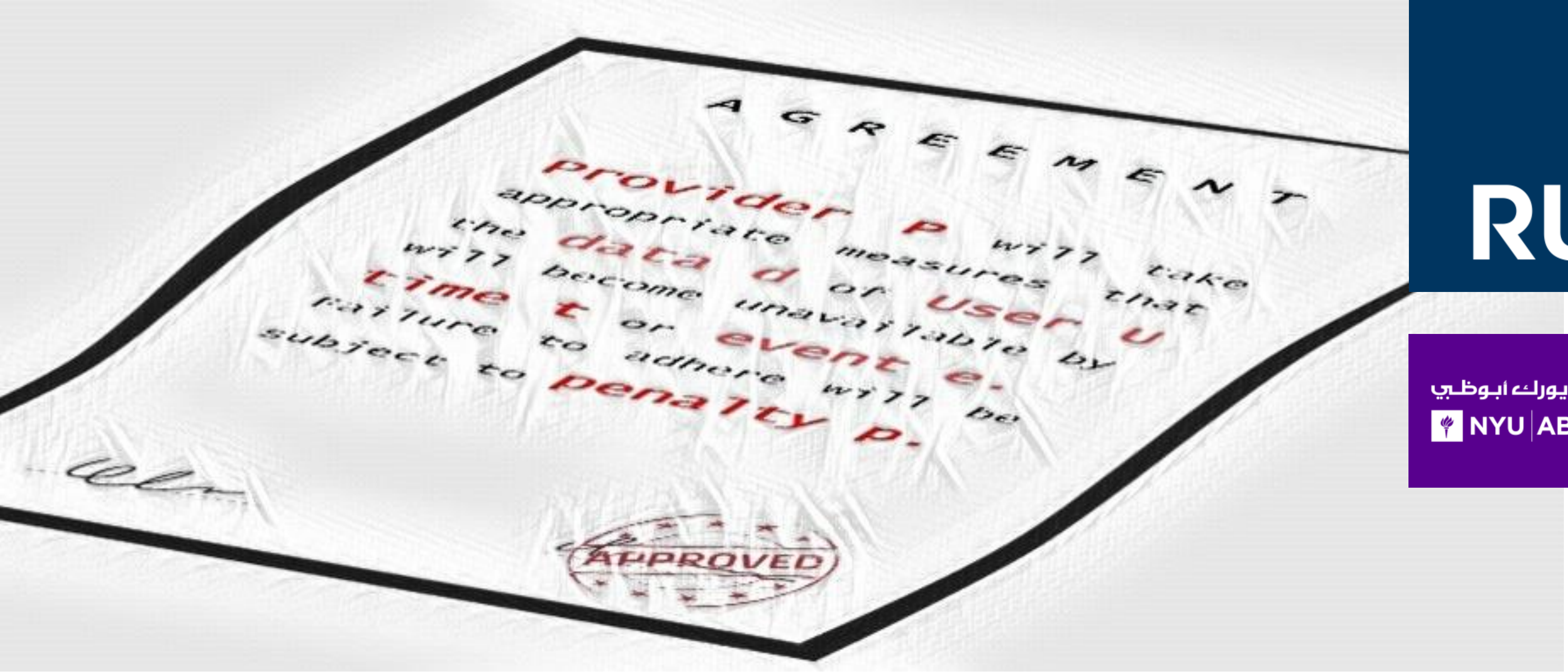


RUHR-UNIVERSITÄT BOCHUM

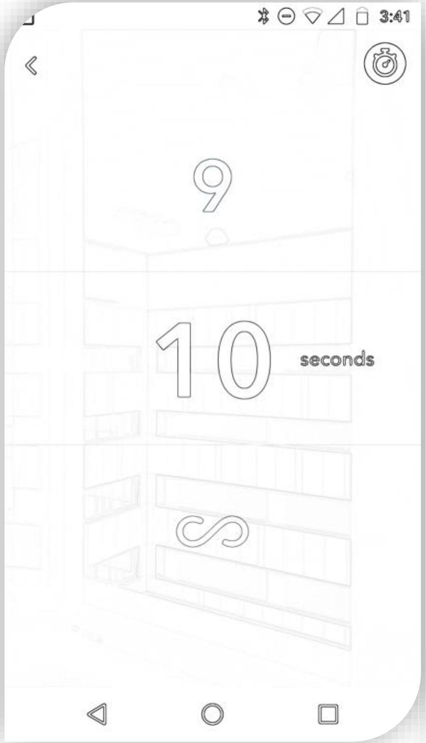
TOWARDS CONTRACTUAL AGREEMENTS FOR REVOCATION OF ONLINE DATA

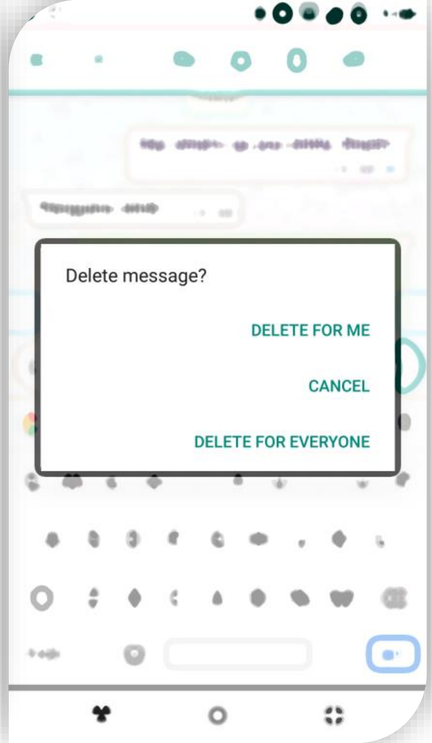
IFIP SEC 2019, Lisbon, Portugal, 25 June 2019

Theodor Schnitzler, Markus Dürmuth
Ruhr-Universität Bochum

Christina Pöpper
New York University Abu Dhabi

DATA REVOCATION APPLICATIONS

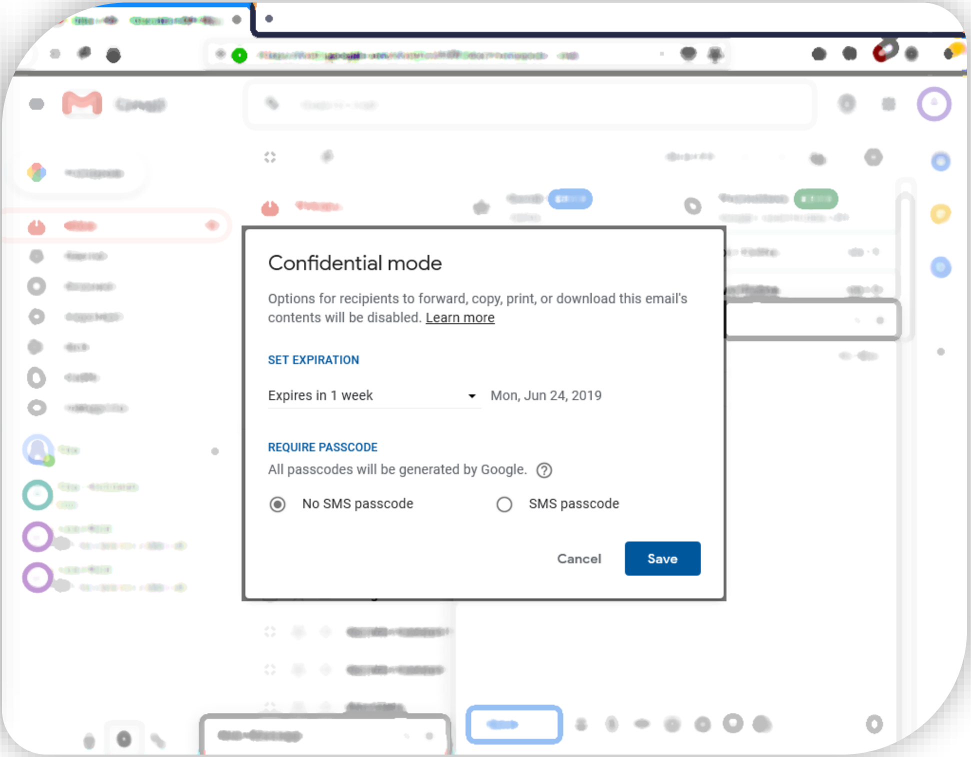



Delete message?

DELETE FOR ME

CANCEL

DELETE FOR EVERYONE


Confidential mode

Options for recipients to forward, copy, print, or download this email's contents will be disabled. Learn more

SET EXPIRATION

Expires in 1 week ▾ Mon, Jun 24, 2019

REQUIRE PASSCODE

All passcodes will be generated by Google. ?

● No SMS passcode ○ SMS passcode

Cancel Save

TOWARDS CONTRACTUAL AGREEENTS FOR REVOCATION OF ONLINE DATA

IFIP SEC 2019, Lisbon, Portugal, 25 June 2019

Theodor Schnitzler, Markus Dürmuth, Christina Pöpper

DATA REVOCATION RESEARCH

Encrypted Publishing

- Encrypt data symmetrically
- Publish ciphertext and key retrieval information

Cumbersome Data Access

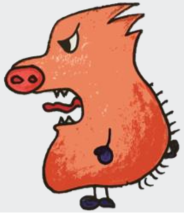
- Extract and retrieve key information
- Decrypt data

Key Storage Infrastructures

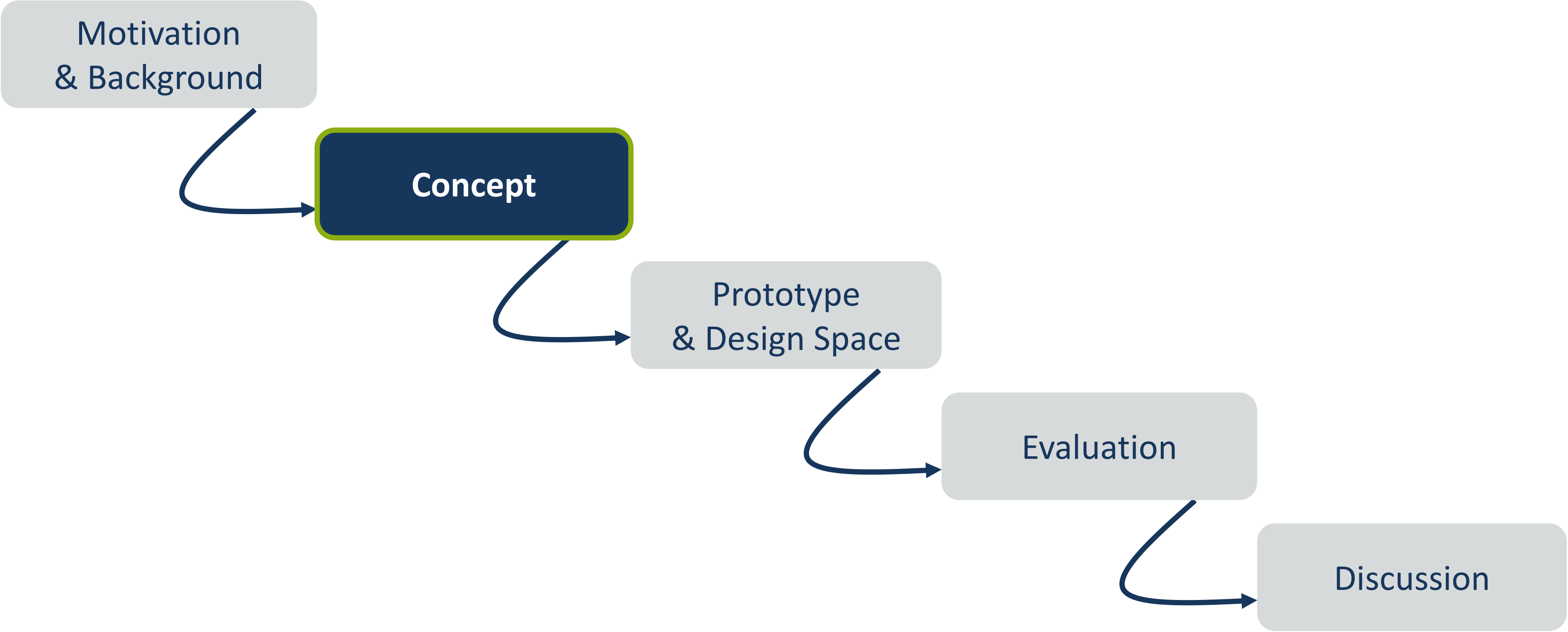
- Centralized servers that only return keys under specifc circumstances
- Distribute key in publicly accessible ever-changing infrastructure (e.g. DHT, DNS)

Possible Attacks

- Store / copy data when decrypted
- Proactively collect decryption keys



OUTLINE



Motivation & Background

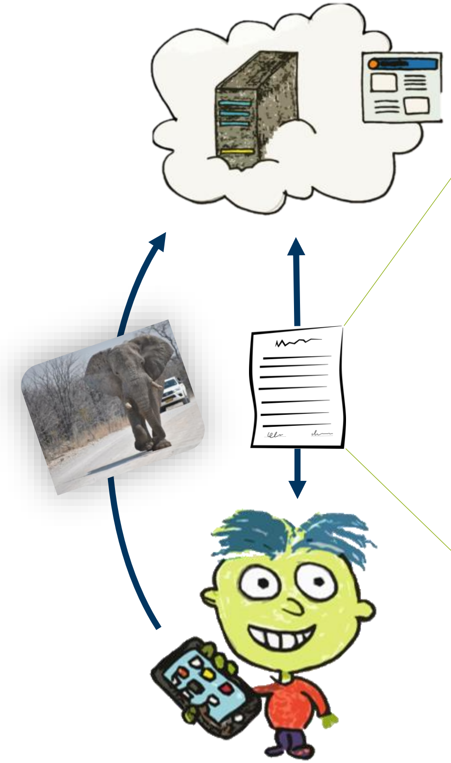
Concept

Prototype & Design Space

Evaluation

Discussion

OVERVIEW

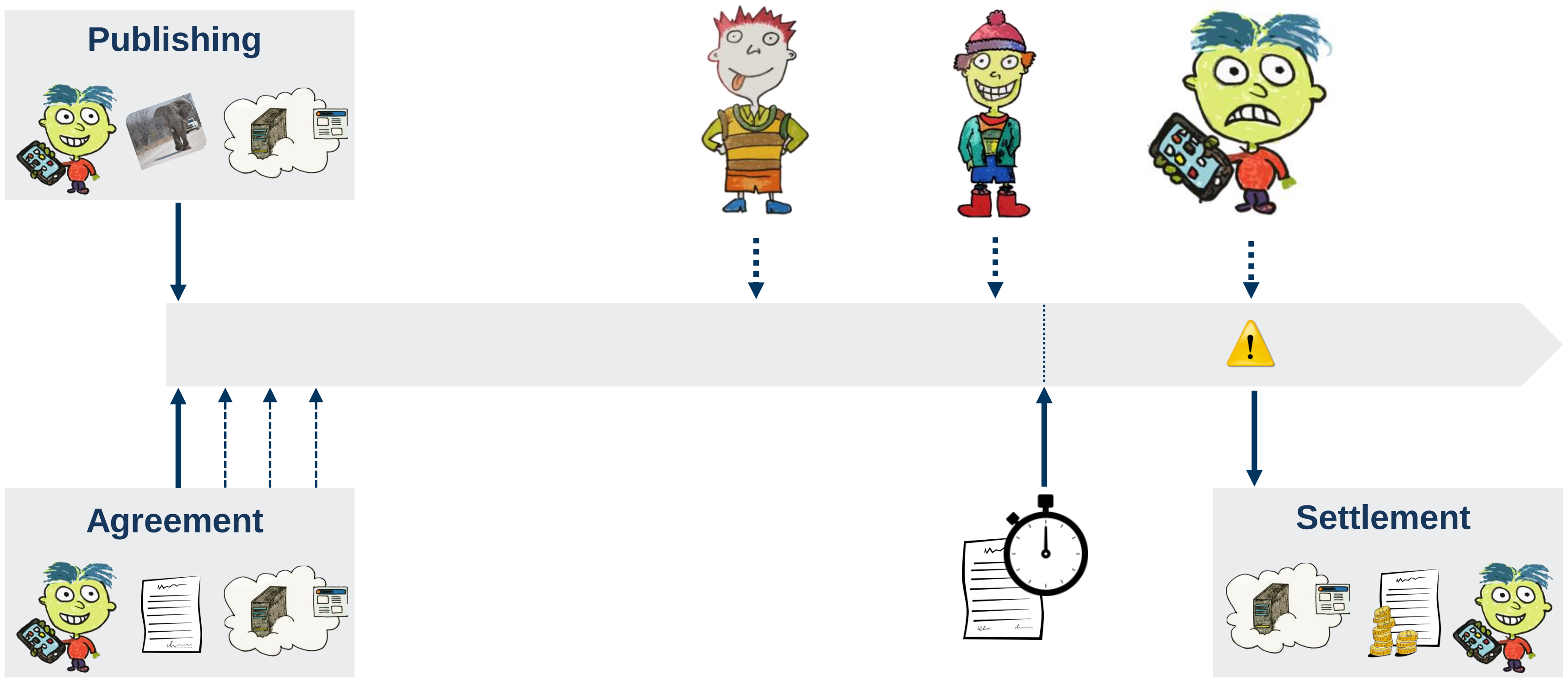


AGREEMENT

Provider P will take appropriate measures that the data d of User U will become unavailable by time t or event e. Failure to adhere will be subject to penalty p.

APPROVED

TIMELINE



Publishing

Agreement

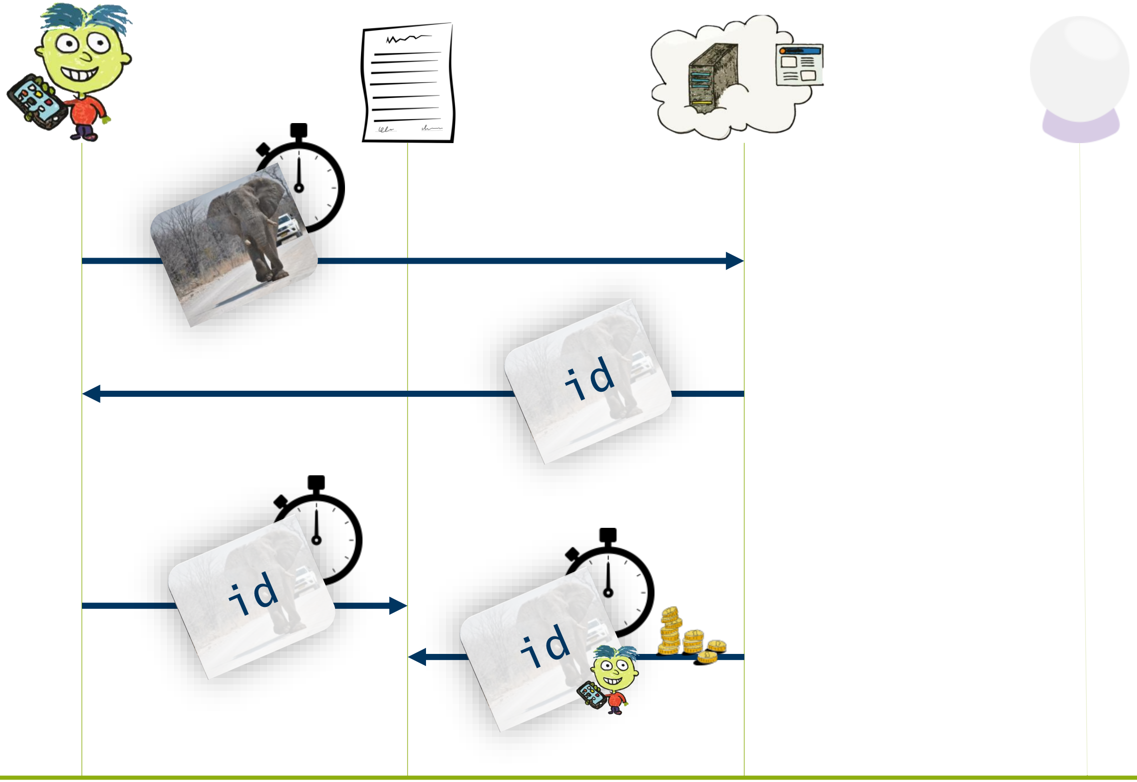
Settlement

SMART CONTRACTS

Registration

User uploads data

Both commit information to contract

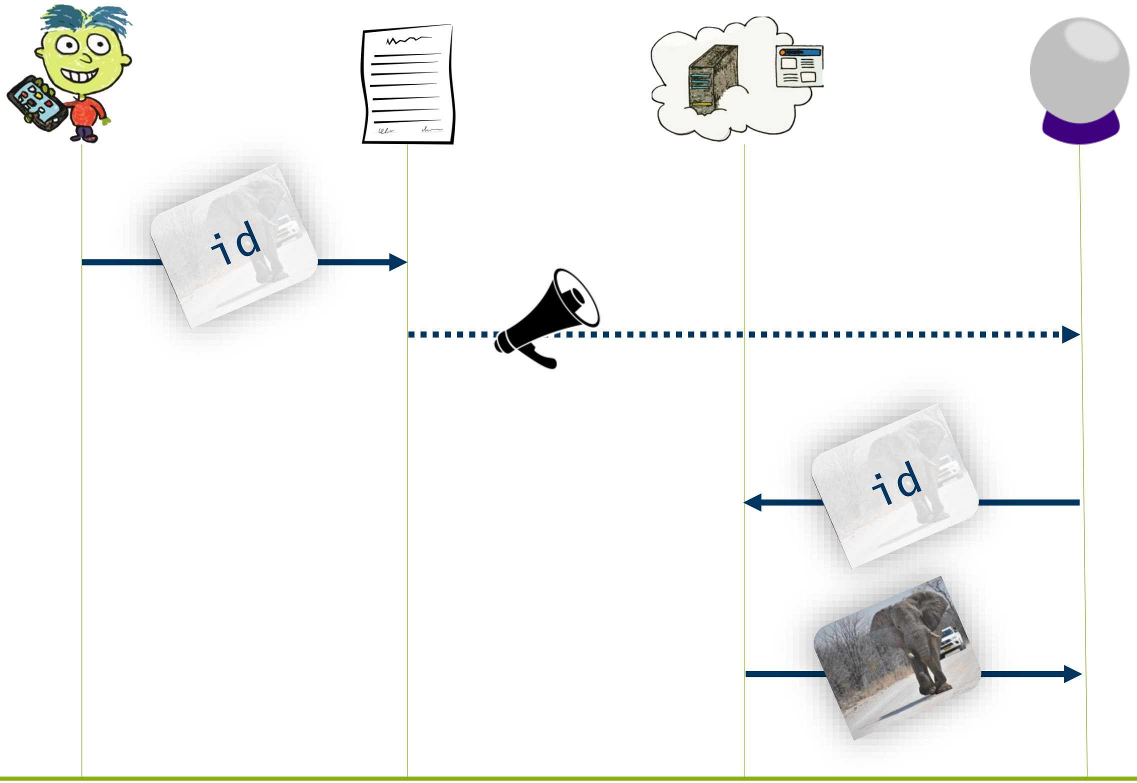


SMART CONTRACTS

Violation Claim

Notifying contract triggers alert

Verifier requests access to data

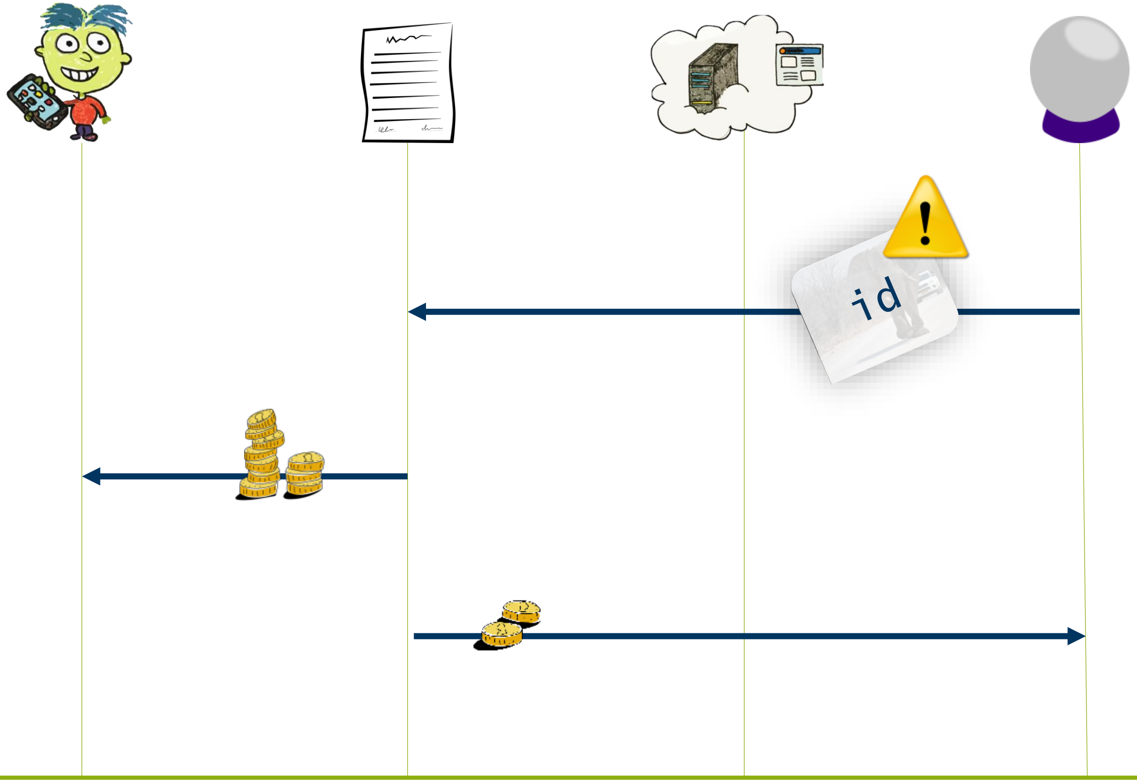


SMART CONTRACTS

Settlement

Verifier reports violation

Penalty payout



ADVANTAGES

Retroactive Application

- No need to determine conditions in advance
- Set-up agreement even after data publishing

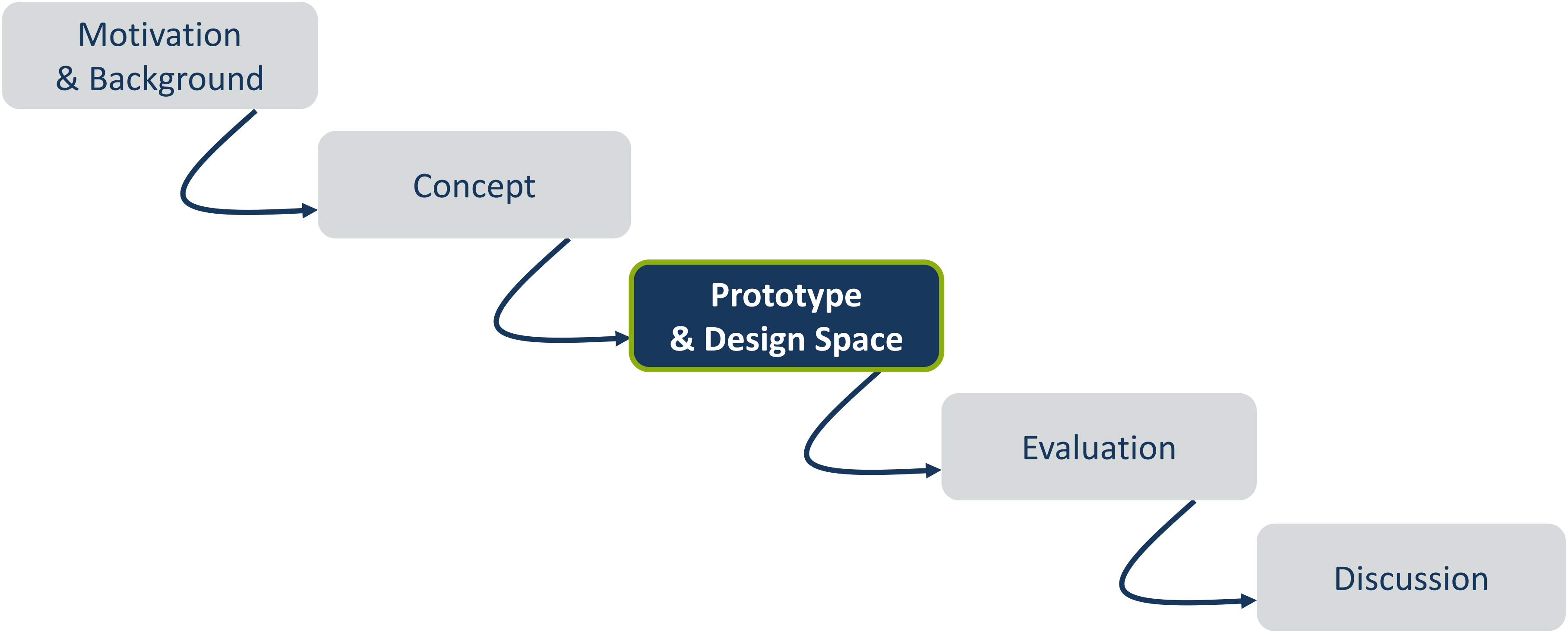
Flexible Expiration

- Extending lifetime could be easily achieved
- Reducing lifetime should take into account provider‘s needs

Convenient Data Access

- No additional tools or measures required
- Regular users are kept away from the process

OUTLINE



Motivation & Background

Concept

Prototype & Design Space

Evaluation

Discussion

PROTOTYPE

Overview

- Local Ethereum instance
- Accounts for participants
- Example Contract

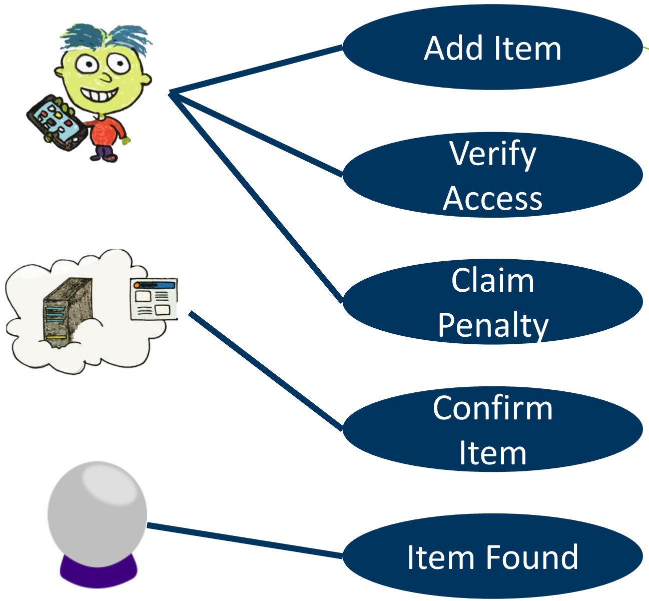
Contract Features

- Time-based expiration
- Provider-defined IDs

What we did NOT do

- Integrate real data feed

Participants **Interfaces**



```
function addItem(
  uint256 id,
  uint256 tLeft) public{
  ...
}
```

PROTOTYPE

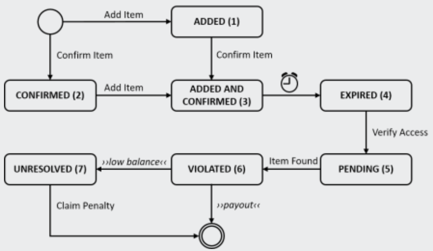
Contract Properties

- Provider Address
- Data Feed Address
- Data Item Set
- Compensation Amount
- Financial Threshold

Data Item Properties

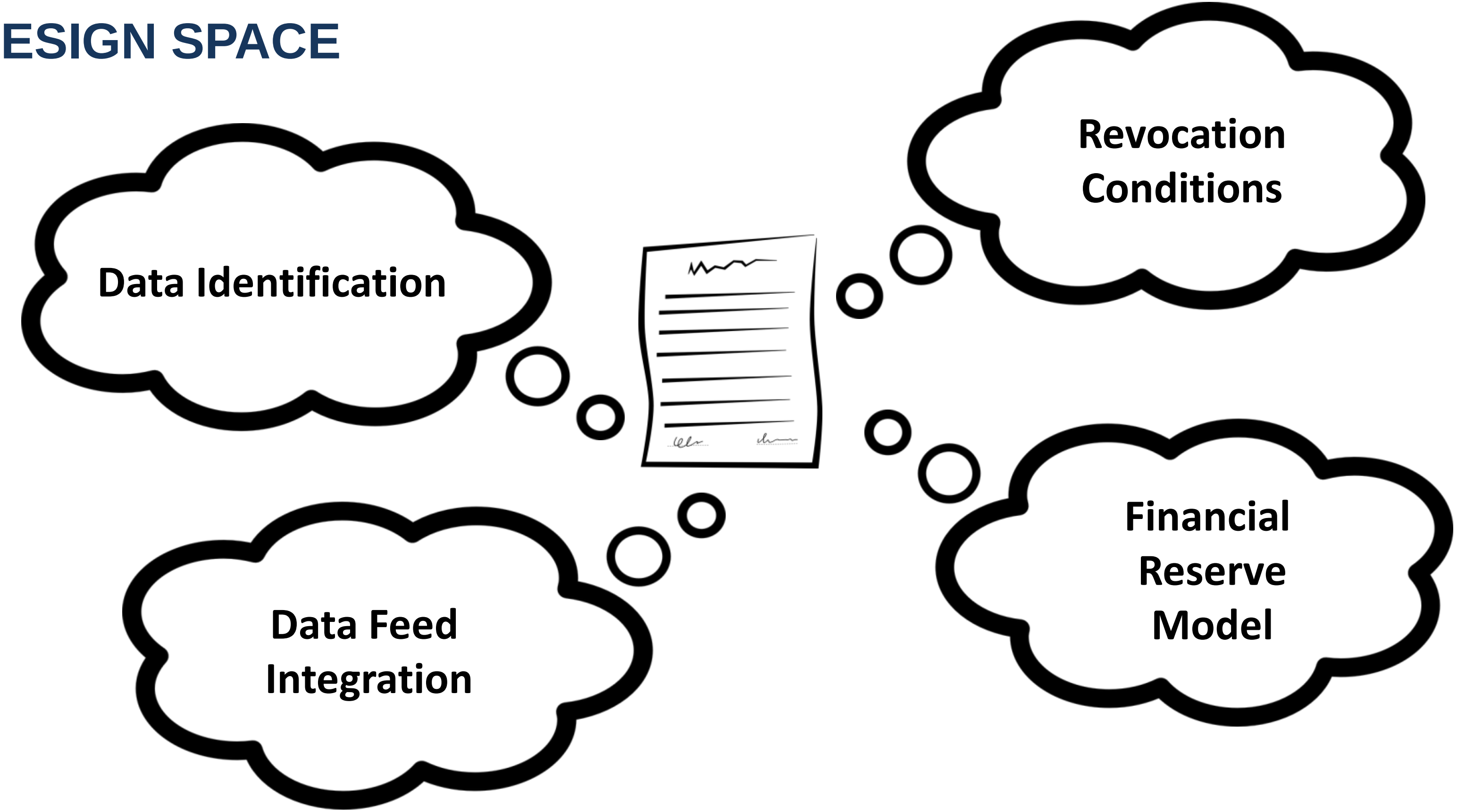
- Owner Address
- Expiration Time
- **Item State**

Data Item States



- Created
- Expired
- Violated
- ...

DESIGN SPACE



Data Identification

Revocation Conditions

Data Feed Integration

Financial Reserve Model

DESIGN SPACE: DATA IDENTIFICATION

Provider-defined identifiers

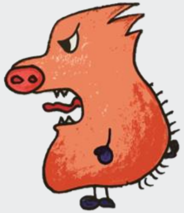
- `network.io/my-content-id`
- Contract bound to one specific location

Robust hashes

- Use data to generate identifiers
- Tolerate minor data modifications
- Different data result in the same hash

Provider Accountability

- Unclear, to what extent a provider can be held accountable for
- Malicious users re-upload data
- Multiple copies of the data on the same platform
- Data copied to different platform



DESIGN SPACE: DATA FEEDS

Challenges

- Incorporating real-world into cryptocurrency
- Miners do not access external resources
- Additional Third Contract Party

Requirements

- Correctness
- Time-boundness

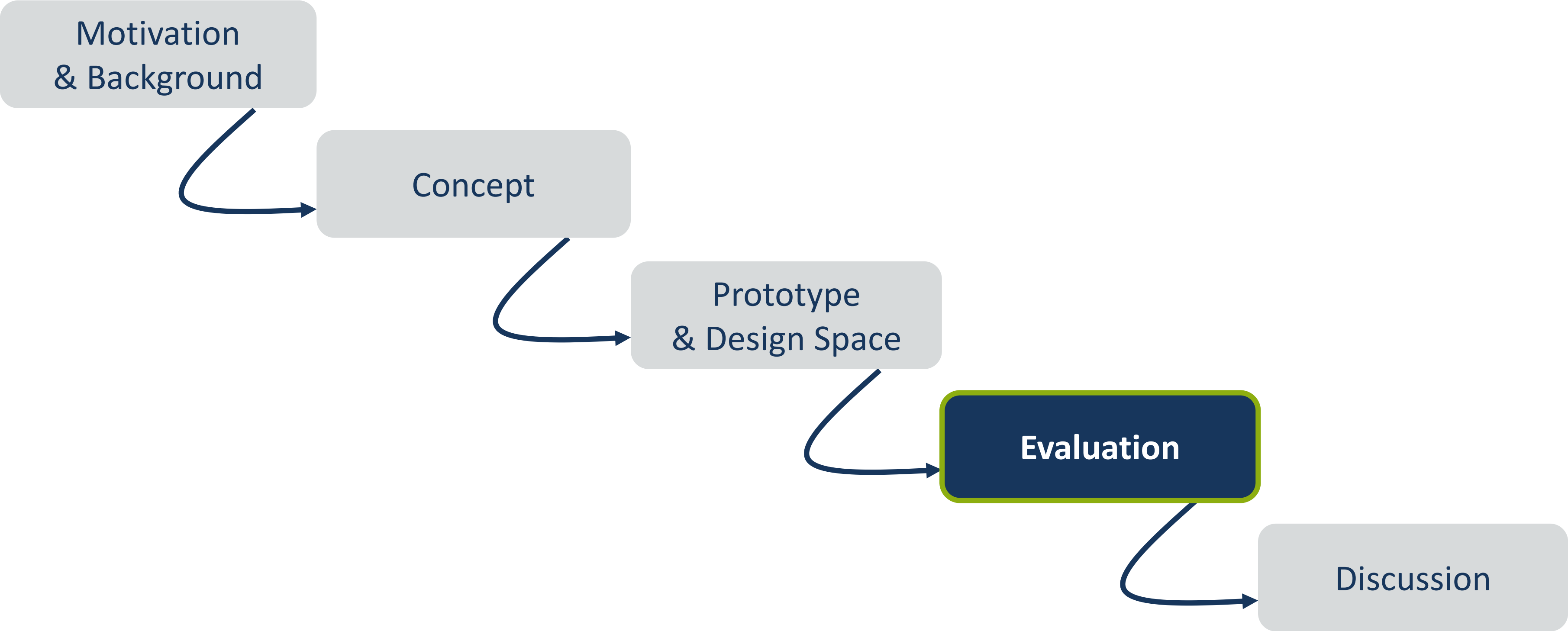
Trusted Execution Environments

- Cryptographic attestations
- Retrieve and process data in secure enclave

Crowd-sourcing

- Multiple individual data feeds
- Aggregate results from distributed responses
- Majority Voting

OUTLINE



Motivation & Background

Concept

Prototype & Design Space

Evaluation

Discussion

EVALUATION: 101

Transaction processing consumes gas

- Depends on computational complexity
- Well-defined for each EVM instruction
- Reward for miners

Opcode	Name	Gas
0x00	STOP	0
0x01	ADD	3
0x02	MUL	5
0x03	SUB	3
0x04	DIV	5

Gas price

- Paid in ETH by transaction sender
- Subject to „negotiations“ between sender and miner
- Miners declare their lower bound
- Minimum: **1.0 x 10^{-9}** ETH (= 1 GWei)

Higher Provision
=
Faster Processing

EVALUATION: EXECUTION COST

Service	Gas	USD	Actor
Add Item	82.4k	$0.0205	User
Confirm Item	35.1k	$0.0087	Provider
Verify Access	28.6k	$0.0073	User
Item Found	22.1k	$0.0055	Data Feed
Claim Penalty	21.9k	$0.0055	User

Publishing one data item costs ~ 3 cents

- (if everyone complies with the contract)
- ~ 2 cents for users
- other cost only incur in case of violation
- negligible compared to compensation

Exchange Rates (June 2019)

- 10^{-9} ETH per Gas Unit
- $250.00 per ETH

EVALUATION: EXECUTION COST

Service	Gas	USD	Actor
Add Item	82.4k	$0.0205	User
Confirm Item	35.1k	$0.0087	Provider
Verify Access	28.6k	$0.0073	User
Item Found	22.1k	$0.0055	Data Feed
Claim Penalty	21.9k	$0.0055	User

Publishing one data item costs ~ 3 cents

- (if everyone complies with the contract)
- ~ 2 cents for users
- other cost only incur in case of violation
- negligible compared to compensation

Exchange Rates (June 2019)

- 10^{-9} ETH per Gas Unit
- $250.00 per ETH

Settlement costs another ~ 1.8 cents

- only in exceptional cases

EVALUATION: SCALABILITY

Publishing consumes **117.5k gas**

8M gas can be included in each block

New block created every **15 seconds**

68 items per **block**

272 items per **minute**

16,320 items per **hour**

391,620 items per **day**

[0.7% of 55M status updates every day]

[If Ethereum was only used for Data Revocation]

Google received **530k requests** to un-list URLs

0.37% of Ethereum limit

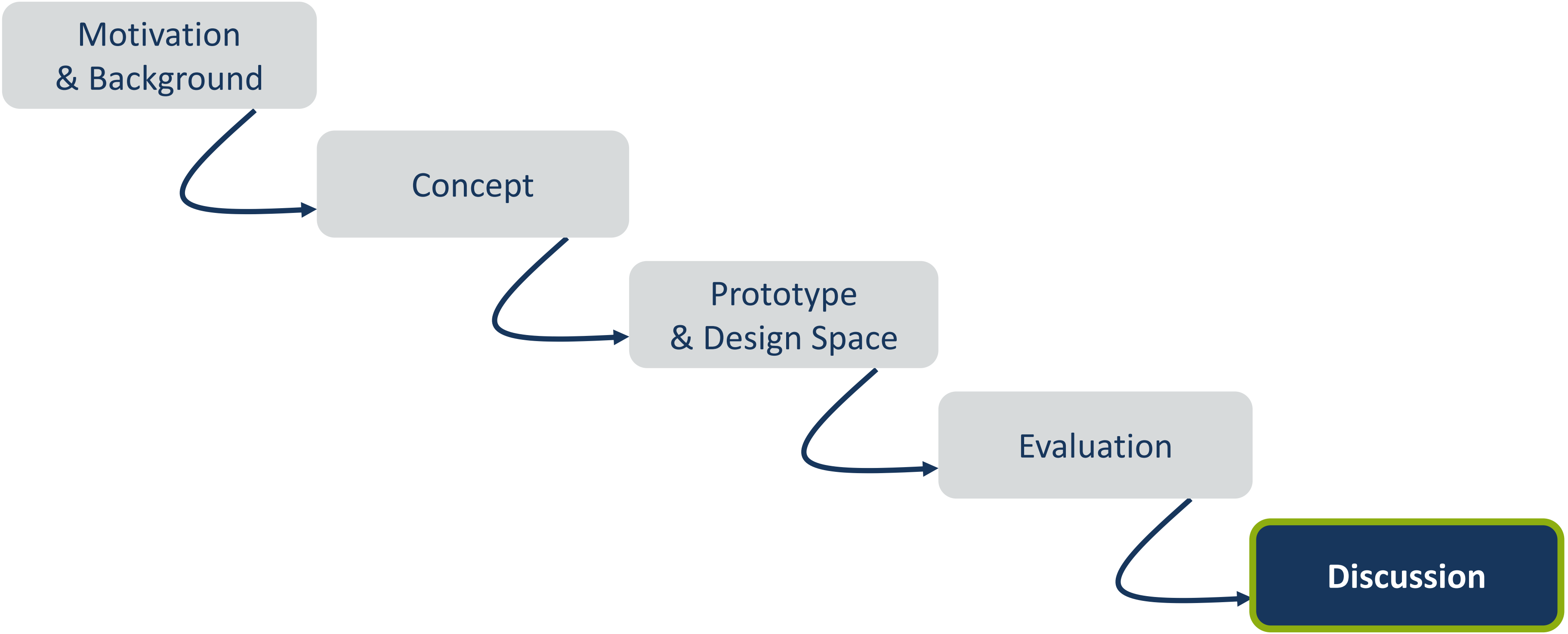
240k URLs have been removed from search results

What data should our mechanism be used for?

?

BROAD ADOPTION REMAINS A DEPLOYMENT CHALLENGE

OUTLINE



Motivation & Background

Concept

Prototype & Design Space

Evaluation

Discussion

DISCUSSION

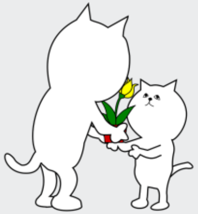
Metadata Privacy

- Public database of privacy-sensitive data?
- Privacy preferences of individual users?

Provider Participation

- Willingness to participate required
- Privacy transparency as a selling point

Trust Requirements



- Reduce trust in provider by applying penalties
- Data feeds may still require some trust

TAKEAWAY

Revocation Contract

- Extend/Shift Responsibility
- Account Providers
- Concept inspired from Right to be Forgotten

Advantages

- Retroactive Application
- Flexible Expiration
- Convenient Data Access

From Theory to Practice

- Adoption Barriers
- Deployment Issues
- User Acceptance?

TOWARDS CONTRACTUAL AGREEMENTS FOR REVOCATION OF ONLINE DATA

IFIP SEC 2019, Lisbon, Portugal, 25 June 2019

Theodor Schnitzler, Markus Dürmuth
Ruhr-Universität Bochum

Christina Pöpper
New York University Abu Dhabi

Illustrations: Katharina Kohls