black hat
ASIA 2022

MAY 12-13

BRIEFINGS

#BHASIA @BlackHatEvents

black hat ASIA 2022

TMoC : Threat Modelers on Chain

School of Cybersecurity, Korea University

Yejun Kim (v3locy@korea.ac.kr)
Kwangsoo Cho (cks4386@korea.ac.kr)
Paul Hong (visitator00@korea.ac.kr)
Seungjoo Kim (skim71@korea.ac.kr) *

✓ This work is supported by the Korea Agency for Infrastructure Technology Advancement (KAIA) grant funded by the Ministry of Land, Infrastructure and Transport (Grant 21AMDP-C162334-01).

* Corresponding Author

Who are we?

- Yejun Kim (v3locy at korea.ac.kr)
  - A graduate student(Ph.D. course) at SANE Lab., School of Cybersecurity, Korea University
  - Research Interests: Threat Modeling, Threat Intelligence, Malware Analysis, Incident Response, Pentesting

- Paul Hong (visitator00 at korea.ac.kr)
  - A graduate student(Ph.D. course) at SANE Lab., School of Cybersecurity, Korea University
  - Research Interests: Threat Modeling, Security Assessment & Authorization(such as Common Criteria, CMVP, and SSE-CMM), Software Development

- Kwangsoo Cho (cks4386 at korea.ac.kr)
  - A graduate student(Ph.D. course) at SANE Lab., School of Cybersecurity, Korea University
  - Research Interests: Threat Modeling, Risk Management Framework Assessment & Authorization, Software Development

Who are we?

Seungjoo Kim
Professor at Korea University

skim71 at korea.ac.kr
(Corresponding Author)

Seungjoo (Gabriel) Kim has been a professor at the School of Cybersecurity in Korea University from 2011. For the past 7 years he was an associate professor in Sungkyunkwan University and had 5 years of background as a team leader of KISA(Korea Internet & Security Agency).

In addition to being a professor, he is a director of AR2C(Army RMF Research Center), a director of CHAOS(Center for High-Assurance Operating Systems), a head of SANE(Security Assessment aNd Engineering) Lab, an adviser of undergraduate hacking club CyKor(DEFCON CTF 2015 & 2018 winner) at Korea University, and a founder/advisory director of an international security & hacking conference SECUINSIDE. Since 2018, he has been a review board member of Black Hat Asia.

His research interests lie primarily in building "inherently secure, high-assurance, and provably secure systems and architectures" & "composable and scalable secure systems".

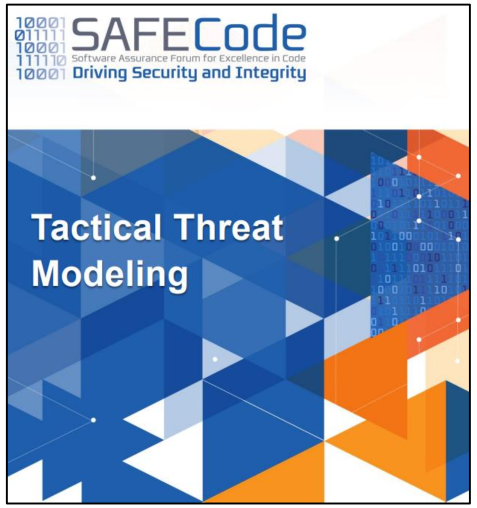
Threat Modeling is a Team Sport Method

[Adam Shostack, Threat Modeling (Elevation of Privilege: the Threat Modeling Game)]

- To motivate “The Crowd” to participate in Threat Modeling, collective intelligence is required, we propose threat modeling in the form of a game

[SAFECode, Tactical Threat Modeling]

- Threat modeling is like a “team sport” where that helps different participants to derive threats from analysis target



SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

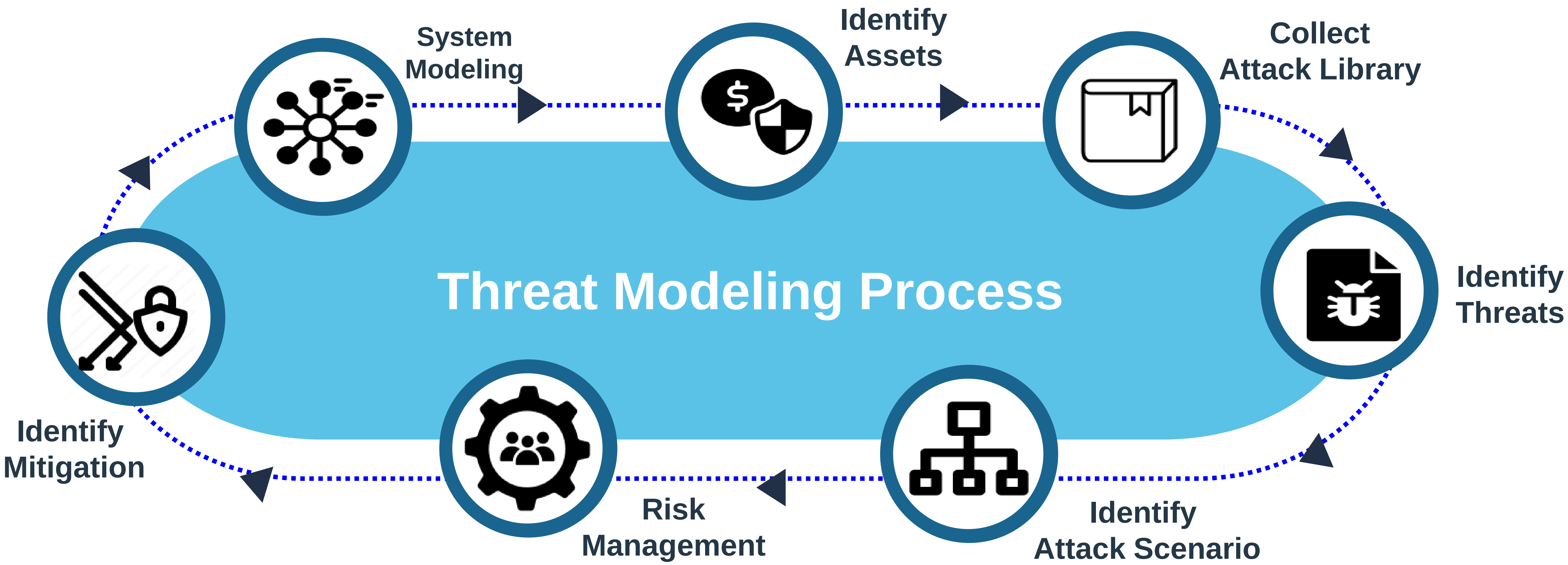
Tactical Threat Modeling

How to approach
Threat Modeling
AWS Well-Architected

[Amazon AWS(Darran Boyd), How to approach threat modeling]

- Threat modeling is a “team sport” that requires the knowledge and skills of various teams.
- All inputs have equal value

Threat Modeling Process



Threat Modeling Process

System Modeling

Identify Assets

Collect Attack Library

Identify Threats

Identify Attack Scenario

Risk Management

Identify Mitigation

Existing Threat Modeling Tools

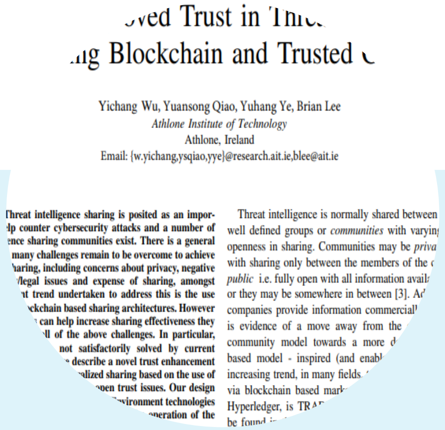
Year	Tool Name	Model Form	Threat Library Source	Open Source	Interface		Automation Scope				
					App	Web	System Model	Threat	Attack Scenario	Mitigation	Reporting
2013	ThreatModeler	Diagram	Self-defined, CAPEC, OWASP, WASC, …	X	O	X	O	O	O	O	O
2014	Microsoft Threat Modeling Tool (TMT)	Diagram	Self-defined, STRIDE	X	O	X	X	O	X	O	O
2015	IriusRisk	Diagram	Self-defined, CAPEC, CVE, CWE	X	X	O	X	O	X	O	O
2019	Open Weakness and Vulnerability Modeler (OVVL)	Diagram	Self-defined, STRIDE, CVE	O	X	O	X	O	O	X	O
2020	OWASP Threat Dragon	Diagram	Self-defined, STRIDE, LINDDUN, CIA	O	O	O	X	O	X	X	O
2019	OWASP pytm	Text (Python)	Self-defined, CAPEC, CVE, CWE	O	O	X	O	O	X	O	O
2020	Threagile	Text (YAML)	Self-defined, CWE	O	O	O	O	O	X	O	O

* Zhenpeng Shi, Kalman Graffi, David Starobinski, Nikolay Matyunin, “Threat Modeling Tools: A Taxonomy”, 2021

Existing Blockchain-based Tools

PolySwarm

PolySwarm is a threat intelligence platform used by security experts to analyze, detect & get intel on malicious files & digital artifacts



ɔved Trust in Threa
ɪng Blockchain and Trusted C

Yichang Wu, Yuansong Qiao, Yuhang Ye, Brian Lee
Athlone Institute of Technology
Athlone, Ireland
Email: {w.yichang,ysqiao,yye}@research.ait.ie,blee@ait.ie

Threat intelligence sharing is posited as an impor-
lp counter cybersecurity attacks and a number of
ence sharing communities exist. There is a general
many challenges remain to be overcome to achieve
haring, including concerns about privacy, negative
/legal issues and expense of sharing, amongst
nt trend undertaken to address this is the use
ckchain based sharing architectures. However
can help increase sharing effectiveness they
ll of the above challenges. In particular,
not satisfactorily solved by current
describe a novel trust enhancement
alized sharing based on the use of
open trust issues. Our design
vironment technologies
operation of the

Threat intelligence is normally shared between
well defined groups or *communities* with varyin
openness in sharing. Communities may be *priva*
with sharing only between the members of the c
public i.e. fully open with all information avail
or they may be somewhere in between [3]. Ad
companies provide information commerciall
is evidence of a move away from the
community model towards a more d
based model - inspired (and enabl
increasing trend, in many fields.
via blockchain based mark
Hyperledger, is TRA
be found i

TITAN

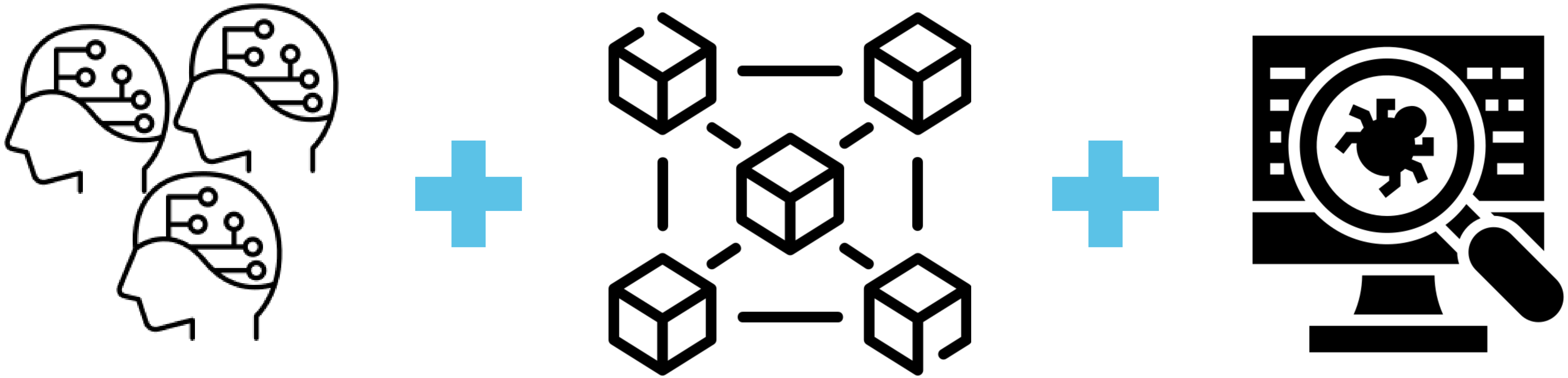
TITAN is a framework and It is aimed to be a general solution for trusted threat Intelligence sharing for use across different Threat Intelligence Platform

CryptoCVEs

CryptoCVEs is NFT collectibles. A CVE is a software vulnerability in the cybersecurity world. CryptoCVE makes you mint famous CVE's as collectibles

Then What is TMoC?

- TMoC(Threat Modelers on Chain) is a first block-chain based collective intelligence threat modeling tool
  - TMoC is a follow-up study on “Blockchain as a Threat Modeling Thinking Tools” at DEFCON 29
  - We call this MMOTM(Massive Multiplayer Online Threat Modeling)



MMO

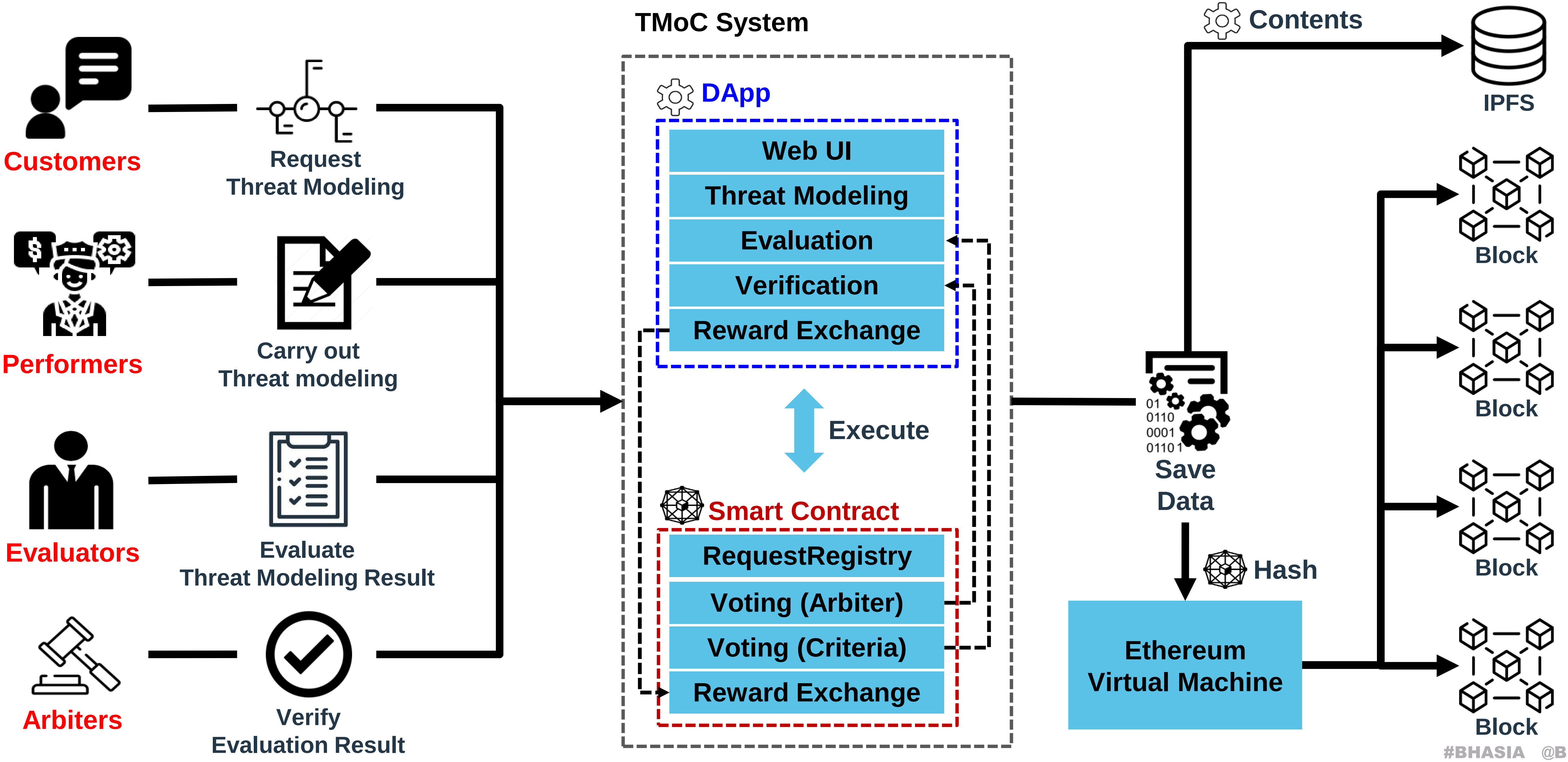
Block-chain

Threat Modeling

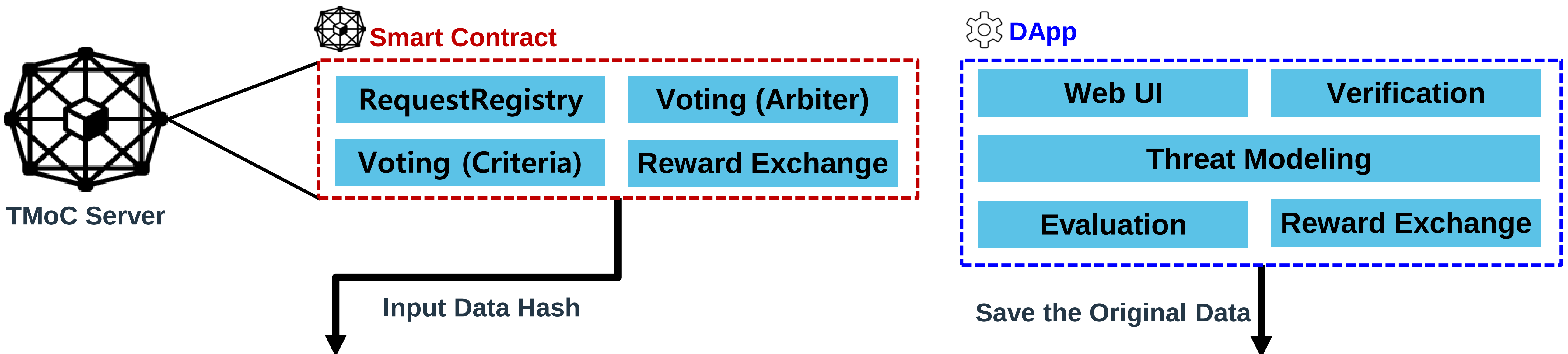
Participants of TMoC

- A Customer
  - Customers are people who request to perform threat modeling by the collective intelligence of experts
  - If customers would like to request threat modeling, they deposit a certain amount of bounty
- A Performer
  - Each security expert can be a performer or an evaluator of the TMoC
  - Performers carry out threat modeling tasks requested by customers
- An Evaluator
  - Each security expert can be a performer or an evaluator of the TMoC
  - Evaluators verify an performer's task
- An Arbiter
  - An arbiter is determined by the vote of the evaluators
  - Arbiters verify an evaluator's task

TMoC System Model



TMoC Data Storage



TMoC Server

Smart Contract

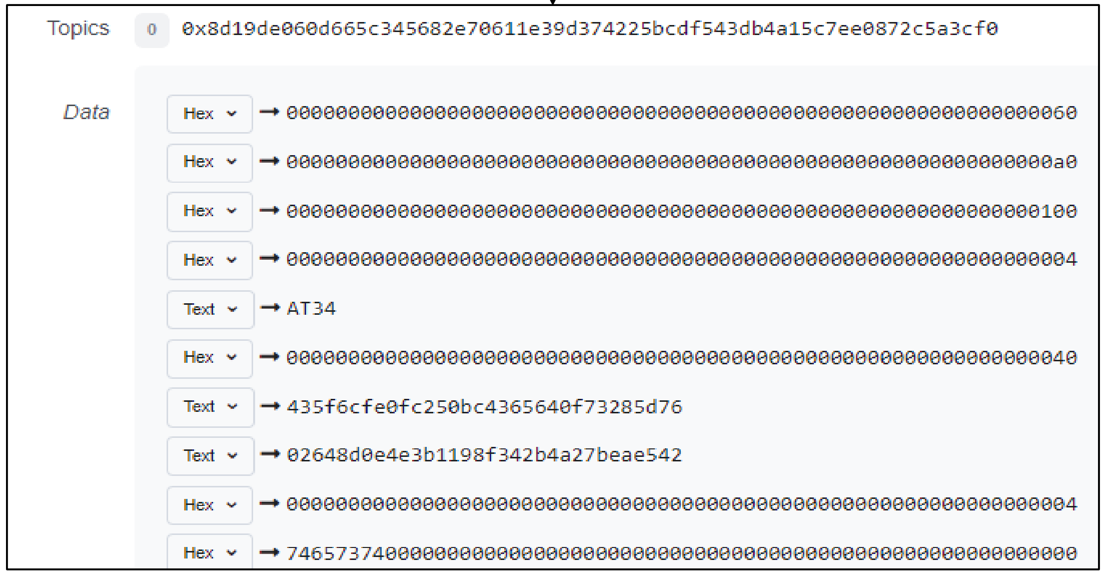
- RequestRegistry
- Voting (Arbiter)
- Voting (Criteria)
- Reward Exchange

DApp

- Web UI
- Verification
- Threat Modeling
- Evaluation
- Reward Exchange

Input Data Hash

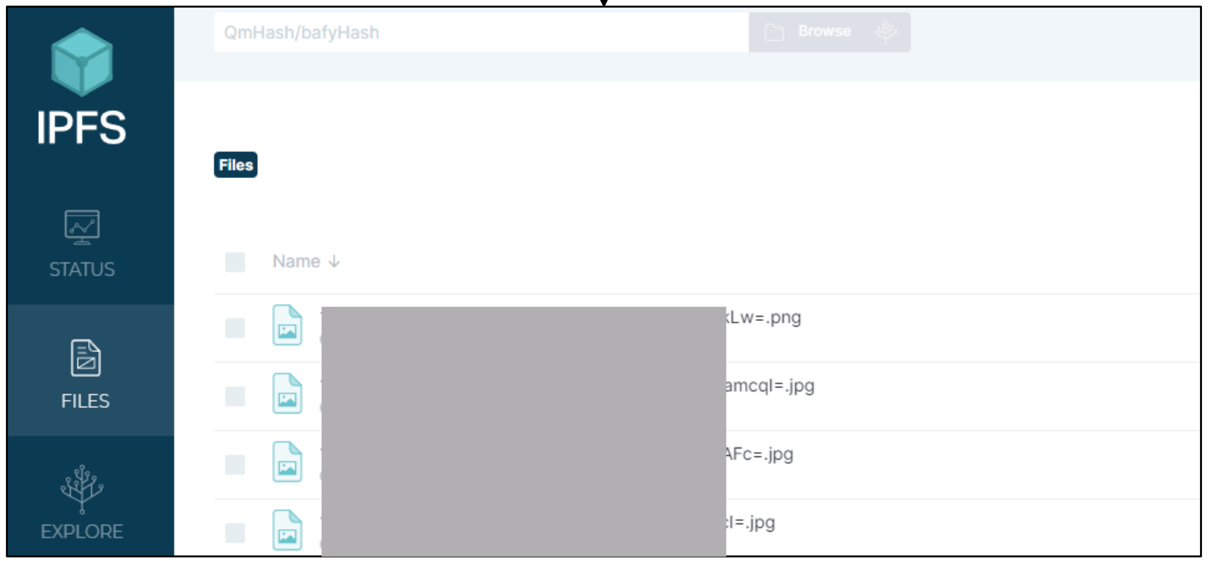
Save the Original Data



```
Topics  0  0x8d19de060d665c345682e70611e39d374225bcdf543db4a15c7ee0872c5a3cf0

Data    Hex  ⌄  → 0000000000000000000000000000000000000000000000000000000000000060
        Hex  ⌄  → 00000000000000000000000000000000000000000000000000000000000000a0
        Hex  ⌄  → 0000000000000000000000000000000000000000000000000000000000000100
        Hex  ⌄  → 0000000000000000000000000000000000000000000000000000000000000004
        Text ⌄  → AT34
        Hex  ⌄  → 0000000000000000000000000000000000000000000000000000000000000040
        Text ⌄  → 435f6cfe0fc250bc4365640f73285d76
        Text ⌄  → 02648d0e4e3b1198f342b4a27beae542
        Hex  ⌄  → 0000000000000000000000000000000000000000000000000000000000000004
        Hex  ⌄  → 7465737400000000000000000000000000000000000000000000000000000000
```

Block



Name ↓

[redacted]Lw=.png

[redacted]amcql=.jpg

[redacted]AFc=.jpg

[redacted]l=.jpg

IPFS

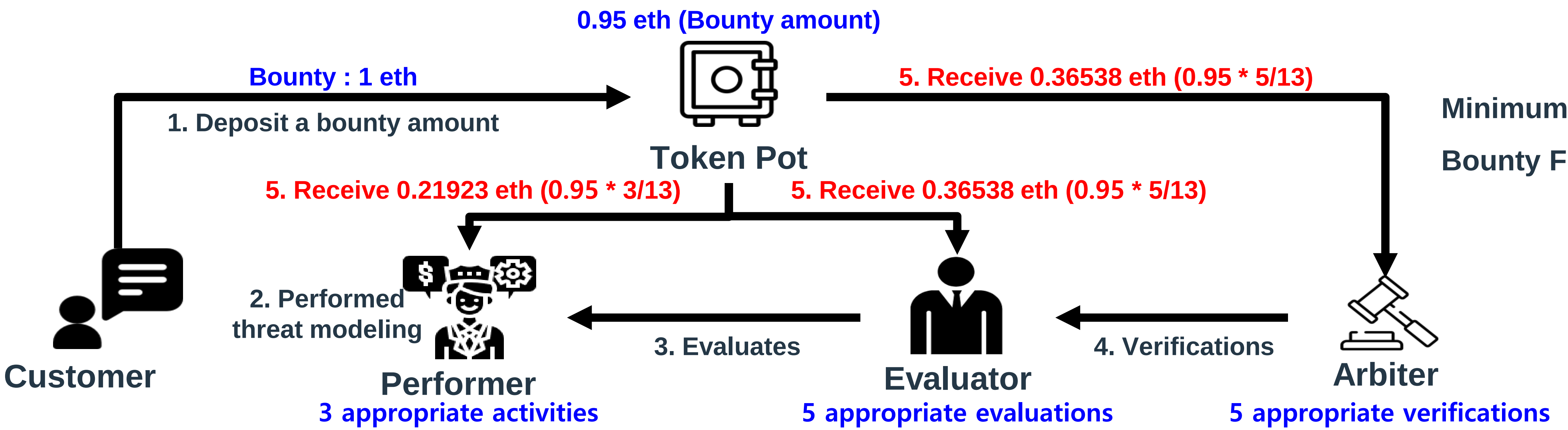
TMoC Basic Process

- **The operation sequence of TMoC is 7 steps as follows**

# 01	# 02	# 03	# 04	# 05	# 06	# 07
Request of Threat Modeling	**Perform task**	**Submit task**	**Program update**	**Evaluation**	**Arbitration**	**Provide Reward**
A customer requests threat modeling from TMoC system	Performers carry out threat modeling task	Tasks are submitted by the performers who has completed threat modeling	Blockchain is updated	Evaluates the threat modeling results	If there is a problem of the evaluation, the Arbiter will verify the evaluation	TMoC participants will receive rewards

Reward Lifecycle

- Participants can earn tokens by performing appropriate threat modeling activities
  - If a participant performs at least one appropriate activity, he or she can earn token
  - Divide and distribute tokens from the Token pot, tokens are given by the rate of the performance in appropriate activity **(“Bounty * (1 – Fees) * appropriate activity/all appropriate activity”)**

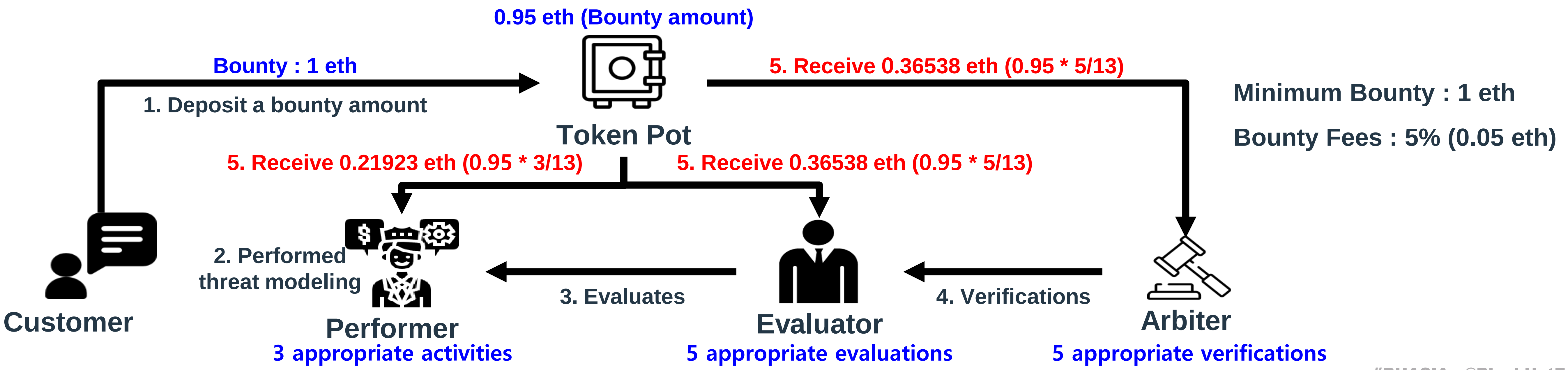

0.95 eth (Bounty amount)
Bounty : 1 eth
1. Deposit a bounty amount
Token Pot
5. Receive 0.36538 eth (0.95 * 5/13)
5. Receive 0.21923 eth (0.95 * 3/13)
5. Receive 0.36538 eth (0.95 * 5/13)
2. Performed threat modeling
3. Evaluates
4. Verifications
Customer
Performer
3 appropriate activities
Evaluator
5 appropriate evaluations
Arbiter
5 appropriate verifications

Minimum Bounty : 1 eth

Bounty Fees : 5% (0.05 eth)

Reward Lifecycle

- Assessment method is used to determine the appropriate activity of participants
  - It is expected that by evaluating the threat modeling results by two or more evaluators, some problems that may be incorrectly evaluated can be solved



0.95 eth (Bounty amount)

Bounty : 1 eth

1. Deposit a bounty amount

Token Pot

5. Receive 0.36538 eth (0.95 * 5/13)

5. Receive 0.21923 eth (0.95 * 3/13)

5. Receive 0.36538 eth (0.95 * 5/13)

Minimum Bounty : 1 eth

Bounty Fees : 5% (0.05 eth)

Customer

2. Performed threat modeling

Performer

3 appropriate activities

3. Evaluates

Evaluator

5 appropriate evaluations

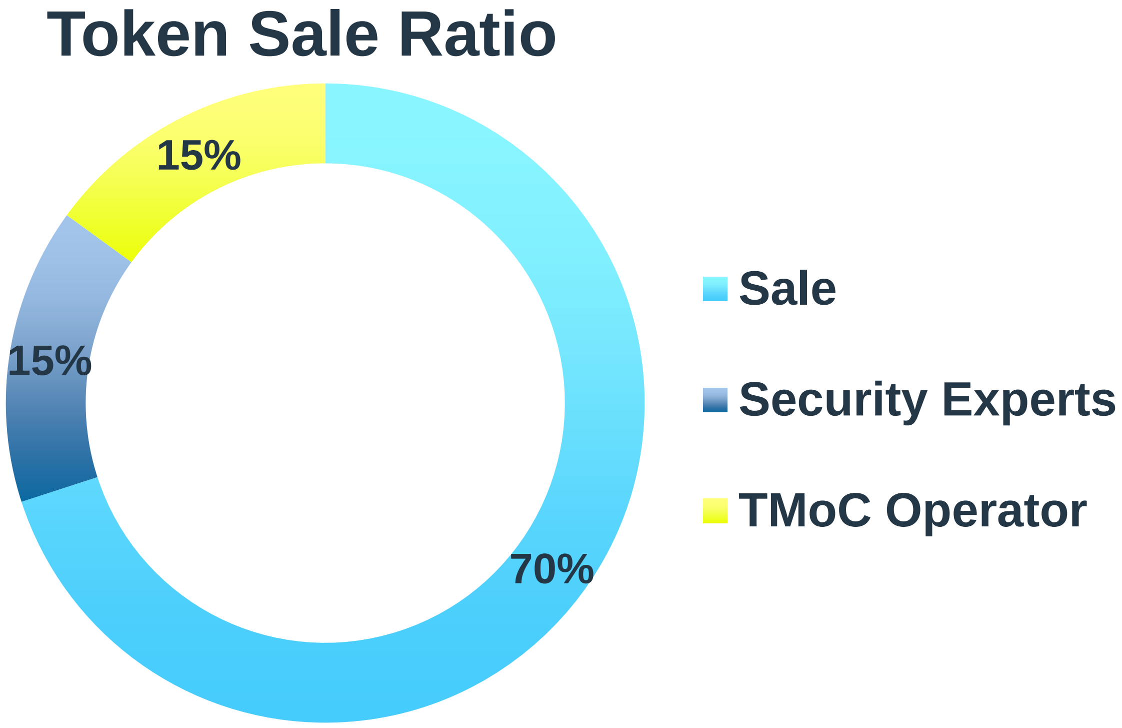
4. Verifications

Arbiter

5 appropriate verifications

TMoC’s Revenue Model

- TMoC operators can raise initial funding by bounty fees and token trading
  - Operators can earn revenue as token trading becomes more active by sharing a portion of the token
  - TMoC tokens are created and sales for a certain period of time, determining the maximum number of tokens



Demo

Possible Effects of TMoC

- TMoC is the first blockchain-based threat modeling tool that utilizes a collective intelligence, anyone can be a participant
  - Participants can be encouraged by giving tokens to them who performs right threat modeling activities or evaluates correctly
  - By encouraging participants, the TMoC can derive better threat modeling result

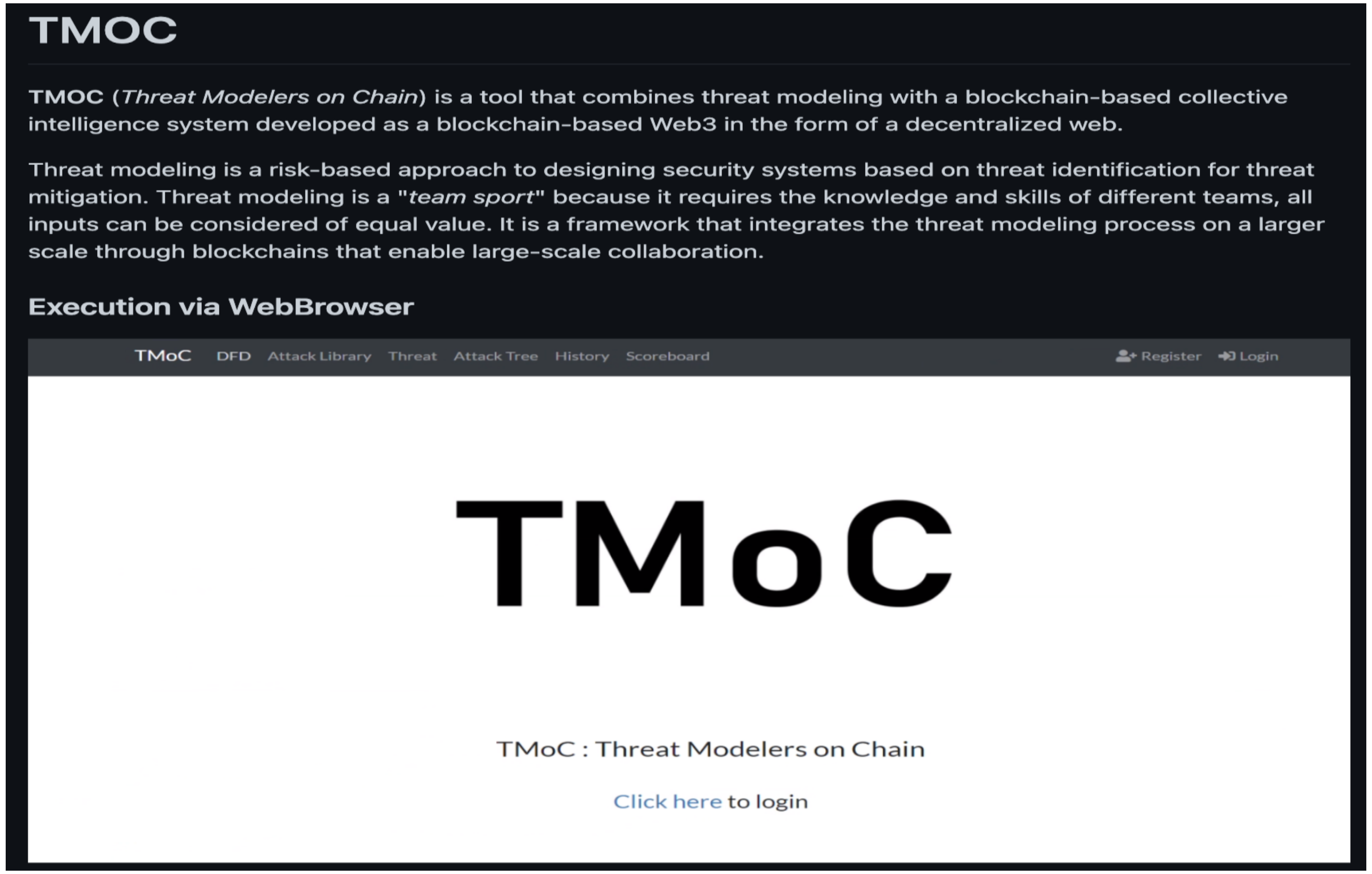
Next Step

- Current TMoC is a prototype that works on the test network
  - Next, we will build our own TMoC blockchain network
  - Additionally, we will make a governance token and develop voting system for decision-making in the TMoC(e.g. electing evaluation criteria or arbiter)

- Current TMoC is not scalable(i.e. It doesn’t provide APIs for add-on developers)
  - To improve user experience and scalability we will provide APIs for add-on developers (e.g. add-on for drawing a DFD, add-on for automatically collecting CVEs …)

TMoC is Open Source Tool

- TMoC is uploaded in our Github repo(open source license)
  - Github Link : https://github.com/HackProof/TMoC



TMOC

TMOC (*Threat Modelers on Chain*) is a tool that combines threat modeling with a blockchain-based collective intelligence system developed as a blockchain-based Web3 in the form of a decentralized web.

Threat modeling is a risk-based approach to designing security systems based on threat identification for threat mitigation. Threat modeling is a "*team sport*" because it requires the knowledge and skills of different teams, all inputs can be considered of equal value. It is a framework that integrates the threat modeling process on a larger scale through blockchains that enable large-scale collaboration.

Execution via WebBrowser

TMoC

TMoC : Threat Modelers on Chain

Click here to login

Thank you

Q & A

Yejun Kim (v3locy@korea.ac.kr)
Kwangsoo Cho (cks4386@korea.ac.kr)
Paul Hong (visitator00@korea.ac.kr)
Seungjoo Kim (skim71@korea.ac.kr)