Private Names & Some other stuff

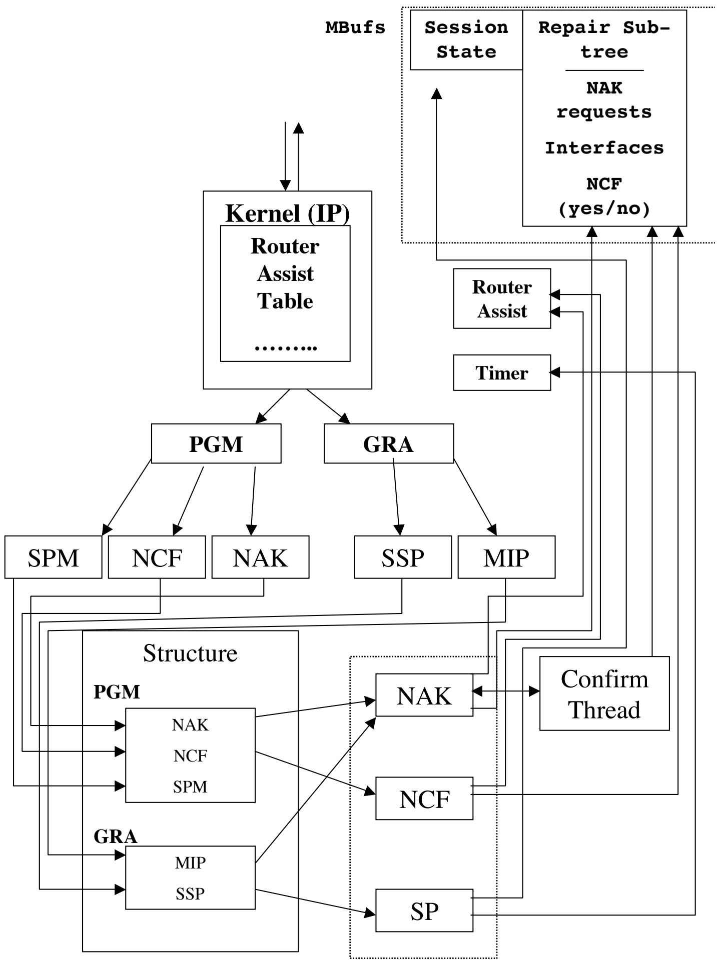
Jon Crowcroft, Cristina Munoz

http://www.cl.cam.ac.uk/~jac22

Past, present, future

- Past
  - TIB, PGM etc
- Present
  - Private Name Spaces and Virtual Private Concent Centric Networks
- Future
  - Distributed Ledger & ICN chains

1. Bit of history: who knows this?



Way back when, Reuters trading…

- TIBCo (The Information Bus Company)
  - Out of Cornell
  - Pub/Sub
  - Content Based Addressing
  - Name Based Routing
- "Multicast" Distribution in net
  - Reuters ran a global trading net & live TV
  - Bit like Bloomberg&others
  - Innovative networking

PGM, routing and congestion ctl

- All scaled very well,Network was global
  - three fold redundant between major stock exchanges
    - 2 terrestrial, one satellite
  - Various clever tricks to manage traffic
    - Including Rizzo's PGM Congestion Ctl
  - Not sure why it isn't all used more ☺
    - Does cost money for router support…
    - Router alert can hit slow path...

To scale the network…

- Used IP multicast, sort of
  - Including PIM & router alerts
  - Name hashes to multicast address
- Cisco et al developed PGM
  - Pragmatic Generalized Multicast (RFC3208)
  - Cross layer transport & forwarding
  - Nack suppressor/aggregator
  - Time based window on retransmission avail
  - Redirect rtx&subscription to local cache

2.Private Name Spaces – what&why

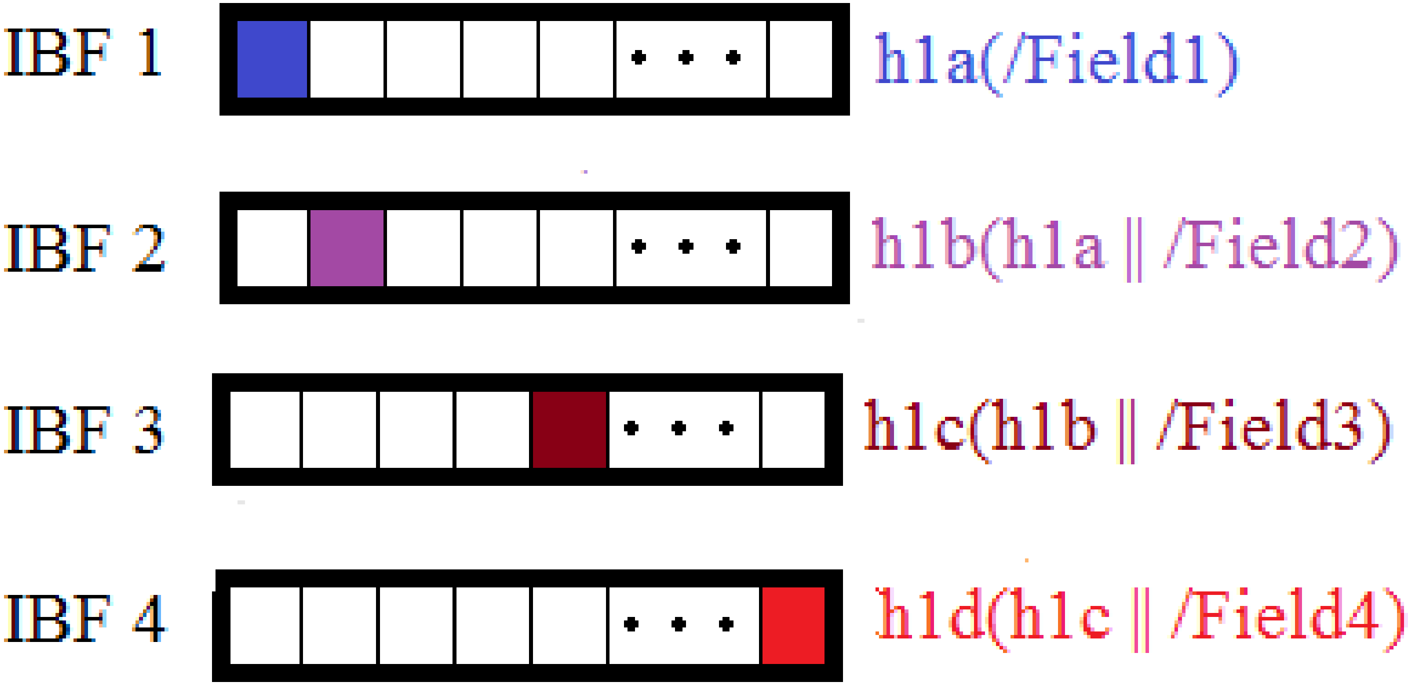
- Names contain rich semantics
  - and so knowing who is interested in which named data can represent an invasion of privacy.
- At the sametime, name structures can help with organising information
  - (ontologies etc) –
- In this talk I'll discuss some ideas about creation and use of private name spaces.

Last year, we presented I(FIB)F

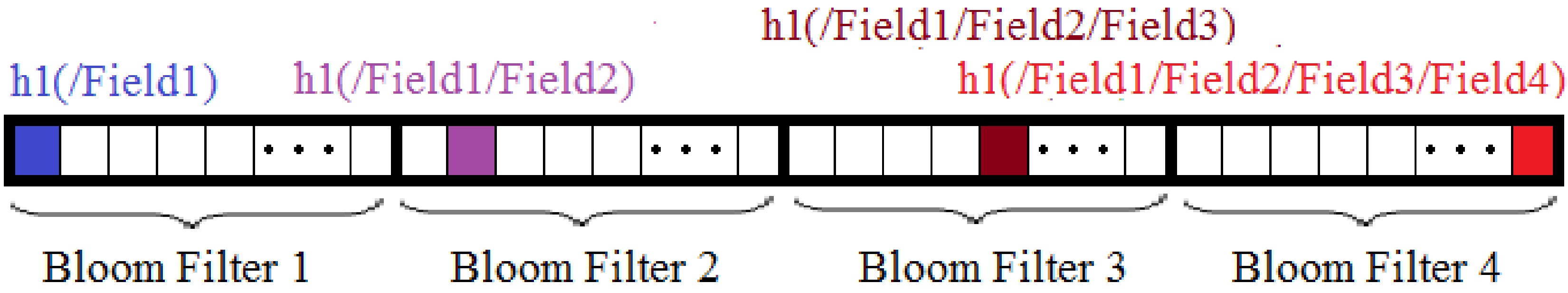
- Iterated bloom filters
  - Multiple iterations over the name
  - Hierarchy -> flat name
  - With low collision probability
  - and lowish space needs
- Can use forvirtual private name space?
  - Requirement is to keep map from name to "routing" field, so we can still cache
  - But keep subscriber/content confidential

Iterated bloom filters ++

Iterated Bloom Filters (IBF)



And vpn


h1(/Field1/Field2/Field3)
h1(/Field1)
h1(/Field1/Field2)
h1(/Field1/Field2/Field3/Field4)
Bloom Filter 1
Bloom Filter 2
Bloom Filter 3
Bloom Filter 4

How to boot this

- Initial idea is to have trusted third party provide a per session/content HMAC and use with the I(FIB)F
    - Upside – simple
    - Downside – needs trusted third party
        - Goes somewhat against *democritization* goal of ICN (as compared to CDN)
        - Could we re-decentralize the session info?...

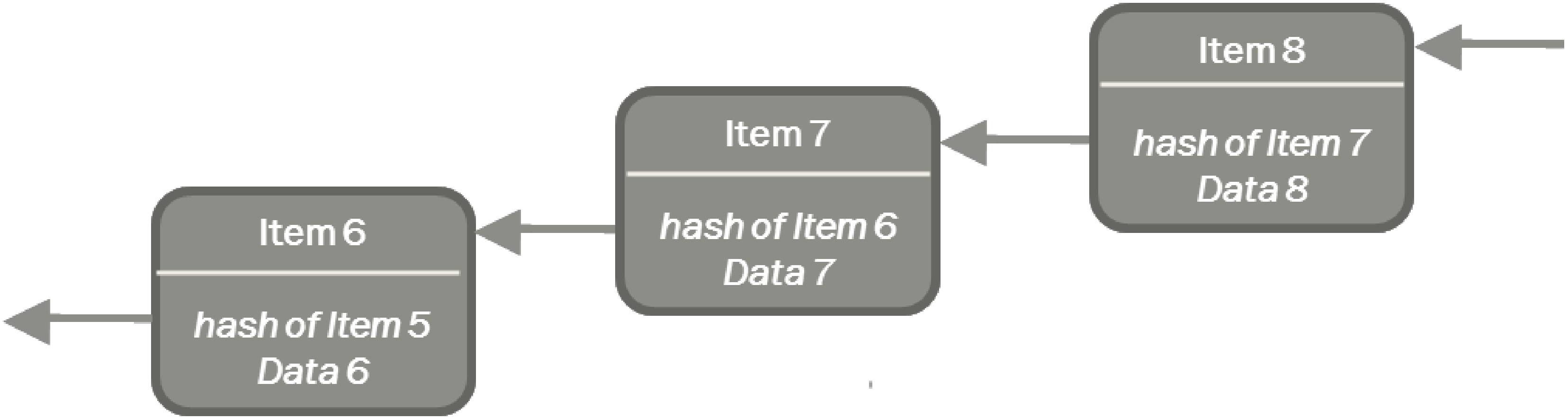
3. DLT

No.	Assumption	Explanation
a)	Long-term persistent, indisputable record	There is a requirement for a long-term persistent, indisputable record of transactions associated with the DLT application.
b)	Associated party or parties can be ascertained	For each transaction, the associated party or parties can be ascertained. This may or may not be as conventional, real-world identities; a pseudonym or digital identity may instead be recorded.

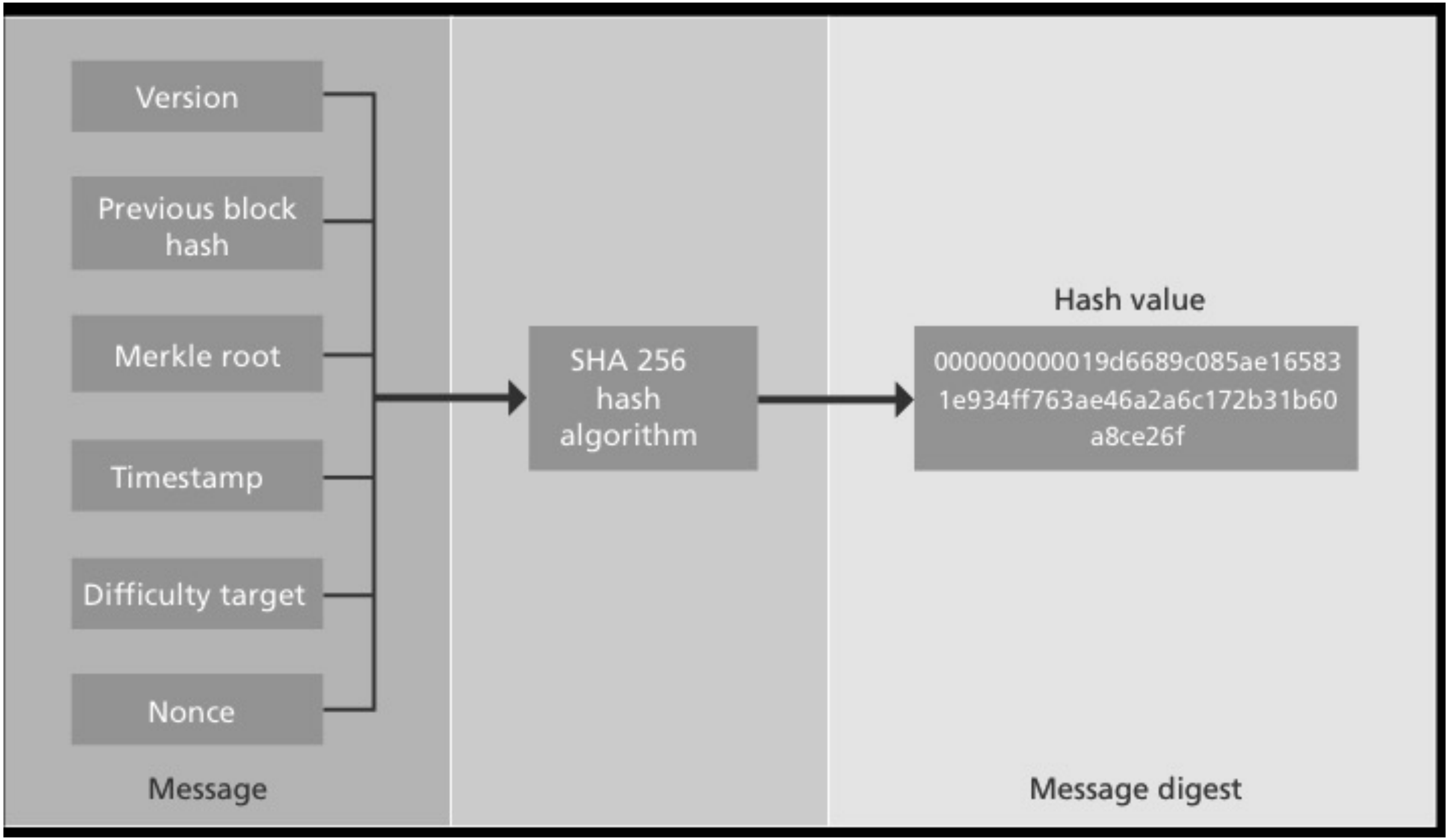
Hash chain

Fig. 1 A tamper-proof chain of Items using hash pointers

Item N hash = hash (Item N data, Item N-1 hash)

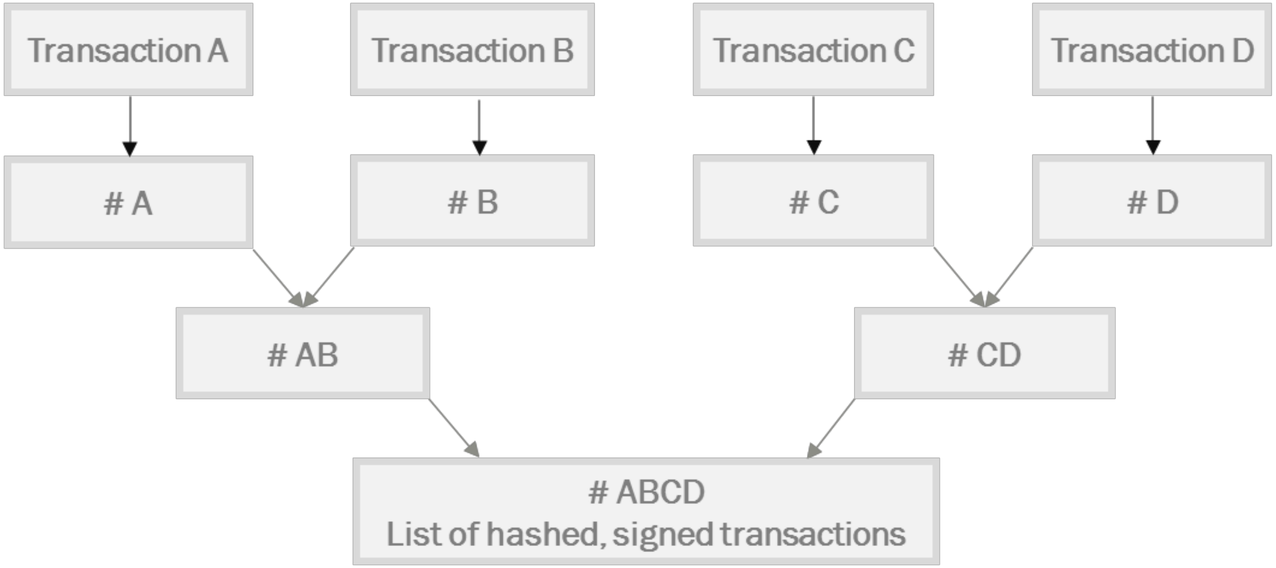


What’s hashed



Immutable bits (c.f. irmin/docker)

Fig 3. A Merkle Tree lists hashed transactions in the body of a block (showing only four transactions)



Permissioned&private

- Need a mix of permissioned & private
  - Permissioned to link dlt to vpndn
  - Private to do re-keying
- Needs more thought ☺

So what could DLT provide for ICN

- Or ICN for DLT

1. Off chain resources (content) in ICN
   - Scalable consensus tools for update e.g. see Canopus at Conext 2017 or Teechan
2. Direct p2p payment, if you really like:
3. Cryptocurrency is the source for HMAC for virtual private name space
   - whether used for payment or not…

Acknowledgements & References

1. Emiliano Cristofaro et al (discussed) https://arxiv.org/abs/1211.5183
2. Fotiou&Polyzos , Securing Content Sharing over ICN, ICN 2016
3. When Encryption is not enough – Tsudik et al, ICN 2017
4. Fotiou&Polyzos: Decentralized name-based Security for content distribution using blockchains, Infocom 2016 workshop

Acknowledgements

- Umobile&Rife EU projects – including discussion with Ionnis Psaras & George Pavlou of UCL of LIRA ephemeral names
- Microsoft Cloud Computing project http://www.mccrc.eu/

Who Am I?

UMOBILE

RIFe

http://www.mccrc.eu/