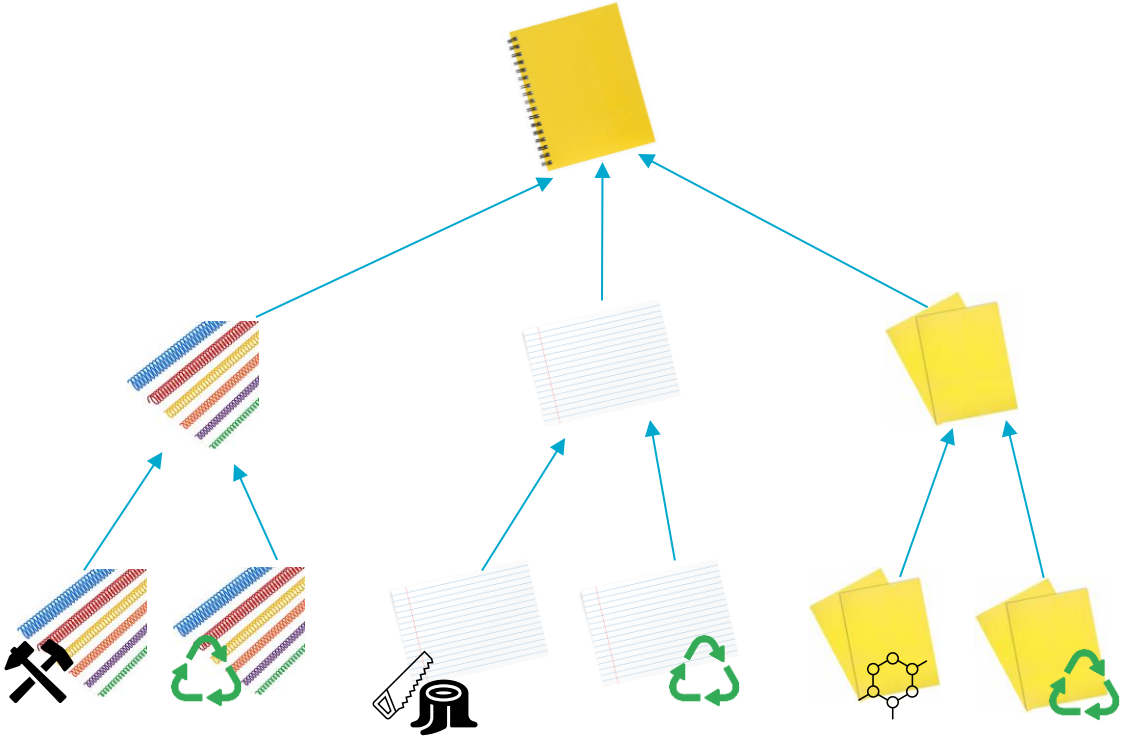
Material Insight – Privacy-Preserving Supply Chain Data Propagation

Dilum Bandara, PhD
Architecture and Analytics Platform Team
CSIRO's Data61
Dilum.Bandara@csiro.au

Use Case



- What % of the notebook is recycled?
- What % of that is recycled in NSW?
- Do these claims add up?

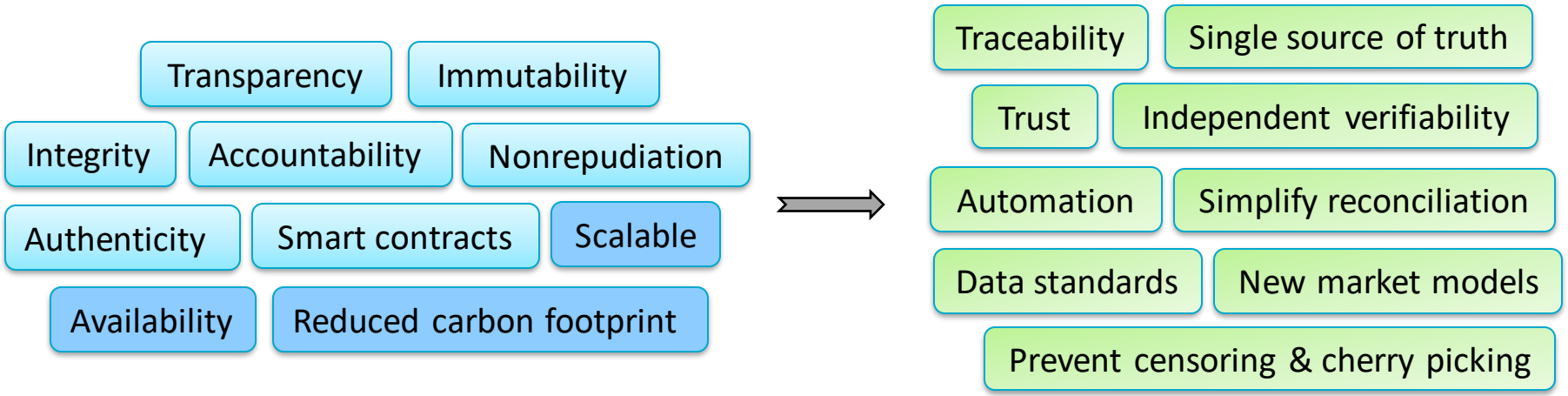
How are these questions answered today?

- Self-made claims
  - Greenwashing?
- Trusted 3rd-party claims
  - Annual audits
  - Doesn't reflect variability across time/batches
  - Lack independent verification

- Increasing demand for better transparency & accountability
  - Through provenance, chain of custody, & traceability

Blockchain is a Good Fit for Supply Chains

- Blockchains are good for multi-party business processes



- Maintaining business confidentiality when data on a blockchain?
  1. Data segregation
  2. Computations on encrypted data

Work with conventional technologies too

Essential Data vs Business Confidentiality

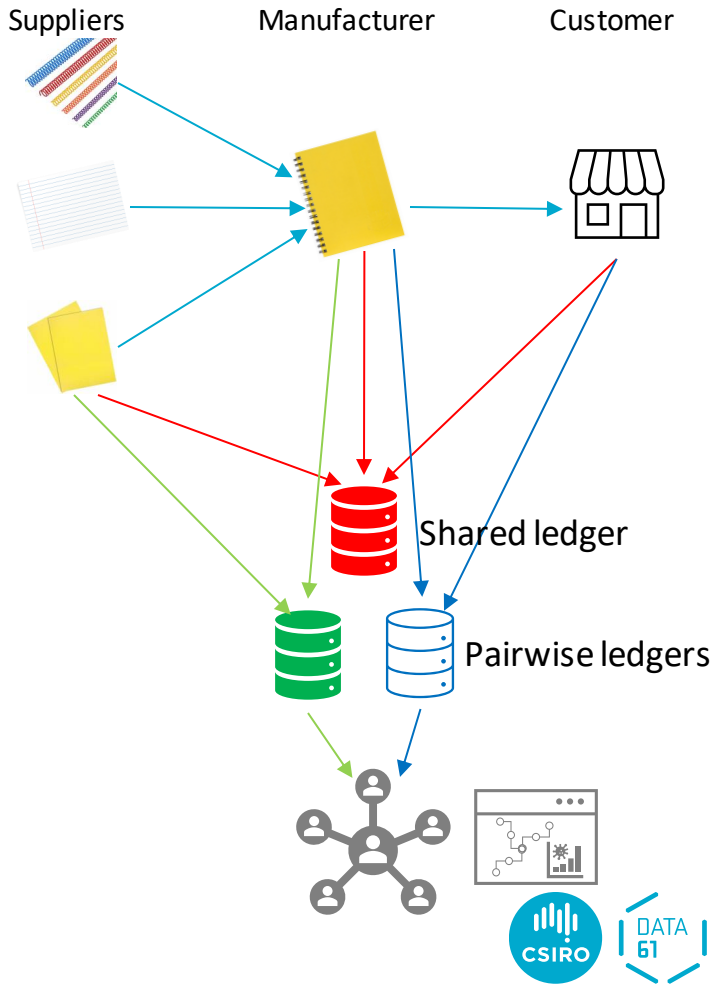
- Quantities
  - Mass, volume, ratios
- Recycle %
- Location
  - GPS, ZIP code, local government area
- Input/output transformation
  - Mechanical, chemical
- Identities
  - Organisations, individuals
- Batch #
- Date/time
- Material passport/composition

$$Recycle\ \% = \frac{w_m r_m + w_{pa} r_{pa} + w_{pl} r_{pl}}{w_m + w_{pa} + w_{pl}} \times 100$$

$$Mass\ balance =$$
$$w_m + w_{pa} + w_{pl} \approx w_n + w_l + w_r$$

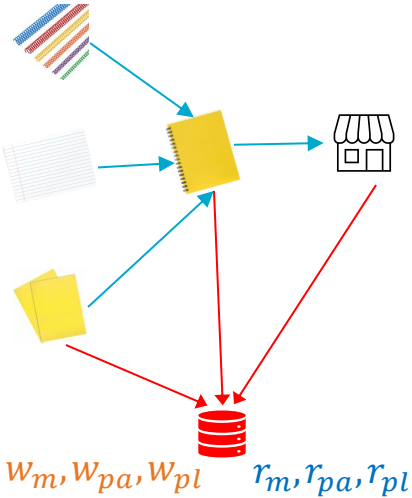
Data Segregation

- One step up & down focus at every step
- Shared access is undesirable
  - Suppliers shouldn't see outputs
  - Customers shouldn't see inputs
- Segregate inputs & outputs
  - E.g., pairwise blockchain ledgers
- Needs a "trusted" supply chain integrator to get a holistic view
  - Integrator calculates recycle % & checks mass balances



Computations on Encrypted Data

- Homomorphic Encryption (HE)
  - Computations on encrypted data & produce encrypted results
  - Addition & multiplication of encrypted & plaintext data
  - Different keys to encrypt & decrypt data after computation



- Recycle % calculation
  - Suppliers/manufacturer publish encrypted masses & plaintext recycle %s
  - Use HE to calculate

$$Recycle\ \% = \frac{w_m r_m + w_{pa} r_{pa} + w_{pl} r_{pl}}{w_m + w_{pa} + w_{pl}} \times 100$$

    - HE can't divide, so either publish encrypted $1/(w_m + w_{pa} + w_{pl})$ or use encrypted mass ratios

Computations on Encrypted Data (Cont.)

- Mass-balance check
  - Suppliers/manufacturer publish encrypted masses
  - Use HE to calculate & compare results

$$Mass\ balance = w_m + w_{pa} + w_{pl} \approx w_n + w_l + w_r$$

- Caveats
  - Computationally expensive
    - Impractical to compute within a smart contract
    - Oracles (i.e., trusted 3rd-parties) can compute off-chain using encrypted data & report results
    - Computation can be performed infrequently
  - Cryptographic key management complexity
  - Nontrivial HE configuration