Beyond Secure Channels:

Cryptography for privacy, anonymity and Digital Currencies

Dr George Danezis

University College London

The new cryptography

- Diffie-Hellman 1976 – public key exchange.
  Rivest-Shamir-Adelman 1978 – encryption & digital signatures.

- Initial focus: secure channels.
  - Alice <-> Bob: Confidentiality, Authenticity, Integrity…

- Subsequent focus: Privacy Enhancing Technologies
  - Anonymous communications
  - Private Statistics and Billing
  - Electronic Cash
  - Cryptographic currencies

Network identity today
Neither privacy nor authenticity / integrity

No anonymity

- Weak identifiers everywhere:
  - IP, MAC
  - Logging at all levels
  - Login names / authentication
  - PK certificates in clear
- Also:
  - Location data leaked
  - Application data leakage

No identification

- Weak identifiers easy to modulate
  - Expensive / unreliable logs.
  - IP / MAC address changes
  - Open Wi-Fi access points
  - Bot-nets
- Partial solution
  - Authentication
- Open issues:
  - DoS and network level attacks

IP packet format

RFC: 791

INTERNET PROTOCOL

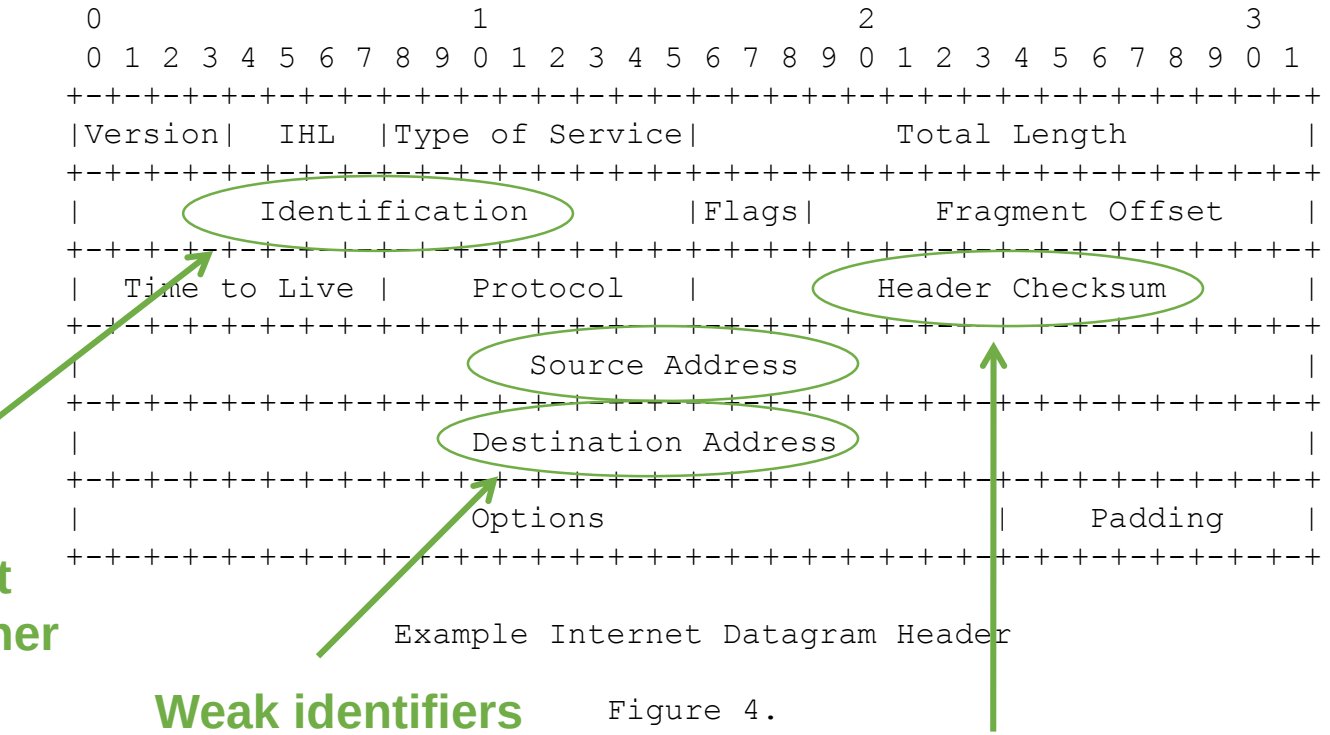
DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

3.1. Internet Header Format

A summary of the contents of the internet header follows:



Example Internet Datagram Header

Figure 4.

Link different packets together

Weak identifiers

No integrity / authenticity

Same for TCP, SMTP, IRC, HTTP, ...

Anonymity in communications

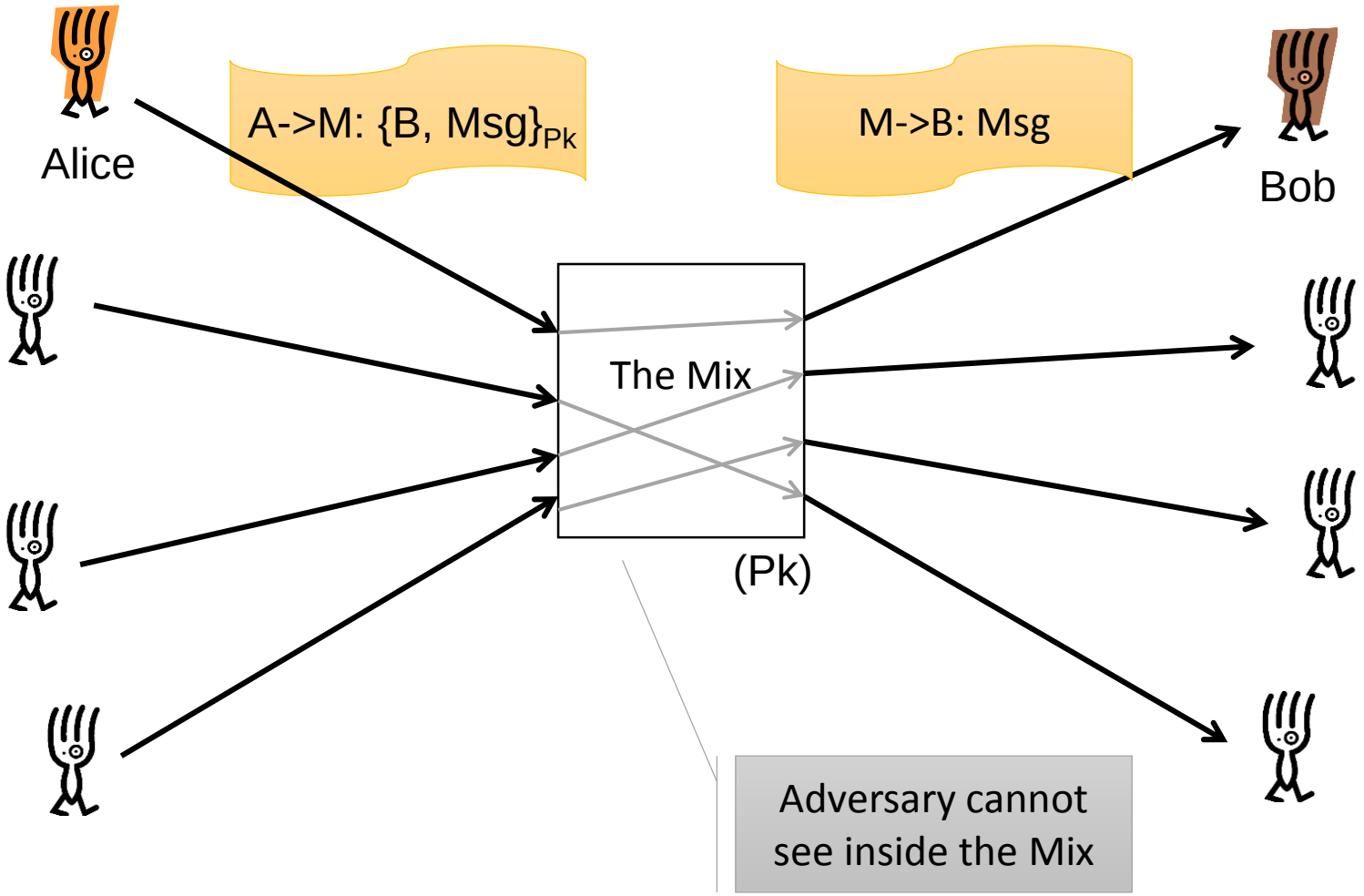
- Specialized applications
  - Electronic voting
  - Auctions / bidding / stock market
  - Incident reporting
  - Witness protection / whistle blowing
  - Showing anonymous credentials!

- General applications
  - Freedom of speech
  - Profiling / price discrimination
  - Spam avoidance
  - Investigation / market research
  - Censorship resistance

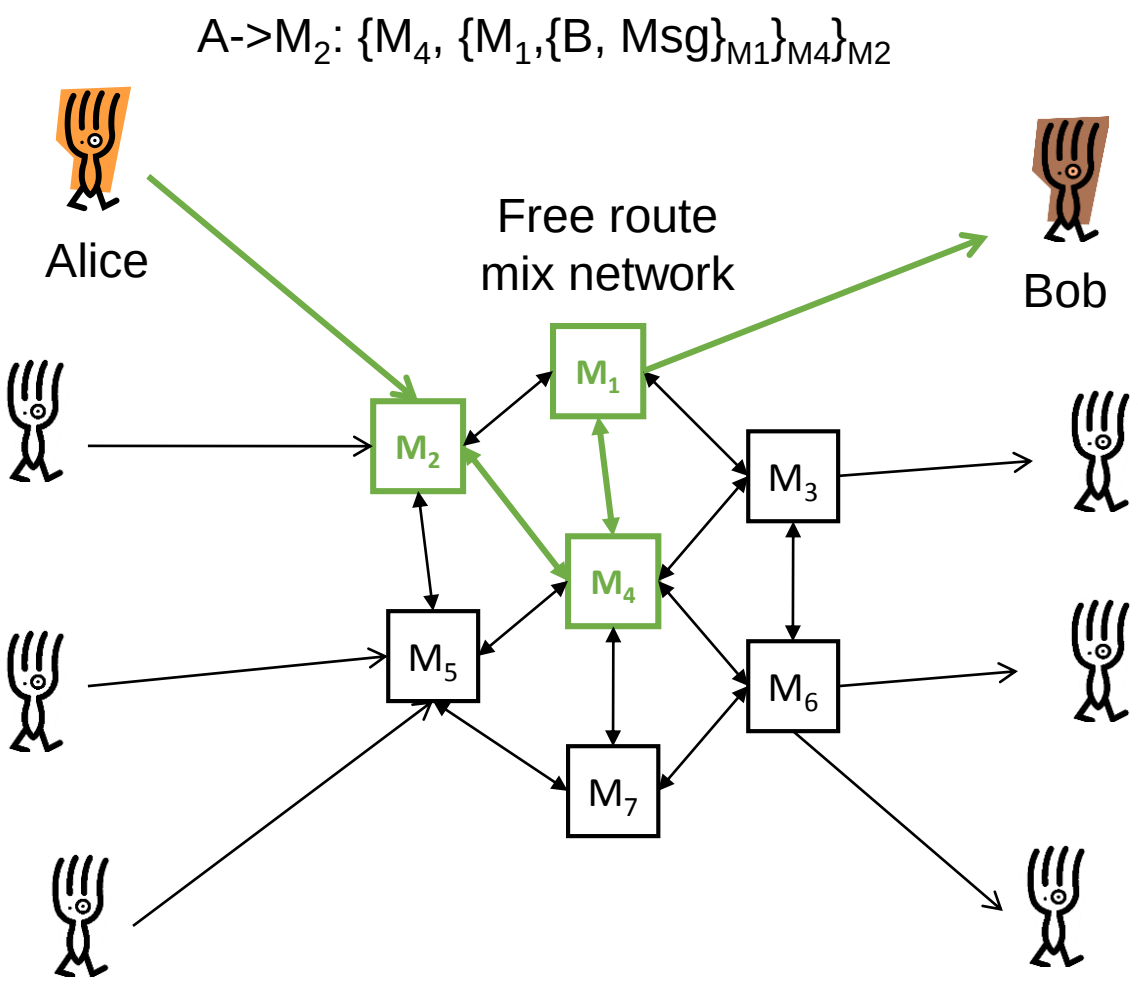
Mix – practical anonymity

- David Chaum (concept 1979 – publish 1981)
  - Reference is marker in anonymity bibliography
- Makes uses of cryptographic relays
  - Break the link between sender and receiver
- Security
  - Computational (public key primitives must be secure)

The mix – illustrated



The free route example



Case Study 1: SecureDrop for whistle blowing

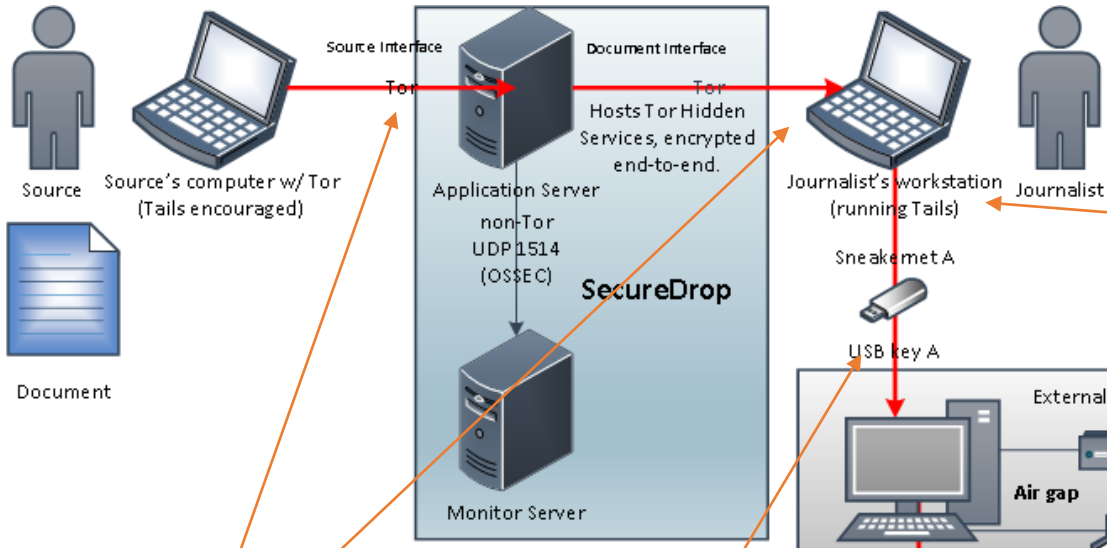
- Sources within Gov / Industry want to help journalists uncover wrong doing.

- Privacy Risks:
  (1) The identity of the source may be uncovered.
  (2) The documents may contain too much information.

- Requirements:
  - “Source can submit story / documents”
  - “Journalist may converse with source”
  - “Documents can be redacted / selected”
  - “Selected documents can be made public”

Freedom of the Press Foundation -- https://securedrop.org/

SecureDrop Architecture



Tails (**OS Privacy**)

Airgap (**Architecture**)

Tor
(**anonymous comms.**)

Encryption + H/W keys
(**Encryption**)

Architecture can also be a privacy mechanism!

https://github.com/freedomofpress/securedrop/issues/274

Signatures & Universal Verifiability

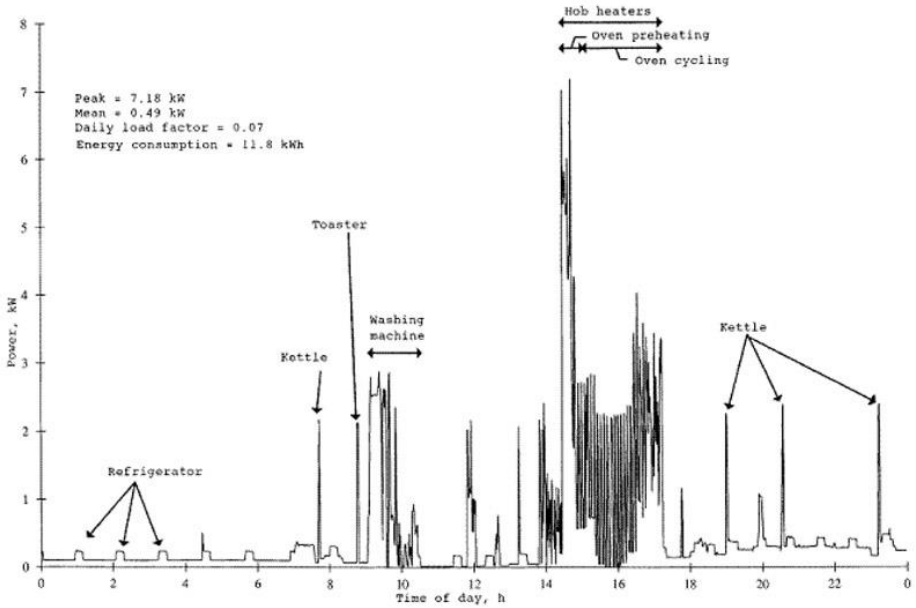
- Digital signatures:
  - Generate a signature key (secret) and a verification key (public)
  - Sign: use the signature key to sign a message and generate a signature
  - Verify: use the verification key, signature and message to verify.
- Universal Verifiability:
  - Anyone can verify, only one can produce.
  - “Non-repudiation” (binding contracts)
- Public keys as “names”:
  - Can verify the “authority” behind a public key
  - Use the ability to produce a signature to authorize actions
- Generalization: Zero-knowledge Proofs

Zero-knowledge

- Setting:
  - Prover: uses some secret and public values to generate the proof of a statement.
  - Verifier: uses the public values, statement and proof to verify the truth of the statement.
- Key properties:
  - Can prove true statement.
  - Cannot prove untrue statements.
  - Secrets do not leak through the proof.
- Signature schemes are special case of zero-knowledge proof.

Case Study 2: Smart metering privacy

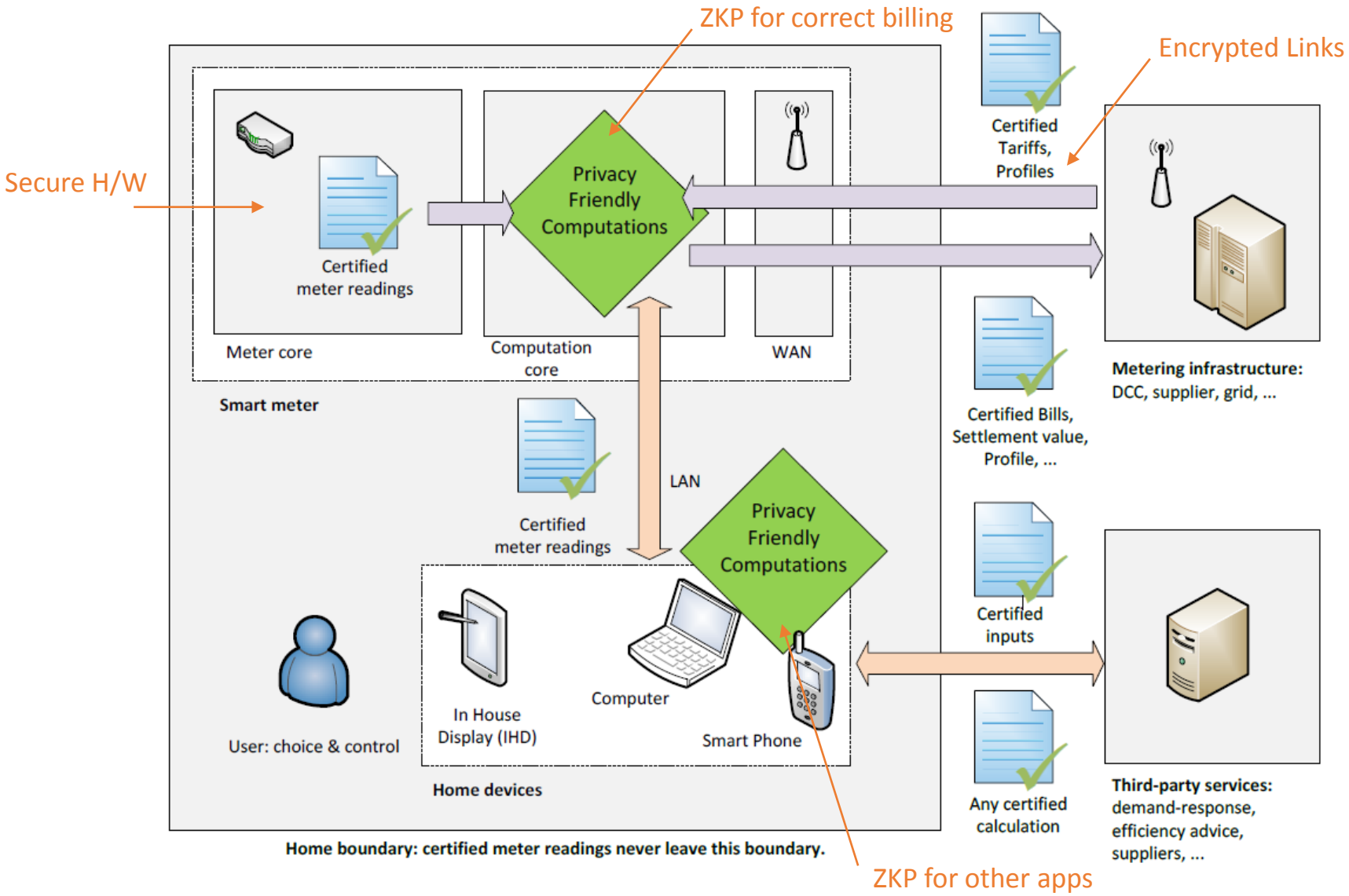
- Smart energy meters record household consumption every 30 mins.
- Privacy Risks:
  (1) Inference of sensitive personal attributes. (Health, religion, work)



- Requirements:
  - "Billing should be correct"
  - "Aggregate statistics per household or group should be available"
  - "Fraud / tampering detection"

Alfredo Rial and George Danezis. Privacy-Preserving Smart Metering. Proceedings of the 2011 ACM WPES 2011, Chicago, USA, October 17, 2008.
Klaus Kursawe, George Danezis, Markulf Kohlweiss: Privacy-Friendly Aggregation for the Smart-Grid. PETS 2011, Waterloo, ON, Canada, July 27-29, 2011.

Smart meter private billing architecture



Rabid decentralization

- Central “Trusted” Third Parties are bad for you:
  - **Cost**: what is the business model? How to implement cheaply?
  - **Corruption**: How do you really know that it will not side with the adversary?
  - **Compulsion**: Legal or extra-legal compulsion to reveal secrets.
  - **Compromise**: It may get hacked!

- Modern cryptography:
  - Maintain the functionality as if there was a trusted third party,
  - Without a trusted third party or hardware
  - Relying instead on: hard math problems, multiple semi-trusted parties

- Pattern for extremely survivable security systems.

Anti-Case study: e-gold

- Established in **1996**.
  - 1 million user accounts by **2002**.
- Features:
  - Centralized ledger of transactions.
  - Currency backed by real commodity, gold.
  - Network of international e-gold resellers.
- E-gold becomes a crime magnet:
  - Difficult to identify customers.
  - Easy to transfer internationally.
- Changing legal ground:
  - US Patriot Act (2001) requires money transmitters to be regulated.
  - In 2006-8 DOJ: money transmitter for any value system, not just money.
  - In **2008** directors face charges of money laundering and operating without a licence.
    They are found guilty and get away with fines, and suspended sentence.
    Asserts liquidated: $90M in gold (more than the central banks of bottom 1/3 countries).
  - California (2010) and other states: all digital value transfer systems are money transmitters.
- Lesson: **Centralization brings (legal) fragility**, unless it is backed by the state (even then).

Bitcoin (BTC)

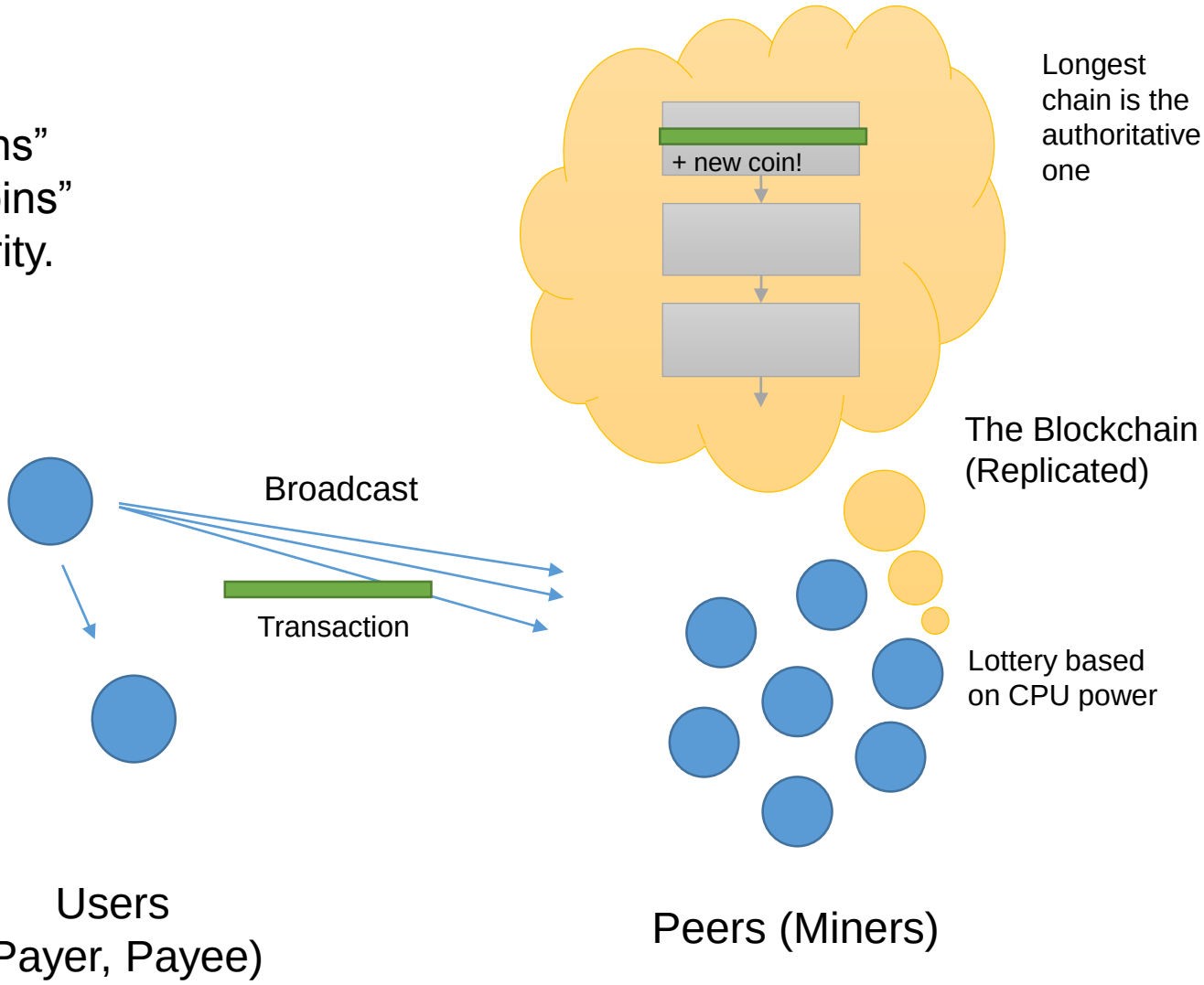
- Paper in late October **2008**.
  - Released as open source software in 2009
  - Pseudonymous developer(s) Satoshi Nakamoto.
  - Disappears in mid-2010.
  - He is estimated to have about 1M BTC.

- Bitcoin features (as in the original email):
  - `Double-spending is prevented with a peer-to-peer network.`
  - `No mint or other trusted parties.`
  - `Participants can be anonymous.`
  - `New coins are made from Hashcash style proof-of-work.`
  - `The proof-of-work for new coin generation also powers the network to prevent double-spending.`

The Bitcoin Architecture

Transactions:
- Link to old “coins”
- Create new “coins”
- Transfer authority.

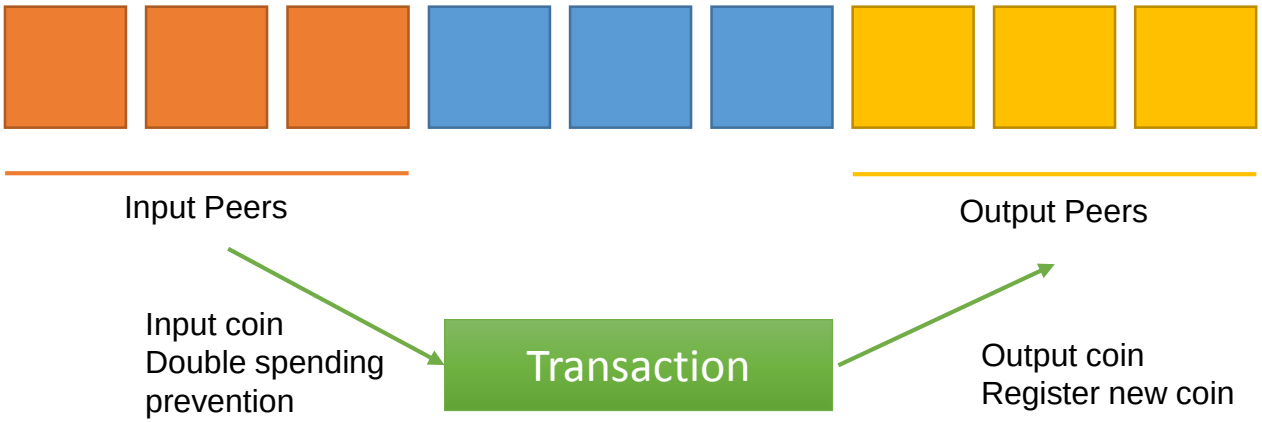
(Signatures)



Bitcoin as a currency

- **Who has control of the money supply in a currency?**
  - By convention it follows a well understood and committed curve.
  - Will max out.
  - Convention enforced by software.
- **Who gets the new money? Who deletes the old money?**
  - No money is deleted
  - Money is created by hashing blocks and adding them to the block chain.
  - The Miner gets the new coin.
- **How do we make sure we will always remember who has how much money?**
  - Large block-chain is recorded by all.
  - Authoritative one is the one with most work (long) – race for aggregate CPU power.
- **Who has it to start with? (Does it matter?)**
  - Satoshi Nakamoto.
- **Where did the demand come from?**
  - “Business spaces let down by traditional finance”.
  - Decentralization is driven by active suppression / disruption (bitcoin, bittorrent).

Scalable Crypto-currencies?



- Avoid proof-of-work and broadcast
- Assume an entity (Central Bank) appoints peers (no Sybil attack)
- Clear usage of coins with subset of peers.
- Register new coins with peers.

George Danezis, Sarah Meiklejohn. Centrally Banked Cryptocurrencies. NDSS 2016, February 2016

The future of on-line currencies

- Regulator attention cannot be avoided:
  - US: Bitcoin friendly – for the moment.
  - China: Not so friendly to the currency, but friendly to mining!
  - How it can be regulated depends on the mechanism – decentralization.
- Rapid evolution of payment instruments and mechanisms:
  - Banks and EMV are dinosaurs.
  - Bitcoin can act as a backing currency to innovate in payments and finance.
  - Whatever works will become mainstream.
  - **Prediction: in 20 years the Euro or Pound will "look like" bitcoin (digital).**
- Is there room for more than one on-line currency?
  - Litecoin, Dogecoin, and and all that?
  - Unclear: bootstrapping problem – lucky Cyprus crisis – gambling & drugs markets benefited Bitcoin growth.
  - What Benefit? Better anonymity? Cheaper to run?
- **Is a zero-governance currency possible?**