WP2 - Scalability and distributed Bigdata

Marc X. Makkes

Email: m.x.makkes@vu.nl

WP2 Status

"Scalability and distributed Bigdata"

- A1: Reduced resource requirements for blockchain clients.
- A2: Blockchain bootstrapping mechanism for clients.
- A3: High performance cryptographic primitives using accelerators

Marc X. Makkes (AP @ Vrije Universiteit, but currently @ CWI)

Research output:

[KBWM20] The Banking Industry Underestimates Costs of Cloud Migrations

[KGWM20] Governance in peer-to-peer networks is a design problem

[KGWM19] Exploring governance in a decentralized energy trading eco-system

[DMUWB19] Aves: A decision engine for energy-efficient stream analytics across low-power device.

[MD19] Apex: a High-Performance Hierarchical Distributed Ledger

[DMRTV19] Dietcoin: Hardening Bitcoin Transaction Verification Process For Mobile Devices.

WP2 Research Output:

Blockchain bootstrapping & reducing storage requirements

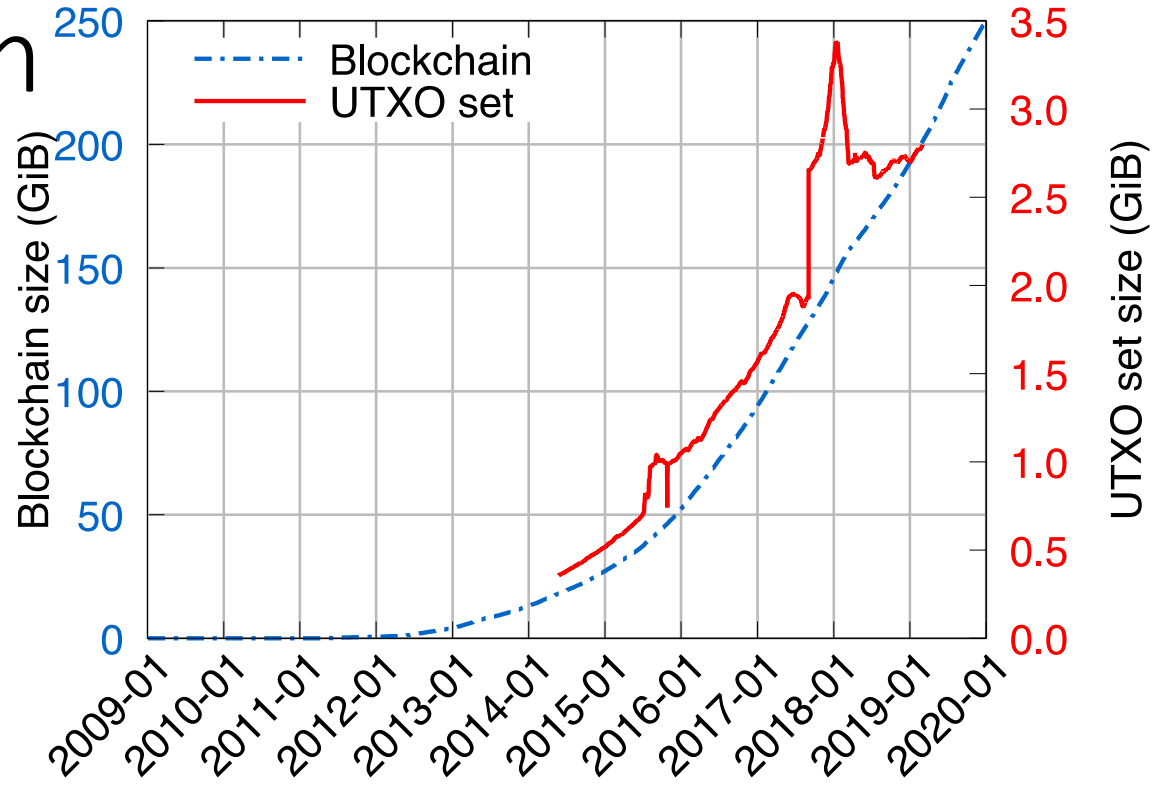
WP2 – Blockchain

- Blockchains are essentially a distributed database.
- A Block consists of a list of transactions.
- Blocks are sent every ~10 minutes.
- The maximum block-size is currently ~2M bytes.
- Every block has a fingerprint that of the previous block.
- And a solution to a very hard puzzle.

1. Clients verify transactions in a new block using there local databases (called State or UTXO set).
2. If correct, the clients update there local database.
3. Clients keep blocks for replication purposes.

WP2 A1 & A2 - Problem

- Blockchains grow endlessly.
- Big problem for small devices (IoT)
  - Many devices have only a small amount storage (**A1**).
  - Processing all transactions requires weeks or months to participate actively(**A2**).



Dietcoin: Blockchain for IoT

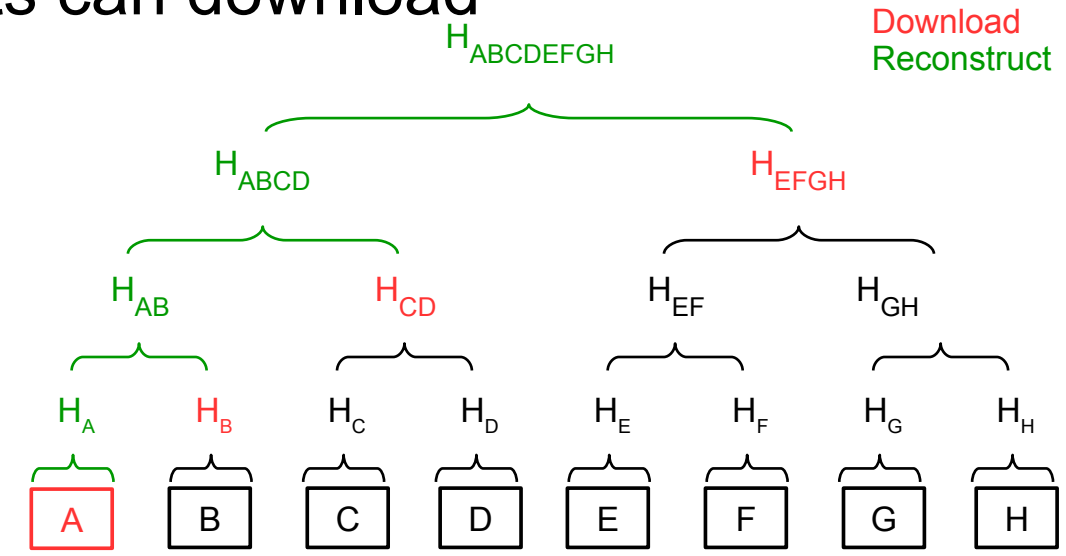
- Generic Blockchain technology
- Applied to Bitcoin.
  - Data set of 250+ GB Transaction log and 4+ GB State

Solution.

Make blockchain state queryable.

Solution – Dietcoin

- Create state database, based on a Merkle-tree
- Each leave (a,b,c,…,h) has a shard with multiple transactions.
- Each block incorporate the root of the hash.
- Dietcoin clients download only headers (45 MByte).
- To verify an interesting transaction, clients can download and verity shards



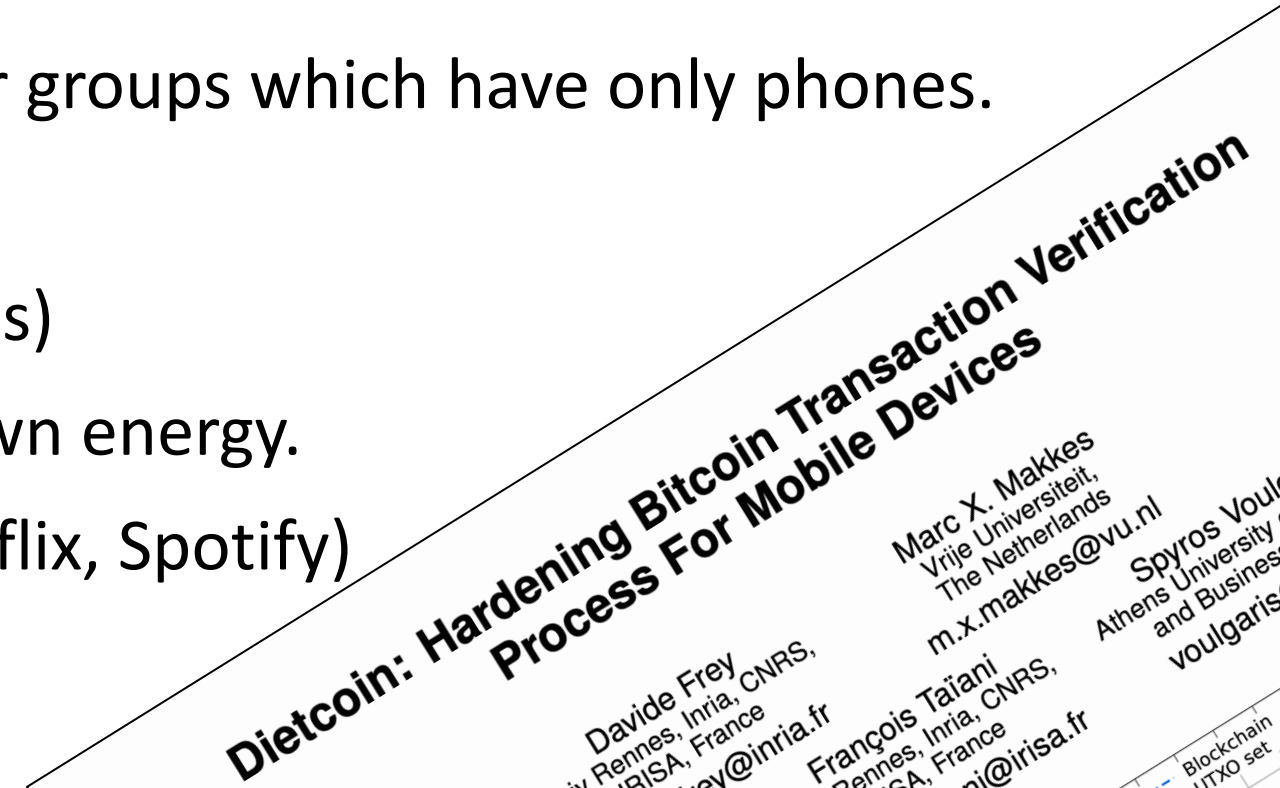
Results Dietcoin:

	Bitcoin	Dietcoin
Bootstrapping	weeks	minutes
Required storage for blockchains	250.000 MB	~45Mb
Required state storage	3.000 MB	0 MB
Cost for verification	0Mb	2-4Mb

Results & Potential Use Cases

- Working prototype, publicly available.
- Paper published in Very Lange DataBases (VLDB).

- Potential; Adaptability by large user groups which have only phones.
- Other applications
  - Pay as you go (lightning services)
    - Solar panels trading their own energy.
    - Streaming applications (Netflix, Spotify)
  - Access devices to buildings.



WP2 Plans

Planning

- Follow-up on A1 & A2 Dietcoin version 2.0 (starts soon)
    - Improve throughput Dietcoin
    - Improve energy efficiency of implementation
    - Addition measurements on different devices

- Start of A3: High performance cryptographic primitives
    - GPUs (AMD/NVIDIA) ~~and Intel XEON PHI~~
    - Improving Secure Multi-Party Computation for KYC risk computation in combination with WP1 Activity 5.
    - Goal to improve throughput and lower latency to enhance the applicability.