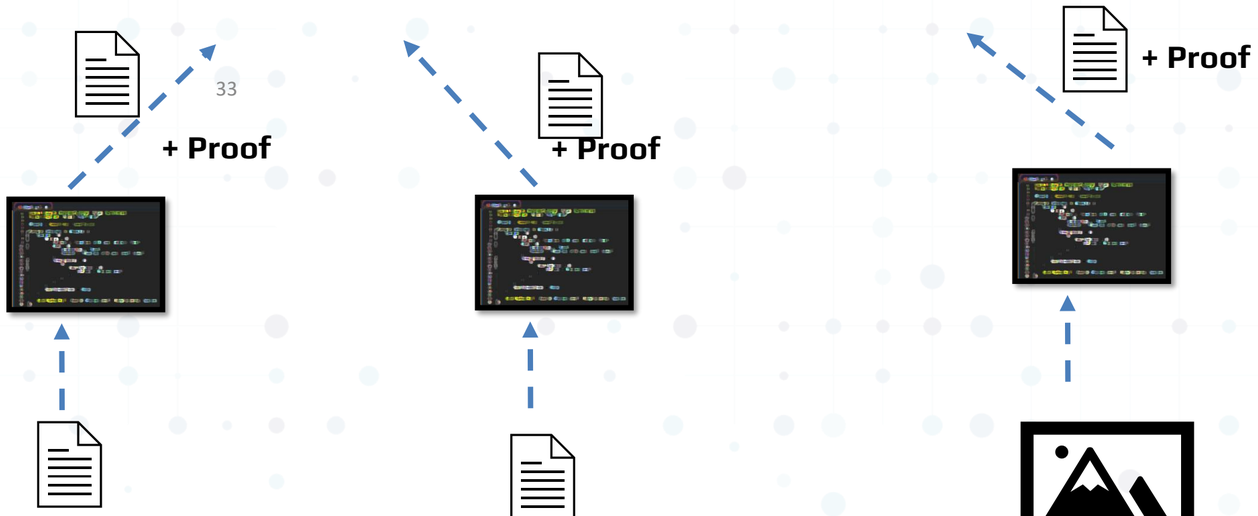
Real World

Vision of Future

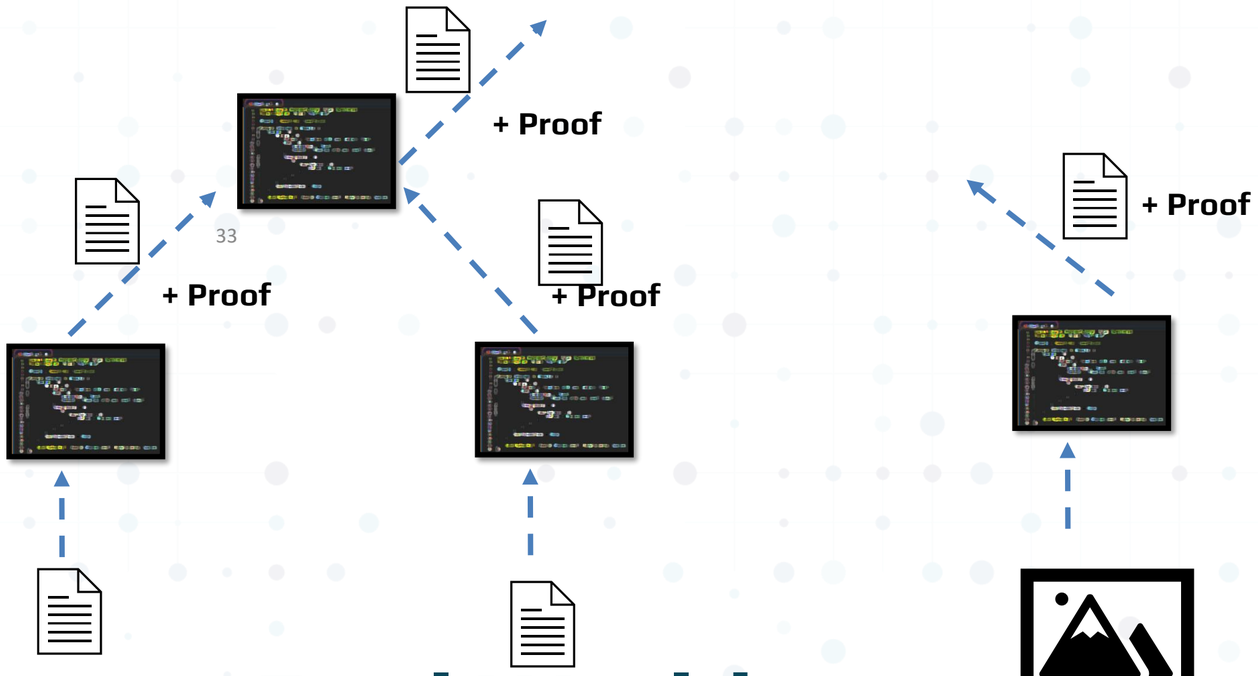
33

Real World

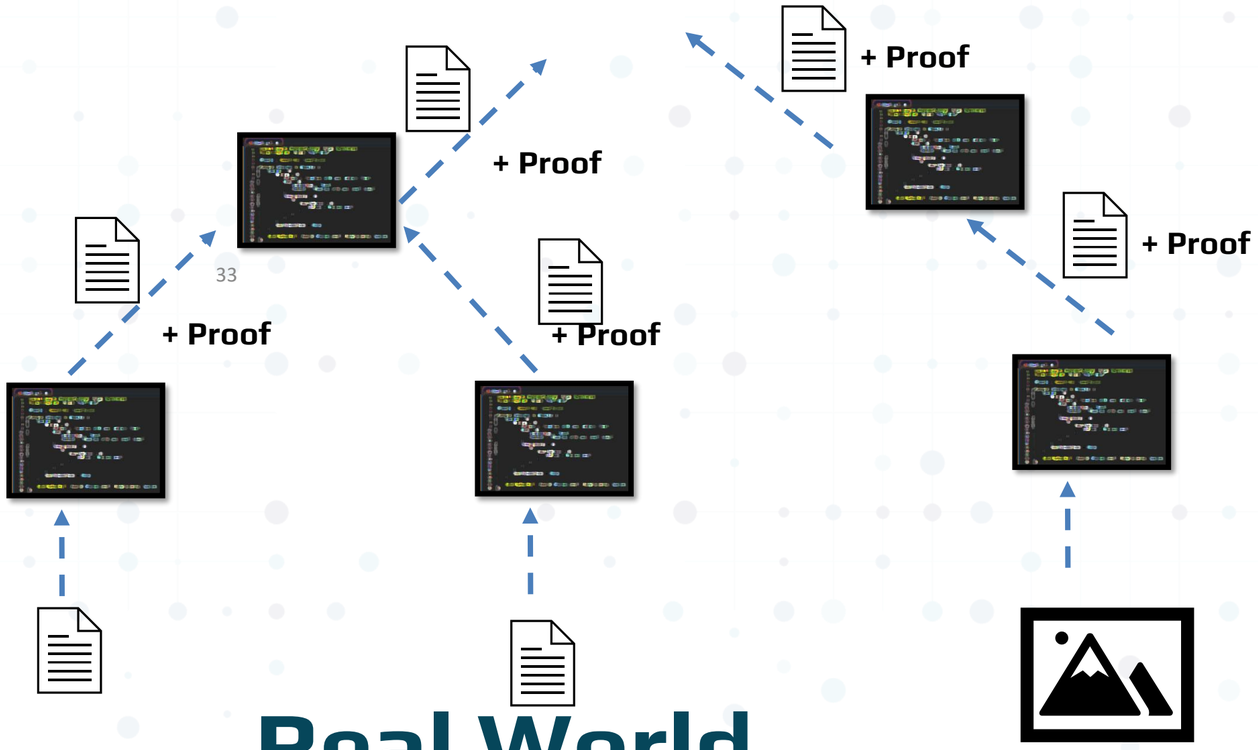
Vision of Future



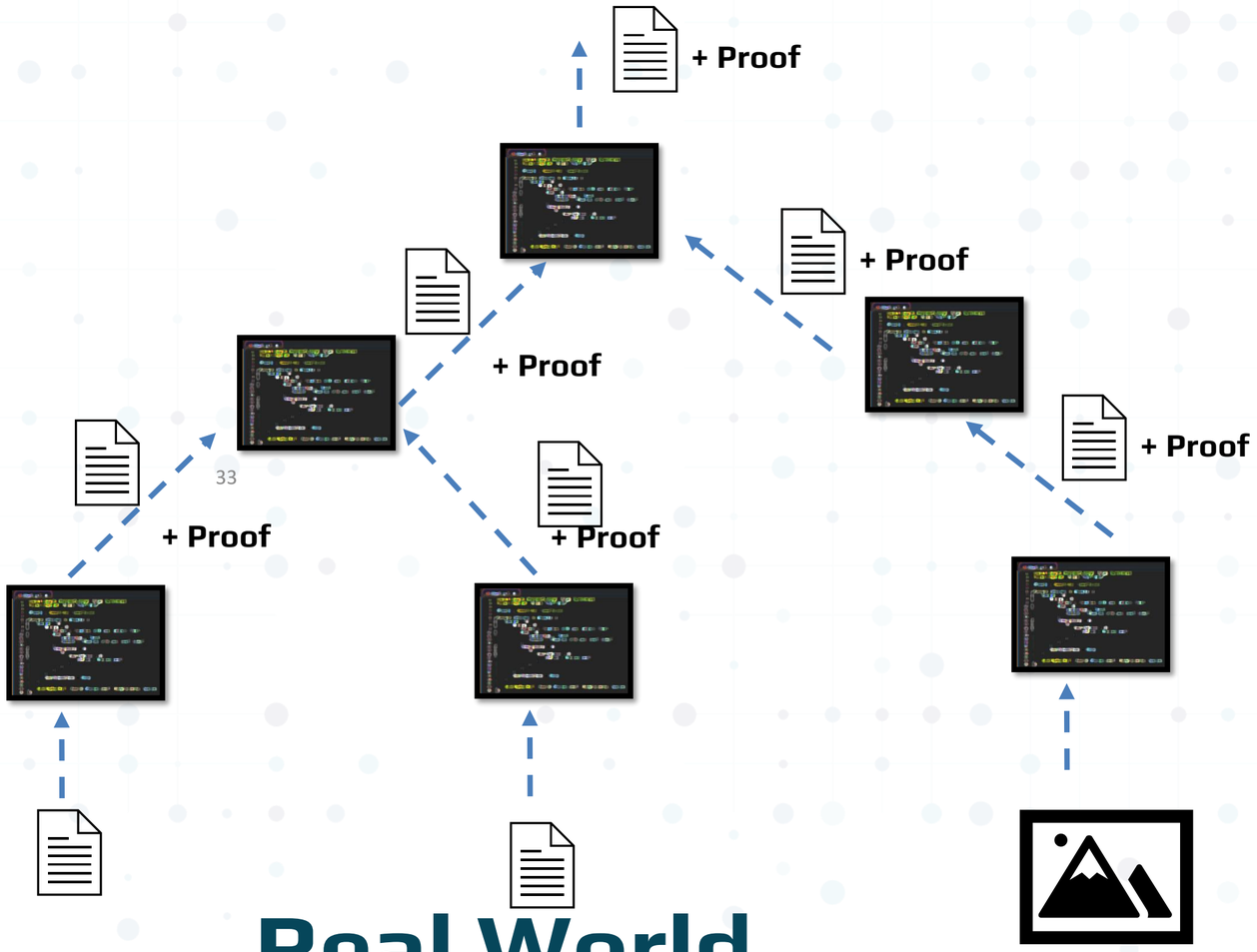
Vision of Future



Vision of Future

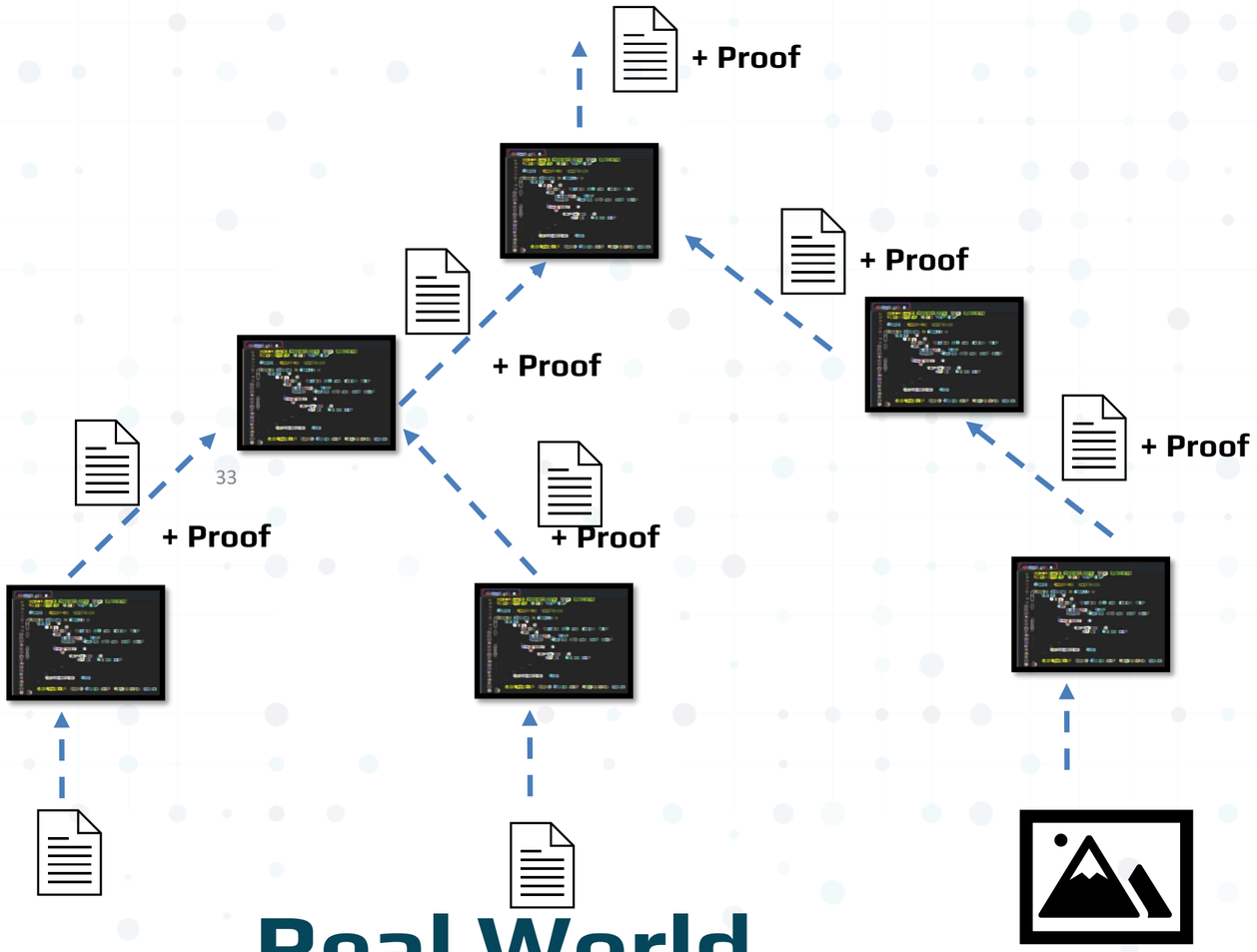


Vision of Future



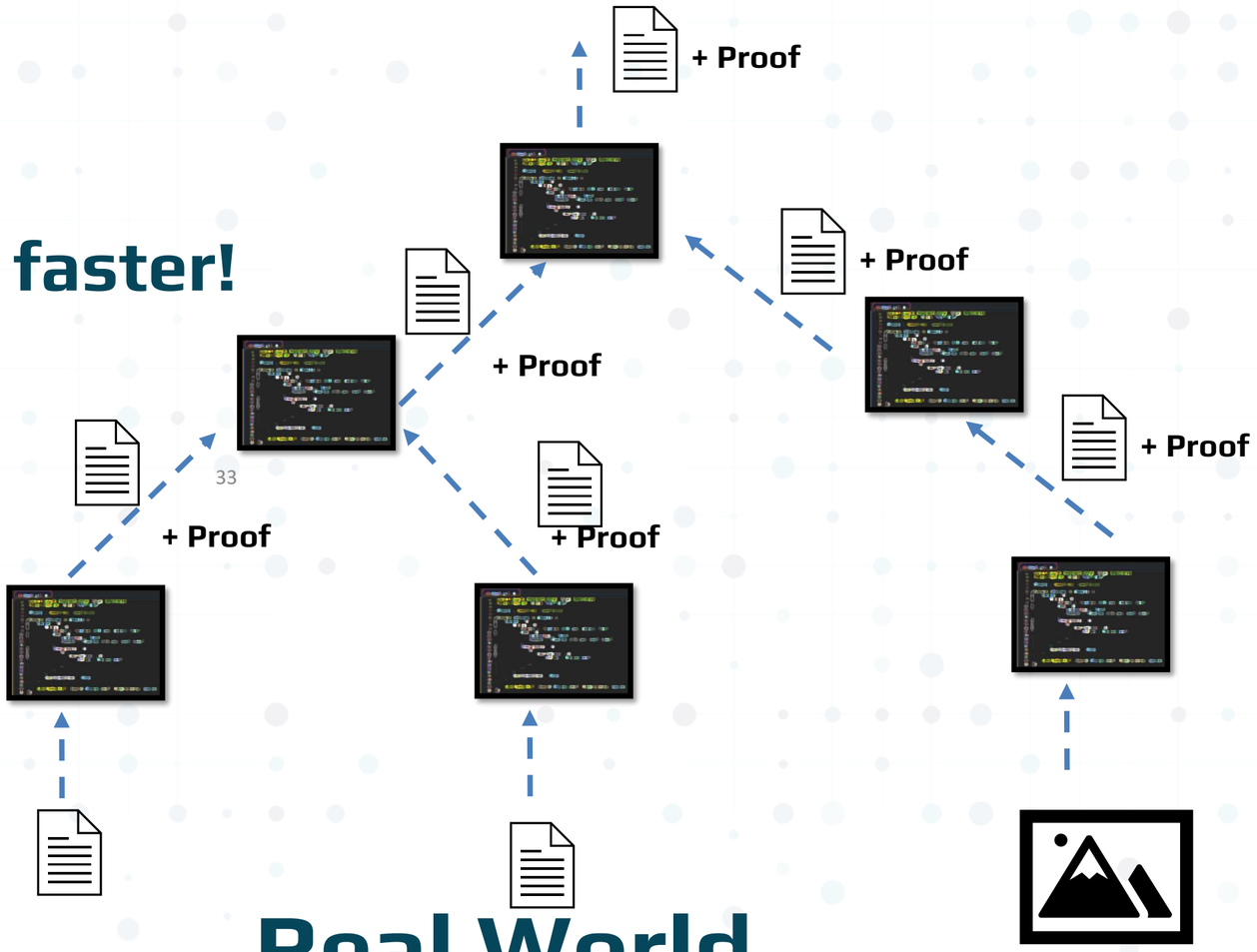
Vision of Future

- Proof carrying data



Vision of Future

- Proof carrying data
- Proving must become faster!



THANK YOU FOR LISTENING!

UNIVERSITY OF TARTU
1632
UNIVERSITAS TARTUENSIS