Private Data OBJECTS

Smart Contracts For Data Access AND MORE

Mic Bowman
Intel Labs

Legal Disclaimers

- Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- For more information go to http://www.Intel.Com/performance.
- All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Private Data Objects (PDOs)

Private Data Objects enable sharing of data and coordinating action amongst distrusting parties.

- Privacy Preserving Smart Contract
  - Access Policy: Smart contract defines data access and update policies
  - Confidentiality: Data can only be accessed through SGX enclave executing the smart contract
  - Stickiness: Policies are enforced wherever the object resides
- Blockchain-based Ledger
  - Commitment: Auditable record of agreements and policy
  - Integrity: Ensures that there is one authoritative instance of an object
  - Coordination: Guarantees atomicity of updates across interacting objects

Example: Transient-Driver Profiles

Trends

- Changing sense of vehicle ownership (long-term owner ☾ short-term lease)
- Insurance companies moving to metered services

Solution Requirements

- Verifiable and representative log of driver history over all vehicles
- Rapid evaluation of that history leading to personalized quotes
- Without exposing personal information inappropriately

Driver Profile → Personalized Insurance Quote ← Insurance Risk Analytics

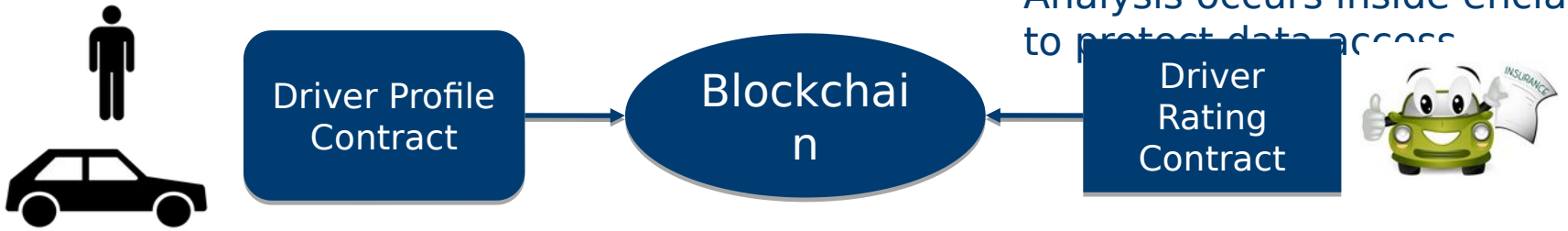
Example: Transient-Driver Profiles

Trends

- Changing sense of vehicle ownership (long-term owner ☾ short-term lease)
- Insurance companies moving to metered services

PDO Solution

- Contracts ensure appropriate access to the driver profile
- Blockchain provides immutable, verifiable log for profile integrity
- Analysis occurs inside enclave to protect data access

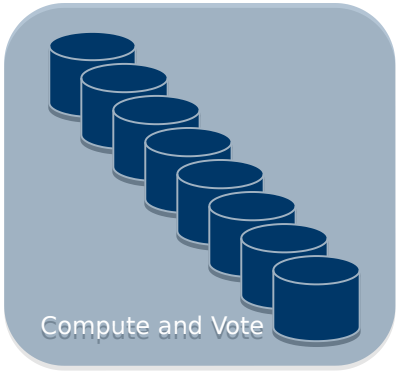


Insurance company analytics can be applied to a verifiable driver profile without exposing any personal data about the driver.

Smart Contracts Today

Redundant Compute Replaces Centralized Trust

Single Organization
Centralized Trust
Single Computation



Multiple Organizations
Decentralized Trust
Redundant Computations and a Final Vote

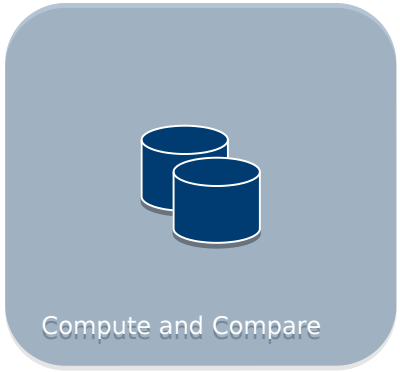
- Every validator executes every update on every transaction
- All of the validators must agree on the result for it to be committed

Public, Inefficient, Slow

Smart Contracts Based On Intel SGX

Replace Redundant Compute with Trusted Execution

Single Organization
Centralized Trust
Single Computation



Multiple Organizations
Decentralized Trust
Trusted Computation and Attestation

- Update executes in one enclave and produces a proof of correctness
- Other validators verify the proof and accept the update

Private, Efficient, Scalable

Private Data Objects in SGX

How It Works With SGX:

- An SGX enclave executes an operation on the PDO smart contract
- The enclave generates a “proof of correctness” that is verified by the ledger
- The ledger ensures that updates to the PDO are serialized

Implication

- Ledger doesn’t need contract or state
  - The contract and its state can be kept private (encrypted and off chain)
- Performance impact is minimal
  - Only execute once, SGX overhead
  - More servers ☾ better performance!
- Updates need not be deterministic
  - No need for global agreement

Access/Use Policy Universally Enforced

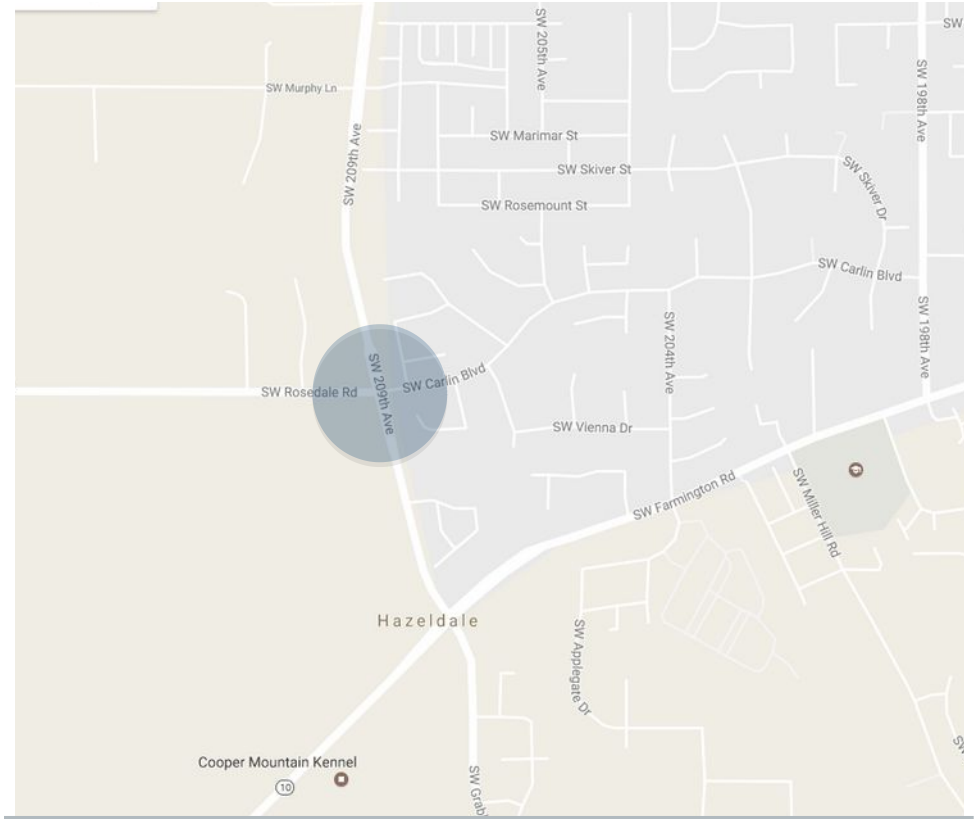
- Contract state is always encrypted outside of the enclave
  - Even the contract owner cannot see the contract state
  - The smart contract may allow externalization of data
- Consequence: access policy is enforced no matter how the data is shared

- This enables some interesting policies
  - Differentially private access that doesn't require the data owner to see the data
  - Owner of the data can prove "compliance" to a set of operations on the data
    - External bid for a contract job
    - Constrained analysis on visual data
  - Automated data aging
    - De-anonymized research data may be released after 5 years
  - Multi-participant, confidential audit
    - Verifiable financial transactions
    - Information provenance

Traffic Planning

Scenario for Information Sharing

- The intersection at Rosedale & 209th backs up every weekday afternoon
- How to solve the problem?
  - Put in a stoplight at that intersection (expensive)
  - Redirect traffic away from that intersection (possibly less expensive)
- Need source & destination for cars going through the intersection
- But… getting that information is hard… for many reasons



Would you trust your DOT with the knowledge of where you are at all times when you are driving? Even if it would most likely lead to a better commute?

How To Use PDO For Route Data

DOT implements a smart contract to collect route information from drivers

- Any individual may put route data into the contract
- Any individual may remove from the contract route data they put in
- DOT may only see heat maps of source and destination through a specific intersection
  - Contract enforces a form of k-anonymity
- DOT may only request data about (for example) 10 intersections per day

Observations

- Details of the smart contract are available for public inspection
- Driver data is always encrypted outside of the enclave, even DOT cannot see it
- Analysis of the data occurs through the smart contract inside the enclave
- Driver data can be removed from future use, and the contract can prove that it has been removed

And… we could add "rewards" for participation if appropriate

Summary

Private Data Objects enable sharing of data and coordinating action amongst mutually distrusting parties.

Status

- Prototype code available through Hyperledger Labs
- Contracts are defined in a functional language evaluated in an enclave
- Contracts for driver profiles, asset markets with fair exchange & auctions

Ongoing Work

- Support more ledgers
- Support additional contract interpreters

Links

DEMO: https://www.youtube.com/watch?v=I1HbFPwo4gg

PAPER: https://arxiv.org/abs/1807.05686

CODE: https://github.com/hyperledger-labs/private-data-objects