

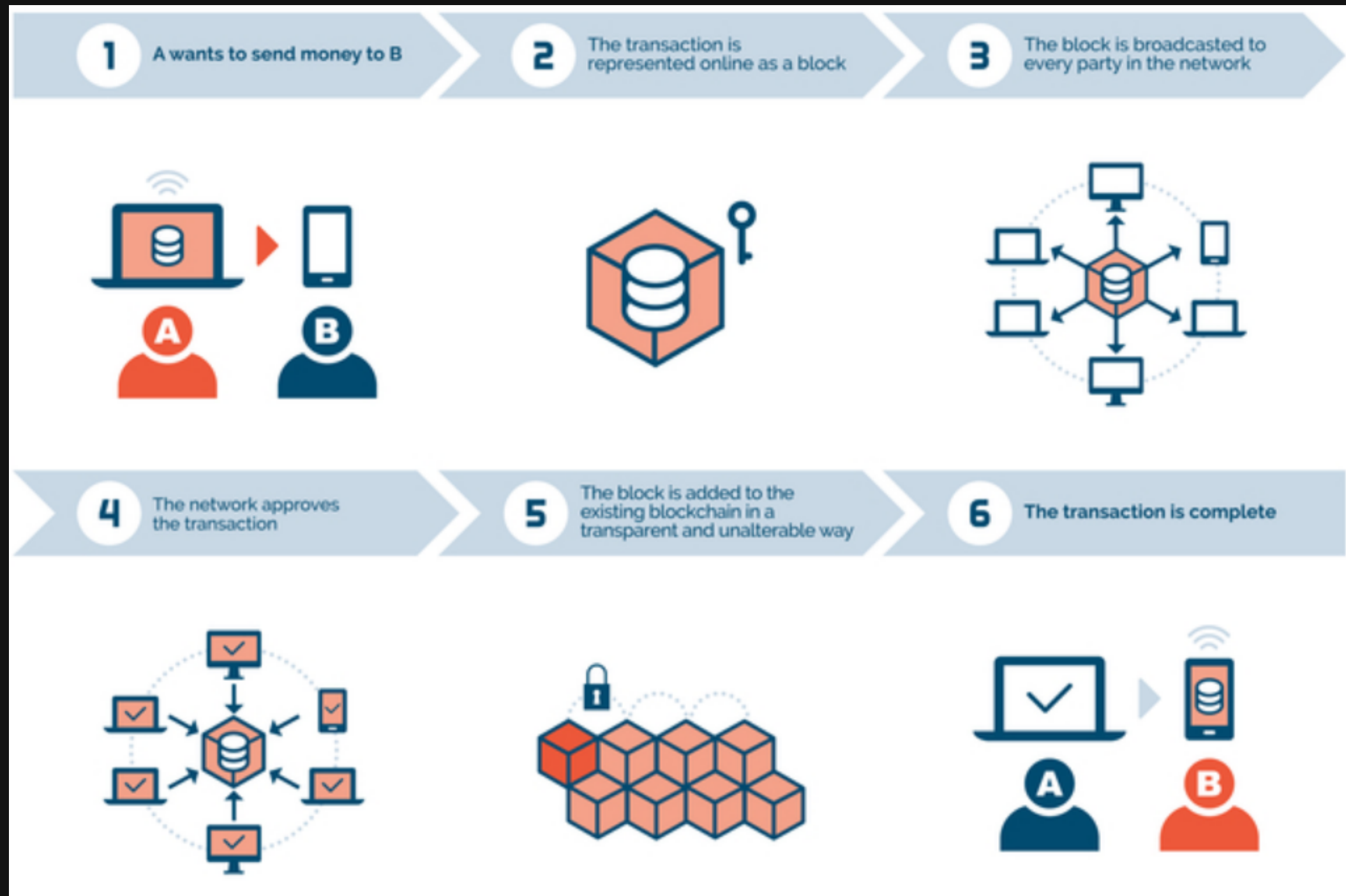
F-WINE

Author : Sangsup Lee, Hyunki Kim @ syssec

Fuzzing Webassembly IN EOS

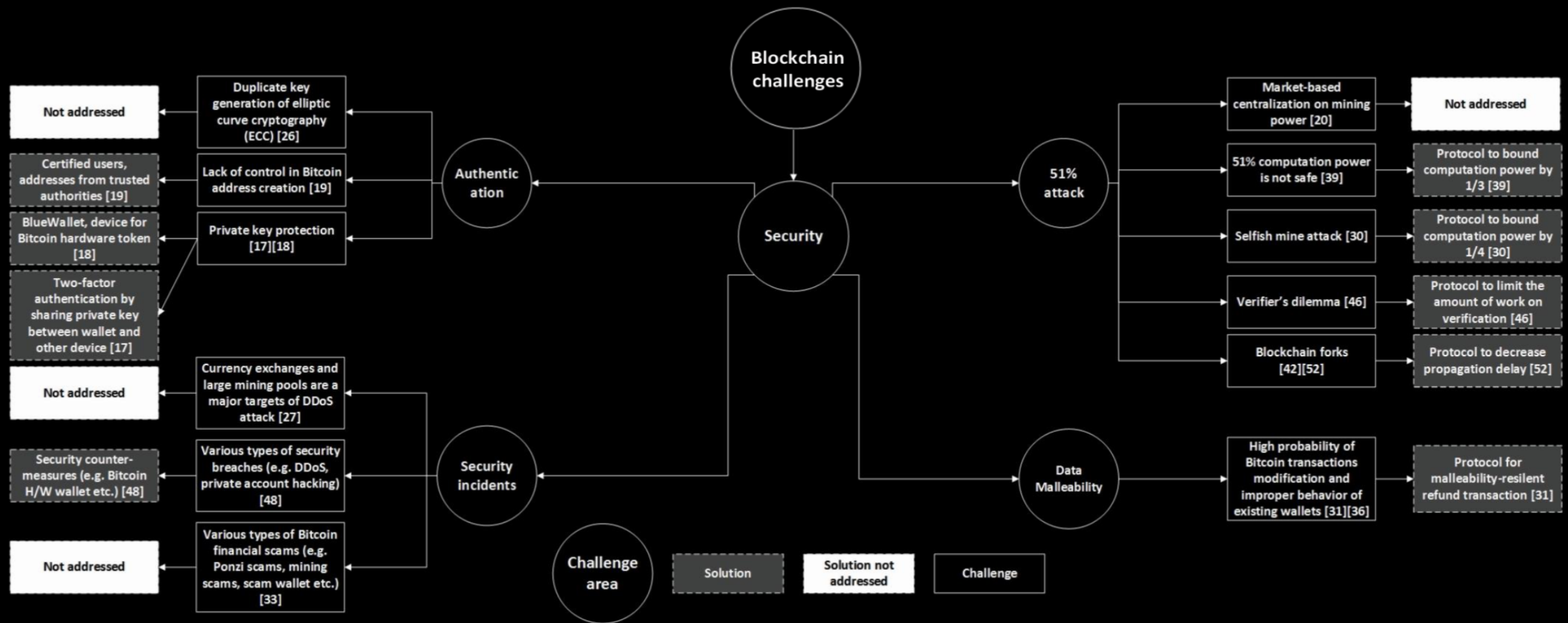


What is a block chain?





What is a block chain?



There is no attack for Node



What is a block chain?

	Reentrancy	Access Control	Arithmetic Issues	Unchecked Low Level Calls	Denial of Services	Bad Randomness	Front Running	Time Manipulation	Short Addresses
Oyente	O	X	O	X	Δ	X	O	O	X
Mythril	X	X	O	Δ	Δ	X	O	X	X
Zeus	O	X	O	O	X	X	O	O	X
Manticore	O	X	O	O	Δ	X	X	X	X
SmartCheck	O	X	O	Δ	Δ	X	X	O	X
Remix	O	X	O	Δ	Δ	X	X	X	X














There is no attack for Node



What is a block chain?

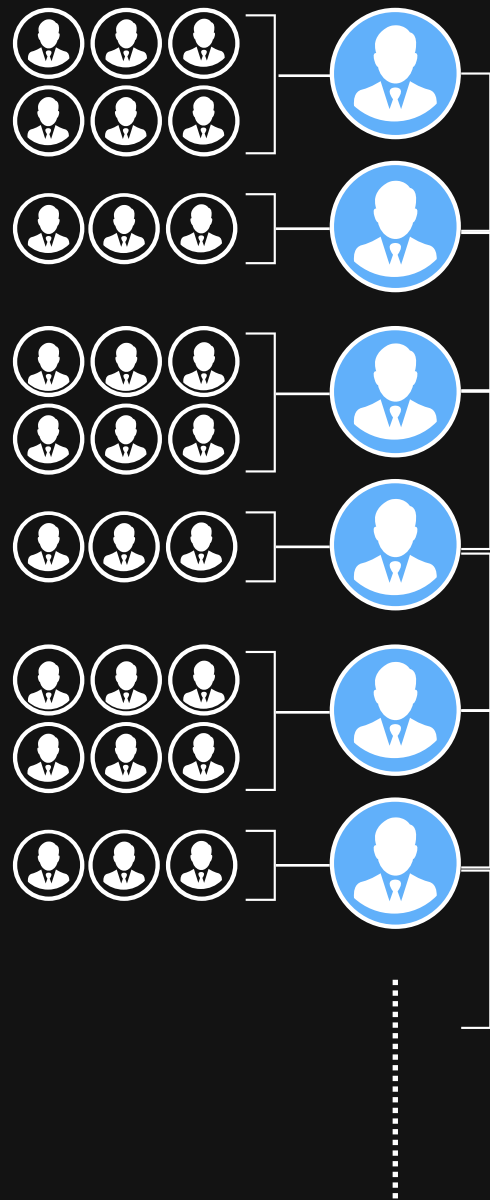
COMPARISON OF BLOCKCHAIN PLATFORMS

Updated 7-23-2018

	ETH	NULS	ARDOR	NEO	WAVES	LISK	EOS	CARDANO	ICON	ARK	STRATIS	WANCHAIN	NXT
													
Language	Go, C++, Rust	Java	Java	C#	Scala	JavaScript	C++	Haskell	Python	JavaScript	C#, .NET	Go, C++	Java
Consensus	PoW	PoC	PoS	dBFT	LPoS	DPoS	DPoS	PoS	LFT	DPoS	PoS	PoW	PoS
Block Time (seconds)	14-15	10	60	15-20	3	10	0.5	20	1	8	60	~13	60
Smart Contracts	✓	⚙️	🧩	✓	⚙️	✗	✓	⚙️	⚙️	⚙️	⚙️	✓	🧩
Atomic Swaps	✗	⚙️	⚙️	⚙️	⚙️	✗	✗	⚙️	⚙️	✗	⚙️	✗	⚙️
Contract Language	Solidity	Java	Java	JS, C++, .NET Java, Kotlin, Go	RIDE	N/A	C, C++	Plutus	Python	N/A	C#, .NET	Solidity	Java
DEX	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	⚙️	✗	✓
Side / Child Chains	⚙️	⚙️	✓	⚙️	✗	⚙️	✗	⚙️	⚙️	⚙️	⚙️	⚙️	✗
Privacy Feature	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Mainnet Launch	July 2015	July 2018	Jan 2018	Oct 2016	Jun 2016	May 2016	Jun 2018	Sept 2017	Jun 2018	Mar 2017	Aug 2016	Jan 2018	Nov 2013
Token Creation	✓	⚙️	✓	✓	✓	⚙️	✓	⚙️	⚙️	⚙️	⚙️	✓	✓
Transaction Cost	21000 GAS	0.01 NULS	1 ARDR	Free	0.0001 WAVES	0.1 LSK	Free	0.155381 ADA	0.01 ICX	0.1 ARK	0.001 STRAT	21000 GAS	1 NXT
% Top 10 non-exchange addresses control	9.91%	>60%	24.21%	58.12%	27.99%	18.52%	N/A	23.01%	31.50%	33.44%	20.34%	N/A	20.58%
Wallets	Web, Windows, MacOS, Linux, Android, ERC20, Ledger, & More	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android	Windows, MacOS, Linux, Ledger	Windows, MacOS, Linux	Windows, MacOS, Linux	TREZOR, Web	Windows, MacOS	Web	Desktop, Ledger, Web, Android, iOS	Ledger, Web, Developer (Win, Mac, Linux), Android, PI, Electrum, Breeze	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android
Main Selling Point	Popularity, Smart Contracts	Modular	Child Chains, Built-in Contracts & Features	NEP-5, Digital Identity	Fast and Secure, DEX	JavaScript based SideChains	Scalable, Flexible, Fast	Improved ETH with sidechains and PoS	Multiple Blockchain Integration	Smartbridges	Simple Easy SideChains	Improved ETH with PoS & Asset Privacy	Built-in Contracts



Why we choose EOS?



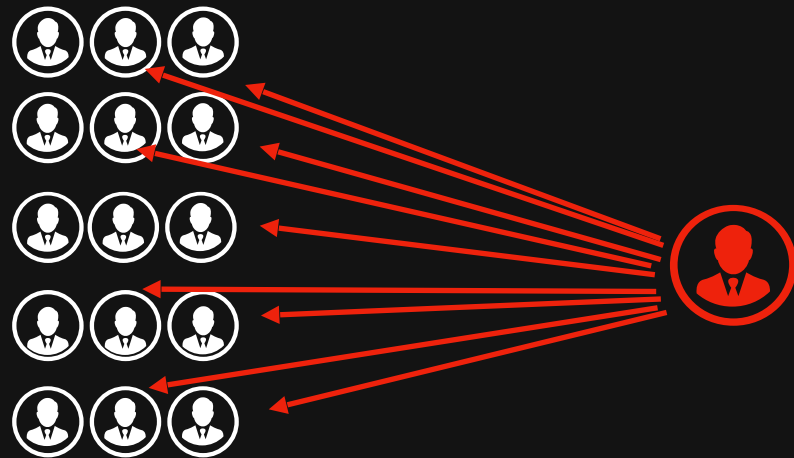
21 * BP Nodes



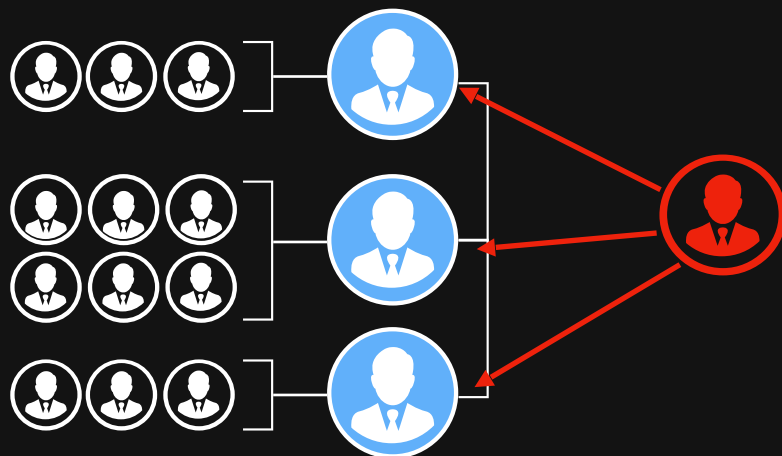


Why we choose EOS?

Other Blockchain



EOS Blockchain



Inbox - HackerOne

Block.one: Bug Bounty Program

HackerOne, Inc. [US] | <https://hackerone.com/eosio>

Hacktivity

Directory

Inbox

Hacker Dashboard

Qualifying vulnerabilities

Only the following design or implementation issues that substantially affect the stability or security of the project is in scope for the program. Common examples include:

1. Cause nodeos to crash via the P2P plugins (net_plugin or bnet_plugin)
2. Cause nodeos to crash via the HTTP RPC API (http_plugin) with Patroneos protection
3. Send a contract into an infinite loop
4. Cause a contract to use large amount of memory (more than 64MB)
5. Crash nodeos with a contract
6. Trigger unauthorized actions on accounts
7. Cause a contract to run for more than 10 ms over deadline

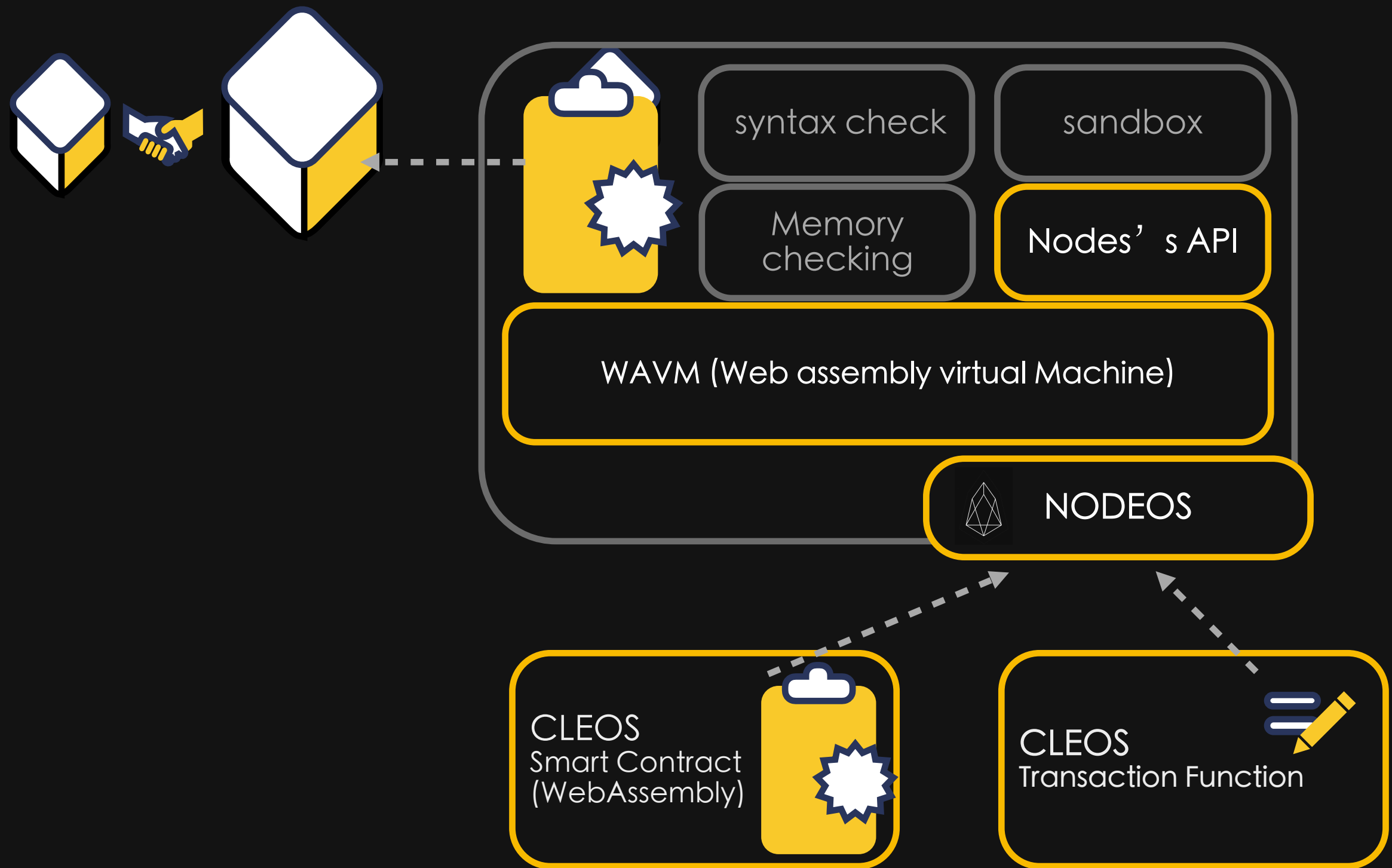
For scenarios that do not fall within one of the above categories, Block.one still appreciates reports that help us secure our infrastructure and our customers. As such, we will reward those reports based on the following table. Please note these are general guidelines, and that reward decisions are up to the discretion of Block.one.

Min/Max	Critical (CVSS 9.0 - 10.0)	High (CVSS 7.0 - 8.9)	Medium (CVSS 4.0 - 6.9)	Low (CVSS 0.0 - 3.9)
Minimum	\$5,000	\$2,500	\$1,000	\$100
Maximum	\$10,000	\$5,000	\$2,500	\$1,000

Note that the scope of the program is limited to technical vulnerabilities in Block.one software only; please do not try to sneak into Block.one offices, attempt phishing attacks against our employees, and so on.



Smart contract in EOS



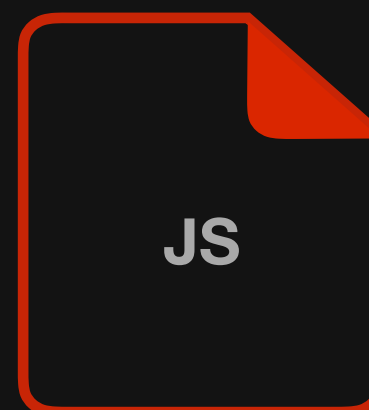


Smart contract in EOS

Web Browser

web sockets, WebRTC, Canvas

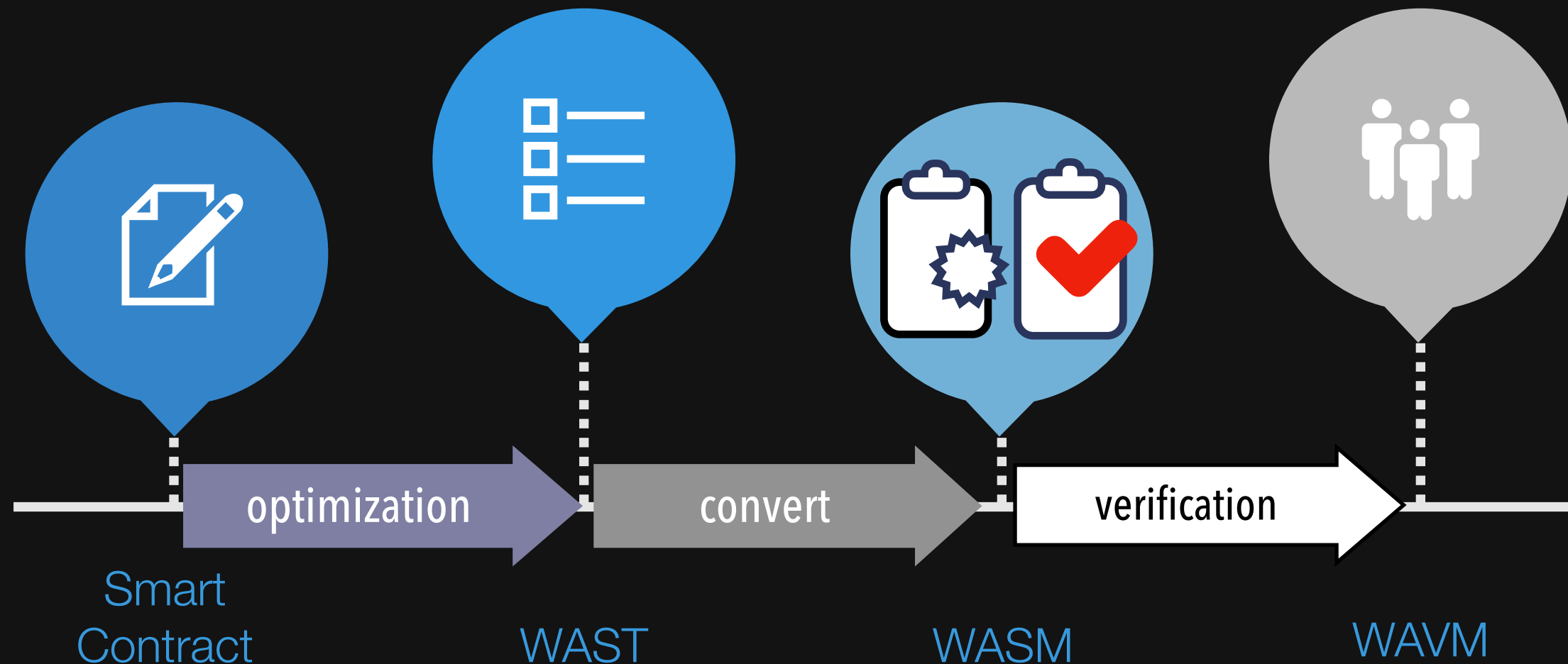
Web Storage, Web Audio,
Media, WebGL..



Javascript runtime

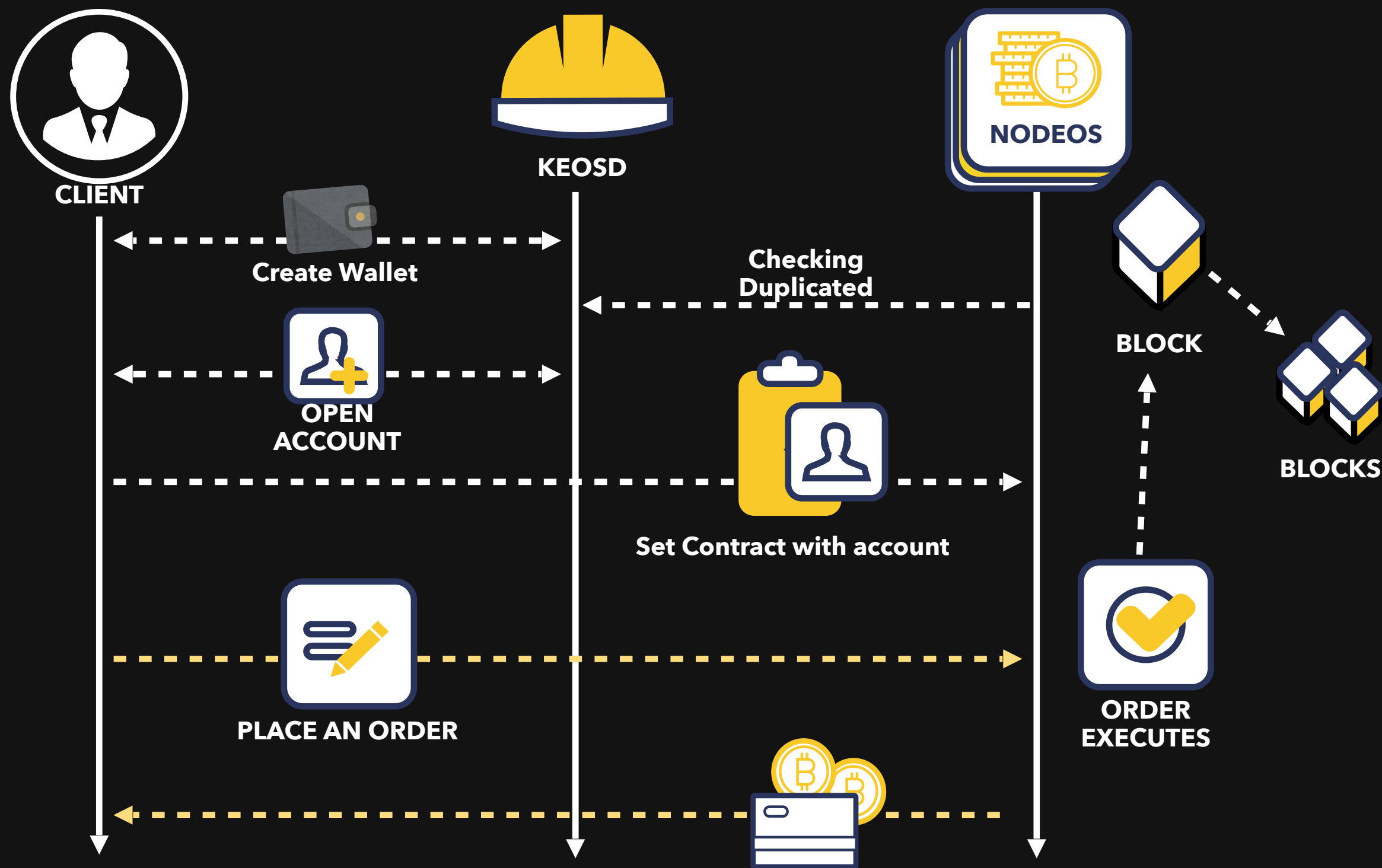


Smart contract in EOS





Smart contract in EOS





Implementation (Fuzzer)

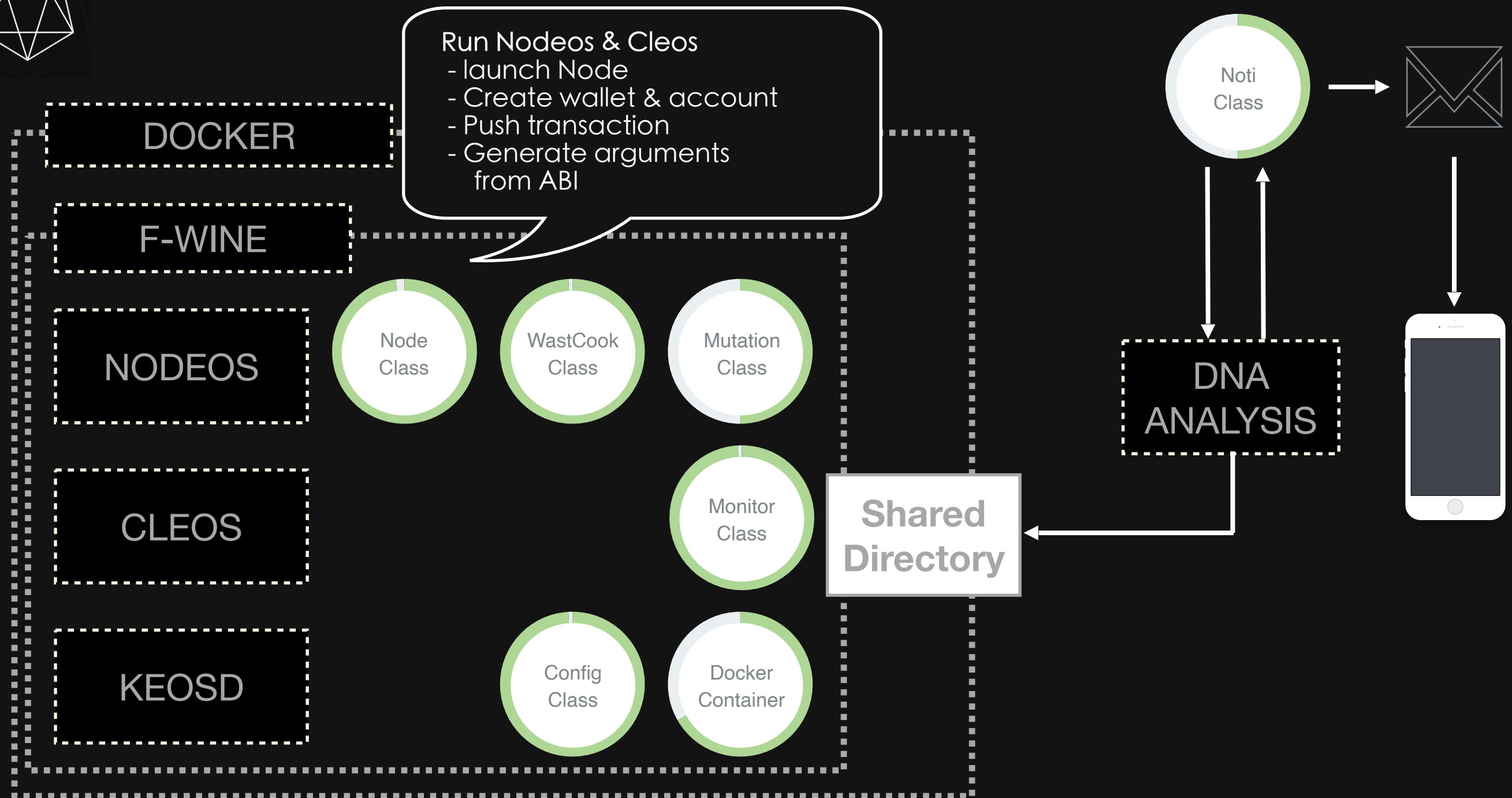
Architecture Progress



Development Progress



Fuzzing Webassembly IN EOS



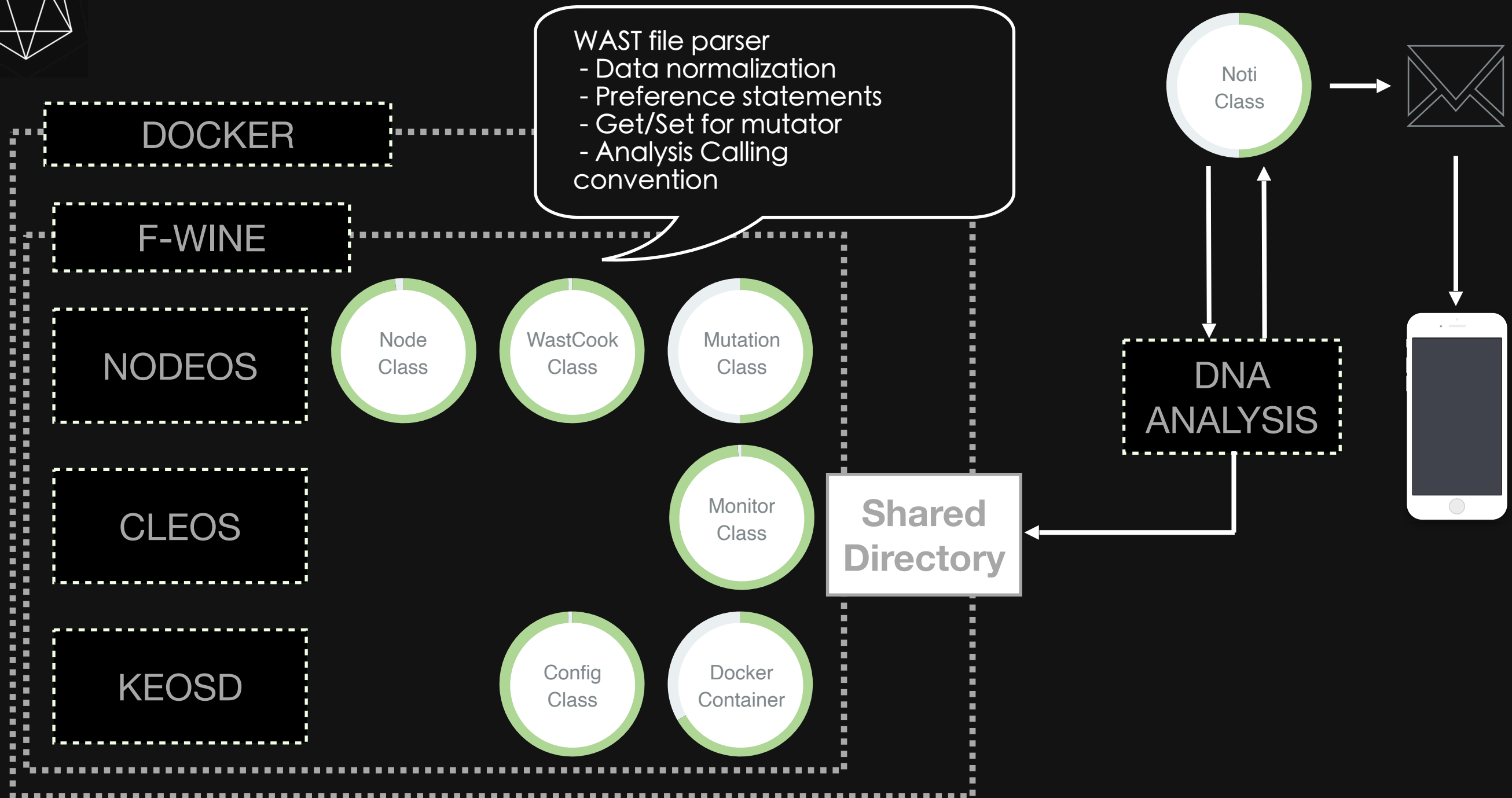
Background

Implementation

Evaluation

Conclusion

Fuzzing Webassembly IN EOS

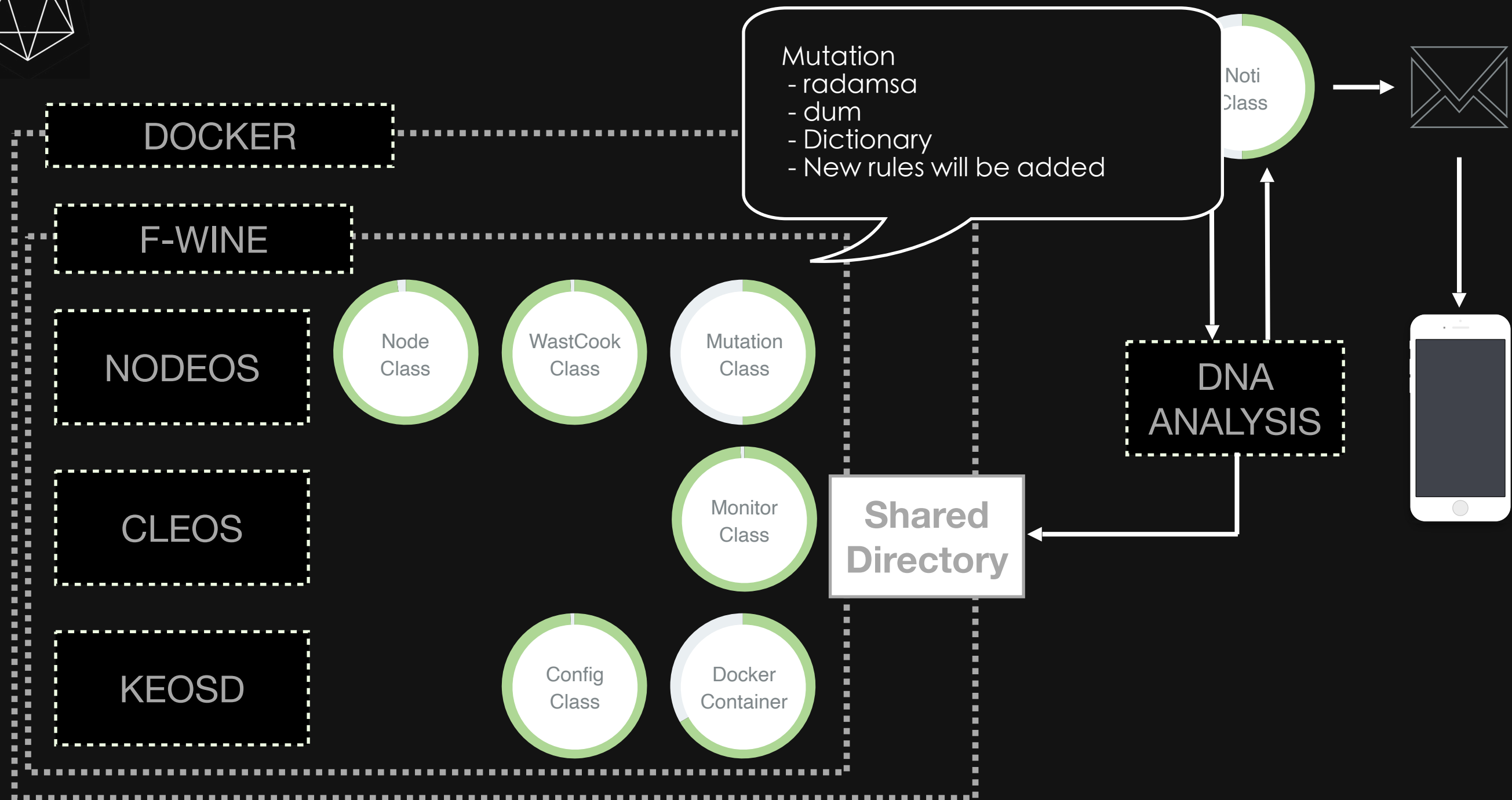


Background

Implementation

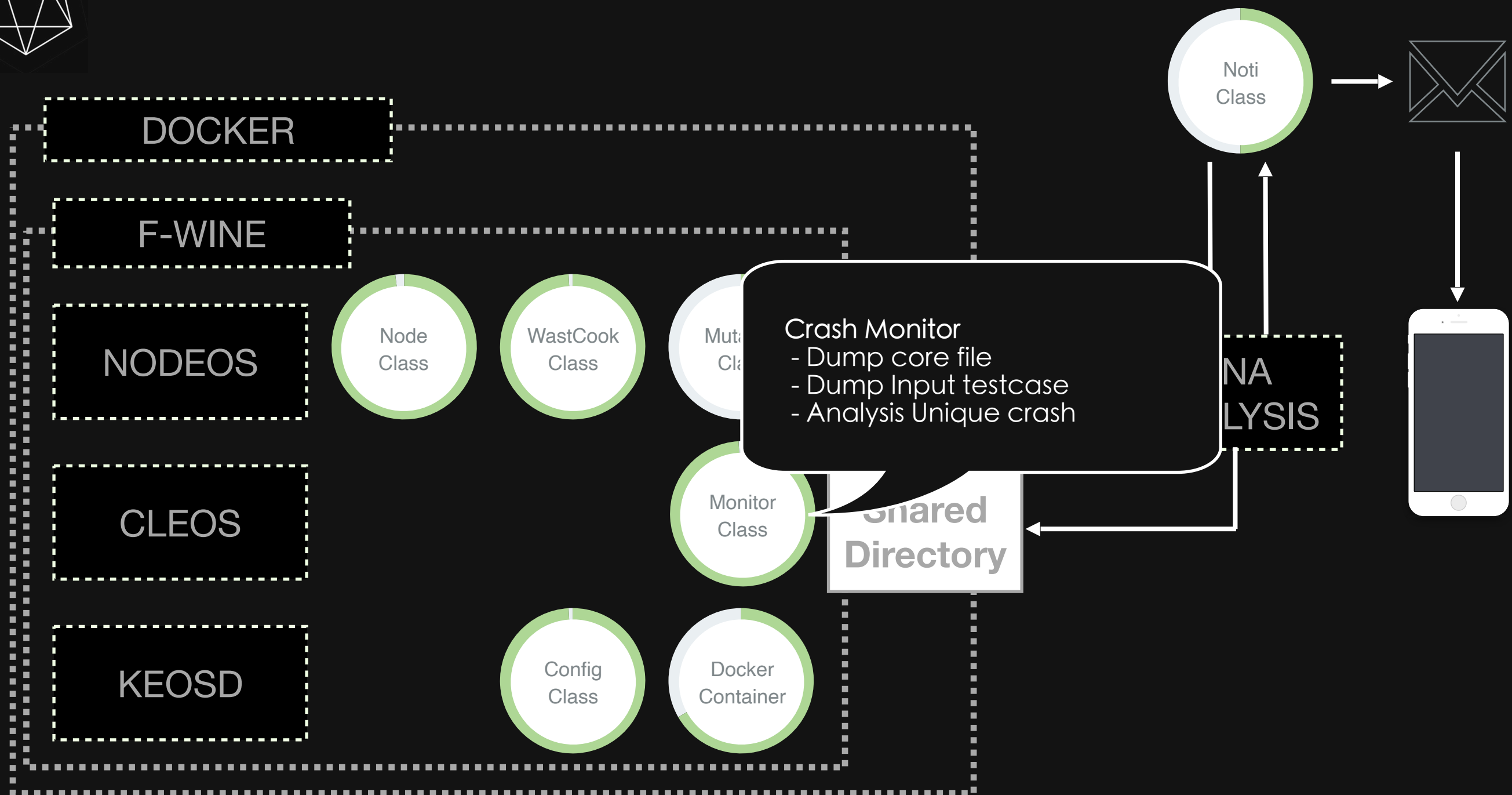
Evaluation

Conclusion



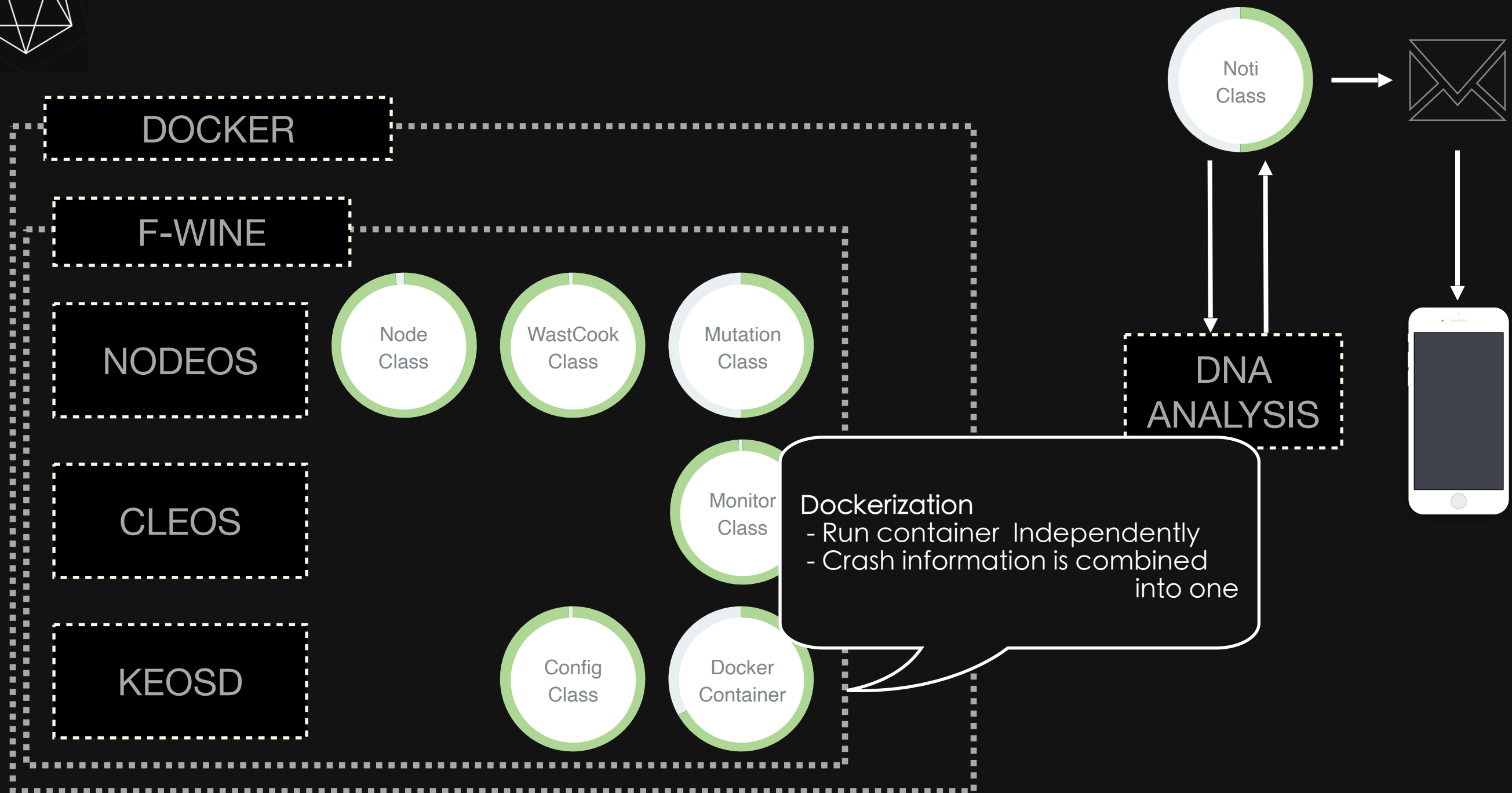


Fuzzing Webassembly IN EOS





Fuzzing Webassembly IN EOS



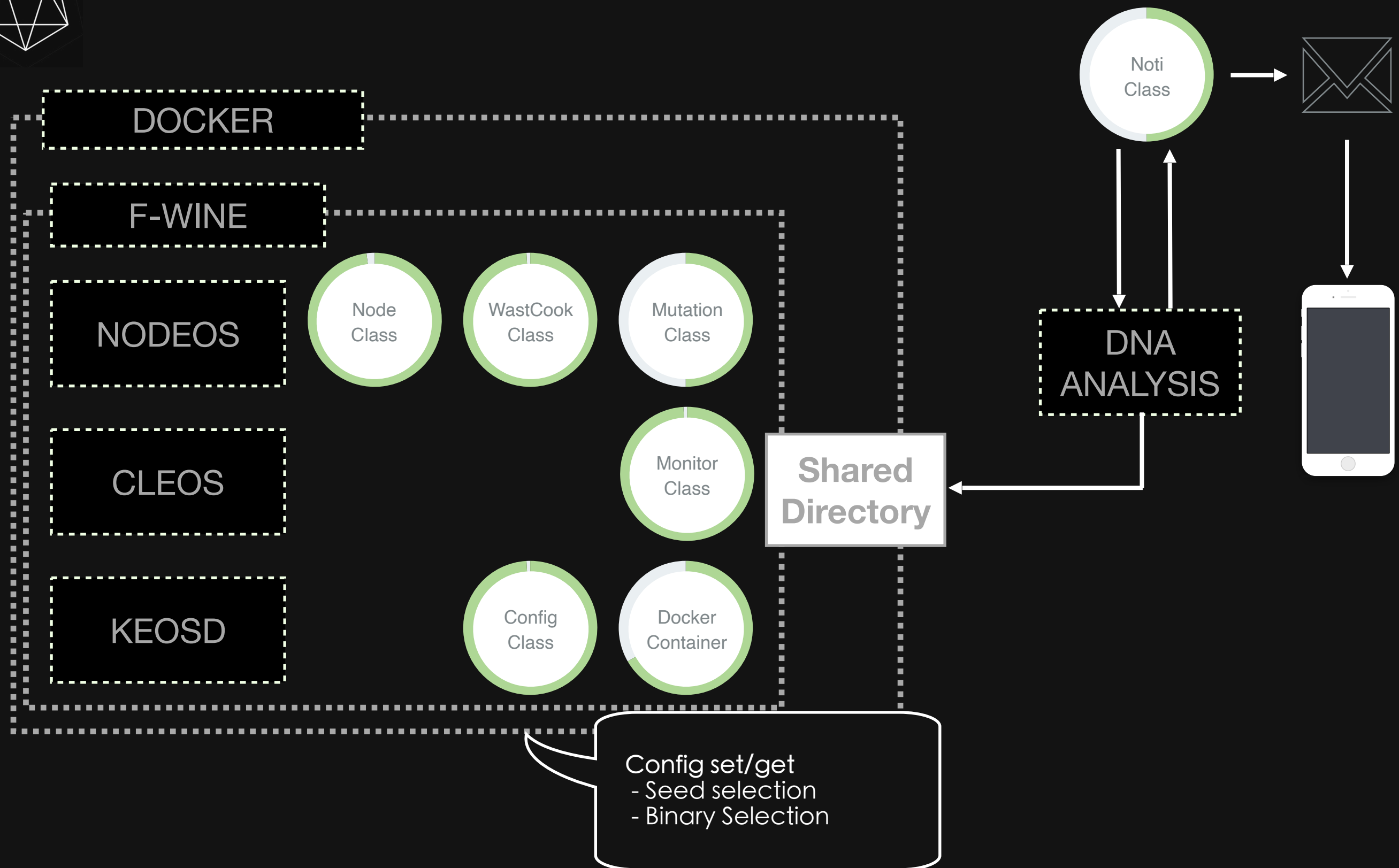
Background

Implementation

Evaluation

Conclusion

Fuzzing Webassembly IN EOS

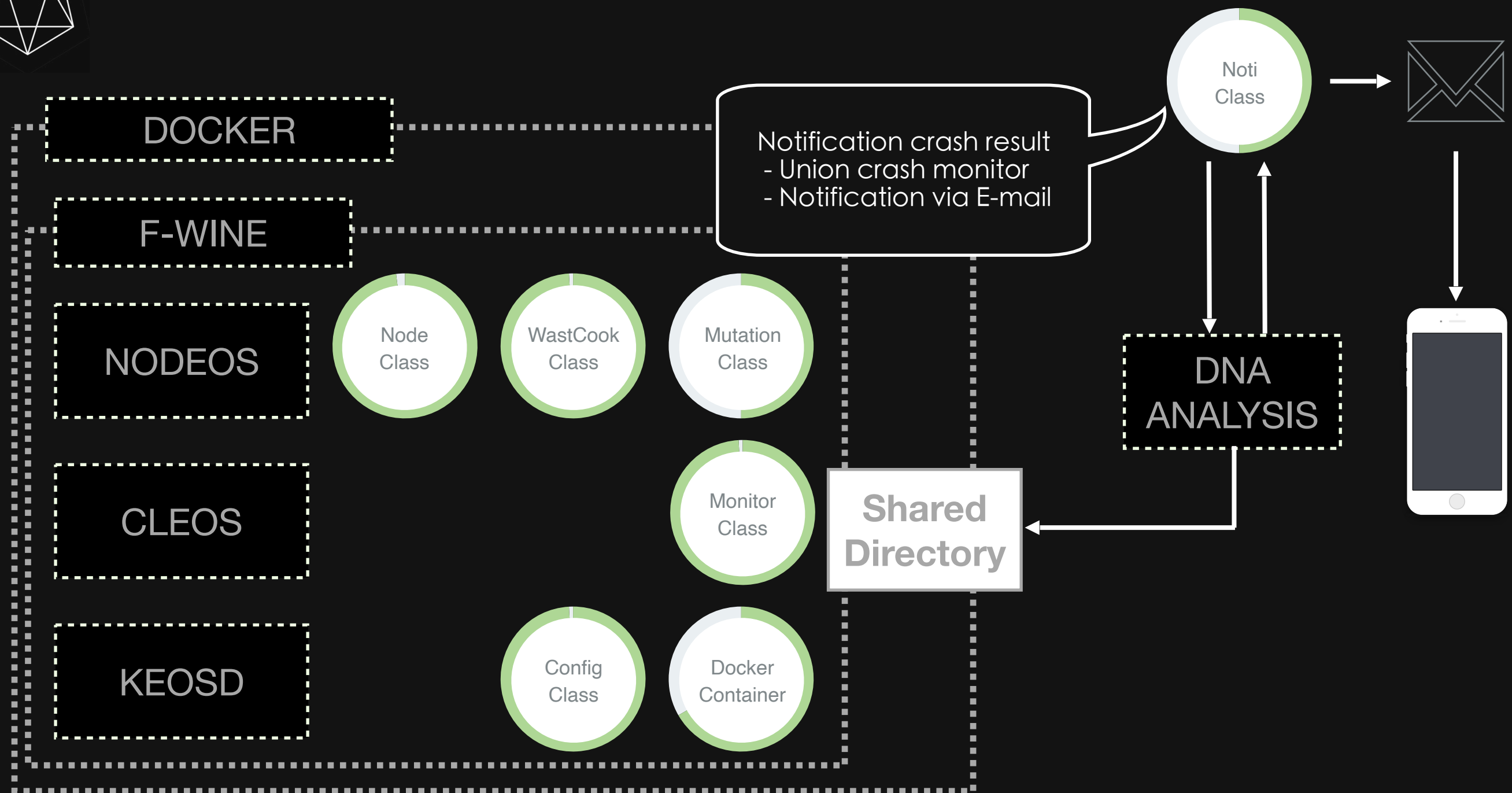


Background

Implementation

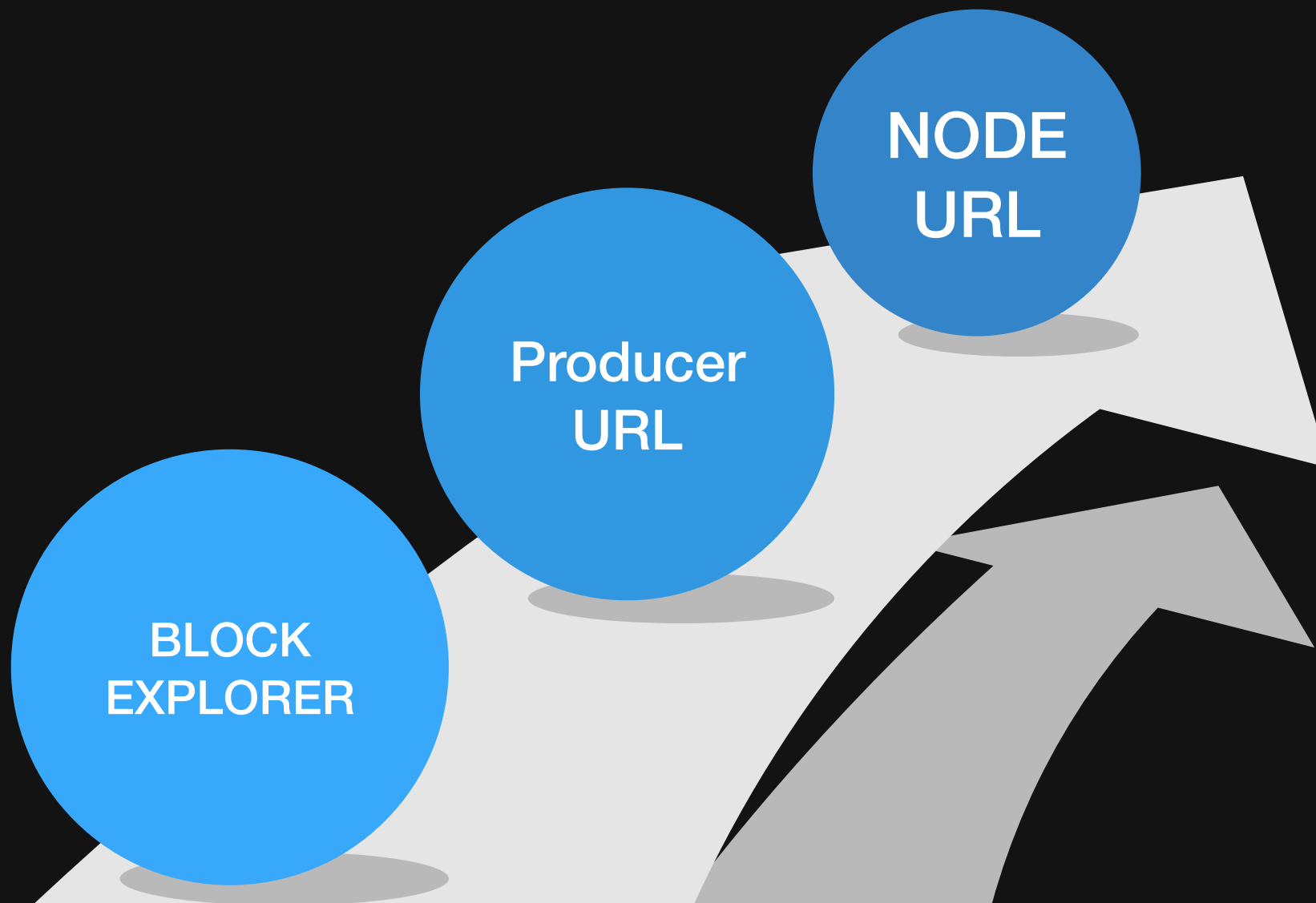
Evaluation

Conclusion



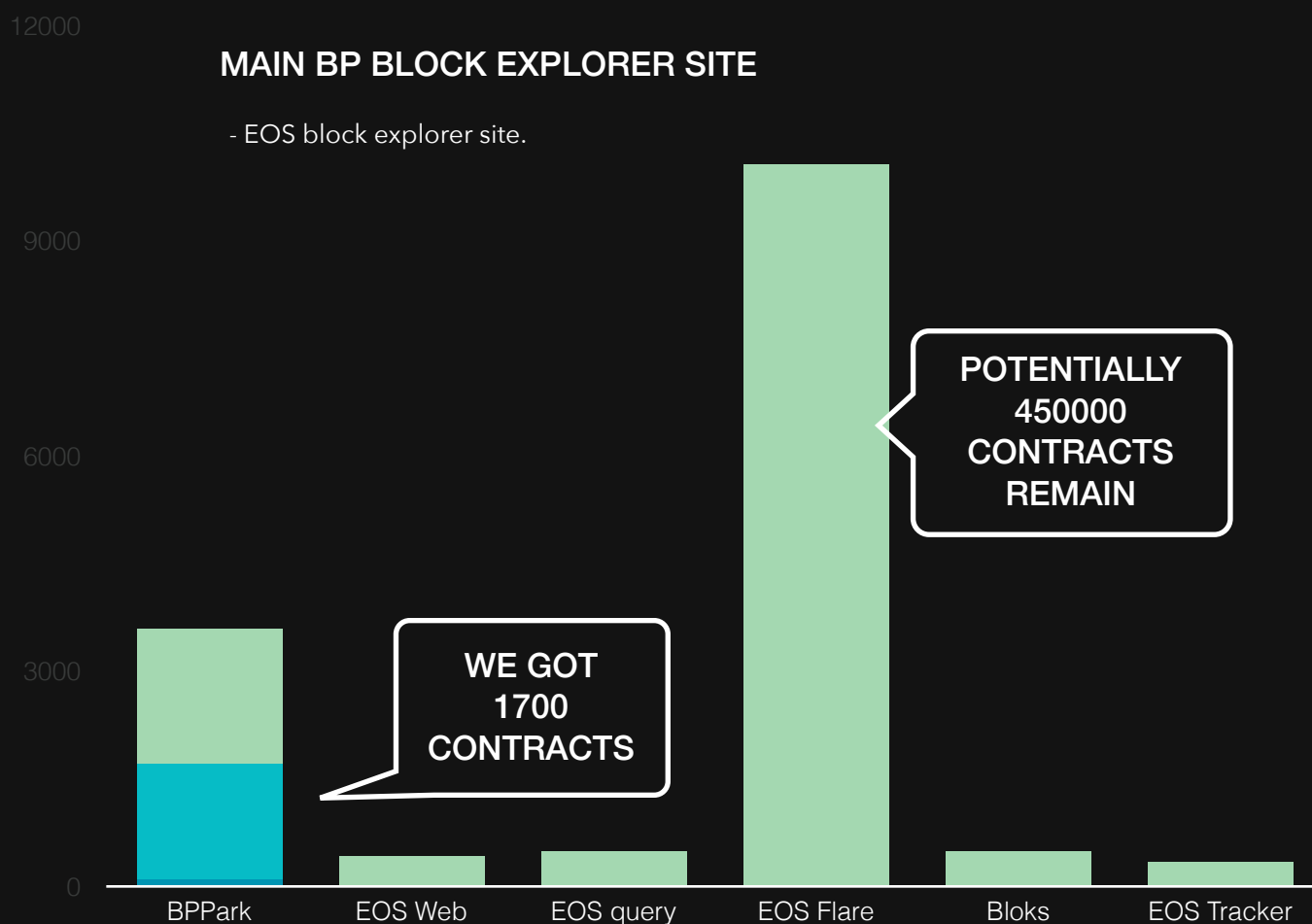


Implementation (Crawler)



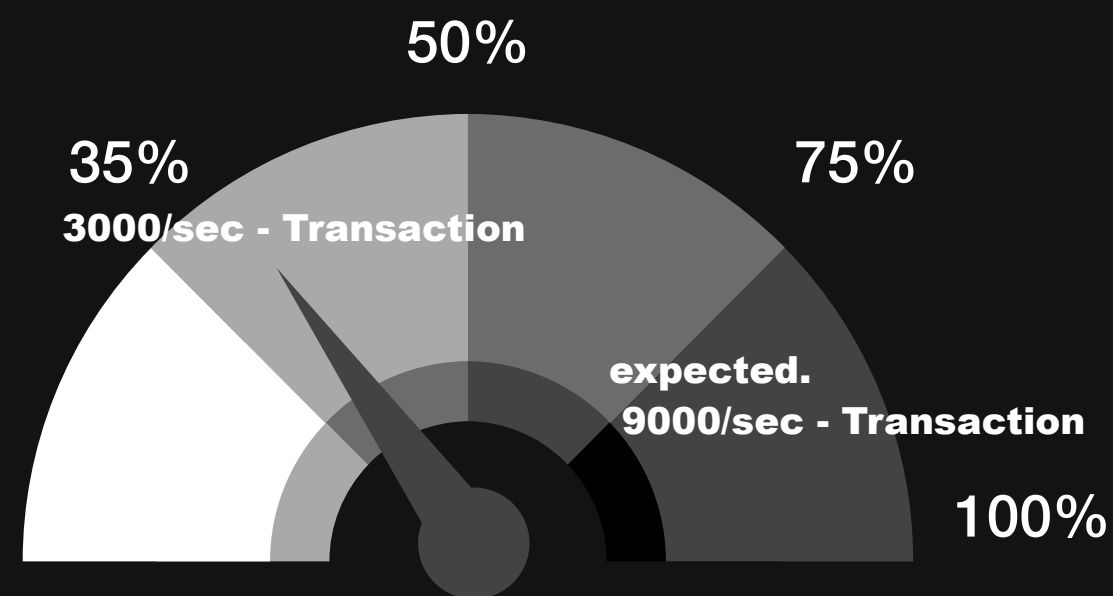


Evaluation



Fuzzing system spec

- Ubuntu Base
- 12Core
- 64GB RAM
- 100 Docker Container





Evaluation

saykim (saykim)

102
Reputation

-
Rank

#411367 **Memory corruption via Uninitialized pointer free in EOS node**

State

● Duplicate (Closed)

Reported To

[Block.one](#)

Asset

<https://github.com/EOSIO/eos>
(Source code)

Weakness

Memory Corruption - Generic

Severity

Critical (9.3)

Participants

Duplicate Of

[#388522](#)

Visibility

Private

Collapse

hokiecsgrad posted a comment.

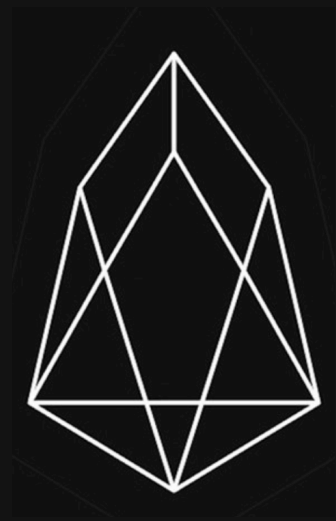
Sep 29th (2 months ago)

We have reviewed this report and, unfortunately, it's a duplicate of a previously submitted report. I'll link to the duplicate momentarily.

hokiecsgrad closed the report and changed the status to ● Duplicate ([#388522](#)).

Sep 29th (2 months ago)

We found a bug, but it's duplicated, F-WINE is still running!



Question & Answer
