Blockchain Economics

Joseph Abadi       Markus Brunnermeier

Princeton University
How can we generate consensus?

- Fundamental problem of record-keeping: Create trusted ledger

- What are the assumptions required to operate a trusted ledger?
  - Centralized ledger: Rents
  - PoS blockchain: External trust
  - PoW blockchain: Resource costs

- What are the tradeoffs and constraints in record-keeping?
  - When is PoW necessary?
  - How is PoS trust different from centralized trust?
  - Does the desired mechanism imply an optimal consensus algorithm?
Blockchain Trilemma
Self-sufficiency and external trust

- External trust: Capacity to **punish** other agents
  - a. Mutually beneficial relationships
    - Business relationships (news media, non-ledger related business)
    - Social connections (friends, colleagues)
    - Elected officials
  - b. Legal enforcement relationships

- Tradeoff: Lose social trust ⇒ System collapses

- Different from traditional centralized trust model! Local trust can be **scaled globally**
Summary of Trilemma

- Economic reasoning behind trilemma?
  - Three ways of distorting consensus
    - Digital signatures  (lose rents)
    - Social messages  (lose external trust)
    - PoW  (pay resource cost)

- Guiding framework about optimal record-keeping system
  - Small rent distortions  \(\Rightarrow\) Centralized/Permissioned
  - Robust external trust  \(\Rightarrow\) PoS, Ripple
  - No external trust + large rent distortions  \(\Rightarrow\) PoW
Roadmap

- Challenge of digital record-keeping
- Key model ingredients
- Benchmark example
  a. Centralized
  b. PoS blockchain
  c. PoW blockchain
- Proof idea
Challenge of digital record-keeping

- Key issue: No scarcity of digital “assets”
  - Unlike physical tokens
  - Ordering of messages matters
Solution: Consensus algorithm

- Three types: Differ in info. requirements to determine state
  - **Objective**: Set of messages sufficient for all users to achieve consensus
    - E.g. PoW “longest chain rule”
  - **Weakly subjective**: Set of messages + recent past state needed
    - Attacker votes twice ⇒ “Checkpoint” might be necessary
    - E.g. PoS “supermajority rule”
  - **Subjective**: Different users can come to different conclusions
    - E.g. Centralized system, Ripple

- Consensus guaranteed by incentive schemes
  - **Objective**: Cost of participation
  - **Weakly subjective**: Short-run punishments + Long-run reputation
  - **Subjective**: Long-run reputation
Roadmap

- Challenge of digital record-keeping
- Key model ingredients
  - Benchmark example
    a. Centralized
    b. PoS blockchain
    c. PoW blockchain
- Proof idea
Model: Users and mechanism

- **Users**: (Large number $N$)
  - External *trust relationships* between users $i, j \Rightarrow$ Bilateral utilities $u_{ij}$
    - Underlying graph $G$ of social connections
  - Users may pay *physical cost* $\kappa w$ to produce $w$ units of PoW
  - Two types of communication: Social messages + (pseudonymous) digital messages

- **Mechanism**:
  - State $s$ summarized by token holdings in pseudonymously-owned addresses
  - Mechanism $\mathcal{M}$ specifies actions $a_i(s)$ as a function of state, address ownership
    - Implicitly defines *rents* $r_{ij}$ extracted by user $i$ when $j$ is present
  - Utility of user $i$:
    $$U_i = V_i(s)_{\text{Tokens}} + \sum_j r_{ij} + \sum_j u_{ij} - \kappa W_i(s)_{\text{Exp. PoW}}$$
Model: Blocks and record-keeping

- **State** $s$: Allocation of tokens to addresses
  - Purpose of blockchain: Generate consensus on current state

- **Token transfer messages**: Message $(n, n', q)$ transfers $q$ tokens from $n$ to $n'$
  - Also incorporate seignorage/block rewards

- **Votes**: Arbitrary collection of messages $\mathcal{V}$ used to update state
  - Two types of permissions:
    - **Digital signatures**: E.g. PoS: Fraction of validators who sign a checkpoint
    - **External Proof**: E.g. PoW: Expected quantity of work required

- **Blocks**: Tuple $b = (m, v, p)$
  - $m$ Token transfer messages,
  - $v$ Votes cast on block
  - $p$ Pointer to previous block
Model: Consensus

- **Block tree**: Partially ordered set $B$ of blocks
  - Ordering induced by block pointers $p$
  - Blockchain: Ordered subset $C \subset B$

- **Consensus algorithm**: Update consensus chain given previous consensus $C^*_t$, blocks $B_{t+1}$
  - Function $C^*_{t+1} = g(C^*_t, B_{t+1})$
  - Previous state may be needed to determine consensus chain

- **Fundamental problem**: Desire to distort consensus
  - Three ways of distorting consensus $\Rightarrow$ Three types of costs

\[
U_i = V_i(s) + r_i + u_i - \kappa W_i(s)
\]

\[
\Rightarrow \Delta V_i \leq \Delta r_i + \Delta u_i - \kappa \Delta W_i
\]
Roadmap

- Challenge of digital record-keeping
- Key model ingredients
  - **Benchmark example**
    a. Centralized
    b. PoS blockchain
    c. PoW blockchain
- Proof idea
Benchmark example

- Consensus history \((H)\): A sent 50 tokens to B and 50 tokens to own account
- Alternate history \((H')\): A sent tokens to own account only
  - Can A convince a new user C of the alternate history?
  - Can A generate consensus on alternate history?
Example: Centralized ledger

- Monopolist A communicates history to users (**subjective**)
  - Old user B: Knows state transitioned from $s_0$ to $s_1$
  - New user C: Can be fooled by fraudulent report

Honest reporting: $A$ extracts rents from $B$ and $C$

$$U_A = V(s_1) + r_{AB} + r_{AC}$$
Example: Centralized ledger

- Dishonest reporting: Send entirely different ledger to C
  - C is fooled by A initially but stops using the system afterwards

\[
U_A = V(s_1) + r_{AB} + V_A
\]

\[\Rightarrow IC: V_A \leq r_{AC}\]
Example: PoS blockchain

- PoS consensus algorithm: Supermajority rule (weakly subjective)
  - Old user $B$: Knows state transitioned from $s_0$ to $s_1$
  - New user $C$: Concludes state is $s_1$ by supermajority rule
Example: PoS blockchain

- PoS consensus algorithm: Supermajority rule (weakly subjective)
  - Old user $B$: Knows state transitioned from $s_0$ to $s_1$
  - New user $C$: Needs input from trusted connection $A$

\[
\begin{align*}
D & \xrightarrow{u_{BD}} B \\
A & \xrightarrow{u_{AC}} C \\
H & (\text{doesn't know recent checkpoint})
\end{align*}
\]

Consensus History

\[
\begin{align*}
\text{Genesis} & \\
D & \xrightarrow{u_{BD}} B \\
A & \xrightarrow{u_{AC}} C \\
H & (\text{doesn't know recent checkpoint})
\end{align*}
\]

Honest reporting: A benefits from trust relationship with C

\[
U_A = V(s_1) + u_{AB} + u_{AC}
\]
Example: PoS blockchain

- PoS consensus algorithm: Supermajority rule (**weakly subjective**)
  - Old user $B$: Knows state transitioned from $s_0$ to $s_1$
  - New user $C$: Needs input from trusted connection $A$

Long-range attack: $A$ benefits from attack, loses trust with $C$

\[ U_A = V(s_1) + V_A \]
\[ \Rightarrow IC: V_A \leq u_{AC} \]
Example: PoW blockchain

- PoW consensus algorithm: Longest chain rule (objective)
  - Any user (old or new) can determine current state

Honest mining: Consensus is $s_1$

$$U_A = V(s_1)$$
Example: PoW blockchain

- PoW consensus algorithm: Longest chain rule (objective)
  - Any user (old or new) can determine current state

Double-spend: Consensus is $s_2$, pay physical resource cost

$$U_A = V(s_2) - (c_H - c_L)$$

$$\Rightarrow IC: V_A = V(s_2) - V(s_1) \leq c_H - c_L$$
Roadmap

- Challenge of digital record-keeping
- Key model ingredients
- Benchmark example
  - Centralized
  - PoS blockchain
  - PoW blockchain
- Proof idea
Statement of Blockchain Trilemma

- In order to achieve consensus in equilibrium, it must be that for any attacking coalition,

\[ V_A \leq r + u + c \]

- Impossible to have all three properties:
Statement of Blockchain Trilemma

- In order to achieve consensus in equilibrium, it must be that for any attacking coalition,

\[ V_A \leq r + u + c \]

- Depends on features of mechanism, external environment, and consensus algorithm
  - Rents/value of attack: Features of mechanism
  - External trust: Feature of environment
  - Resource cost: Feature of consensus algorithm
Proof sketch: Mimicking Lemma

- Always possible to present new user with a cryptographically valid alternate history
  - Centralized system: Give new user entirely different ledger
  - PoS blockchain: Long-range attack
  - PoW blockchain: Standard double-spend

- Extends to arbitrary hybrid consensus algorithms
  - Social messages + digital signatures + PoW are sufficient to create valid ledger
  - Who can attack?
    - Depends on writing permissions/possibilities for collusion
  - How much does it cost to attack?
    - Digital signature: Ex-post loss of rents
    - Social message: Ex-post loss of external trust
    - PoW: Ex-ante resource cost
Possession vs. Ownership: Enforcement

- Blockchain as a ledger for all kinds of assets— not just cryptocurrencies

- Who will enforce the ledger?

- So far: Ignored distinction between **ownership** and **possession**
  - Ownership is traded in a market
  - Possession is conferred by previous possessor and must be enforced
    - E.g. Owning a house with squatters inside

- Cryptocurrency is special: No need to enforce any agreements

---

You see, in this world, there are two types of people, my friend— those with loaded guns, and those who dig. You dig.
Conclusion

- Blockchain Trilemma:
  - Guiding framework to answer questions about how records should be kept
    - What security assumptions underlie different models of record-keeping?
    - Local external trust: Globally scalable with blockchain
  - Ownership vs. possession: Record-keeping is useful only if there’s enforcement