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) *

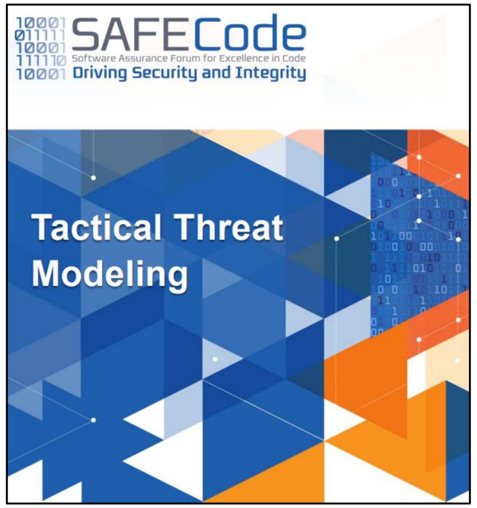
✓ This work is supported by the Korea Agency for Infrastructure Technology Advancement (KAIA) grant funded by the Ministry of Land, Infrastructure and Transport (Grant 21AMDP-C162334-01).

* Corresponding Author

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

Software Assurance Forum for Excellence in Code

Driving Security and Integrity

Tactical Threat Modeling

[SAFECode, Tactical Threat Modeling]

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

How to approach

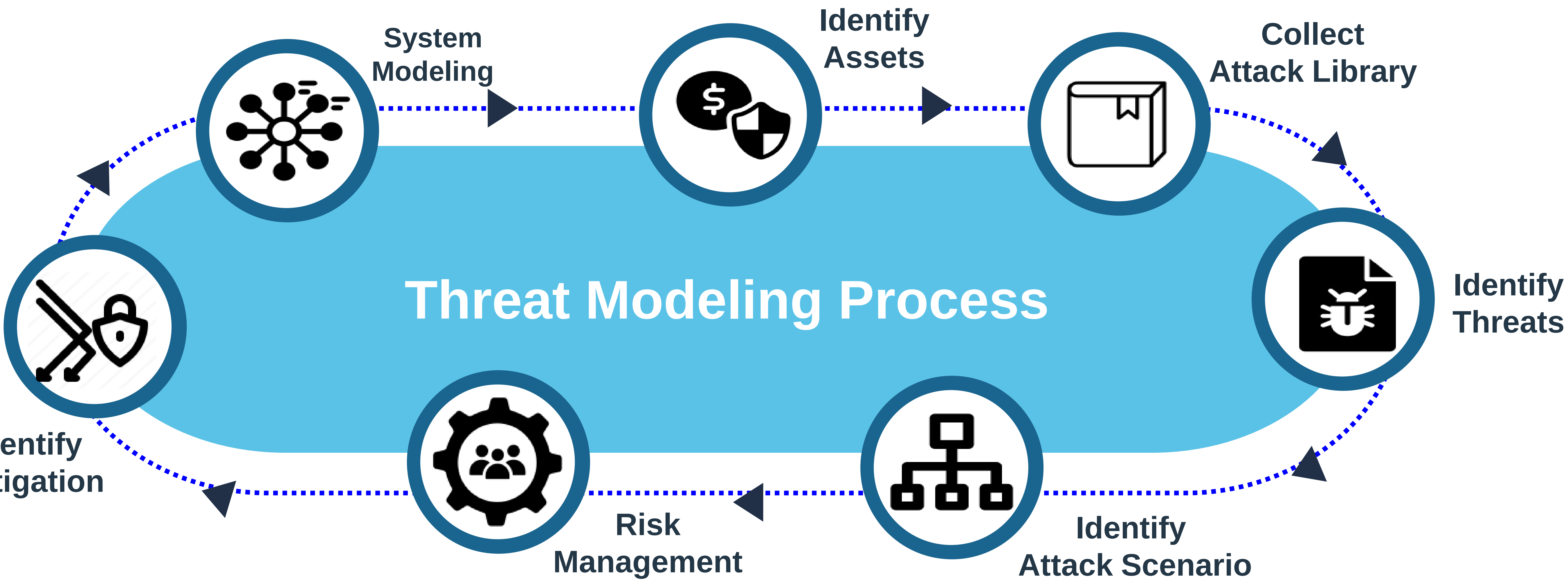
Threat Modeling

AWS Well-Architected

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

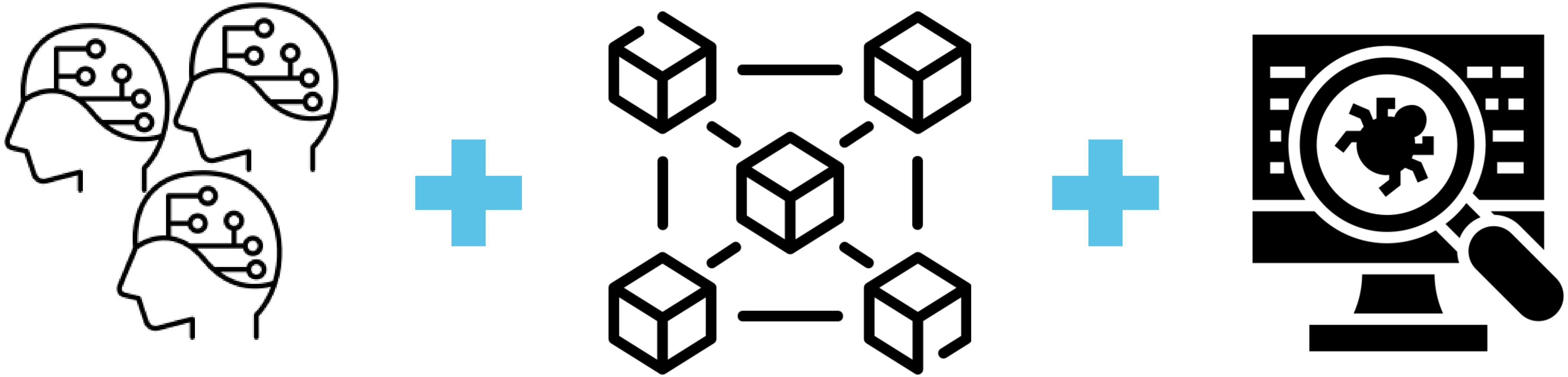
- Threat modeling is a “team sport” that requires the knowledge and skills of various teams.
- All inputs have equal value

Threat Modeling Process



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

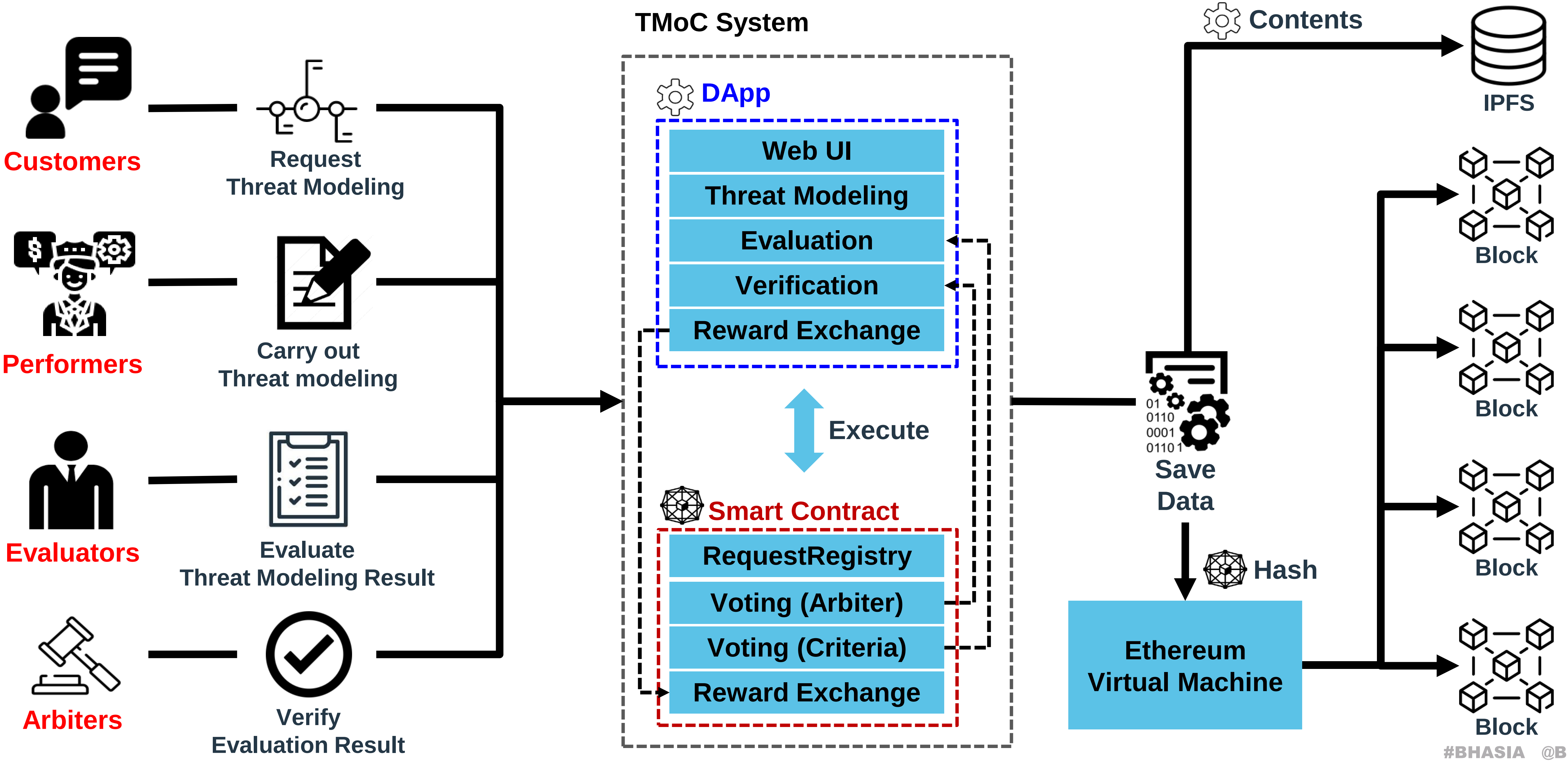
Block-chain

Threat Modeling

Participants of TMoC

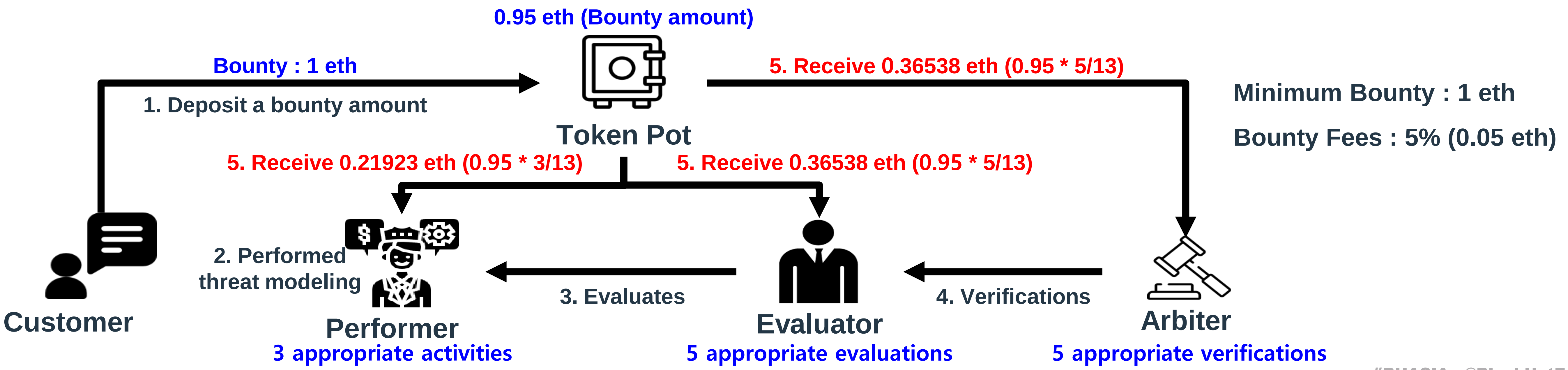
- A Customer
    - Customers are people who request to perform threat modeling by the collective intelligence of experts
    - If customers would like to request threat modeling, they deposit a certain amount of bounty
- A Performer
    - Each security expert can be a performer or an evaluator of the 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



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)
Minimum Bounty : 1 eth
Bounty Fees : 5% (0.05 eth)
2. Performed threat modeling
3. Evaluates
4. Verifications
Customer
Performer
3 appropriate activities
Evaluator
5 appropriate evaluations
Arbiter
5 appropriate verifications

TMoC Basic Process

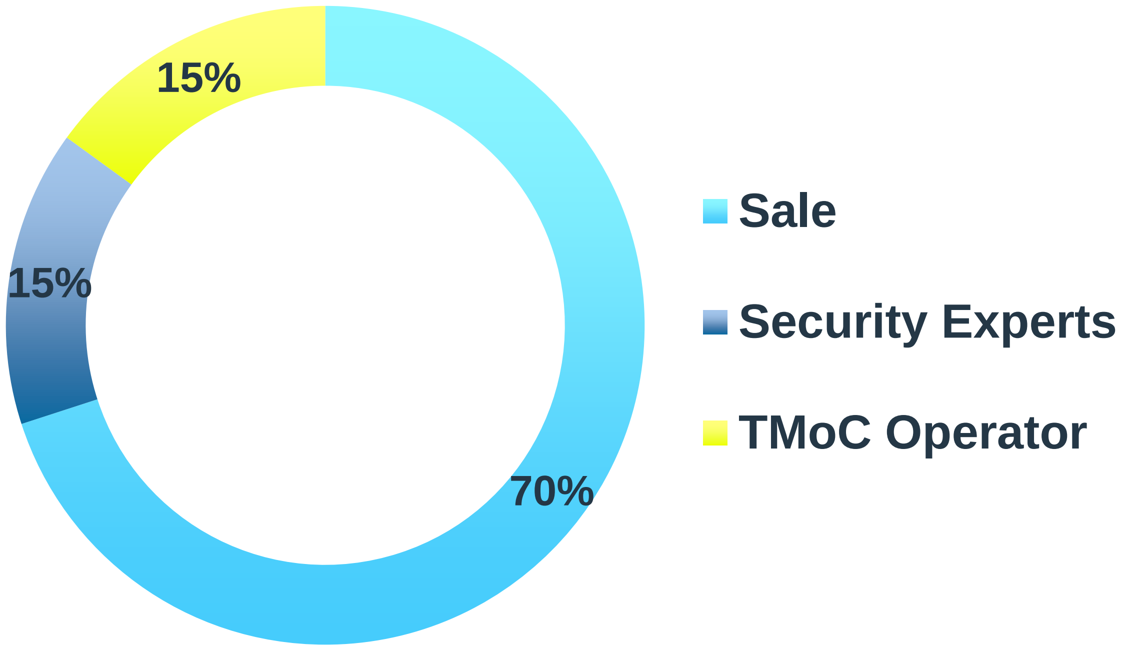
- **The operation sequence of TMoC is 7 steps as follows**

# 01 **Request of Threat Modeling**	# 02 **Perform task**	# 03 **Submit task**	# 04 **Program update**	# 05 **Evaluation**	# 06 **Arbitration**	# 07 **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

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

Token Sale Ratio



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

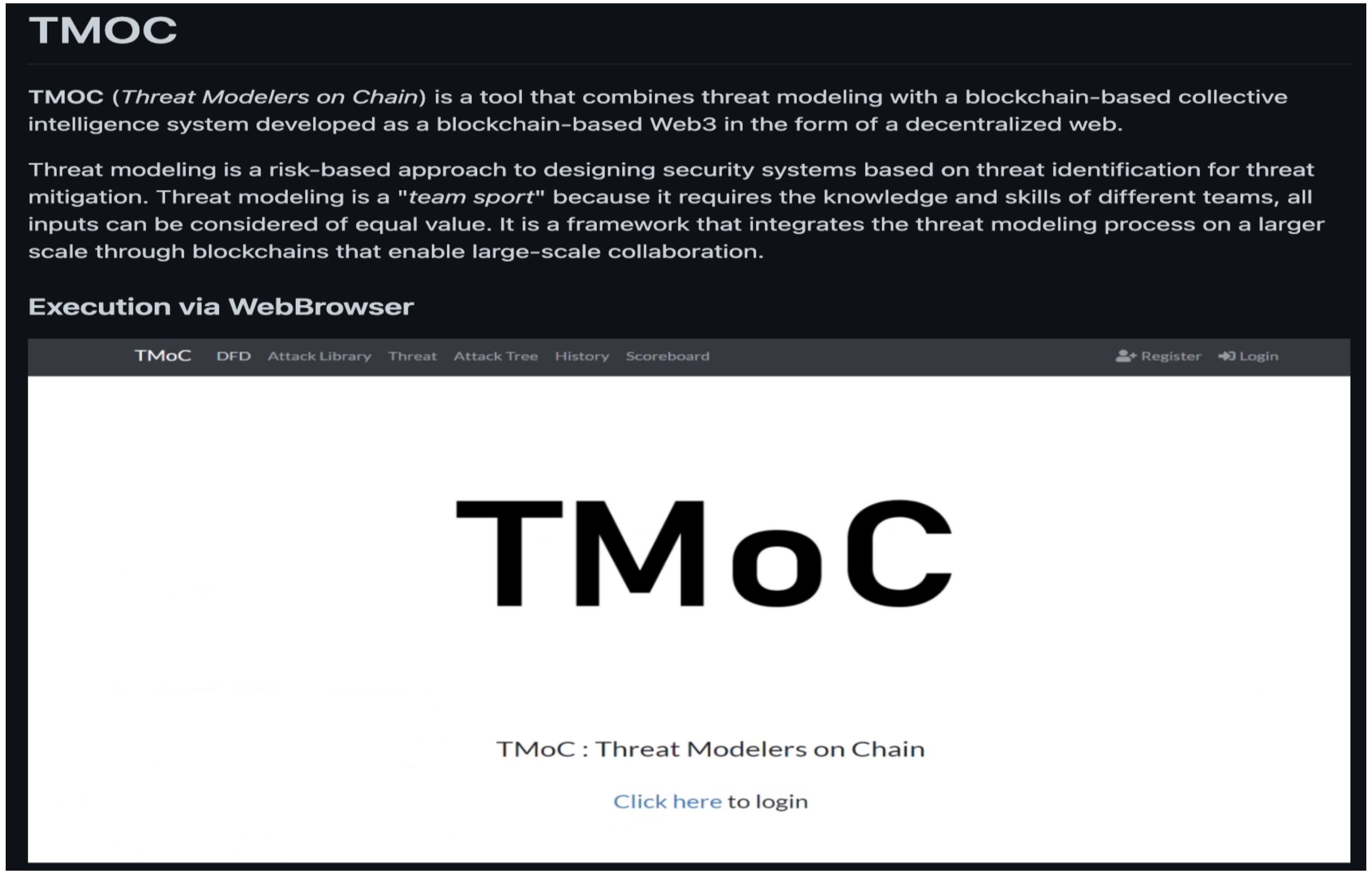
Next Step

- 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)