Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

## 4TH INTERNATIONAL CONFERENCE ON

# PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2023)

SEPTEMBER 8-9TH, 2023

## Scalable Model-Based Decentralized Applications in the Cloud Using Certificates and Blockchains

Felix Härer, University of Fribourg, Switzerland

# Scalable Cloud Applications

- ***State-of-the-art***
  - *Auto scaling of virtual machines (e.g. EC2 Autoscaling, Azure Scale Sets etc.)*
  - *Lambda functions (e.g. AWS Lambda)*
  - *Serverless computing independent of virtual machines (e.g. AWS Step Functions)*
- ***Result***
  - *Vertical and horizontal scaling*
  - *Distribution across servers and data center regions*
  - *Ideally: distribution, high performance, scalability, availability*

# Decentralization

***Challenges***

- *Partially conflicting goals (CAP theorem)*
- *Centralized architectures of cloud providers*
  - *Dependency on individual providers*
  - *Dependency on centralized technical infrastructures*
- *Centralized coordination of application executions*
  - *Limitations when executing applications in distributed or federated scenarios*
  - *Distributed parties cannot observe and verify application executions*

→ ***Distribution does not imply decentralization***

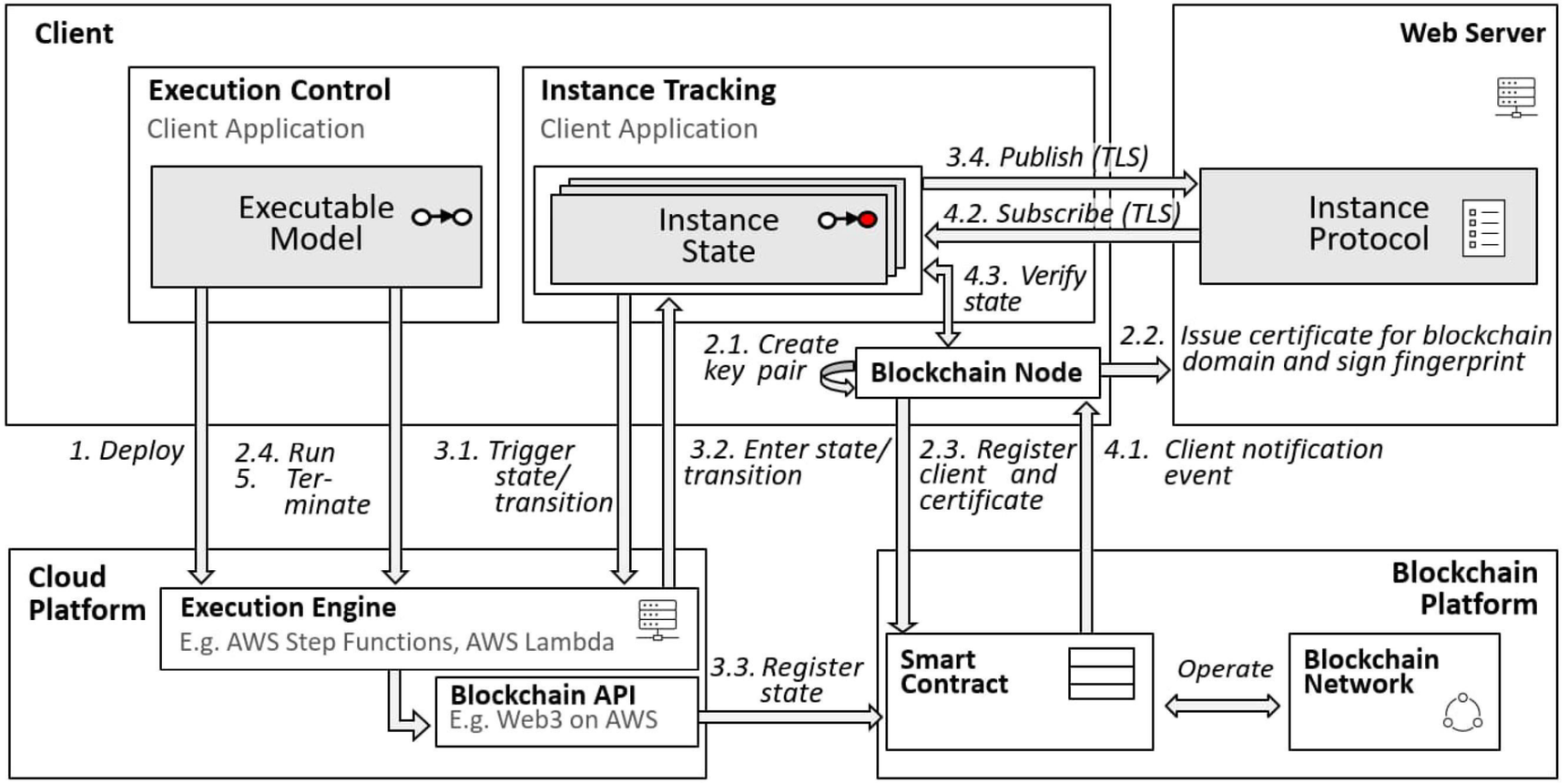
→ ***Decentralization: distribution and non-centralized coordination***

# Architectures for Decentralized Applications

- *Blockchain*
  - *Execution of application logic in smart contracts, verifiable execution*
  - *Problems: insufficient scalability, websites and applications outside the blockchain out of scope*
- *Combination of cloud platforms and blockchains*
  - *Execution of applications on cloud platforms with instance tracking on a blockchain*
  - *Prior Work:* Härer(2022): Executable Models and Instance Tracking for Decentralized Applications - Towards an Architecture Based on Blockchains and Cloud Platforms

***Research Objective: Extension of a decentralized application architecture for authenticated and scalable distribution, execution, and tracking.***

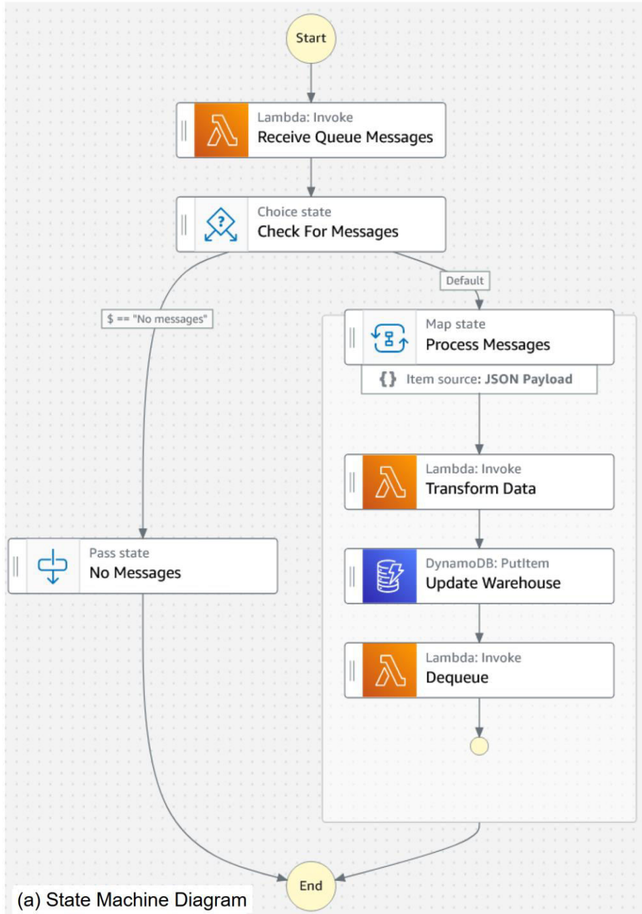
# System Architecture



# Model-based Specification

*1. Deploy*

- *Deployment of executable model with content-based identifier*
  *m = (model_id, model_data)*
  *model_id = H(model_data)*
- *Platform-specific model data*
- *Example: State machine representation for AWS Step Functions using JSON data*




```
{
  "StartAt": "Receive Queue Messages",
  "States": {
    "Receive Queue Messages": {
      "Type": "Task",
      "Resource": "arn:aws:states:::lambda:invoke",
      "OutputPath": "$.Payload",
      "Parameters": {
        "FunctionName": "arn:aws:lambda:us-east-1:72621(
      },
      "Next": "Check For Messages"
    },
    "Check For Messages": {
      "Type": "choice",
      "Choices": [
        {
          "Variable": "$",
          "StringEquals": "No messages",
          "Next": "No Messages"
        }
      ],
      "Default": "Process Messages"
    },
    "No Messages": {
      "Type": "Pass",
      "End": true
    },
    "Process Messages": {
      "Type": "Map",
      "ItemsPath": "$",
      "Parameters": {
        "MessageNumber.$": "$$.Map.Item.Index",
        "MessageDetails.$": "$$.Map.Item.Value"
      },
      "Iterator": {
        "StartAt": "Transform Data",
        "States": {
          "Transform Data": {
            "Type": "Task",
            "Resource": "arn:aws:states:::lambda:invoke",
            "OutputPath": "$.Payload",
            "Parameters": {
              "Payload.$": "$",
```

(b) JSON

h = c632cb64251cfdb18cb6dcab680b9fc82952aea783538ed246a4cb84f65b81e1

# Setup: Keys, Certificate and Blockchain Domain

*2.1 Key Pair*

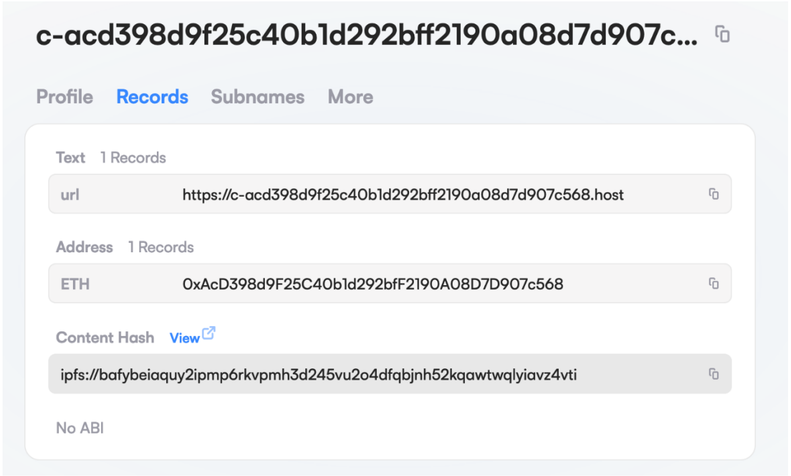
- *Local generation of (k_pub, k_prv) and blockchain address, here: Ethereum w/ ECDSA, scp256k1*

*2.2 Certificate and Blockchain Domain*

- *Web server for distribution of model, instance protocol with X.509 certificate*
- *Blockchain domain records linking address, domain, uri*
  - *Here: Ethereum Name Service (ENS)*
  - *Resolves: bc.-address → uri and uri →* bc.-address

*2.3 Register client certificate*

- *Smart contract for registering addresses with certificates*
- *Certificate is signed with k_prv and stored by fingerprint in the contract*



# Instance States

*3.1 Trigger state / transition*

- *Cloud platform or client triggers state change*

*3.2 Enter state / transition*

- *Execution engine changes state*
- *Captures state with content-based identifier and triggers event*

*3.3 Register state*

- *Records in smart contract*

*3.4 Publish*

- *Updates instance protocol via TLS*

| | event_ | state_hash | time | block_ | client_address | transaction_hash |
|---|---|---|---|---|---|---|
| 1 | Register State | 2f5017eb565ae673b27f22e43ecd4fe8e71dce1b18f887fac725403205bc0e25 | 1678443257 | 3,060,324 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | e21489fa54c832f95275e |
| 2 | Register State | 54dc36f33bbedce87d29a2862436de6084e9fccc6354645949818f94ec48d6d6 | 1678443268 | 3,060,325 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 1c2bc34e9ee4d0724130 |
| 3 | Register State | d4630c072363adfcc080209eb21b4f53eed94bb136a14598b9e8fd6c62a488ff | 1678443278 | 3,060,326 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 65a131ec6e0292147c55 |
| 4 | Register State | cdec2cb2a3ab16c8802e27d9eb03d9176945b56758e7dea1a14fa3c6024906f3 | 1678443299 | 3,060,327 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 5b89790aa2be2d226a3d |
| 5 | Register State | d2baee1c5d7454af61c8511ae1ed2ec5c3a1c3d6e013c14a2be97cf758621cb8 | 1678443310 | 3,060,328 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 1d89e0c91b8c4a634659 |
| 6 | Register State | 084350dbf128e5477cddfe2c2b08f8b1475542b8f24f2b0a743222c6018a2826 | 1678443320 | 3,060,329 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | e50f93ef2250912d77445 |
| 7 | Register State | c959ce88840609f42a6b47512e8c34899bab7947fc9e15b8482d5529aa318e97 | 1678443331 | 3,060,330 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | a78eb682b6c8d4985e2d |
| 8 | Register State | 192f9904ea2a961f9cb88784a27390aa1fdea5c0b12e89d17bbffd26c06c6d5e | 1678443342 | 3,060,331 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | ee4fe65d48c1cefc6853c |
| 9 | Register State | 6aeafcd9da42a3de40a2ebc46987b1c4890a0843694396704fb56a33c68e354d | 1678443352 | 3,060,332 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 90878ede0db98441e106 |
| 10 | Register State | 21b22a3ba31b4edbf26fdda49c7494659a37a8052a5798f673537f1e540b784c | 1678443363 | 3,060,333 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 51049b42463182f012ace |
| 11 | Register State | f09abbd8dedd90de383417cb0edb1c658dea96bd20750e724faa4499f418841f | 1678443373 | 3,060,334 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 1b488e7fd311c946468d |
| 12 | Register State | 45ee5c0ce528c078ee18e0697df410758197594771b3eb993e0f76c77b96e9ae | 1678443394 | 3,060,335 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | e910d4193094c134348c |
| 13 | Register State | 3407328ab665e45f3640965bfd894bf47433d8e7f70ede1e7730edb99279c460 | 1678443405 | 3,060,336 | AcD398d9F25C40b1d292bfF2190A08D7D907c568 | 2c66b9903828a84b8b4ff |

https://c-acd398d9f25c40b1d292bff2190a08d7d907c568.host/a681a01f3b9d2673b7fcf7f622274d55b4634ea313330c3705f631bee2ae779d.json 130%

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON


```
model_hash: "c632cb64251cfdb18cb6dcab680b9fc82952aea783538ed246a4cb84f65b81e1"
instance_hash: "a681a01f3b9d2673b7fcf7f6…3330c3705f631bee2ae779d"
instance_data: "https://c-acd398d9f25c40b1d292bff2190a08d7d907c568.host/data-queue-warehouse-etl-d02ebfb0-4074-436c-9d3f-f9e4e48223fc.json"
model_data: "https://c-acd398d9f25c40b1d292bff2190a08d7d907c568.host/data-queue-warehouse-etl.json"
instance_protocol:
  0:
    event_type: "Register State"
    state_hash: "2f5017eb565ae673b27f22e43ecd4fe8e71dce1b18f887fac725403205bc0e25"
    timestamp: 1678443257
    block_nr: 3060324
    client_address: "acd398d9f25c40b1d292bff2190a08d7d907c568"
    transaction_hash: "e21489fa54c832f95275ef6800be0df71fa43dd2417cf190d3f9a1897428c6df"
    state_data: "https://c-acd398d9f25c40b1d292bff2190a08d7d907c568.host/data-queue-warehouse-etl-d02ebfb0-4074-436c-9d3f-f9e4e48223fc-2.json"
  1:
    event_type: "Register State"
    state_hash: "54dc36f33bbedce87d29a2862436de6084e9fccc6354645949818f94ec48d6d6"
```

# Instance Tracking

*4. Tracking and verifying states*

- *Subscription to state change events and instance protocol over HTTPS/TLS*
- *Validation of states using the smart contract:*
  - *State exists: retrieval and validation of instance state ID / hash value*
  - *Model and instance exist: retrieval and validation of instance and model IDs / hash values*
  - *Blockchain address created model or state: address resolves to known web server uri using ENS*
  - *Instance protocol server certificate known: retrieval of signature from contract*
  - *Instance protocol linked to address: signature check correct for key of blockchain address*

→ *Verifies: each instance state, instance protocol and model with issuer and timestamps*

# Conclusion

***Extended Decentralized Application Architecture***

- *Executable Models on cloud platforms with instance tracking on a blockchain (Härer 2022)*
- *Web- and blockchain authentication*
  - → *Web servers distribute executable models and instances*
  - → *Binding between web resources, certificates and blockchain identities possible*
- *Scalable execution on cloud platforms by an executable model for serverless computing*
  - → *Enhanced scalability for data- and compute intensive applications*
- *Distributed instance tracking on a blockchain*
  - → *Distributed observation and validation of application executions*

→ ***Scalable Model-Based Decentralized Applications***

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

G20 भारत 2023 INDIA

# THANK YOU

भगत संगणन विकास केंद्र
सीडैक CDAC
॥ज्ञानादेव तु कैवल्यम्॥
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING

IEEE COMPUTER SOCIETY
Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY
Linking Research to Practice
Bangalore Chapter