DSbD Programme – Digital Catapult Cohort 2 Tier 1

KATLAS Technology

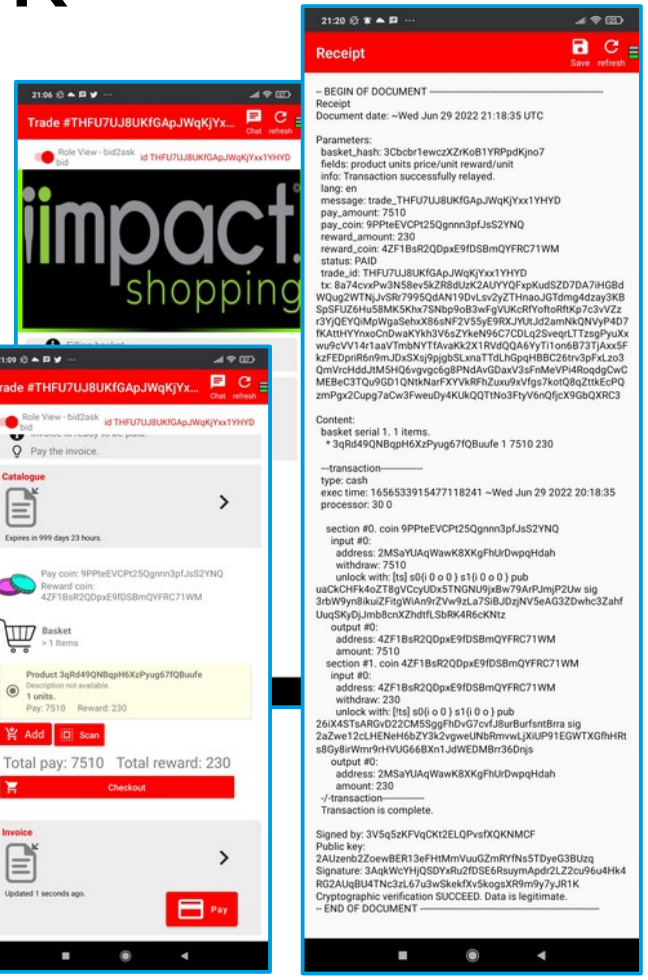
WEB3 - Privacy wallets

Marcos Mayorga
CTO at KATLAS Technology

KATLAS
Accelerating innovation

KATLAS network

- Cryptocurrency protocol. Settlement.
- Smart wallets with trading role-2-role trading protocols.



Source Code

GitHub

https://github.com/root1m3/plebble

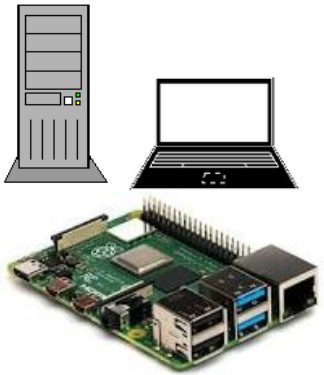
Android App

Google play

KATLASNET

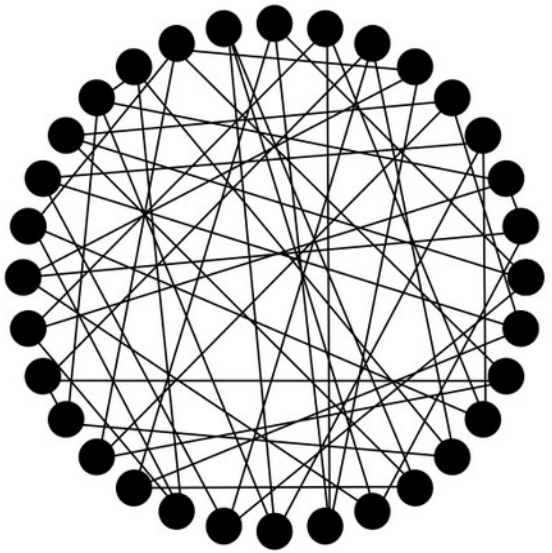
KATLAS
Accelerating innovation

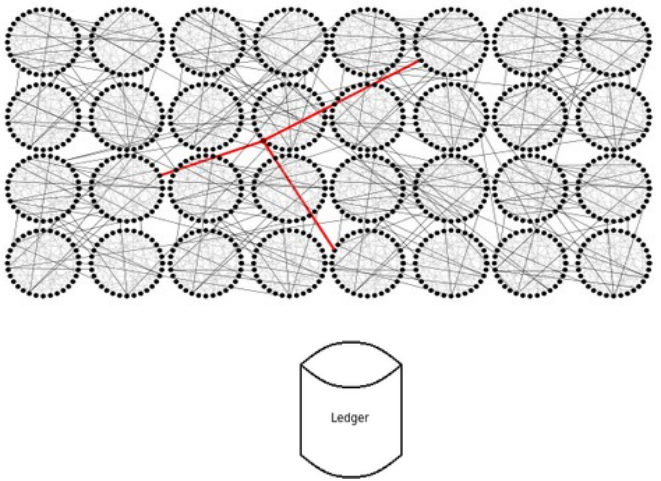
KATLAS network



Node

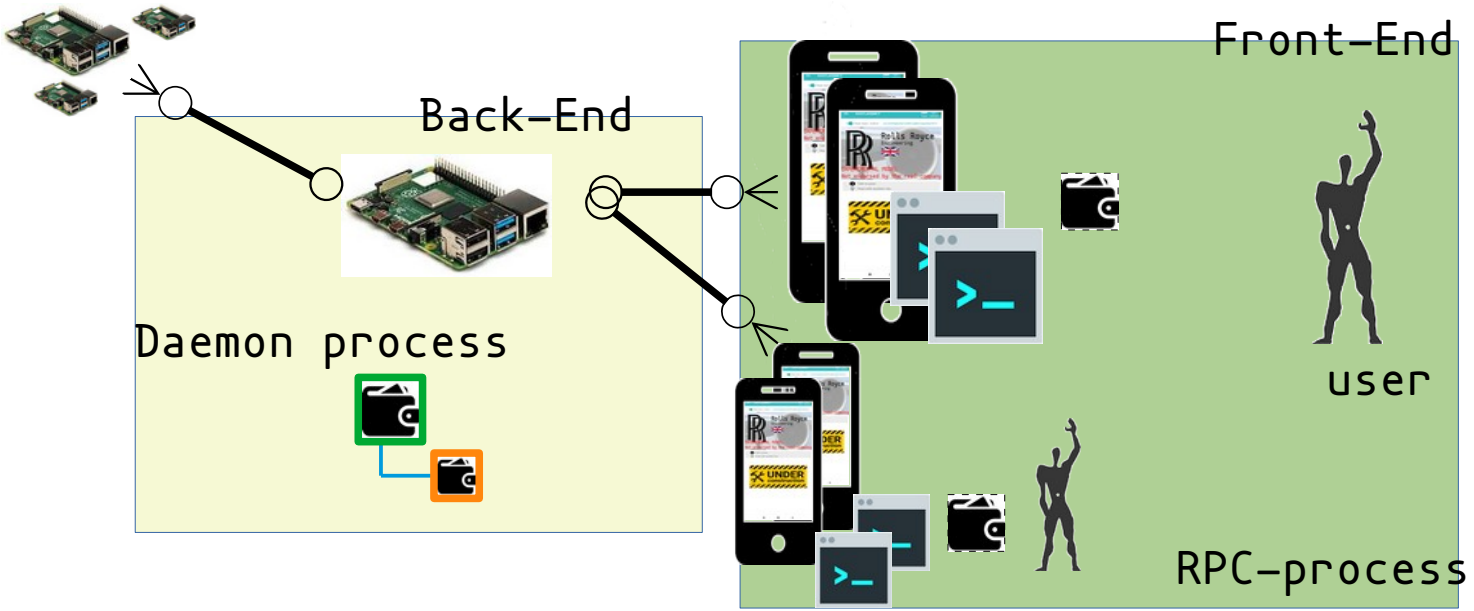
P2P Network





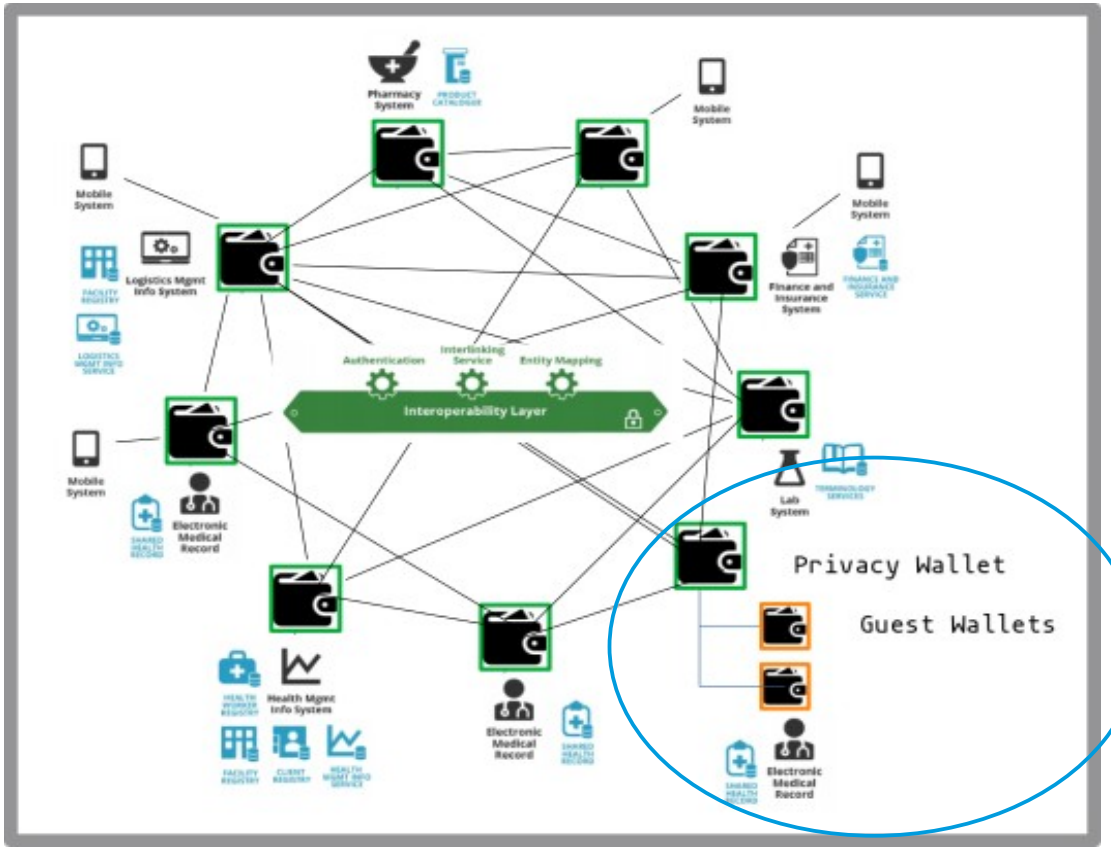
KATLAS
Accelerating innovation

wallet



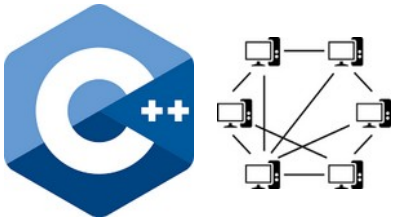
KATLAS
Accelerating innovation

wallet



KATLAS
Accelerating innovation

wallet



Daemon - user private data

- 1- User authentication → 64 bit id → Worker thread.
- 2- API request → Access to user wallet → Response

Risks:

- Code flaw could leak data from other user’s wallet.
- Today’s flawless code could contain a flaw tomorrow.

KATLAS
Accelerating innovation

System tests – purecap ~50K LoC

- RPC API calls
- Threads
- TCP/IP sockets
- Cryptography (ECC, DSA, AES, HASH)
- B58 Encoder/decoder. Binary serialization.
- String manipulation (trim, split, replace, ...)

Detected transmission of pointers via IPC. Got provenance failure exception.

Once fixed...

package zstd

- root@cheripleb:~ # zstd /etc/motd.template
- zstd: error 11 : Allocation error : not enough memory
- morello/cheribsd
- qemu-riskv64-purecap/cheribsd

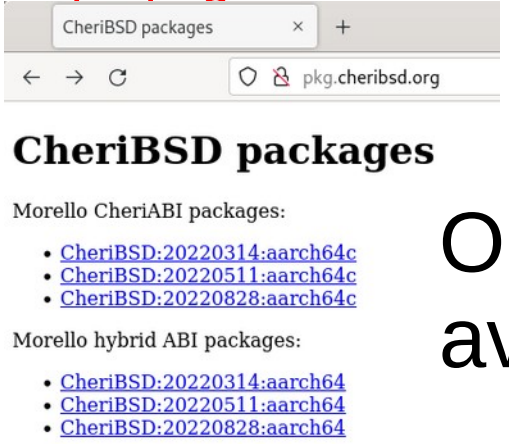
cheribuild.py - riscv

git clone https://github.com/CTSRD-CHERI/cheribuild

./cheribuild.py run-riscv64-purecap -d

root@cheribsd-riscv64-purecap:~# **pkg64c install** git

Error fetching http://pkg.CheriBSD.org/CheriBSD:20220828:riscv64c/Latest/pkg.txz



Only aarch64/aarch64c ports are available

KATLAS
Accelerating innovation

TEE

wallet

CHERI / CheriBSD / Morello

Risks we'd like to reduce using compartmentalization:

- Code flaw could leak data from other user's wallet.
- Today's flawless code could contain a flaw tomorrow.

- How to guarantee that users can only access the right wallet...
- Even when evil users take advantage of current (or future) flaws in the code, gaining -anyhow- access to other's wallet.

KATLAS
Accelerating innovation

TEE

Compartmentalization models

CHERI / CheriBSD / Morello

- Shared library compartments.
  We need more granularity → C++ Objects.

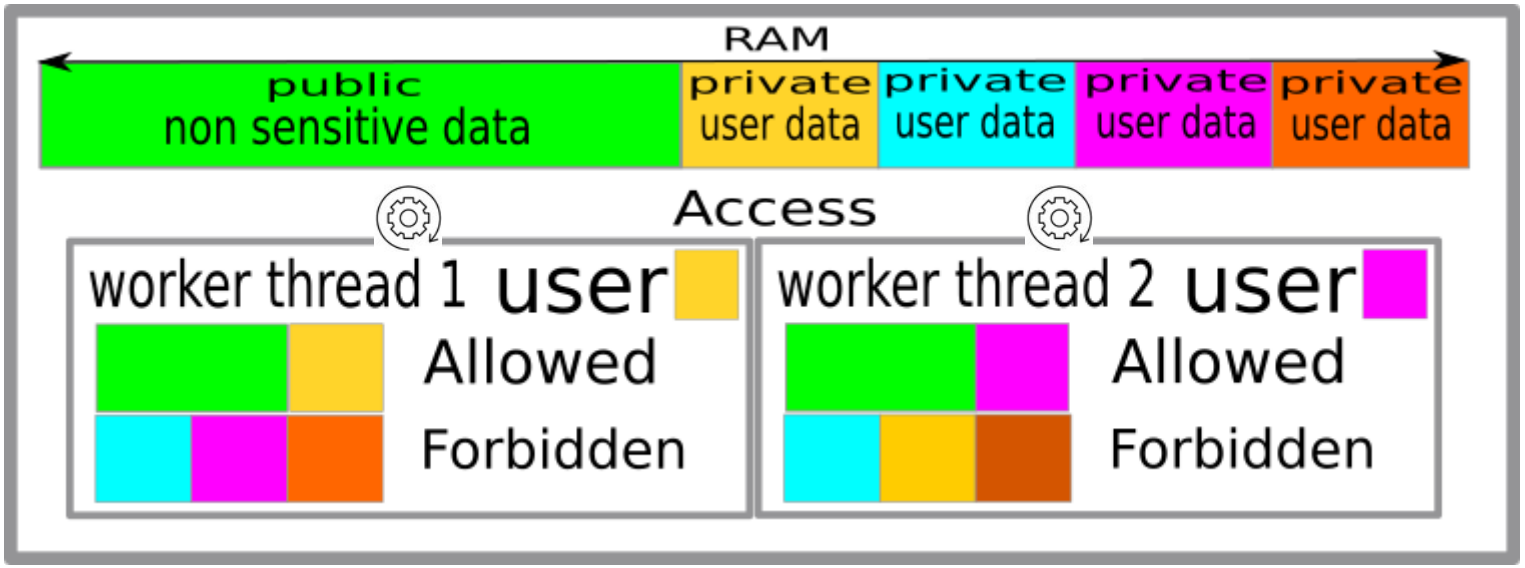
- Enclaves, Protection domains, trampolines
  Requires a significant software refactoring effort.
  → allocators, sealed capabilities

- We are figuring out how to achieve a model that:
  mitigates aforementioned risks
  minimizes development effort, easiest change

KATLAS
Accelerating innovation

TEE

wallet

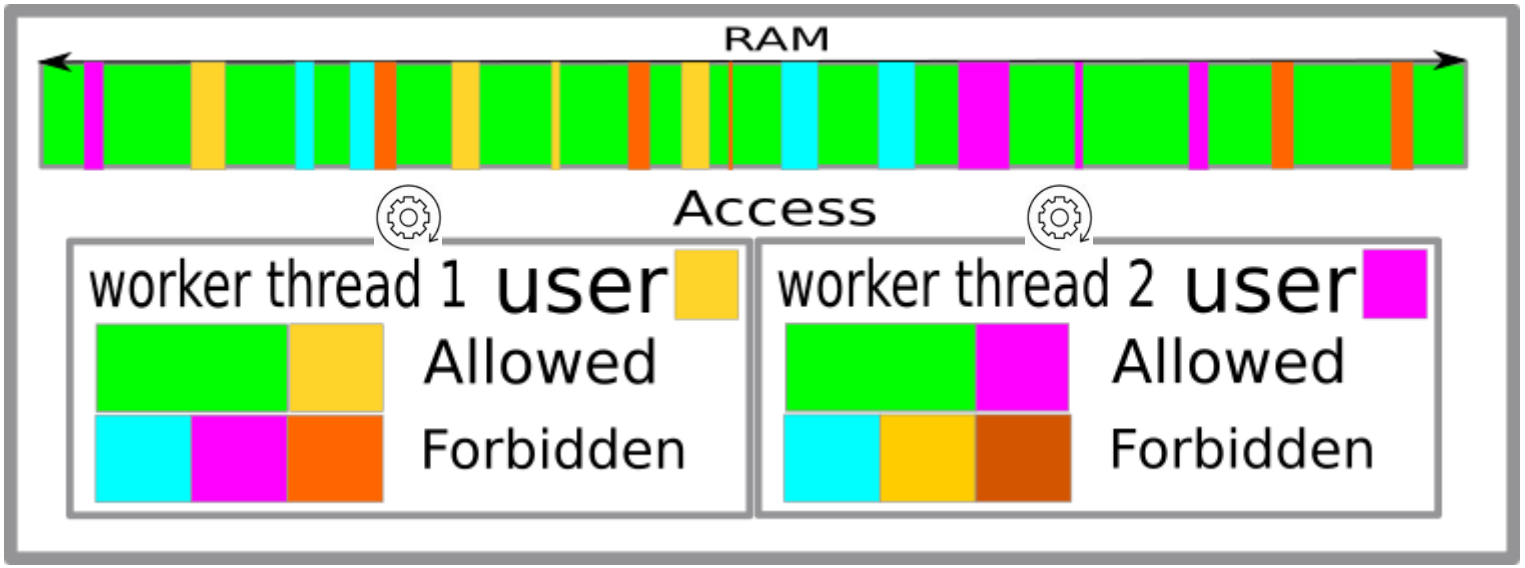


Coloured compartments

KATLAS
Accelerating innovation

TEE

wallet



Coloured fragmented compartments

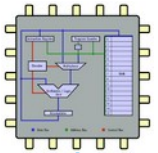
KATLAS
Accelerating innovation

TEE

CPU

RAM

Execution thread



Load 64 bit id into register

New C++ object – **encode** id

Access/dereference
C++ object

Reg Id !- cap Id ?

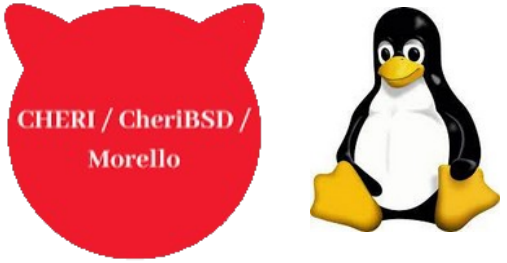
→

raise PROT Exception

KATLAS
Accelerating innovation

Continuity

- Privacy++ wallets
  featuring compartmentalized wallets with CHERI



- KATLAS W3 Privacy router.

  Internet router + P2P Node + family/business wallets in one computer.


UK Research and Innovation
CATAPULT Digital
CHERI / CheriBSD / Morello
KATLAS
Accelerating innovation
Thank you !
This presentation URL
https://katlastechnology.com