Building High Throughput Permissioned Blockchain Fabrics: Challenges and Opportunities

Suyash Gupta  Jelle Hellings  Sajjad Rahnama  Mohammad Sadoghi
Exploratory Systems Lab at UC Davis

Goal: High-performance resilient data processing.

- 1 Professor, 1 Postdoc, 3 Ph.D. students, 6 M.Sc. and B.Sc. students.
- Recent papers at VLDB, ICDCS, ICDT, DISC, EDBT, and more.
- Intersection of blockchain and database technology.
- ResilientDB: A pioneering new data platform.
Goal: High-performance resilient data processing

Questions

1. Why?
2. What is the relation with blockchains?
3. What do we already have?
4. Where can we improve?
5. What new tools do we need?
Towards high-performance resilient data processing:

Why?
Why resilient data processing?

Go beyond assumptions of traditional transaction processing!

Example

- Provide continuous services during failures.
- Provide services in federated environments.
Why high-performance?

Support requirements of future applications!

- Ever-growing volumes of data (e.g., sensor networks).
- Ever-growing demands of applications (e.g., machine learning).
Towards high-performance resilient data processing:

What is the relation with blockchains?
What is a blockchain?

Bitcoin: Management of monetary tokens (Bitcoins)
▶ Open and decentralized transfer of tokens (transactions).
▶ History of transactions (ledger) stored in the blockchain.

\[
\text{hash}_1 \quad \text{puzzle}_1 \quad T_1, \ldots, T_{100} \quad \text{hash}_2 \quad \text{puzzle}_2 \quad T_{101}, \ldots, T_{200} \quad \text{hash}_3 \quad \text{puzzle}_3 \quad T_{201}, \ldots, T_{300} \quad \text{hash}_4 \quad \text{puzzle}_4 \quad T_{301}, \ldots, T_{400}
\]

▶ Many participants hold a copy of the blockchain.
▶ Blockchain structure is tamper-proof by design.
What is a blockchain?

Bitcoin: Management of monetary tokens (Bitcoins)

- Open and decentralized transfer of tokens (transactions).
- History of transactions (ledger) stored in the blockchain.

Many participants hold a copy of the blockchain.

Blockchain structure is tamper-proof by design.
What is a blockchain? - Malicious behavior

Bitcoin: Preventing malicious behavior

- Malicious attempts to change a chain.

```
<table>
<thead>
<tr>
<th>Block B₁</th>
<th>Block B₂</th>
<th>Block B₃</th>
<th>Block B₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>hashᵥ puzzle₁</td>
<td>hash₁ puzzle₂</td>
<td>hash₂ puzzle₃</td>
<td>hash₃ puzzle₄</td>
</tr>
<tr>
<td>T₁, . . . , T₁₀₀</td>
<td>T₁₀₁, . . . , T₂₀₀</td>
<td>T₂₀₁, . . . , T₃₀₀</td>
<td>T₃₀₁, . . . , T₄₀₀</td>
</tr>
</tbody>
</table>
```
What is a blockchain? - Malicious behavior

Bitcoin: Preventing malicious behavior

- Malicious attempts to change a chain.

<table>
<thead>
<tr>
<th>Block $B_1$</th>
<th>Block $B_2$</th>
<th>Block $B_3$</th>
<th>Block $B_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash, puzzle</td>
<td>hash, puzzle</td>
<td>hash, puzzle</td>
<td>hash, puzzle</td>
</tr>
<tr>
<td>$T_1, \ldots, T_{100}$</td>
<td>$T_{101}, \ldots, T_{200}$</td>
<td>$T_{201}, \ldots, T_{300}$</td>
<td>$T_{301}, \ldots, T_{400}$</td>
</tr>
</tbody>
</table>

- Longest chain has highest incentives.
- Making blocks (solving puzzles) is very costly.
- Malicious attempt leads to a *dead end.*
What is a blockchain? - A definition

A resilient tamper-proof ledger maintained by many participants.

- **Ledger.**
  Append-only sequence of transactions.
  In database terms: a journal or log.

- **Resilient.**
  High availability via full replication among participants.

- **Tamper-proof.**
  Changes can only be made with majority participation.

Blockchains are *distributed fully-replicated systems!*
Components of blockchain systems

1. Replicas.
Components of blockchain systems

1. Replicas.
2. Holding the ledger of transactions.
Components of blockchain systems

1. Replicas.
2. Holding the ledger of transactions.
3. Clients with new transactions.
Components of blockchain systems

1. Replicas.
2. Holding the ledger of transactions.
3. Clients with new transactions.
4. Transaction agreement via consensus.
Components of blockchain systems

1. Replicas.
2. Holding the ledger of transactions.
3. Clients with new transactions.
4. Transaction agreement via consensus.
5. Append-only updates to ledger.
Components of blockchain systems

1. Replicas.
2. Holding the ledger of transactions.
3. Clients with new transactions.
4. Transaction agreement via consensus.
5. Append-only updates to ledger.
Bitcoin: A permissionless blockchain

The participants are not known and can change.

Rationale: Fully decentralized and open cryptocurrencies

- Bitcoin, Ethereum, ….  
- Scale to thousands of participants.  
- Low transaction processing throughput.  
- Very high transaction latencies.
We focus on permissioned blockchains

All participants are known.

Rationale: Data processing in managed environment

- Support different attack models than cryptocurrencies.
- Easier to support low latencies and high throughputs.
- Downside: changing participants is hard.

Many ideas also apply to permissionless blockchains.
Towards high-performance resilient data processing:

What do we already have?
We have consensus: PBFT, Paxos, PoW, …

Termination  Each non-faulty replica decides on a transaction.
Non-divergence  Non-faulty replicas decide on the same transaction.
We have consensus: PBFT, Paxos, PoW, …

**Termination** Each non-faulty replica decides on a transaction.

**Non-divergence** Non-faulty replicas decide on the same transaction.

**Validity** Every decided-on transaction is a client request.

**Response** Clients learn about the outcome of their requests.

**Service** Every client will be able to request transactions.
We have consensus: PbFT, Paxos, PoW, …

**Termination**  Each non-faulty replica decides on a transaction.

**Non-divergence**  Non-faulty replicas decide on the same transaction.

**Validity**  Every decided-on transaction is a client request.

**Response**  Clients learn about the outcome of their requests.

**Service**  Every client will be able to request transactions.
Operating a fully-replicated ledger using consensus

Each replica maintains a copy of the ledger:
Append-only sequence of transactions.
1. Use consensus to select the $\rho$-th client request $T$.
2. Append $T$ as the $\rho$-th entry to the ledger.
3. Execute $T$ as the $\rho$-th entry, inform client.

Consistent state: Linearizable order and deterministic execution
On identical inputs, execution of transactions at all non-faulty replicas
must produce identical outputs.
Variations on consensus: Byzantine Broadcast (Generals)

Assume a replica $g$ is the general and holds transaction $T$.

A *Byzantine broadcast algorithm* is an algorithm satisfying:

- **Termination** Each non-faulty replica decides on a transaction.
- **Non-divergence** Non-faulty replicas decide on the same transaction.
- **Dependence** If the general $g$ is non-faulty, then non-faulty replicas will decide on $T$.

$(T' = T$ if the general $g$ is non-faulty).
Variations on consensus: Interactive consistency

Assume $n$ replicas and each replica $R_i$ holds a transaction $T_i$. An interactive consistency algorithm is an algorithm satisfying:

**Termination** Each non-faulty replica decides on $n$ transactions.

**Non-divergence** Non-faulty replicas decide on the same transactions.

**Dependence** If replica $R_j$ is non-faulty,
then non-faulty replicas will decide on $T_j$.

(As $R_3$ is faulty: $\times$ can be anything)
Distributed fully-replicated systems: The CAP Theorem

Consistency  Does every participant have exactly the same data?
Availability  Does the system continuously provide services?
Partitioning  Can the system cope with network disturbances?

Theorem (The CAP Theorem)

*Can provide at most two-out-of-three of these properties.*
Distributed fully-replicated systems: The CAP Theorem

Consistency  Does every participant have exactly the same data?
Availability  Does the system continuously provide services?
Partitioning  Can the system cope with network disturbances?

Theorem (The CAP Theorem)

*Can provide at most two-out-of-three of these properties.*

CAP Theorem uses narrow definitions!
Permissionless Blockchains
Open membership focuses on Availability and Partitioning.
⇒ Consistency not guaranteed (e.g., forks).
The CAP Theorem and Blockchains

Permissioned Blockchains
Consistency at all costs.

⇒ Availability when communication is reliable.
⇒ Some network failure when replicas are reliable.
What else do we have?

- A lot of *theory* on consensus: consensus is costly.
- **PBFT**: A practical Byzantine fault-tolerant consensus protocol.
- Tamper-proof *ledgers*.

```
                      hash_v puzzle_1
  hash_v puzzle_1 ⇄ hash_1 puzzle_2 ⇄ hash_2 puzzle_3 ⇄ hash_3 puzzle_4
  T_1, ..., T_{100}  ⇄ T_{101}, ..., T_{200}  ⇄ T_{201}, ..., T_{300}  ⇄ T_{301}, ..., T_{400}
```

Exact details: depend on consensus, application, attack model, ...
- Many *cryptographic tools*. 
What else do we have?

- A lot of *theory* on consensus: consensus is costly.
- **PBFT**: A practical Byzantine fault-tolerant consensus protocol.
- Tamper-proof *ledgers*.

$$\begin{align*}
&\text{hash}_v \text{ puzzle}_1 \leftarrow T_1, \ldots, T_{100} \\
&\text{hash}_1 \text{ puzzle}_2 \leftarrow T_{101}, \ldots, T_{200} \\
&\text{hash}_2 \text{ puzzle}_3 \leftarrow T_{201}, \ldots, T_{300} \\
&\text{hash}_3 \text{ puzzle}_4 \leftarrow T_{301}, \ldots, T_{400}
\end{align*}$$

Exact details: depend on consensus, application, attack model, …

- Many *cryptographic tools*.

*What about high-performance?*
Theory on consensus: Summary

Limitations of practical consensus

- No asynchronous communication!
- Dealing with $f$ malicious failures requires $n > 3f$ replicas.
- Worst-case: at least $\Omega (f + 1)$ phases of communication.
- Worst-case: at least $\Omega (nf)$ signatures and $\Omega (n + f^2)$ messages.
- Network must stay connected when removing $2f$ replicas.

Consensus in practice

Asynchronous communication, $n > 3f$, clique network:

$\implies$ termination only when communication is reliable.
Towards high-performance resilient data processing:

What do we already have?

PBFT
PBFT: Practical Byzantine Fault Tolerance

**Primary** Coordinates consensus: propose transactions to replicate.

**Backup** Accept transactions and verifies behavior of primary.
PBFT: Normal-case protocol in view $\nu$

$\langle T \rangle_c$.
PBFT: Normal-case protocol in view $\nu$

$\textbf{PrePrepare}(\langle T \rangle_c, \nu, \rho)$. 
PBFT: Normal-case protocol in view $\nu$

If receive PrePrepare message $m$: Prepare($m$).
PBFT: Normal-case protocol in view $v$

If $n - f$ identical $\text{PREPARE}(m)$ messages: $\text{COMMIT}(m)$. 
PBFT: Normal-case protocol in view $\nu$

If $n - f$ identical $\text{Commit}(m)$ messages: execute, $\text{Inform}(\langle T \rangle_c, \rho, r)$. 
Theorem

If the primary is non-faulty and communication is reliable, then the normal-case of PBFT ensures consensus on $T$ in round $\rho$. 
PBFT: Normal-case consensus

**Theorem**

*If the primary is non-faulty and communication is reliable, then the normal-case of PBFT ensures consensus on T in round \( \rho \).*

**Example (Byzantine primary, \( n = 4, f = 1, n - f = 3 \))**

![Diagram](image-url)
PBFT: Normal-case consensus

Theorem

If the primary is non-faulty and communication is reliable, then the normal-case of PBFT ensures consensus on $T$ in round $\rho$.

Example (Byzantine primary, $n = 4$, $f = 1$, $n - f = 3$)
PBFT: A normal-case property when $n > 3f$

Theorem (Castro et al.)

If replicas $R_i$, $i \in \{1, 2\}$, commit to $m_i = \text{PrePrepare}(\langle T_i \rangle_{c_i}, v, \rho)$, then $\langle T_1 \rangle_{c_1} = \langle T_2 \rangle_{c_2}$. 

Proof.

Replica $R_i$ commits to $m_i$:

\[ B_i \geq n - 2f \] non-faulty \leq \[ f \] faulty

If $\langle T_1 \rangle_{c_1} \neq \langle T_2 \rangle_{c_2}$, then $B_1 \cap B_2 = \emptyset$ and $|B_1 \cup B_2| \geq 2(n - 2f)$. 

\[ 2(n - 2f) \leq n - f \iff 2n - 4f \leq n - f \iff n \leq 3f. \]
PBFT: A normal-case property when $n > 3f$

Theorem (Castro et al.)

*If replicas $r_i$, $i \in \{1, 2\}$, commit to $m_i = \text{PrePrepare}(⟨T_i⟩_{c_i}, v, ρ)$, then $⟨T_1⟩_{c_1} = ⟨T_2⟩_{c_2}$.*

Proof.

Replica $r_i$ commits to $m_i$:

$n - f$ messages $\text{Prepare}(m_i)$

\[ R_i \]
PBF T: A normal-case property when \( n > 3f \)

Theorem (Castro et al.)

If replicas \( r_i, i \in \{1, 2\} \), commit to \( m_i = \text{PREPARE}(\langle T_i \rangle_{c_i}, v, \rho) \), then \( \langle T_1 \rangle_{c_1} = \langle T_2 \rangle_{c_2} \).

Proof.
Replica \( r_i \) commits to \( m_i \):

\[
\begin{align*}
n - f \text{ messages} & \quad \text{PREPARE}(m_i) \\
\geq n - 2f \text{ non-faulty} & \quad B_i \\
\leq f \text{ faulty} & \quad F_i \\
& \quad r_i
\end{align*}
\]
PBFT: A normal-case property when $n > 3f$

Theorem (Castro et al.)

*If replicas $r_i$, $i \in \{1, 2\}$, commit to $m_i = \text{PREPARE}(\langle T_i \rangle_{c_i}, v, \rho)$, then $\langle T_1 \rangle_{c_1} = \langle T_2 \rangle_{c_2}$.*

Proof.
Replica $r_i$ commits to $m_i$:

$n - f$ messages $\text{PREPARE}(m_i)$

$\geq n - 2f$ non-faulty $B_i$

$\leq f$ faulty $F_i$

If $\langle T_1 \rangle_{c_1} \neq \langle T_2 \rangle_{c_2}$, then $B_1 \cap B_2 = \emptyset$ and $|B_1 \cup B_2| \geq 2(n - 2f)$. 
PBFT: A normal-case property when $n > 3f$

Theorem (Castro et al.)

If replicas $r_i$, $i \in \{1, 2\}$, commit to $m_i = \text{PREPARE}(\langle T_i \rangle_{c_i}, v, \rho)$, then $\langle T_1 \rangle_{c_1} = \langle T_2 \rangle_{c_2}$.

Proof.

Replica $r_i$ commits to $m_i$:

- $n - f$ messages $\text{PREPARE}(m_i)$
- $\geq n - 2f$ non-faulty
- $\leq f$ faulty

If $\langle T_1 \rangle_{c_1} \neq \langle T_2 \rangle_{c_2}$, then $B_1 \cap B_2 = \emptyset$ and $|B_1 \cup B_2| \geq 2(n - 2f)$.

$$2(n - 2f) \leq n - f$$
**PBFT: A normal-case property when \( n > 3f \)**

Theorem (Castro et al.)

*If replicas \( r_i, i \in \{1, 2\}, \) commit to \( m_i = \text{PREPARE}(\langle T_i \rangle_{c_i}, v, \rho), \) then \( \langle T_1 \rangle_{c_1} = \langle T_2 \rangle_{c_2} \).*

**Proof.**

Replica \( r_i \) commits to \( m_i: \)

\[
\begin{align*}
n - f \text{ messages } & \text{PREPARE}(m_i) \\
\geq n - 2f \text{ non-faulty } & \rightarrow B_i \\
\leq f \text{ faulty } & \rightarrow F_i \\
\end{align*}
\]

If \( \langle T_1 \rangle_{c_1} \neq \langle T_2 \rangle_{c_2} \), then \( B_1 \cap B_2 = \emptyset \) and \( |B_1 \cup B_2| \geq 2(n - 2f). \)

\[
2(n - 2f) \leq n - f \quad \text{iff} \quad 2n - 4f \leq n - f
\]
PBFT: A normal-case property when $n > 3f$

Theorem (Castro et al.)

If replicas $r_i$, $i \in \{1, 2\}$, commit to $m_i = \text{PREPARE}(<T_i>_{c_i}, v, \rho)$, then $<T_1>_{c_1} = <T_2>_{c_2}$.

Proof.

Replica $r_i$ commits to $m_i$:

$n - f$ messages $\text{PREPARE}(m_i)$

$\geq n - 2f$ non-faulty $\rightarrow B_i$

$\leq f$ faulty $\rightarrow F_i$

If $<T_1>_{c_1} \neq <T_2>_{c_2}$, then $B_1 \cap B_2 = \emptyset$ and $|B_1 \cup B_2| \geq 2(n - 2f)$.

$2(n - 2f) \leq n - f$ \iff $2n - 4f \leq n - f$ \iff $n \leq 3f$. $\square$
PBFT: Primary failure versus malicious replicas

Primary $p$ is faulty ignores $r_3$
PBFT: Primary failure versus malicious replicas

Primary $p$ is faulty

*ignores* $r_3$
Primary \( p \) is faulty

ignores \( r_3 \)

Replica \( r_3 \) is malicious

pretends to be ignored
PBFT: Primary failure versus malicious replicas

Primary $p$ is faulty

*ignores* $r_3$

Replica $r_3$ is malicious

*pretends to be ignored*
PBFT: Detectable primary failures

If the primary behaves faulty to > f non-faulty replicas, then failure of the primary is detectable.

Replacing the primary: View-change at replica R

1. R detects failure of the current primary P.
2. R chooses a new primary P' (the next replica).
3. R provides P' with its current state.
4. P' proposes a new view.
5. If the new view is valid, then R switches to this view.
Send $\text{ViewChange}(E, v)$ with $E$ all prepared transactions.
PBFT: A view-change in view $v$

Indirect failure detection by $r_2$. 
PBFT: A view-change in view $v$

If $n - f$ valid $\text{ViewChange}(E, v)$ messages: $\text{NewView}(v + 1, E, N)$.

- $E$ contains $n - f$ valid $\text{ViewChange}$ messages.
- $N$ contains no-op proposals for missing rounds.
PBFT: A view-change in view $v$

Move to view $v + 1$ if $\text{NEWVIEW}(v + 1, \mathcal{E}, \mathcal{N})$ is valid.

- $\mathcal{E}$ contains $n - f$ valid $\text{VIEWCHANGE}$ messages.
- $\mathcal{N}$ contains no-op proposals for missing rounds.
PBFT: A property of view-changes when $n > 3f$

Theorem (Castro et al.)

Let $\text{NEWVIEW}(v', \mathcal{E}, N)$ be a well-formed $\text{NEWVIEW}$ message.
If a set $S$ of $n - 2f$ non-faulty replicas committed to $m$ in view $v < v'$, then $\mathcal{E}$ contains a $\text{VIEWCHANGE}$ message preparing $m$. 

PBFT: A property of view-changes when $n > 3f$

Theorem (Castro et al.)

Let $\text{NEWVIEW}(v', \mathcal{E}, N)$ be a well-formed $\text{NEWVIEW}$ message. If a set $S$ of $n - 2f$ non-faulty replicas committed to $m$ in view $v < v'$, then $\mathcal{E}$ contains a $\text{VIEWCHANGE}$ message preparing $m$.

Proof.

The $\text{VIEWCHANGE}$ messages in $\mathcal{E}$:

$n - f$ messages $\text{VIEWCHANGE}(E, v' - 1)$

$\geq n - 2f$ non-faulty $\rightarrow B$

$\leq f$ faulty $\rightarrow F$
PBFT: A property of view-changes when $n > 3f$

Theorem (Castro et al.)

Let $\text{NEWVIEW}(v', E, N)$ be a well-formed $\text{NEWVIEW}$ message. If a set $S$ of $n - 2f$ non-faulty replicas committed to $m$ in view $v < v'$, then $E$ contains a $\text{VIEWCHANGE}$ message preparing $m$.

Proof.
The $\text{VIEWCHANGE}$ messages in $E$:

- $n - f$ messages $\text{VIEWCHANGE}(E, v' - 1)$
- $\geq n - 2f$ non-faulty
- $\leq f$ faulty

if $S \cap B = \emptyset$, then $|S \cup B| \geq 2(n - 2f)$, a contradiction!
PBFT: Further dealing with failures

1. **Undetected failures**: e.g., ignored replicas.
   At least $n - 2f > f$ non-faulty replicas participate: checkpoints.
PBFT: Further dealing with failures

1. Undetected failures: e.g., ignored replicas.
   At least \( n - 2f > f \) non-faulty replicas participate: checkpoints.

2. Detected failures: primary replacement.
   Worst-case: a sequence of \( f \) view-changes (\( \Omega (f) \) phases).
PBFT: Further dealing with failures

1. **Undetected failures**: e.g., ignored replicas.
   At least \( n - 2f > f \) non-faulty replicas participate: *checkpoints*.

2. **Detected failures**: primary replacement.
   Worst-case: a sequence of \( f \) view-changes (\( \Omega(f) \) phases).

3. **View-change cost**: includes all previous transactions!
   Checkpoints: view-change includes *last successful* checkpoint.
1. **Undetected failures**: e.g., ignored replicas. At least \( n - 2f > f \) non-faulty replicas participate: *checkpoints*.

2. **Detected failures**: primary replacement. Worst-case: a sequence of \( f \) view-changes (\( \Omega(f) \) phases).

3. **View-change cost**: includes all previous transactions! Checkpoints: view-change includes *last successful* checkpoint.

4. **Unreliable communication**: replacement of non-faulty primaries. Worst-case: replacements until communication becomes *reliable*.
PBFT: Modeling real-world performance\textsuperscript{1}

\begin{itemize}
\item \textbf{Throughput (txn/s, 15 ms delay)}
\begin{itemize}
\item \( T_{\text{max}} \)
\end{itemize}
\end{itemize}

\begin{itemize}
\item \textbf{Throughput (txn/s, 7 replicas)}
\begin{itemize}
\end{itemize}
\end{itemize}

(Maximum throughput of any primary-backup broadcast protocol)

\textsuperscript{1}Bandwidth: 100 MiB/s, PrePrepare message size: 1024 B, Prepare and Commit message size: 256 B.
PBFT: Modeling real-world performance

Throughput (txn/s, 15 ms delay)

- $T_{\text{max}}$
- $T_{\text{PBFT}}$

Throughput (txn/s, 7 replicas)

(Maximum throughput of in-order PBFT)

1 Bandwidth: 100 MiB/s, PrePrepare message size: 1024 B, Prepare and Commit message size: 256 B.
PBFT: Modeling real-world performance

(Maximum throughput of in-order PBFT with batching, 256 txn/batch)

1Bandwidth: 100 MiB/s, PrePrepare message size: 1024 B, Prepare and Commit message size: 256 B.
PBFT: Modeling real-world performance

(Maximum throughput of out-of-order PBFT)

1Bandwidth: 100 MiB/s, PrePrepare message size: 1024 B, Prepare and Commit message size: 256 B.
PBFT: Modeling real-world performance

(Maximum throughput of out-of-order PBFT with batching, 256 txn/batch)

1Bandwidth: 100 MiB/s, PrePrepare message size: 1024 B, Prepare and Commit message size: 256 B.
Towards high-performance resilient data processing:

Where can we improve?
A look at high-performance data processing

*Scalability: adding resources $\Longrightarrow$ adding performance.*

Full replication: adding resources (replicas) $\Longrightarrow$ less performance!
Sharding and Geo-scale aware sharding

Adding shards $\implies$ adding throughput (parallel processing), adding storage.
Role Specialization: Read-only workloads

Specializing roles \(\Rightarrow\) adding throughput (parallel processing, specialized hardware, …).
Towards high-performance resilient data processing:

*What new tools do we need?*
Reminder
We can make a resilient cluster that manages data: blockchains.

▶ **Sharding**: make each shard an independent blockchain.
  Requires: *reliable communication between blockchains.*
  Permissionless blockchains: relays, atomic swaps!

▶ **Role Specialization**: make the storage system a blockchain.
  Requires: *reliable read-only updates of the blockchain.*
  Permissionless blockchains: light clients!

Consensus is of no use here if we want efficiency.
Towards high-performance resilient data processing:

What new tools do we need?

Sharding
Sharding: Reliable communication between blockchains

Cluster (All Data)

Requests (All Data)

$\Rightarrow$

Cluster (European Data)

Requests (European Data)

Cluster-Sending (coordination)

Requests (Mixed Data)

Cluster (American Data)

Requests (American Data)

The Byzantine cluster-sending problem.
The problem of sending a value $v$ from a cluster $C_1$ to a cluster $C_2$ such that

- all non-faulty replicas in $C_2$ **receive** the value $v$;
- all non-faulty replicas in $C_1$ **confirm** that the value $v$ was received; and
- $C_2$ only receives a value $v$ if all non-faulty replicas in $C_1$ **agree** upon sending $v$.

*Requirements to provide reliable communication between clusters with Byzantine replicas.*
Global communication versus local communication

Straightforward cluster-sending solution (crash failures)
Pair-wise broadcasting with $(f_1 + 1)(f_2 + 1) \approx f_1 \times f_2$ messages.
Global communication versus local communication

Straightforward cluster-sending solution (crash failures)

Pair-wise broadcasting with \((f_1 + 1)(f_2 + 1) \approx f_1 \times f_2\) messages.

<table>
<thead>
<tr>
<th></th>
<th>Ping round-trip times (ms)</th>
<th>Bandwidth (Mbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OR</td>
<td>IA</td>
</tr>
<tr>
<td>Oregon</td>
<td>≤ 1</td>
<td>38</td>
</tr>
<tr>
<td>Iowa</td>
<td>≤ 1</td>
<td>33</td>
</tr>
<tr>
<td>Montreal</td>
<td>≤ 1</td>
<td>82</td>
</tr>
<tr>
<td>Belgium</td>
<td>≤ 1</td>
<td>252</td>
</tr>
<tr>
<td>Taiwan</td>
<td>≤ 1</td>
<td>137</td>
</tr>
<tr>
<td>Sydney</td>
<td>≤ 1</td>
<td></td>
</tr>
</tbody>
</table>
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad f_1 = 7 \]
\[ n_2 = 5 \quad f_2 = 2 \]

Claim (crash failures)

Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad \quad f_1 = 7 \]
\[ n_2 = 5 \quad \quad f_2 = 2 \]

Claim (crash failures)
Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad f_1 = 7 \]
\[ n_2 = 5 \quad f_2 = 2 \]

Claim (crash failures)

Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad f_1 = 7 \]
\[ n_2 = 5 \quad f_2 = 2 \]

Claim (crash failures)
Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad f_1 = 7 \]
\[ n_2 = 5 \quad f_2 = 2 \]

Claim (crash failures)

Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Example

\[ n_1 = 15 \quad f_1 = 7 \]
\[ n_2 = 5 \quad f_2 = 2 \]

Claim (crash failures)

Any correct protocol needs to send at least 14 messages.
Lower bounds for cluster-sending: Results

Theorem (Cluster-sending lower bound, simplified)

We need to exchange \( \max(n_1, n_2) \) messages to do cluster-sending.

Theorem (Cluster-sending lower bound, crash failures)

Assume \( n_1 \geq n_2 \) and let

\[
q = (f_1 + 1) \div nf_2; \quad r = (f_1 + 1) \mod nf_2.
\]

We need to exchange at least \( qn_2 + r + f_2 \text{ sgn } r \approx n_1 \) messages to do cluster-sending.
An optimal cluster-sending algorithm (crash failures)

Protocol for the sending cluster $C_1$, $n_1 \geq n_2$, $n_1 \geq \sigma$:

1: \textit{AGREE} on sending $v$ to $C_2$.
2: Choose replicas $\mathcal{P} \subseteq C_1$ with $|\mathcal{P}| = \sigma$.
3: Choose a $n_2$-partition $\text{partition}(\mathcal{P})$ of $\mathcal{P}$.
4: \textbf{for} $P \in \text{partition}(\mathcal{P})$ \textbf{do}
5: \hspace{1em} Choose replicas $Q \subseteq C_2$ with $|Q| = |P|$.
6: \hspace{1em} Choose a bijection $b : P \rightarrow Q$.
7: \hspace{1em} \textbf{for} $r_1 \in P$ \textbf{do}
8: \hspace{2em} Send $v$ from $r_1$ to $b(r_1)$.

Protocol for the receiving cluster $C_2$:

9: \textbf{event} $r_2 \in C_2$ receives $w$ from a replica in $C_1$ \textbf{do}
10: \hspace{1em} Broadcast $w$ to all replicas in $C_2$.
11: \textbf{event} $r_2 \in C_2$ receives $w$ from a replica in $C_2$ \textbf{do}
12: \hspace{1em} $r_2$ considers $w$ \textit{RECEIVED}.
An optimal cluster-sending algorithm—visualized

Crash failures, $n_1 = 7$, $n_2 = 4$, $f_1 = 3$, $f_2 = 1$, $\sigma = 6$
An optimal cluster-sending algorithm—visualized

Crash failures, $n_1 = 7$, $n_2 = 4$, $f_1 = 3$, $f_2 = 1$, $\sigma = 6$

Decide on sending $v$
An optimal cluster-sending algorithm—visualized

Crash failures, \( n_1 = 7, n_2 = 4, f_1 = 3, f_2 = 1, \sigma = 6 \)

Decide on sending \( v \)
An optimal cluster-sending algorithm—visualized

Crash failures, $n_1 = 7$, $n_2 = 4$, $f_1 = 3$, $f_2 = 1$, $\sigma = 6$
An optimal cluster-sending algorithm—visualized

Crash failures, $n_1 = 7$, $n_2 = 4$, $f_1 = 3$, $f_2 = 1$, $\sigma = 6$

Decide on sending $v$

Received $v$
Cluster-sending: Can we do better

**Pessimistic**

*No*: these protocols are worst-case optimal.
Cannot do better than *linear communication* in the size of the clusters.
Cluster-sending: Can we do better

**Pessimistic**

**No**: these protocols are worst-case optimal. Cannot do better than *linear communication* in the size of the clusters.

**Optimistic—upcoming results**

**Yes**: if we randomly choose sender and receiver, then we often do much better! Probabilistic approach: expected-case only *constant communication* (four steps).
Towards high-performance resilient data processing:

What new tools do we need?

Role Specialization
Role Specialization: Reliable read-only updates of the blockchain

System (All Data)

Storage System (All Data)

requests (Reads, Updates)

requests (Updates)

Compute Systems (Copy of Relevant Data)

Analytics

Machine Learning

Visualization (Read-only Workloads)

Byzantine Learning (updates)

The Byzantine learner problem.
The Byzantine learner problem

The problem of sending a ledger $\mathcal{L}$ maintained by a cluster $C$ to a learner $L$ such that:

- the learner $L$ will eventually \textit{receive all} transactions in $\mathcal{L}$; and
- the learner $L$ will \textit{only receive} transactions in $\mathcal{L}$.

Practical requirements

- Minimizing overall communication.
- Load balancing among all replicas in $C$. 

Background: Information dispersal algorithms

Definition
Let $v$ be a value with storage size $s = \|v\|$. An *information dispersal algorithm* can encode $v$ in $n$ pieces $v'$ such that $v$ can be *decoded* from every set of $n - f$ such pieces.

Theorem (Rabin 1989)
The IDA algorithm is an *optimal* information dispersal algorithm:
- Each piece $v'$ has size $\left\lceil \frac{\|v\|}{n-f} \right\rceil$.
- The $n - f$ pieces necessary for decoding have a total size of $(n - f) \left\lceil \frac{\|v\|}{(n-f)} \right\rceil \approx \|v\|$.
The delayed-replication algorithm

Idea: $C$ sends a ledger $L$ to learner $L$

1. Partition the ledger $L$ in sequences $S$ of $n$ transactions.
2. Replica $r_i \in C$ encodes $S$ into the $i$-th IDA piece $S_i$.
3. Replica $r_i \in C$ sends $S_i$ with a checksum $C_i(S)$ of $S$ to learner $L$.
4. Learner $L$ receives at least $n - f$ distinct and valid pieces and decodes $S$.

Observation ($n > 2f$)

- Replica $r_i$ sends at most $B = \left\lceil \frac{\|S\|}{n-f} \right\rceil + c \leq \frac{2\|S\|}{n} + 1 + c = O \left( \frac{\|S\|}{n} + c \right)$ bytes.
- Learner $L$ receives at most $n \cdot B = O (\|S\| + cn)$ bytes.
Communication by the delayed-replication algorithm

Update decision in ledger \( \mathcal{L} \rightarrow \)

No dispersal

First 4 updates

Second 4 updates

Learned \( \mathcal{L}[0:4] \)

Learned \( \mathcal{L}[4:8] \)
Checksums: Use Merkle-trees to construct checksums

Consider 8 replicas and a sequence $S$. We construct the checksum $C_5(S)$ of $S$ (used by $R_5$).

Construct a Merkle tree for pieces $S_0, \ldots, S_7$. 
Checksums: Use Merkle-trees to construct checksums

Consider 8 replicas and a sequence $S$. We construct the checksum $C_5(S)$ of $S$ (used by $R_5$).

Determine the path from root to $S_5$. 

\[ h_0, h_1, h_2, h_3, h_4, h_5, h_6, h_7 \]

\[ (S_0), (S_1), (S_2), (S_3), (S_4), (S_5), (S_6), (S_7) \]
Consider 8 replicas and a sequence $S$. We construct the checksum $C_5(S)$ of $S$ (used by $R_5$).

Select root and neighbors: $C_5(S) = [h_4, h_7, h_{0123}, h_{01234567}]$. 
Checksums: Use Merkle-trees to construct checksums

Consider 8 replicas and a sequence $S$. We construct the checksum $C_5(S)$ of $S$ (used by $R_5$).

If one knows the root: validity of individual pieces can be determined.
Delayed-replication: Main result ($n > 2f$)

Theorem

Consider the learner $l$, replica $r \in C$, and ledger $L$.

The delayed-replication algorithm with tree checksums guarantees

1. $l$ will learn $L$;
2. $l$ will receive at most $|L|$ messages with a total size of $O(||L|| + |L| \log n)$;
3. $l$ will only need at most $|L|/n$ decode steps;
4. $r$ will sent at most $|L|/n$ messages to $l$ of size $O\left(\frac{||L|| + |L| \log n}{n}\right)$.

Adding replicas to cluster $C \implies$ less communication per replica!
Application: Scalable storage for resilient systems

- Clusters typically need a view $V$ on the data to decide whether updates are valid.
- Clusters only need the full ledger $L$ for recovery.
- We can use delayed-replication to reduce the data each replica has to store.

**Theorem**

*The storage cost per replica can be reduced from*

$$O (\|L\| + \|V\|) \text{ to } O \left( \frac{\|L\|}{n-f} + \frac{|L|}{n} \log(n) + \|V\| \right).$$
Towards high-performance resilient data processing:

Concluding remarks
Conclusion

We need an extensive toolbox!

- Consensus (permissioned) (permissionless) PBFT, Paxos, … PoW, PoS, …
- Cross-blockchain communication Cluster-sending Relays, atomic swaps
- Read-only participation Byzantine learning Light clients

High-performance resilient data processing is nearby.
Ongoing work

Initial results are available


More about us and our work

- Jelle Hellings  https://jhellings.nl/.
- ExpoLab  https://expolab.org/.
- ResilientDB  https://resilientdb.com/.


References II


References VII


References IX


References X


References XI
