Charta | LESSON NOTES

Tokenisation and Market Inefficiencies

FRM Part II

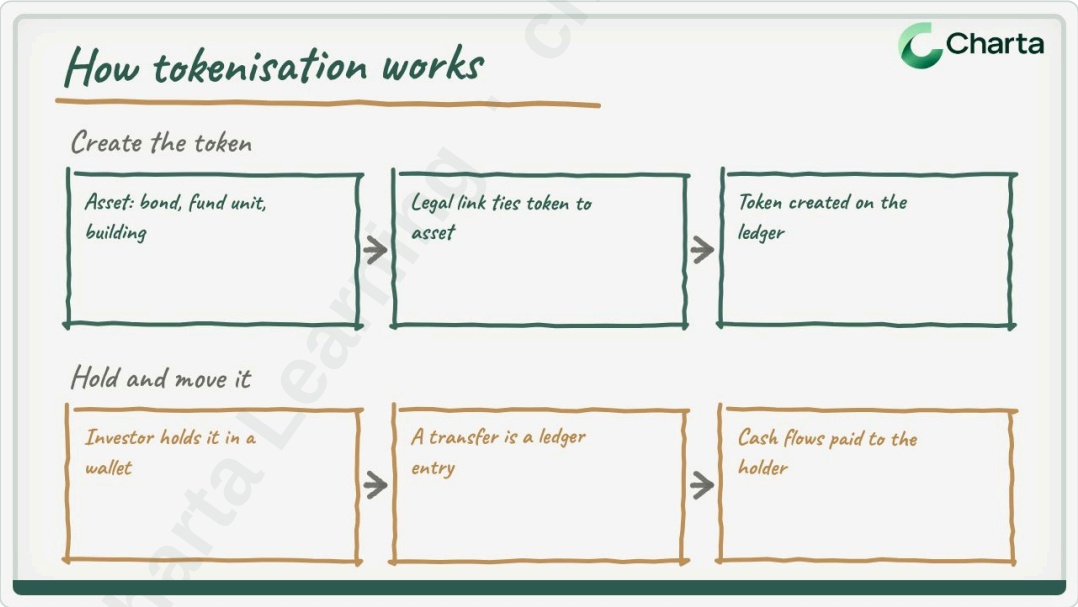
1 A story: Brenmoor's bond

- Brenmoor Bank issues a $50m bond
- Issuing is costly; big minimum purchase
- Trades settle a day or more later
- Chains of custodians keep their own records
- Coupons and votes handled by hand

IN THE LESSON

- Brenmoor Bank wants to issue a fifty million dollar bond.
- Today the process is slow.
- Lawyers, an underwriter and a central securities depository are all involved, and the minimum purchase is so large that only big institutions can buy.
- When a bond trades, it settles a day or more later, and in the meantime each side is exposed to the other.
- Ownership sits in a chain of custodians, each keeping its own copy of the records, which must be reconciled, meaning checked against each other.
- Coupons and votes are processed by hand.
- Brenmoor asks whether recording the bond on a digital ledger would remove these frictions.
- That idea is called tokenisation.

2 How tokenisation works



IN THE LESSON

- Tokenisation means recording a claim on an asset as a digital token on a ledger, so that ownership is held and transferred as ledger entries.
- Follow the first row, creating the token.
- Start with the asset: a bond, a fund unit, or a building.
- Then comes the legal link, a contract or a legal structure that ties the token to the asset.
- Then the token is created on the ledger, a step often called minting.
- Now the second row, holding and moving it.
- An investor holds the token in a digital wallet, an account on the ledger controlled by a private key, which works like a secret password.
- A transfer is simply a ledger entry.
- And the asset's cash flows, such as coupons, are paid to whoever holds the token.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

3 What changes, and what does not

A token is a new wrapper on the same claim

Feature	After tokenisation
Cash flows	Unchanged
Credit risk	Unchanged
How ownership is recorded	Changes
How it is divided	Changes
How it moves	Changes

IN THE LESSON

- A token is a new wrapper on the same claim.
- Be clear about what tokenisation does and does not change.
- The cash flows stay the same.
- A tokenised bond pays the same coupons as the bond itself.
- The credit risk stays the same too.
- If Brenmoor defaults, a token holder loses just as a bondholder would, because the token is only a new wrapper on the same claim.
- What changes is how ownership is recorded: on a shared digital ledger instead of in separate books.
- It changes how ownership can be divided, into small units.
- And it changes how ownership moves: by a ledger entry, possibly at any hour, and possibly at the same moment as the payment.

4 Three properties of a digital ledger

- Shared: many parties see one common record
- Programmable: smart contracts run rules automatically
- e.g. pay coupons; swap asset and cash at once
- Trusted: rely on the record without one counterparty

IN THE LESSON

- A digital ledger is described by three properties.
- First, it is shared.
- Many parties see one common record, instead of each keeping its own books and reconciling them.
- Second, it is programmable.
- Code attached to the ledger, called a smart contract, can carry rules that run automatically.
- A smart contract can pay a coupon on its due date, or exchange an asset for cash at the same instant so that neither side moves first.
- Third, it is trusted.
- Participants can rely on the record being correct without having to rely on any single counterparty.
- Remember the three words, shared, programmable and trusted, because the last part of this lesson asks how each ledger design supplies them.

5 Fungible, unique and fractional tokens

Kinds combine: parts of one building are fractional and fungible

Type	Meaning	Example
Fungible	Units identical, interchangeable	Tokens of one bond
Unique	One specific thing	Title to one gold bar
Fractional	One asset, many small units	Tower in 40,000 parts

IN THE LESSON

- Tokens come in different kinds, and the kinds combine: the parts of one building are both fractional and fungible.
- A fungible token is one where every unit is identical and interchangeable, like banknotes.
- The tokens of one bond issue are fungible: any one is as good as another.
- A unique token, often called non fungible, stands for one specific thing that cannot be swapped one for one, such as the title to a particular gold bar.
- A fractional token splits one asset into many small units, such as an office building divided into forty thousand parts.
- The forty thousand parts of one building are fractional, and they are also fungible with each other, because every part carries the same claim.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

6 Example 1: Brenmoor's bond as tokens

Brenmoor tokenises its $50m 4% bond into tokens of $100 each

Tokens issued	$50m ÷ $100	**500,000**
Total coupon a year	4% × $50m	**$2m**
Coupon per token	4% × $100	**$4**
Investor holds 25 tokens	25 × $100	**$2,500**
Her coupon, paid by code	25 × $4	**$100 a year**

IN THE LESSON

- Brenmoor tokenises its fifty million dollar bond, which pays four per cent a year, into tokens of one hundred dollars each.
- Fifty million divided by one hundred gives five hundred thousand tokens.
- The total coupon is four per cent of fifty million, which is two million dollars a year.
- Each token earns four per cent of one hundred, four dollars a year.
- Now an investor buys twenty five tokens.
- Twenty five times one hundred dollars is a holding of two thousand five hundred dollars.
- Her coupon is twenty five times four dollars, one hundred dollars a year, paid by the smart contract straight to her wallet on the due date.
- The bond is the same; only the size of the slice and the plumbing have changed.

7 Example 2, classic mistake: the token is not the title

Tower worth $40m split into 40,000 tokens. The issuing platform fails

Value per token	$40m ÷ 40,000	**$1,000**
Investor holds 10 tokens	10 × $1,000	**$10,000**
A: SPV owns tower, token = share	tower ring-fenced	**$10,000**
B: token is a claim on platform	30% recovery	**$3,000**

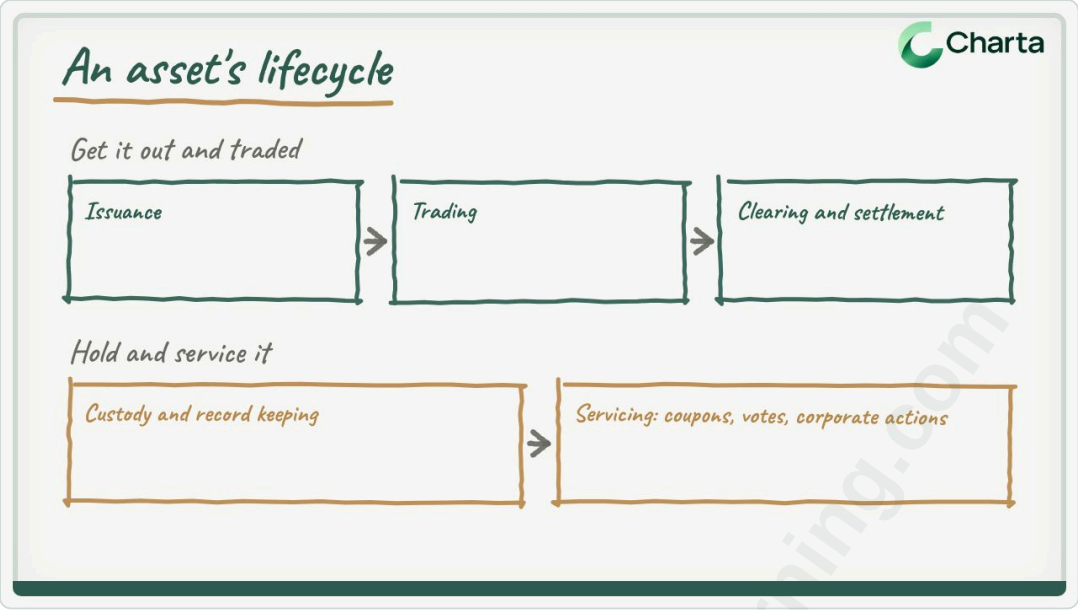
IN THE LESSON

- Now the classic mistake.
- Brenmoor also tokenises an office tower worth forty million dollars into forty thousand tokens, so each is worth one thousand dollars, and the platform that issued the tokens fails.
- An investor holds ten tokens, ten thousand dollars.
- Many people assume the token automatically gives legal title to a slice of the building.
- It does not.
- For an asset kept off the ledger, the legal link decides what the holder owns.
- In structure A, a special purpose vehicle, or S P V, a separate company set up only to own the tower, holds the building, and the token is a share in that vehicle.
- The tower is ring fenced from the platform's failure, so the holder still owns ten thousand dollars of building.
- In structure B, the token is only a contract with the platform.
- The holder is an unsecured creditor, and with a thirty per cent recovery gets three thousand dollars.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

8 An asset's lifecycle



IN THE LESSON

- To see where tokenisation helps, follow an asset through its lifecycle.
- The first row gets the asset out and traded.
- Issuance is when the asset is first created and sold to investors.
- Trading is when investors buy and sell it among themselves.
- Clearing and settlement come next: clearing works out who owes what, and settlement is the actual exchange of the asset for cash.
- The second row is about holding and servicing it.
- Custody and record keeping means safekeeping the asset and keeping the official record of who owns it.
- Servicing covers everything the asset does during its life: paying coupons and dividends, holding votes, and handling corporate actions such as splits or redemptions.

9 Frictions, and the feature that eases each

Pair each friction with the feature that eases it

Stage	Friction	Token feature
Issuance	Costly; big investors only	Fractional units
Trading	Fragmented; market hours	Continuous trading
Settlement	Days; exposure; trapped capital	Atomic settlement
Custody	Chains of copies to reconcile	One shared record
Servicing	Manual coupons and votes	Programmable servicing

IN THE LESSON

- Each stage has a friction, and a token feature that can ease it.
- Issuance is costly and limited to large investors, and fractional units open it to small ones.
- Trading is fragmented across venues and tied to market hours, and tokens can trade continuously.
- Settlement takes days, leaving each side exposed to the other and capital trapped while it waits.
- Atomic settlement cures that: the asset and the payment swap at once, or not at all.
- Custody involves chains of intermediaries holding copies of the same records, which must be reconciled, and one shared record removes that work.
- Servicing is manual, and programmable servicing lets the smart contract pay coupons and run corporate actions automatically.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

10 Atomic settlement

- Traditional: agree today, settle later
- In between: counterparty risk and trapped capital
- Atomic: asset and cash move in one indivisible step
- Both legs move, or neither does
- Window of exposure disappears

IN THE LESSON

- Atomic settlement deserves a closer look.
- In a traditional trade, the buyer and seller agree today and settle later.
- In between, either side could fail, so each faces counterparty risk, the risk that the other does not deliver.
- Both sides also hold collateral or cash against that risk, capital that is trapped and cannot be used elsewhere.
- On a ledger that holds both the token and a digital form of cash, a smart contract can move both legs in one indivisible step.
- Either the asset and the payment both move, or neither does.
- Settlement is then immediate, so the window of exposure disappears.
- The word atomic comes from the idea of a step that cannot be split.

11 Example 3: the settlement window

Brenmoor sells $20m of bonds to a fund; price rises 3% before settlement

Trade value	agreed today	**$20m**
Traditional settlement	trade date plus two	**2 days**
Seller fails after a 3% rise	3% × $20m	**$0.6m**
Atomic settlement	both legs at once	**$0**

IN THE LESSON

- Brenmoor sells bonds to a fund, and the price rises three per cent before settlement.
- The trade value, agreed today, is twenty million dollars.
- Traditional settlement in many markets comes on trade date plus two, which is two days later.
- Now suppose the seller fails to deliver after that three per cent rise.
- The fund must buy the same bonds elsewhere at the higher price, so it loses three per cent of twenty million, which is six hundred thousand dollars.
- That is the replacement cost the fund was exposed to.
- With atomic settlement, the bonds and the cash swap at the moment of the trade, so there is no window and no replacement cost: zero.
- The same logic applies to the cash or collateral that both sides would otherwise hold against that risk.

12 Features that also heighten risk

The same features create new risks

Feature	New risk	What goes wrong
Smart contracts	Code bugs	Faulty rule runs for all
Self-held keys	Theft, errors	Transfers cannot be undone
Many ledgers	Fragmentation	Liquidity split apart
Atomic, gross settlement	No netting	Pre-fund every trade
Automated actions	Mass triggers	Stress amplified

IN THE LESSON

- Now the other side.
- Each feature can also heighten risk.
- Smart contracts can contain code bugs, and a faulty rule runs for everyone at once.
- Keys held by investors themselves can be stolen or mistyped, and a transfer on the ledger generally cannot be undone.
- Many separate ledgers result in fragmentation, so liquidity splits across platforms that may not connect.
- Atomic settlement is gross and pre funded: each trade settles on its own with the cash already in place, so the netting that lets traders settle only their differences disappears, and liquidity needs rise.
- Finally, automated actions such as margin calls and liquidations can fire all at once, amplifying stress.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

13 Example 4: the cost of losing netting

A dealer buys $300m and sells $260m of bond tokens in one day

Netted: pay the difference	300 − 260	**$40m**
Gross, pre-funded: buys first	every purchase funded	**$300m**
Extra cash needed	300 − 40	**$260m**
Gross versus netted	300 ÷ 40	**7.5 times**

IN THE LESSON

- Here is the liquidity cost in numbers.
- A dealer buys three hundred million dollars of bond tokens and sells two hundred and sixty million during a day.
- In a traditional system with netting, the dealer pays only the difference at the end of the day, three hundred minus two hundred and sixty, forty million dollars.
- With gross, pre funded atomic settlement, each purchase needs cash in place when it settles.
- If the purchases settle before the sales, the dealer needs the full three hundred million.
- That is two hundred and sixty million more, and seven and a half times the netted amount.
- Faster settlement removes counterparty risk, but it can raise liquidity risk sharply.

14 Exam point: friction, cure, new risk

- Pair: friction, then cure, then new risk
- Slow settlement → atomic → must pre-fund
- Reconciling copies → shared record → code and key risk
- Shut out → fractional units → investor bears risk
- Manual servicing → programmable → automated stress

IN THE LESSON

- Here is the pattern for any question on the lifecycle.
- Pair each friction with the feature that cures it and the new risk that feature creates.
- Slow settlement is cured by atomic settlement, which brings the need to pre fund every trade.
- Copies of records that must be reconciled are cured by a shared record, which brings smart contract and key risk.
- Small investors shut out of issuance are let in by fractional units, but now they bear risks a broker used to handle.
- And manual servicing is cured by programmable servicing, whose automated actions can amplify stress.
- An answer that lists only the cures, or only the new risks, is half an answer.

15 Externalities: four that tokenisation shifts

- Externality: an unpriced effect on others
- 1. Shock spread
- 2. Infrastructure investment
- 3. Network effects
- 4. Shared knowledge

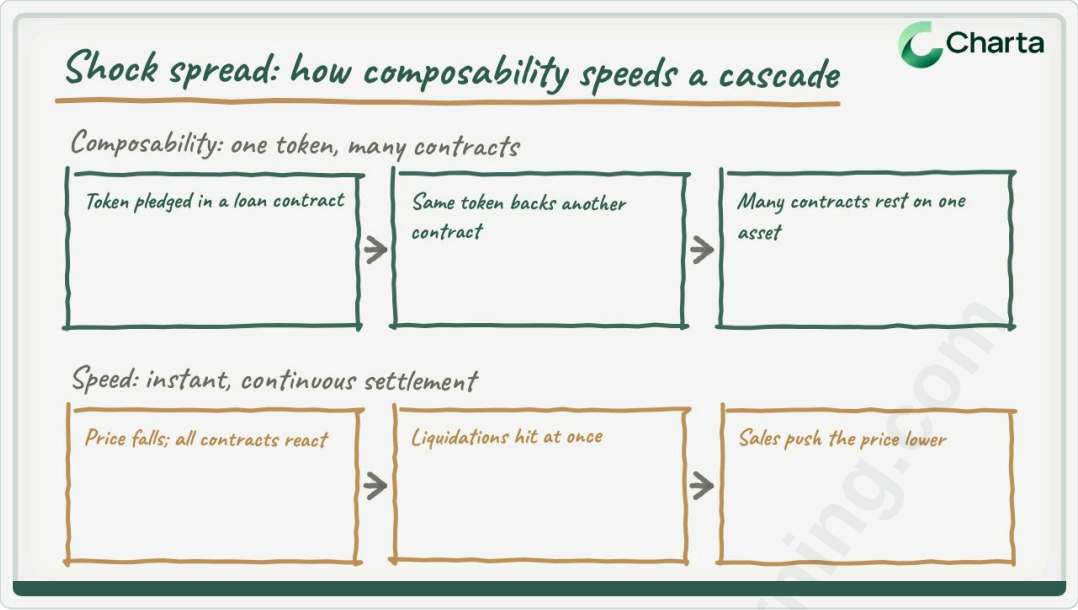
IN THE LESSON

- Now a wider view.
- An externality is an effect of a decision on other people that the decision maker does not price.
- Pollution from a factory is the textbook case.
- Tokenisation shifts four externalities in financial markets.
- First, how shocks spread from one firm to others.
- Second, how much gets invested in market infrastructure, the shared plumbing that everyone uses.
- Third, network effects, where a ledger becomes more valuable as more people use it.
- And fourth, shared knowledge, the spillovers from open code and public data.
- For each one, we will see that tokenisation can help and can harm.
- Keep that two sided view in mind throughout.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

16 Shock spread: how composability speeds a cascade



IN THE LESSON

- Start with shock spread.
- Composability means that tokens and smart contracts can be plugged into each other like building blocks.
- The first row shows what it builds.
- One token can be pledged as collateral in a lending contract.
- The same token, or a claim on it, can back a second contract, such as a derivative.
- So many contracts rest on one asset.
- The second row shows the speed.
- A price falls, and every contract that uses the token reacts.
- Settlement is instant and continuous, with no market close and no settlement delay.
- So liquidations, the forced sales of collateral, hit the market at once, and each sale can push the price down further.

17 Example 5: a liquidation cascade

Funds A and B borrow against the same token; sold when loan > 85% of value

Fund A: $80m on $100m	80 ÷ 100	**LTV 80%**
Fund A trigger: a fall of	1 − 80 ÷ 85	**5.9%**
Fund B: $83m on $100m	83 ÷ 100	**LTV 83%**
Fund B trigger: a fall of	1 − 83 ÷ 85	**2.4%**
B's sales push past A's trigger	2.4% then 5.9%	**cascade**

IN THE LESSON

- Two funds borrow against the same token.
- A smart contract sells the collateral when a loan exceeds eighty five per cent of the collateral's value; that ratio is called loan to value.
- Fund A borrows eighty million against one hundred million, a loan to value, or L T V, of eighty per cent.
- Its trigger comes when the loan reaches eighty five per cent of the value, which takes a fall of one minus eighty over eighty five, about five point nine per cent.
- Fund B borrows eighty three million, a loan to value of eighty three per cent.
- Its trigger is a fall of one minus eighty three over eighty five, about two point four per cent.
- So a dip of two point four per cent forces B to sell, its sales push the price down, and if the price passes five point nine per cent, A is sold too.
- That is a cascade.

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

18 Example 6: infrastructure as a public good

Shared ledger: $50m benefit spread over 10 banks; costs $30m to build

Benefit to the whole market	50 > 30: worth it	**$50m**
Benefit to any one bank	50 ÷ 10	**$5m**
One bank alone pays $30m	5 < 30	**not built**
Ten banks share the cost	30 ÷ 10	**$3m each**
Each bank better off by	5 − 3	**$2m**

IN THE LESSON

- Now infrastructure investment.
- Suppose a shared ledger for Brenmoor's market would bring fifty million dollars of benefit, spread equally over ten banks, and costs thirty million to build.
- Shared infrastructure is partly a public good: once built, everyone benefits, and the builder cannot charge for all of it.
- For the market as a whole, fifty exceeds thirty, so it is worth building.
- But each bank gets fifty divided by ten, five million.
- No single bank will spend thirty million for five million of benefit, so nothing gets built: underinvestment.
- If the ten banks share the cost, each pays three million and gains five, two million better off.
- That is why consortia and open standards matter.
- Open standards also lower the cost for new firms to join.

19 Example 7: network effects and staying apart

Pairs of users who can deal directly on a ledger of n users: n(n − 1) ÷ 2

Ledger of 10 banks	10 × 9 ÷ 2	**45 pairs**
Two ledgers of 10	2 × 45	**90 pairs**
One ledger of 20	20 × 19 ÷ 2	**190 pairs**
Gain from joining up	190 − 90	**100 pairs**
A lone bank that moves first	leaves 9, finds none	**stays put**

IN THE LESSON

- Third, network effects.
- The value of a ledger rises with the number of users, because each new user can deal with all the others.
- A simple count is the number of pairs of users who can deal directly, which is n times n minus one, over two.
- A ledger of ten banks has ten times nine over two, forty five pairs.
- Brenmoor's market has two such ledgers, so ninety pairs.
- One ledger of all twenty banks would have twenty times nineteen over two, one hundred and ninety pairs, a gain of one hundred.
- That pull explains winner take most outcomes.
- Yet a combined ledger starts empty.
- A lone bank that moves first leaves its nine partners and finds nobody there, so nobody moves.
- That is a coordination failure, and the market stays fragmented.

20 Shared knowledge

- Open code and public data create spillovers
- Others learn; good designs spread fast
- Rivals can copy an innovation at once
- Less reward, so less incentive to innovate

IN THE LESSON

- The fourth externality is shared knowledge.
- On many ledgers, the code of smart contracts is open, and the data, such as transactions and positions, are public.
- That creates spillovers, benefits that flow to people who did not pay for them.
- Other firms, researchers and supervisors learn from the code and data, and good designs spread quickly.
- But the same openness lets rivals copy an innovation at once.
- If a firm cannot keep the rewards of its own design, it has less reason to invest in creating it.
- So open code helps learning while weakening the incentive to innovate.
- Once again, the effect cuts both ways.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

21 Each externality cuts both ways

Classic mistake: calling these pure benefits or pure harms

Externality	Can help	Can harm
Shock spread	Transparent positions	Fast cascades via reuse
Infrastructure	Lower entry cost	Too little gets built
Network effects	One large pool of users	Winner takes most; split
Shared knowledge	Spillovers aid learning	Rivals copy; less innovation

IN THE LESSON

- Here is the summary, and it carries the classic mistake: treating these effects as pure benefits or pure harms.
- Shock spread: transparent positions can reduce hidden exposures, because anyone can see who holds what, but reuse of tokens and instant settlement let cascades run fast.
- Infrastructure: open standards lower the cost of entry, but because shared infrastructure is partly a public good, too little of it gets built.
- Network effects: one large pool of users is valuable, but that favours winner take most outcomes, or markets that stay split.
- Shared knowledge: spillovers aid learning, but rivals copy, so there is less innovation.
- Always give both sides.

22 What changes for individual investors

The protections a broker gave move to the investor

Area	Through a broker	On a shared ledger
Minimum size	Large lots	Fractional tokens
Trading, settlement	Market hours; days	Near-continuous; fast
Custody	Broker safeguards	Own private keys
Mistakes and fraud	Checks before transfer	Usually irreversible
Suitability	Broker checks fit	Investor judges, code too

IN THE LESSON

- Now imagine distributed ledgers in wide use.
- What changes for an individual investor?
- The minimum size falls, from large lots to fractional tokens, so access becomes cheaper.
- Trading and settlement move from market hours and days to near continuous trading and fast settlement.
- Custody moves from the broker's safeguards to the investor's own private keys, a model called self custody, which gives direct control, along with programmable rights, such as automatic payouts.
- Mistakes and fraud were once caught by the broker's checks before a transfer, but on a ledger a mistaken or fraudulent transfer is usually irreversible.
- And suitability, the check that a product fits the investor, once done by the broker, now falls to the investor, including judging smart contract risk.

23 Example 8: Nadia, a small saver

Nadia has $2,000. Bond lot $100,000; tokens $100. Fees 1% vs 0.2%

Traditional lot: $100,000	more than her $2,000	**cannot buy**
Tokens she can buy	2,000 ÷ 100	**20 tokens**
Fee: 1% vs 0.2% of $2,000	$20 − $4	**$16 saved**
Key lost or wrong address	no one can reverse it	**−$2,000**

IN THE LESSON

- Meet Nadia, who has two thousand dollars to invest.
- Brenmoor's bond, sold the traditional way, has a minimum lot of one hundred thousand dollars.
- That is more than her two thousand, so she cannot buy it at all.
- In token form she can buy two thousand divided by one hundred, twenty tokens.
- Suppose a broker route to similar assets would charge a one per cent fee on two thousand dollars, twenty dollars, while the token platform charges zero point two per cent, four dollars.
- She saves sixteen dollars.
- Now the other side.
- Nadia holds her own private key.
- If she loses it, or sends her tokens to a wrong address, there is no broker to reverse the transfer, and she can lose the whole two thousand dollars.
- Her risk has not simply fallen.
- It has changed form and moved to her.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

24 Example 9: a broker's revenue

A broker earns $100m a year; $40m of it is intermediation fees

Intermediation fees today	settle, custody, records	**$40m**
Advice, onboarding, access	100 − 40	**$60m**
Shared ledger removes half	40 × 50%	**– $20m**
Advice and access grow 10%	60 × 10%	**+$6m**
New revenue	100 − 20 + 6	**$86m**

IN THE LESSON

- Now the brokers.
- A broker earns one hundred million dollars a year.
- Its intermediation fees today, for settlement, custody, reconciliation and record keeping, bring in forty million.
- That is work a shared ledger partly makes unnecessary.
- Advice, onboarding, compliance and access services bring in the rest, one hundred minus forty, sixty million.
- Suppose the shared ledger removes half of the intermediation fees: forty times fifty per cent, twenty million dollars lost.
- Meanwhile demand grows for advice, access and liquidity provision, the services where trust and the customer relationship still matter.
- Say that business grows ten per cent: sixty times ten per cent, six million dollars gained.
- New revenue is one hundred minus twenty plus six, eighty six million dollars.
- The broker shrinks and changes, but it does not vanish.

25 Brokers change role; risk changes form

- Settlement, custody, record-keeping fees under pressure
- Shift to advice, onboarding, compliance
- Also liquidity provision and access services
- Mistake: brokers disappear entirely
- Mistake: investor risk simply falls; it moves

IN THE LESSON

- Pull this together.
- A large part of brokers' revenue comes from intermediating settlement, custody, reconciliation and record keeping, and a shared ledger makes much of that unnecessary, so those fees come under pressure.
- Brokers are likely to shift toward advice, onboarding and compliance, liquidity provision, and access services such as helping clients hold keys safely, the work where trust still matters.
- Now the two classic mistakes.
- The first is to say brokers disappear entirely.
- They do not; their role changes.
- The second is to say investor risk simply falls.
- It does not; the risk changes form and moves to the investor, who now guards the keys and judges the code.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

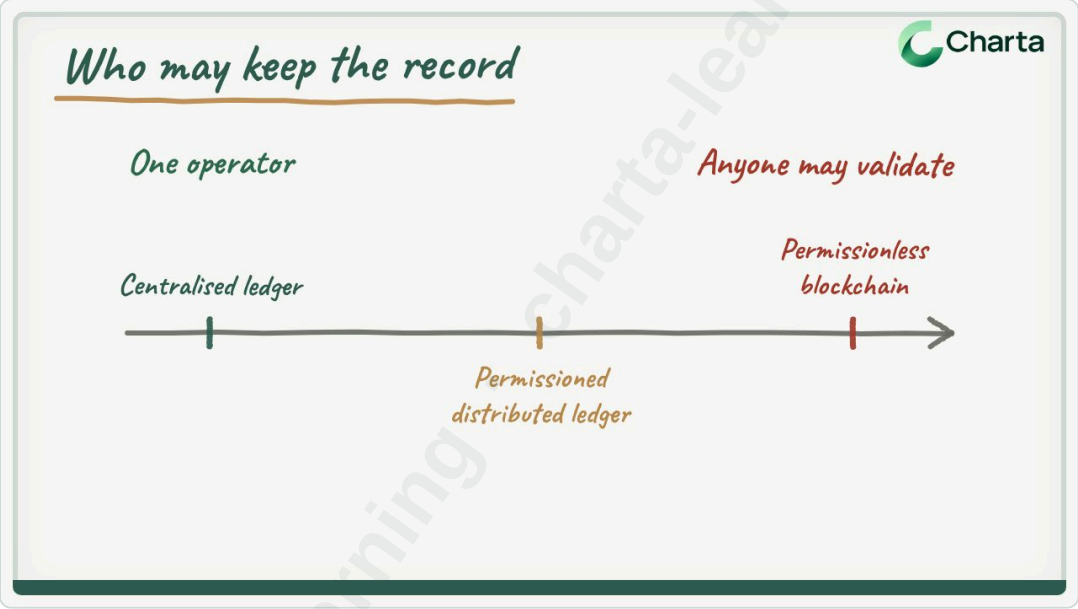
26 Three things every ledger needs

- Sharedness: many parties hold or see one record
- Programmability: rules execute automatically
- Trust: confidence the record is correct
- Ask: whose honesty or code must we rely on?

IN THE LESSON

- Finally, how is a ledger built?
- Every ledger needs three things.
- Sharedness: many parties hold or see the same record.
- Programmability: rules that execute automatically.
- And trust: confidence that the record is correct.
- These are the three properties from the start of the lesson, now treated as things a design must supply.
- There are several ways to supply them, and each has its own point of failure.
- The key question for any design is simple.
- Whose honesty, or whose code, must be relied on for the record to be correct?
- Ask that, and you can see when trust can break down.

27 Who may keep the record



IN THE LESSON

- The designs sit on a line by who may keep the record, from one operator at the left to anyone who wishes at the right.
- At the left is a centralised ledger.
- One operator, such as a central securities depository or a single platform, keeps the record and runs the code.
- Users can see the record, so it is shared in that sense, but it is not distributed.
- In the middle is a permissioned distributed ledger.
- A known, approved group of validators, the parties who check and add entries, each hold a copy and agree on it through a consensus rule.
- At the right is a permissionless blockchain.
- Anyone may validate, and the network relies on cryptography and economic incentives instead of known identities.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

28 Where trust rests, and when it breaks

Each design has its own point of failure

Design	Trust rests on	Breaks if
Centralised	One operator	It fails, errs or is hacked
Permissioned	Known validators	Too many collude; capture
Permissionless	Cryptography, incentives	Majority of work or stake
Smart contracts	Code; oracle (price feed)	Bugs; manipulated oracle

IN THE LESSON

- Now, for each design, where trust rests and when it breaks.
- In a centralised ledger, trust rests on the one operator, and breaks if it fails, makes an error, or is hacked.
- In a permissioned ledger, trust rests on the known validators and their consensus rule, and breaks if too many of them collude, or if the governance that chooses them is captured by one interest.
- In a permissionless blockchain, trust rests on cryptography and incentives, and breaks if an attacker controls a majority of the computing work or of the stake.
- Finally, smart contracts supply programmability on any of these ledgers.
- They depend on code and on oracles, the feeds that bring outside data such as a market price onto the ledger.
- They fail through code bugs or a manipulated oracle, even when consensus works perfectly.

29 How the distributed designs agree

- Permissioned: Byzantine fault tolerant consensus
- Tolerates f faulty validators if n ≥ 3f + 1
- Why: wait for n − f replies; honest n − 2f must exceed f
- n counts all validators; f only the faulty ones
- Permissionless: make attacks expensive
- Proof of work: computing power. Stake: locked tokens
- Majority of work or stake can rewrite the record

IN THE LESSON

- How do the distributed designs agree on one record?
- A permissioned ledger usually uses a Byzantine fault tolerant protocol.
- The name comes from a puzzle about generals who must agree on a plan when some of them may be traitors.
- Such protocols keep the record correct even if some validators are faulty or dishonest, provided there are enough honest ones.
- Classical protocols need n validators to be at least three f plus one, to tolerate f faulty ones.
- Why three f plus one?
- Up to f validators may be silent or lying, so the ledger can only wait for n minus f replies.
- Among those, the honest ones must still outnumber the liars, so n minus two f must exceed f, which gives n at least three f plus one.
- Here n counts all validators, and f only the faulty ones.
- A permissionless blockchain cannot count known validators, so it makes attacks expensive.
- Under proof of work, validators spend computing power.
- Under proof of stake, they lock up tokens they lose if they cheat.
- An attacker with a majority of the work or the stake could rewrite the record.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

30 Example 10: how many faulty validators?

Brenmoor's permissioned ledger has 10 validators. Rule: n ≥ 3f + 1

Most faulty it can tolerate	f ≤ (10 − 1) ÷ 3	**f = 3**
Check the rule	3 × 3 + 1 = 10 ≥ 10	**holds**
To tolerate 4 faulty	3 × 4 + 1	**13 needed**
If 4 of the 10 collude	4 > 3	**trust breaks**

IN THE LESSON

- Brenmoor's permissioned ledger has ten validators.
- How many faulty ones can it tolerate?
- The rule is n at least three f plus one.
- So the most faulty validators it can tolerate is f at most ten minus one, over three.
- Ten minus one is nine, and nine over three is three, so f is three.
- Check it: three times three plus one is ten, and ten is at least ten, so the rule holds.
- To tolerate four faulty validators, the ledger would need three times four plus one, thirteen validators.
- So if four of Brenmoor's ten validators collude, four is more than three, and the guarantee is gone: trust in the record breaks.
- That is why governance matters: who chooses the validators decides how easy collusion is.

31 Example 11: consensus works, the oracle fails

1,000 tokens truly worth $100; loan $70,000; contract liquidates at 90% LTV

Collateral at the true price	1,000 × $100	**$100,000**
Loan to value, true	70,000 ÷ 100,000	**70%**
Oracle reports $70	1,000 × $70	**$70,000**
Loan to value, per oracle	70,000 ÷ 70,000	**100%**
100% > 90%: contract sells	consensus worked	**wrongly sold**

IN THE LESSON

- Now a failure that consensus cannot prevent.
- An oracle is the feed that brings outside data, such as a market price, onto the ledger.
- An investor pledges one thousand tokens, truly worth one hundred dollars each, so the collateral is worth one hundred thousand dollars.
- Her loan is seventy thousand, so the loan to value, true, is seventy thousand over one hundred thousand, seventy per cent.
- The contract liquidates at ninety per cent.
- An attacker manipulates the oracle so that it reports seventy dollars a token.
- The contract now values her collateral at one thousand times seventy, seventy thousand dollars.
- Her loan to value, per the oracle, is seventy thousand over seventy thousand, one hundred per cent.
- One hundred is more than ninety, so the contract sells her tokens, although consensus worked.
- Every validator agreed correctly on what the contract did.
- The record is accurate; the input was wrong.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.

32 Mistakes to avoid

- A token does not automatically carry legal title
- List the new risk with each cure, e.g. lost netting
- Externalities cut both ways
- Brokers change role; investor risk moves, not falls
- Consensus does not protect against bugs or bad oracles

IN THE LESSON

- Before the quiz, here are the mistakes to avoid across the whole topic.
- Do not assume a token carries legal title.
- For an off ledger asset, the legal link decides what the holder owns.
- Do not list only the cures.
- Pair each friction with its feature and the new risk, such as atomic settlement and the loss of netting.
- Do not call the externalities pure benefits or pure harms; each cuts both ways.
- Do not say brokers disappear, or that investor risk simply falls; the roles change and the risk moves.
- And do not think consensus guarantees correct outcomes.
- Bugs and manipulated oracles break smart contracts even when every validator agrees.

33 Try three quick questions

1. A permissioned ledger has 7 validators. How many faulty can it tolerate?
   Answer: f = (7 − 1) ÷ 3 = 2. Check: 3 × 2 + 1 = 7.
2. Dealer buys $50m, sells $45m of tokens. Cash needed: netted, then gross?
   Answer: Netted $5m; gross, buys first, $50m.
3. Does a building token automatically make you its legal owner?
   Answer: No: the legal link decides, e.g. SPV shares.

IN THE LESSON

- Try three quick questions, then listen to the answers.
- Question one.
- A permissioned ledger has seven validators.
- How many faulty validators can it tolerate?
- Seven minus one is six, and six over three is two.
- Check: three times two plus one is seven.
- Question two.
- A dealer buys fifty million dollars of tokens and sells forty five million in a day.
- How much cash does it need with netting, and with gross pre funded settlement if the buys come first?
- With netting, five million.
- Gross, the full fifty million.
- Question three.
- Does holding a building token automatically make you a legal owner of the building?
- No.
- It depends on the legal link, for example shares in a vehicle that owns it.
- Otherwise it may be only a claim on the platform.

Summary notes for the Charta whiteboard lesson. Figures are from the lesson's made-up examples.

Charta Learning · charta-learning.com

© Charta Learning · charta-learning.com · For your own study. Please do not share or redistribute.