DeFi AND THE Future of Finance

Course II:

DeFi Primitives

2. Supply and Ownership

(ii) Supply Adjustment

Supply adjustment

Burn (reduce supply)

- To burn a token means to remove it from circulation.
- Burning a token can take two forms:
  - Manually send a token to an <u>unowned Ethereum address</u>.
  - More efficient is to create a contract that is incapable of spending them.
- Either approach renders the burned tokens unusable, although the decrease in circulating supply would not be "known" by the token contract. Burning is analogous to the destruction or irreversible loss of currency in the traditional finance world, which is unknown to the issuing government.

Supply adjustment

Burn mistakes

- In practice, ETH or ERC-20 tokens have frequently and accidently been burned using both forms.
- Checksums are one method used to prevent accidental burn.
  - These are cryptographic primitives used to verify data integrity.
  - In the context of Ethereum addresses, EIP-55 proposed a specific checksum encoding of addresses to stop incorrect addresses' receiving token transfers.
  - If an address used for a token transfer does not include the correct checksum metadata, the contract assumes the address was mistyped and the transaction would fail.

Supply adjustment

Why burn?

- Here are some practical reasons:
  - Represent exiting of a pool and <u>redemption of underlying</u> (common in equity tokens like cTokens for Compound)
  - Increase scarcity to drive the price upward (e.g., AAVE)
  - Penalize bad acting

Supply adjustment

Minting (increase supply)

- Minting increases the number of tokens in circulation.
- Contrary to burning, there is no mechanism for accidentally or manually minting tokens.
- Any mint mechanics have to be directly encoded into the smart contract mechanism.
- There are many use cases for minting as it can incentivize a wider range of user behavior.

Supply adjustment

Minting (increase supply)

- Here are some examples:
  - Represent entering a pool and acquiring corresponding ownership share (common in equity tokens like cTokens for Compound)
  - Decrease scarcity (increase supply) to drive the price downward (seigniorage Stablecoin models like Basis/ESD)
  - Reward user behavior

Supply adjustment

Minting as an incentive mechanism

- *Inflationary rewards* has become a common practice to encourage actions such as supplying liquidity or using a particular platform.
- Many users engage in *yield farming*, taking actions to seek the highest possible rewards. Platforms can bootstrap their networks by issuing a token with an additional value proposition in their network.
- Users can keep the token or sell it for a profit. Either way, utilization of the token benefits the platform by increasing activity.

Supply adjustment

Bonding curves

- One advantage of being able to adjust supply up and down on a contractual basis is being able to define a bonding curve.
- A bonding curve is the price relationship between the token supply and a corresponding asset used to purchase the token(s).
- In most implementations investors sell back to the curve using the same price relationship.
- The relationship is defined as a mathematical function or as an algorithm with several clauses.

Supply adjustment

Linear bonding curves

- Let TKN to denote the price of a token denominated in ETH (which could be any fungible cryptoasset) and use *S* to represent the supply.
- The simplest possible bonding curve would be TKN=1 (or any constant).
- This algorithmically enforces a one to one peg between ETH and TKN

Supply adjustment

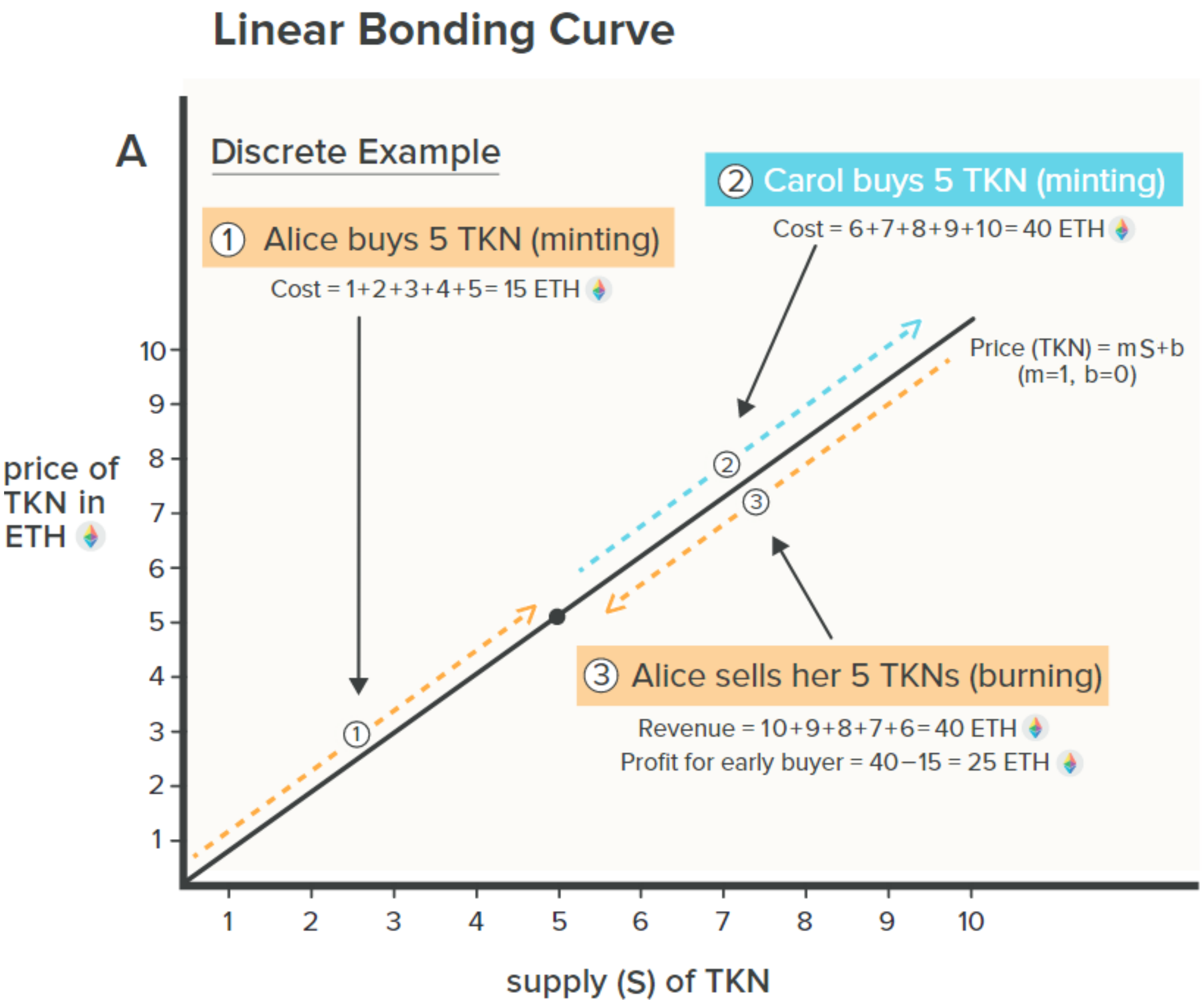
Linear bonding curves

- Next, consider a simple linear bonding curve, where *m* and *b* represent the slope and intercept, respectively, in a standard linear function.
- If *m* = 1 and *b* = 0, the first TKN would cost 1 ETH, the second would cost 2 ETH, and so on.
- A monotonically increasing bonding curve rewards early investors, because any incremental demand beyond their purchase price would allow them to sell back against the curve at a higher price point.

Supply adjustment

Linear bonding curves

- Alice is rewarded for being an early investor



Linear Bonding Curve

Discrete Example

① Alice buys 5 TKN (minting)

Cost = 1+2+3+4+5= 15 ETH

② Carol buys 5 TKN (minting)

Cost = 6+7+8+9+10= 40 ETH

③ Alice sells her 5 TKNs (burning)

Revenue = 10+9+8+7+6= 40 ETH

Profit for early buyer = 40−15 = 25 ETH

Supply adjustment

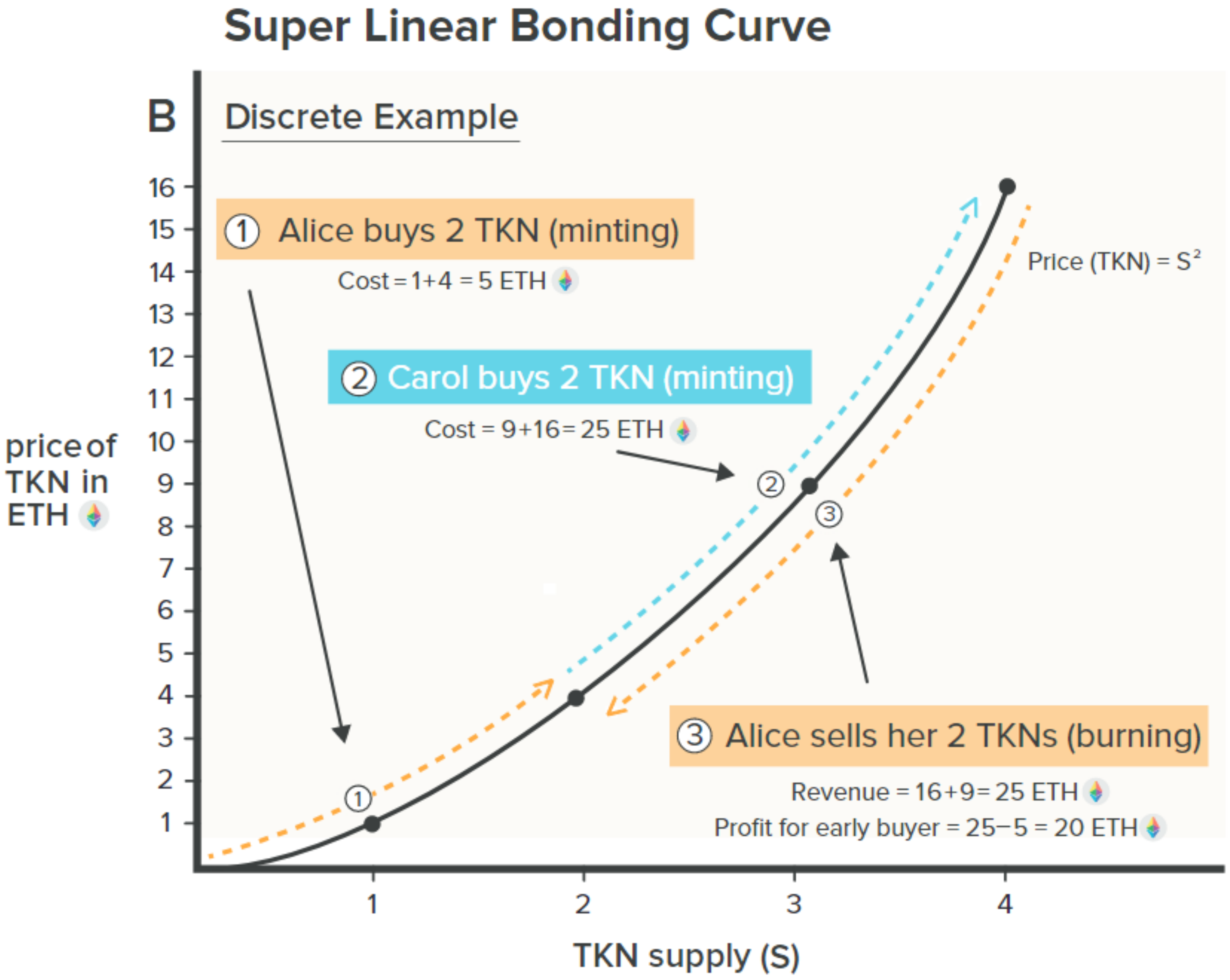
Linear bonding curves mechanics

- The curve can be represented as a single smart contract with options for purchasing and selling the underlying token.
- The token to be sold can have either an uncapped supply with the bonding curve as an authorized minter or a predetermined maximum supply that is escrowed in the bonding curve contract.
- As traders purchase the token, the bonding curve escrows the incoming funding for the point in the future when a trader may want to sell back against the curve.

Supply adjustment

Super-linear bonding curves

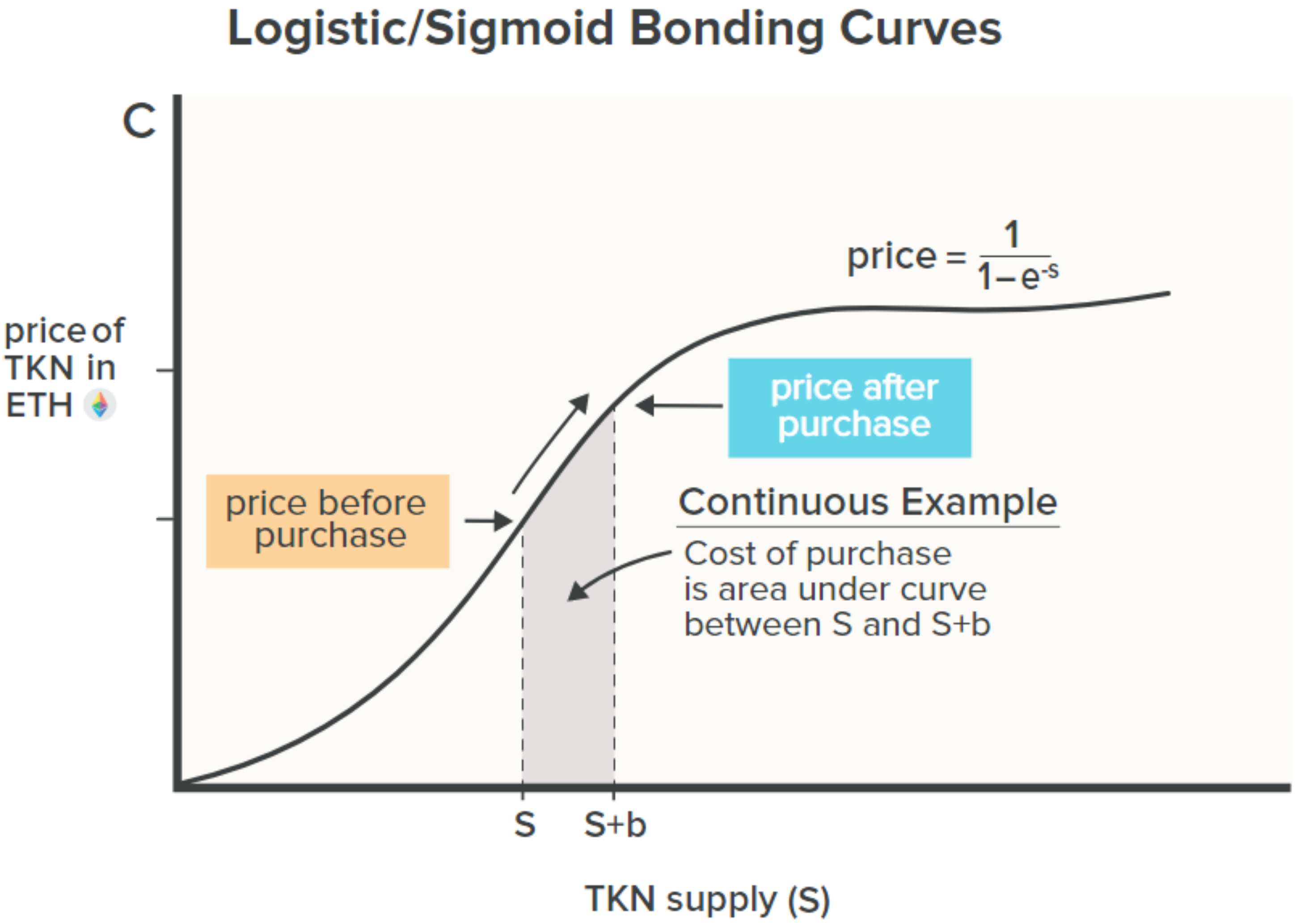
- Example: TKN = S^2
- More extreme rewards for early investors



Supply adjustment

Logistic bonding curves

- Rewards early but then flattens out

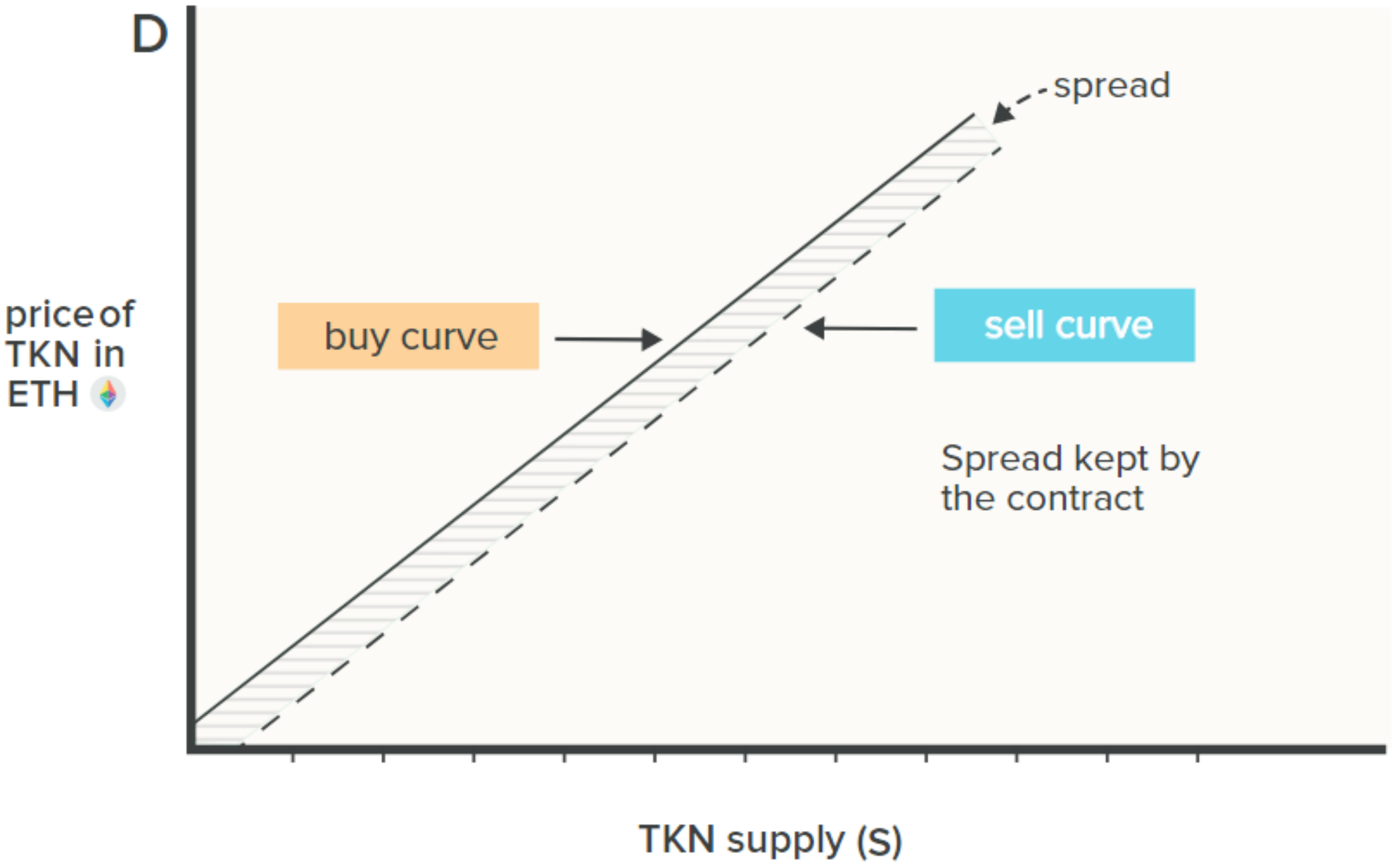


Supply adjustment

Buy vs. sell bonding

- It is possible to have different curves for buying and selling
- The spread is kept by the contract

Bonding Curves: Differences for Purchase & Sales


D
price of TKN in ETH
spread
buy curve
sell curve
Spread kept by the contract
TKN supply (S)