Quarkslab

Map your Firmware!

Eloïse Brocas | Pass The Salt 2023

Introduction

Whoami

- Security R&D Engineer
  - @ Quarkslab
  - Automated Analysis Team

Agenda

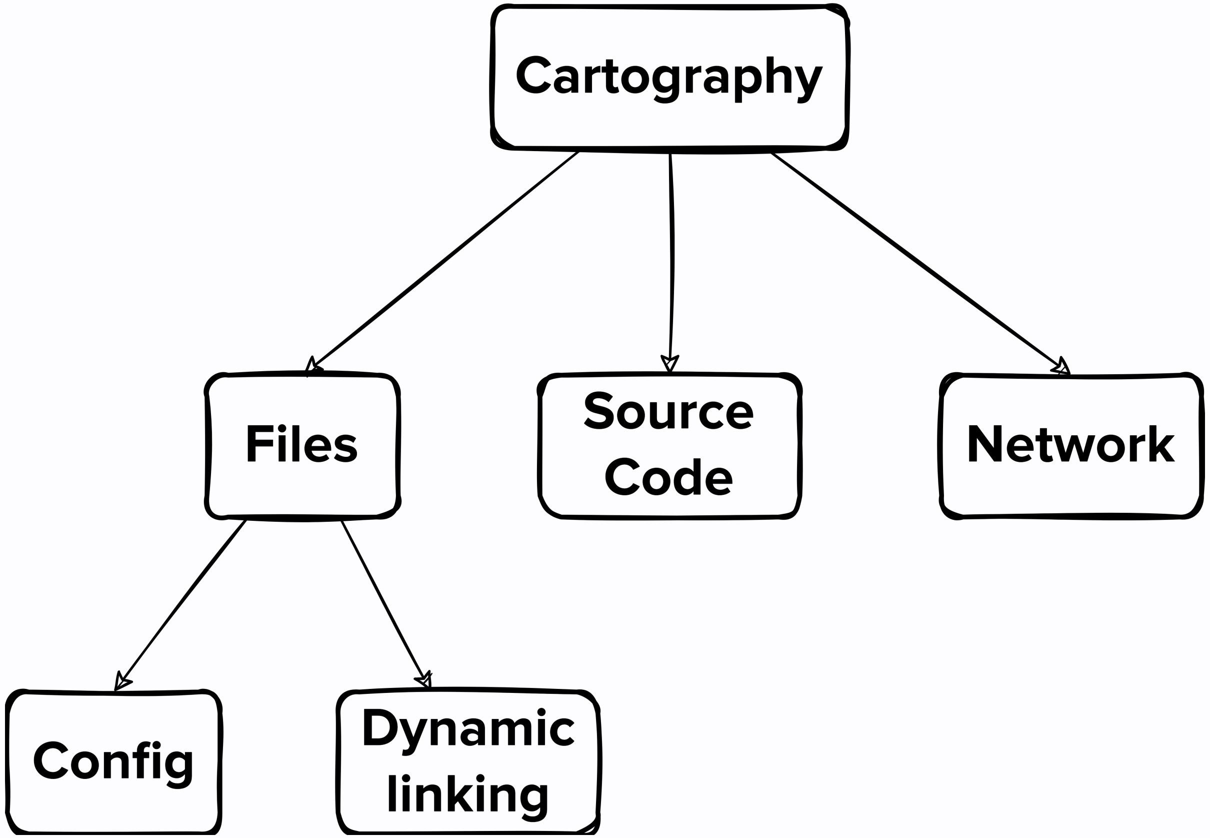
- The problem
- Extending existing tools
- Pyrrha

Firmwares

- embedded into IoT objects
    - routers
    - smartphones
    - automotive
- complete OS (Android, Linux, OpenWRT, ...)
- *structured firmwares*
    - filesystem
    - thousands of files

Cartography

Goal: understand interactions between components



Cartography

Files

Source Code

Network

Config

Dynamic linking

Visualization is the key

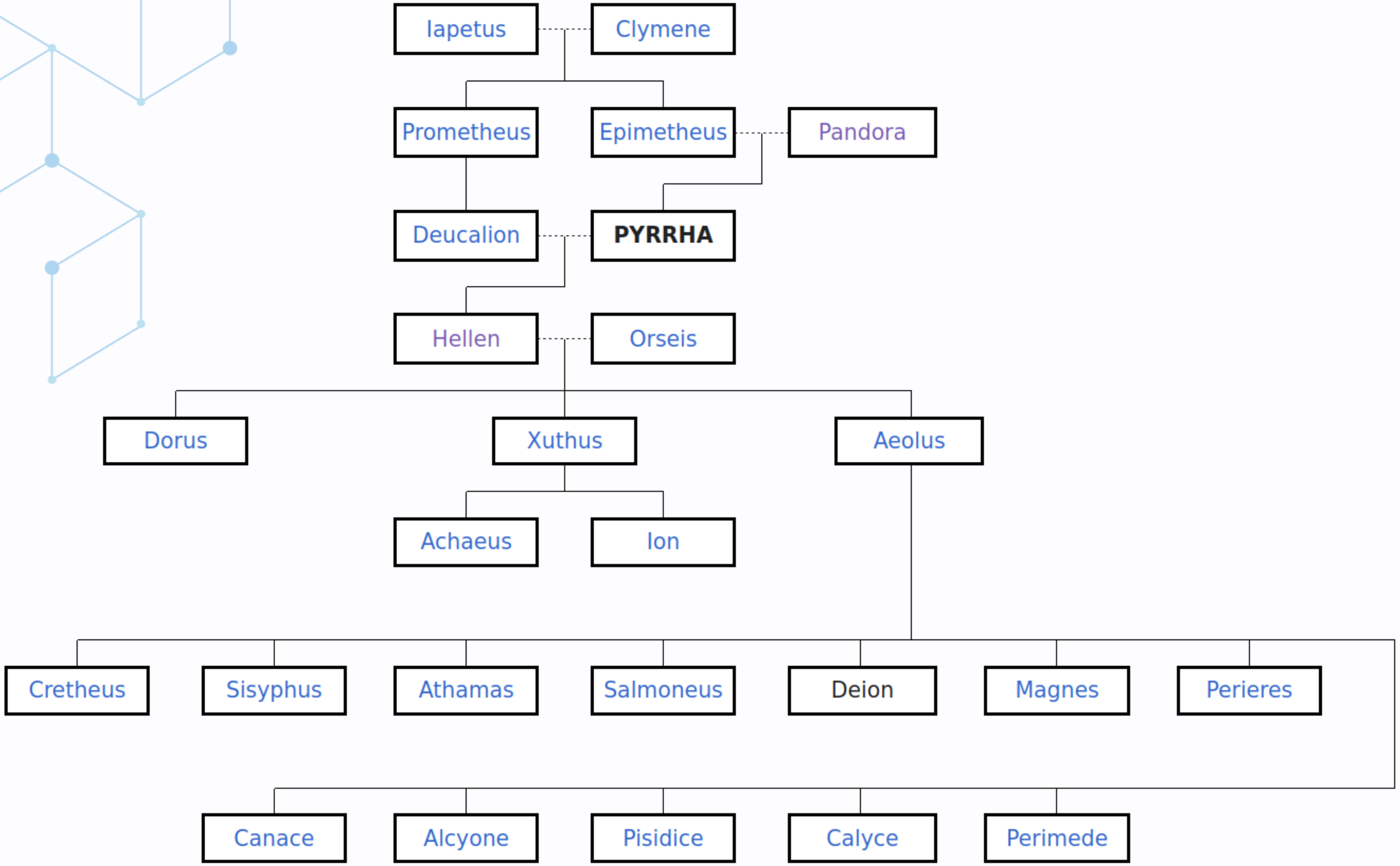
«[1.7.2] And Prometheus had a son Deucalion. He reigning in the regions about Phthia, married Pyrrha, the daughter of Epimetheus and Pandora, the first woman fashioned by the gods. And when Zeus would destroy the men of the Bronze Age, Deucalion by the advice of Prometheus constructed a chest, and having stored it with provisions he embarked in it with Pyrrha. But Zeus by pouring heavy rain from heaven flooded the greater part of Greece, so that all men were destroyed, except a few who fled to the high mountains in the neighborhood. It was then that the mountains in Thessaly parted, and that all the world outside the Isthmus and Peloponnese was overwhelmed. But Deucalion, floating in the chest over the sea for nine days and as many nights, drifted to Parnassus, and there, when the rain ceased, he landed and sacrificed to Zeus, the god of Escape. And Zeus sent Hermes to him and allowed him to choose what he would, and he chose to get men. And at the bidding of Zeus he took up stones and threw them over his head, and the stones which Deucalion threw became men, and the stones which Pyrrha threw became women. Hence people were called metaphorically people (laos) from laas, “a stone.” And Deucalion had children by Pyrrha, first Hellen, whose father some say was Zeus, and second Amphictyon, who reigned over Attica after Cranaus; and third a daughter Protogenia, who became the mother of Aethlius by Zeus

[1.7.3] Hellen had Dorus, Xuthus, and Aeolus by a nymph Orseis. Those who were called Greeks he named Hellenes after himself, and divided the country among his sons. Xuthus received Peloponnese and begat Achaeus and Ion by Creusa, daughter of Erechtheus, and from Achaeus and Ion the Achaeans and Ionians derive their names. Dorus received the country over against Peloponnese and called the settlers Dorians after himself. Aeolus reigned over the regions about Thessaly and named the inhabitants Aeolians. He married Enarete, daughter of Deimachus, and begat seven sons, Cretheus, Sisyphus, Athamas, Salmoneus, Deion, Magnes, Perieres, and five daughters, Canace, Alcyone, Pisidice, Calyce, Perimede.

Perimede had Hippodamas and Orestes by Achelous; and Pisidice had Antiphus and Actor by Myrmidon. »

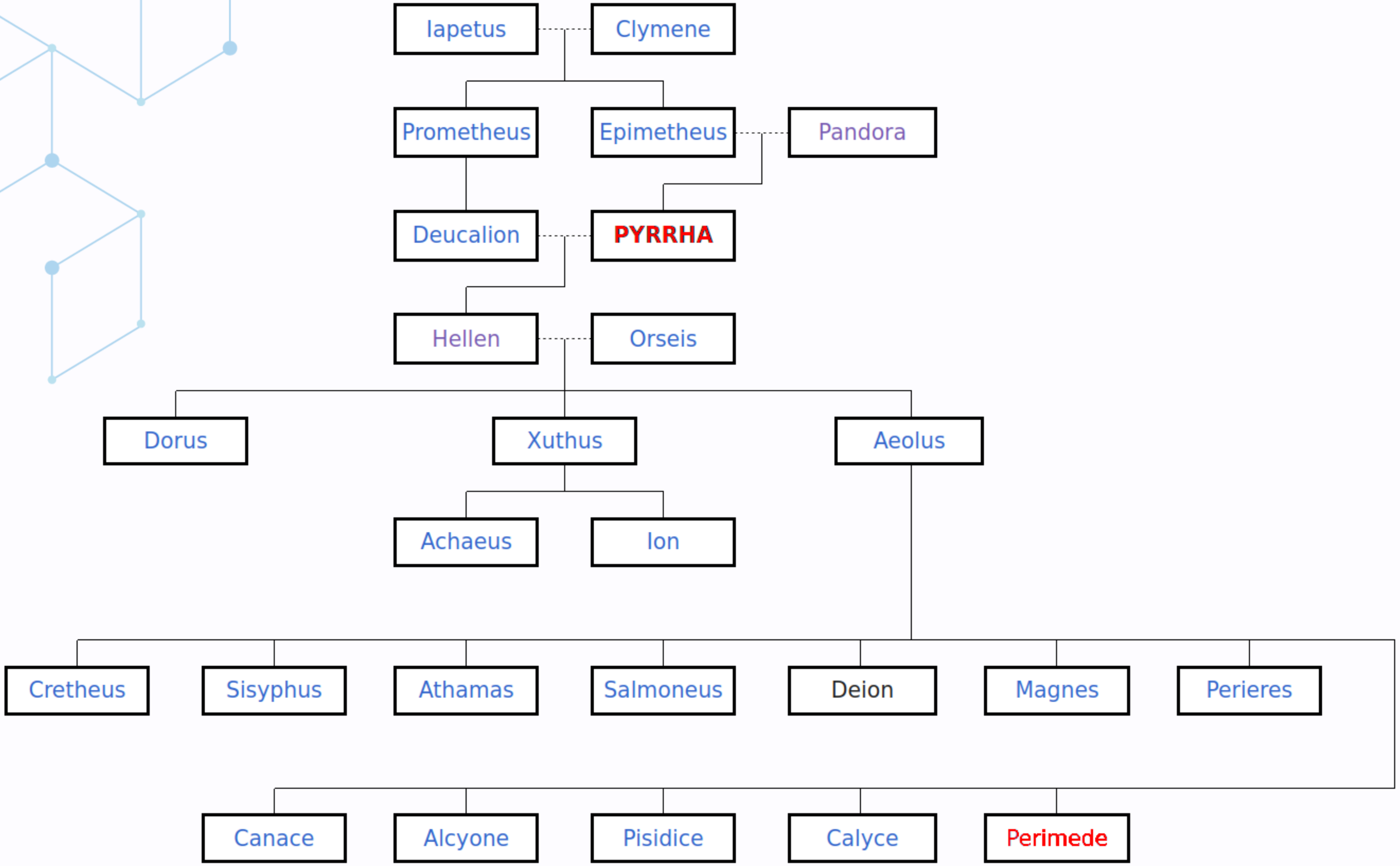
Apollodorus, 1.7.[2-3].

Visualization is the key



Genealogy of Hellenes. Source: Wikipedia.

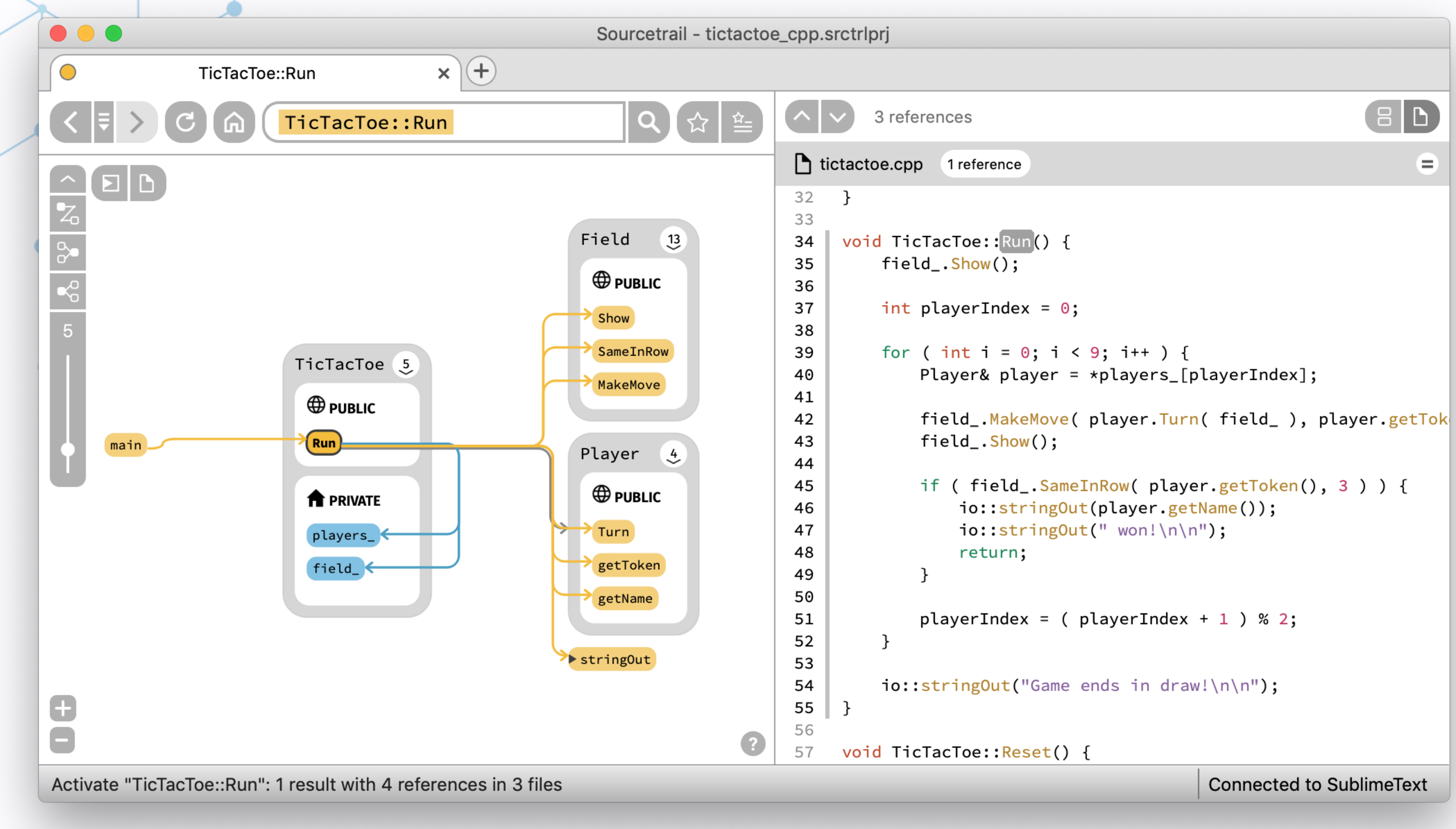
Visualization is the key



Genealogy of Hellenes. Source: Wikipedia.

Let's try not to reinvent the wheel!

Sourcetrail



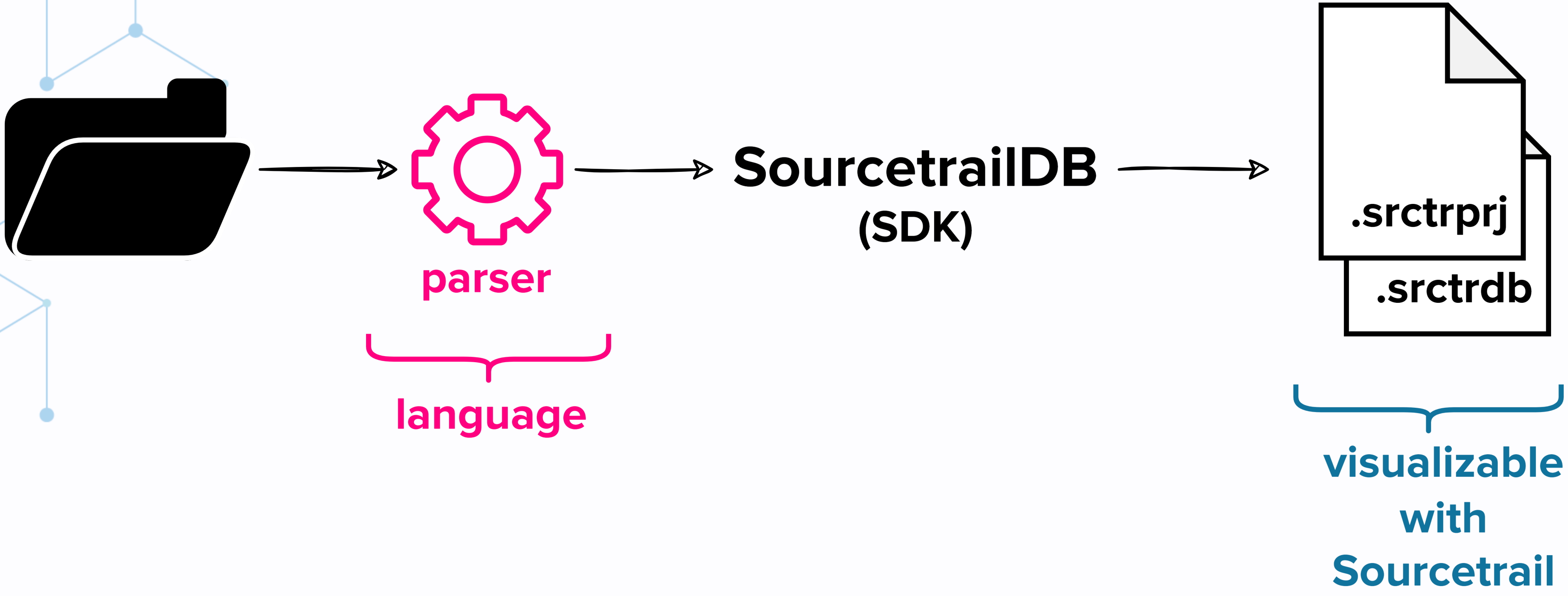
```
}

void TicTacToe::Run() {
    field_.Show();

    int playerIndex = 0;

    for ( int i = 0; i < 9; i++ ) {
        Player& player = *players_[playerIndex];

        field_.MakeMove( player.Turn( field_ ), player.getTok
        field_.Show();

        if ( field_.SameInRow( player.getToken(), 3 ) ) {
            io::stringOut(player.getName());
            io::stringOut(" won!\n\n");
            return;
        }

        playerIndex = ( playerIndex + 1 ) % 2;
    }

    io::stringOut("Game ends in draw!\n\n");
}

void TicTacToe::Reset() {
```

Activate "TicTacToe::Run": 1 result with 4 references in 3 files

Connected to SublimeText

Source: Sourcetrail README.

Extend Sourcetrail



parser

language

SourcetrailDB

(SDK)

.srctrprj

.srctrdb

visualizable with Sourcetrail

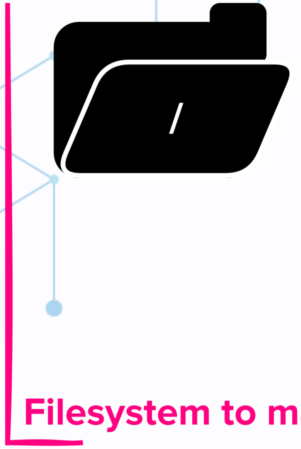
Pyrrha

Filesystem as a language

Binaries	Symlinks
`Class`	→ `TypeDef`

Exported functions	Exported symbols
`function`	`variable`

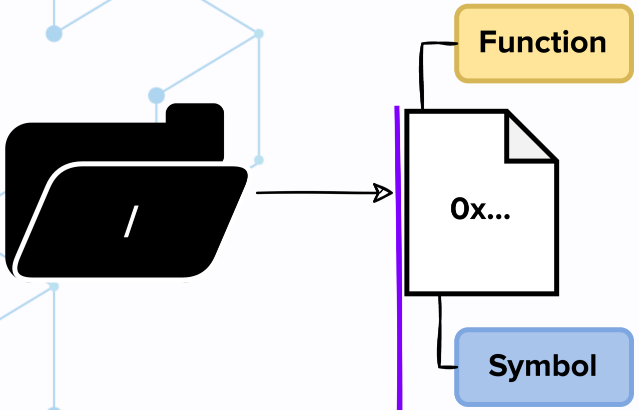
Pyrrha workflow



Filesystem to map

- already extracted
- entry: root directory

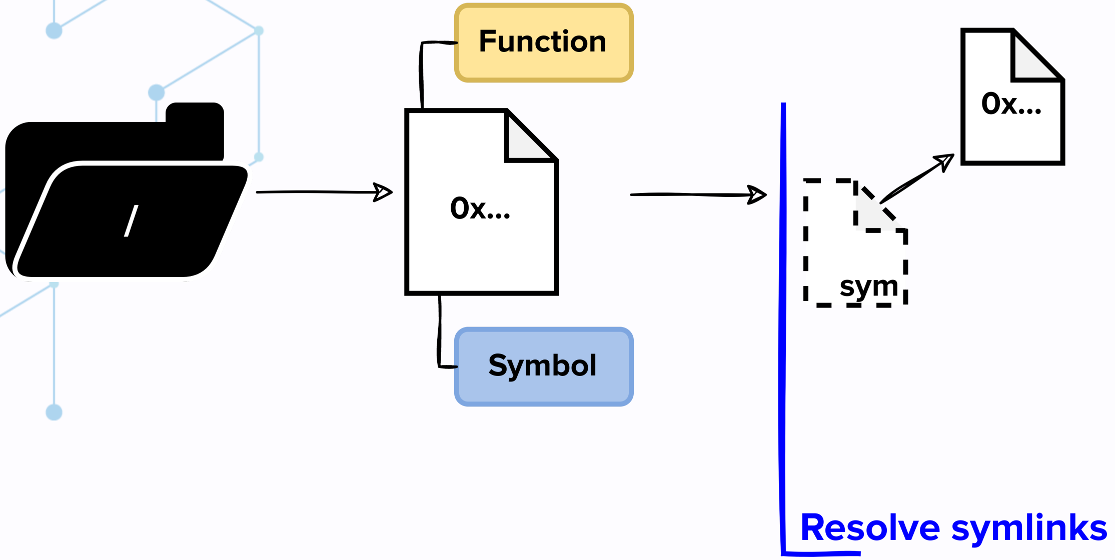
Pyrrha workflow



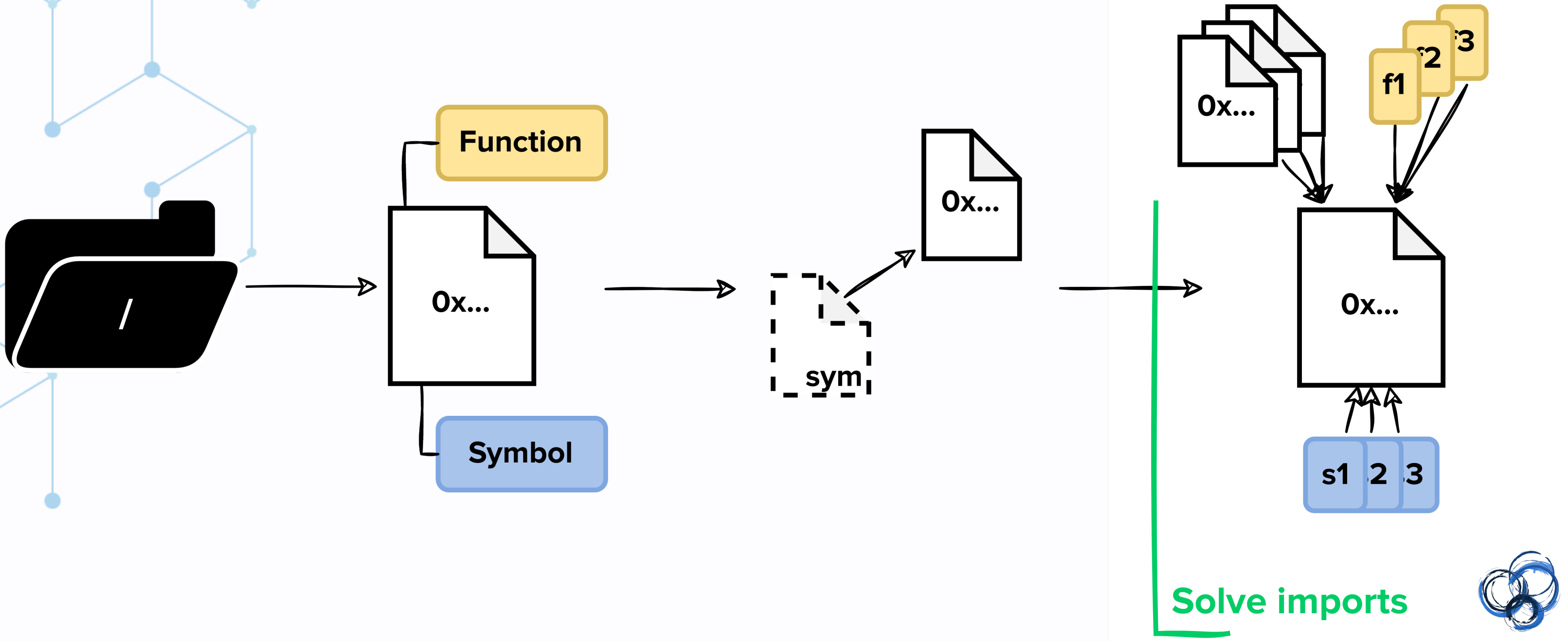
Iterate binaries

- Exported symbols
- Exported functions

Pyrrha workflow



Pyrrha workflow



Solve imports

- Imported libraries
- Imported symbols and functions

Demo Time

2 steps

```
Usage: pyrrha [OPTIONS] ROOT_DIRECTORY

  Map a filesystem into a sourcetrail-compatible db.

Options:
  --db PATH  Sourcetrail DB file path (.srctrldb).  [default: pyrrha.srctrldb]
  --help     Show this message and exit.
```

```
$ pyrrha --db test.srctrldb root-fs
$ sourcetrail test.srctrlprj
```

Conclusion

- Python Package / Docker
- Available on Quarkslab's Github: https://github.com/quarkslab/pyrrha

Thank you!

ebrocas@quarkslab.com

@_cryptocorn_