Blockchain: Why Would You Trust a Machine More Than a Bank?

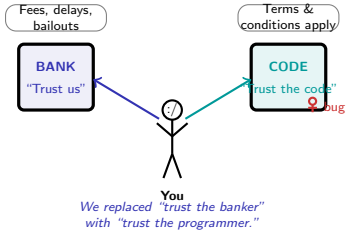
We invented a technology that replaces institutional trust with mathematical proof – and then discovered that trust is harder to remove than we thought

Digital Finance

Why Did Someone Invent a System Designed to Make Banks Unnecessary?

The Origin Story

October 31, 2008, six weeks after Lehman Brothers' 15 September 2008 Chapter 11 bankruptcy (the largest US bankruptcy filing in history, $639bn assets). The global financial system is collapsing. In this moment, a pseudonymous author named Satoshi Nakamoto (identity never confirmed; all public communication between Oct 2008 and Apr 2011 only) publishes a nine-page paper proposing a system where strangers can send money to each other without any bank, government, or intermediary.



The problem Satoshi identified:

- Every digital payment requires a trusted third party
- Trusted third parties charge fees, introduce delays, and can freeze your account
- The 2008 crisis proved that "trusted" institutions can fail catastrophically
- Why not replace the institution with a protocol?

The irony nobody anticipated:

- Bitcoin was designed to eliminate intermediaries
- Today, most people access Bitcoin through centralized exchanges
- FTX, the largest exchange, collapsed in 2022 – exactly like a bank
- We replaced one set of trusted intermediaries with another

Bitcoin was born from a financial crisis and a simple question: what if you did not need to trust anyone? The answer turned out to be more complicated than the question.

How Many Intermediaries Do You Trust With Your Money Right Now?

Reflection Prompt

Count every institution that touches your money between your employer paying your salary and you buying lunch:

Employer's bank → SWIFT/SEPA network → your bank → card network (Visa/Mastercard) → payment processor → merchant's bank.

That is at least **six intermediaries** for a single sandwich. Each one charges a fee, introduces a delay, and could freeze the transaction.

Now imagine they all disappeared overnight. No bank holds your salary. No card network processes your payment. No payment processor settles the merchant's account. Your money exists only as a cryptographic entry on a distributed ledger that nobody controls.

What you would gain:

- No fees to intermediaries – peer-to-peer transfer
- No delays – settlement in minutes, not days
- No one can freeze your account or reverse your transaction
- Access from anywhere with an internet connection

What you would lose:

- No fraud protection – if someone steals your keys, the money is gone
- No consumer protection – no chargebacks, no disputes, no ombudsman
- No deposit insurance – if the system fails, there is no safety net
- No customer service – you are your own IT department

Six intermediaries for a sandwich. Blockchain promises to remove them all – but it also removes every safety net they quietly provided.

(c) Joerg Osterrieder 2026

What Makes a Blockchain Different from a Regular Database?

Dimension	Centralized DB	Public Blockchain	Permissioned Blockchain
Control	Single admin	No admin (open)	Consortium of known parties
Trust model	Trust the operator	Trust the math	Trust the members
Write access	Admin only	Anyone (with fee)	Approved members
Read access	Controlled	Anyone	Members or public
Mutability	Full (update, delete)	Append-only	Append-only
Speed (TPS)	10,000+	7–30 (Bitcoin/ETH)	1,000–3,000
Energy cost	Low	Very high (PoW)	Low–moderate
Use case	Bank ledger, ERP	Cryptocurrency	Supply chain, trade finance

PoW = Proof of Work consensus (Bitcoin, Ethereum pre-Sep 2022): miners race to find a hash below the difficulty target; energy-intensive by design.

The key insight: A blockchain is a *deliberately inefficient database*. It sacrifices speed, storage, and energy efficiency to gain one thing no traditional database offers: the ability for parties who do not trust each other to share a single source of truth without a central authority.

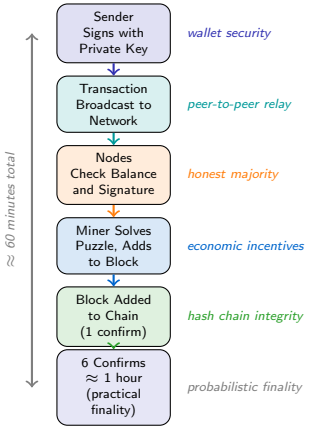
Three architectures, three trust assumptions

- **Centralized database:** One party controls everything. Fast, efficient, and simple – but you must trust the operator not to manipulate the data. Every bank runs on this model.
- **Public blockchain:** No one controls it. Anyone can read, anyone can write (by paying a fee). Trust comes from cryptographic proofs and economic incentives, not from any institution. Bitcoin and Ethereum use this model.
- **Permissioned blockchain:** A middle ground. Known participants share a ledger, but only approved members can write. Faster than public chains, but less decentralized. Hyperledger (Linux Foundation, 2016, IBM-led ecosystem including Fabric & Besu) and R3 Corda (R3 LLC, New York, 2015, 200+ bank consortium) use this model.

The question to ask: If a trusted central party already exists (a regulator, a bank, a clearinghouse), what does a blockchain add that a shared database does not?

A blockchain trades speed for trust – useful when no party can be trusted, wasteful when a trusted operator already exists.

Follow One Bitcoin Transaction from Send Button to Confirmed Block



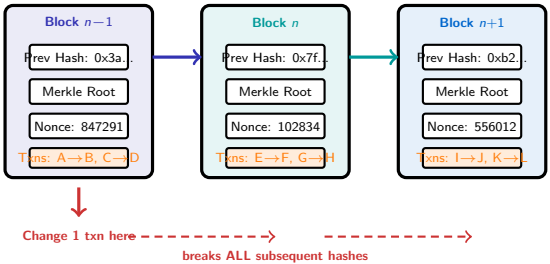
Six steps, no bank involved

- **Digital signature:** The sender proves ownership by signing the transaction with a private key – a secret number only they possess. If the key is lost or stolen, there is no recovery.
- **Network broadcast:** The signed transaction propagates across thousands of nodes. No single point of failure – but also no single party responsible for delivery.
- **Validation:** Every node independently verifies the sender has sufficient balance and the signature is valid. No central authority decides – majority consensus does.
- **Mining:** A miner expends computational energy to find a valid block. The reward (currently 3.125 BTC) incentivizes honest behavior. Cheating costs more than cooperating.
- **Chain inclusion:** The block is cryptographically linked to all previous blocks. Changing one transaction would require re-mining every subsequent block.
- **Finality:** After six confirmations, reversal is economically impractical. Not mathematically impossible – but more expensive than the transaction is worth.

Every step replaces a bank function with a cryptographic or economic mechanism – signing replaces identity, mining replaces clearing, and confirmations replace settlement.

(c) Joerg Osterrieder 2026

How Does a Chain of Blocks Become Tamper-Proof?



Three mechanisms, one guarantee

- **Hash pointers:** Each block contains the hash (cryptographic fingerprint) of the previous block. Change one bit in block $n-1$ and the hash changes – which invalidates block n, which invalidates block $n+1$, and so on. Tampering cascades forward.
- **Merkle root:** All transactions in a block are organized into a binary tree. The root hash summarizes every transaction. Changing any single transaction changes the Merkle root, which changes the block hash.
- **Nonce:** The "puzzle piece" that miners must find. The nonce is the number that, combined with the block contents, produces a hash meeting the difficulty target. Finding it requires enormous computation – re-finding it for a tampered block requires doing the work again.

The fingerprint analogy: Hashing is like taking a fingerprint of the entire block. You can verify the fingerprint instantly (milliseconds), but creating a block that matches a specific fingerprint takes billions of guesses.

Bottom line: Tampering with one block means re-mining every block after it – while the honest network keeps adding new blocks. The attacker can never catch up.

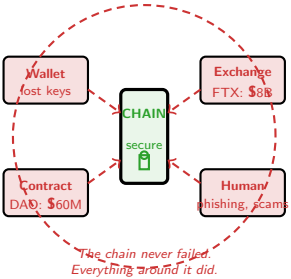
The chain of hash pointers is what makes a blockchain tamper-evident – changing history requires redoing all the work that came after it.

What Happens When a “Trustless” System Requires You to Trust the Wrong People?

The Chain Is Secure. Everything Around It Is Not.
The blockchain protocol itself has never been hacked. Bitcoin’s cryptographic core has operated without failure since 2009. But the ecosystem around it – wallets, exchanges, smart contracts, and humans – has failed spectacularly and repeatedly.

Three categories of trust failure:

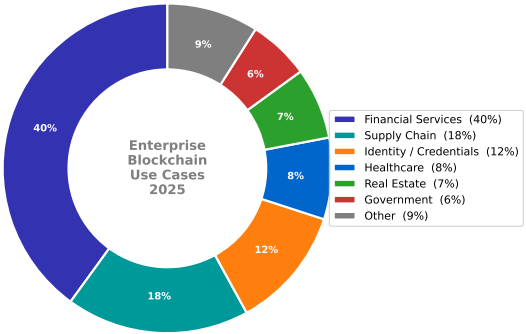
- **51% attack:** If a single entity controls the majority of mining power, it can rewrite recent history. Smaller blockchains (Ethereum Classic, 51% attack Jan 2019 ˜$1M double-spent; Bitcoin Gold, May 2018 $18M double-spent) have suffered this. Bitcoin itself is too expensive to attack – but the principle remains a vulnerability for any chain.
- **Smart contract exploits:** The DAO hack (2016) drained $60 million through a reentrancy bug. The code worked exactly as written – the problem was the design. Ethereum’s community hard-forked to reverse the damage, splitting into two chains and two philosophies.
- **Centralized exchange collapse:** FTX (2022) lost $8 billion of customer funds through fraud and mismanagement – exactly the kind of institutional failure blockchain was invented to prevent.



Blockchain’s cryptographic core is secure – but wallets, exchanges, smart contracts, and humans form a fragile perimeter that has failed repeatedly.

Where Is Blockchain Actually Being Adopted in Finance?

Enterprise Blockchain Use Cases by Sector (2025)



https://digital-ai-finance.github.io/Digital-Finance-Business/05_blockchain_fundamentals/55_blockchain_adoption_timeline

What the adoption pattern reveals

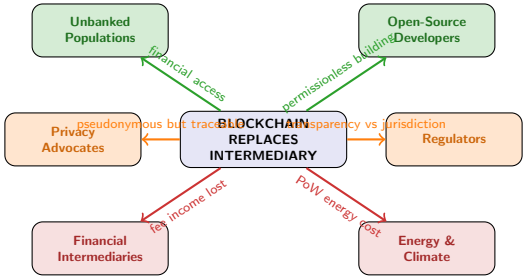
- **Payments lead adoption:** Cross-border payments are the clearest use case – correspondent banking is slow, expensive, and involves multiple intermediaries that blockchain can bypass
- **Securities settlement follows:** Moving from T+2 to near-instant settlement reduces counterparty risk and frees billions in capital currently locked during the settlement window
- **Trade finance is gaining traction:** Digitizing letters of credit and bills of lading on shared ledgers reduces document fraud and processing time from weeks to hours
- **Enterprise adoption outpaces public chains:** Most financial institutions use permissioned blockchains (Hyperledger, R3 Corda), not public ones. They want shared ledgers, not decentralization
- **Pilot-to-production gap persists:** Many projects remain in proof-of-concept phase. The gap between "tested in a lab" and "running in production" is measured in years

The pattern: Blockchain adoption follows the trust cost – the higher the intermediation cost, the stronger the business case for replacement.

Live deployments: Ripple/RippleNet (US, 2012, 300+ banks for cross-border); Stellar (US, 2014, Lumens XLM, IBM World Wire partnership); JP Morgan Onyx Digital Assets (US, 2020, tokenised collateral + JPM Coin); HSBC FX Everywhere (2018, $250bn FX trades); DTCC Project Ion (2022, post-trade settlement pilot); we.trade (EU, 2018–2022, trade finance, discontinued); Marco Polo (IBM+R3, trade finance, discontinued 2023).

Illustrative adoption timeline based on industry reports. Blockchain enters finance where intermediation costs are highest and trust between parties is lowest.

Who Wins and Who Loses When a Database Replaces an Institution?



Winners

+ **Unbanked populations:** 1.4 billion adults lack bank accounts (World Bank Global Findex 2021). Smartphone + internet = access to blockchain-based financial services – no bank required.
+ **Open-source developers:** Permissionless platforms let anyone build financial applications without banks or licenses.

Losers

– **Financial intermediaries:** Correspondent banks, clearinghouses, and payment processors lose fee income that blockchain-based settlement bypasses.
– **Energy and climate:** Bitcoin's Proof of Work consumes as much electricity as some countries (2024 est.: ˜150 TWh/year, Cambridge Bitcoin Electricity Consumption Index – comparable to Poland). Ethereum's Merge (Sep 2022) to Proof of Stake cut 99.95% of energy – but Bitcoin has not followed.

Mixed impact

~ **Privacy advocates:** Pseudonymous transactions offer privacy, but public ledgers are permanently traceable – a paradox.
~ **Regulators:** Gain ledger transparency but lose jurisdictional control over borderless, pseudonymous networks.

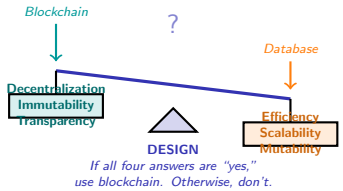
Blockchain creates winners among the excluded and losers among the established – but the environmental cost remains an unresolved tension.

(c) Joerg Osterrieder 2026

Four Questions That Reveal Whether a Use Case Actually Needs a Blockchain

The Blockchain Necessity Test
Before accepting or rejecting any blockchain proposal, ask:

1. **Is there a trust problem between multiple parties?**
   If all parties already trust a single operator (a bank, a regulator, a government), a centralized database is simpler, faster, and cheaper. Blockchain solves multi-party trust – not single-party efficiency.
2. **Do multiple parties need to write to the same ledger?**
   If only one party writes data, you do not need consensus. Blockchain's overhead only pays off when multiple writers must agree on a shared state without a central coordinator.
3. **Is immutability desirable, not just tolerable?**
   In some domains, the right to be forgotten (GDPR = General Data Protection Regulation, EU 2016/679, Article 17, enforced May 2018) or the ability to correct errors is essential. Blockchain's append-only nature is a feature for some use cases and a liability for others.
4. **Can you accept the speed and cost trade-off?**
   If the use case requires thousands of transactions per second at minimal cost, public blockchains cannot deliver. The deliberate inefficiency must be justified by the trust gain.



Most blockchain proposals fail at least one of these four questions – which is why most successful enterprise deployments are permissioned chains, not public ones.

(c) Joerg Osterrieder 2026

Should the Swiss Land Registry Use Blockchain?

Mini-Challenge (15 minutes)

The Swiss Grundbuch (land registry) is centralized, trusted, and efficient. Property ownership is recorded by cantonal land registry offices. Transfers require a notarized deed and are processed in days. The system has worked reliably for over a century. A consortium proposes migrating it to a permissioned blockchain shared across all 26 cantons.

Apply the four-question blockchain necessity test:

1. **Is there a trust problem?**
   - Do the 26 cantons distrust each other's registries?
   - Is there evidence of fraud or manipulation in the current system?
   - Would cross-cantonal property searches benefit from a shared ledger?
2. **Do multiple parties need to write?**
   - Currently, each canton writes to its own registry. Would shared writing across cantons add value or add complexity?
3. **Is immutability desirable?**
   - Property records must sometimes be corrected (boundary disputes, inheritance). Can append-only accommodate this?
4. **Can you accept the speed/cost trade-off?**
   - Property transfers are infrequent. Speed is not the constraint. But implementation cost is – is it justified by the benefit?

Closing thought: The future is not centralized OR decentralized – it is knowing when to use each.

The best way to evaluate blockchain is to apply it to a specific case – the Grundbuch forces you to distinguish genuine trust problems from technology in search of a problem.

(c) Joerg Osterrieder 2026