



Public / Private Keys

and how they will change
financial services

Stefan Loesch
The Short STOrY Podcast
June 2020

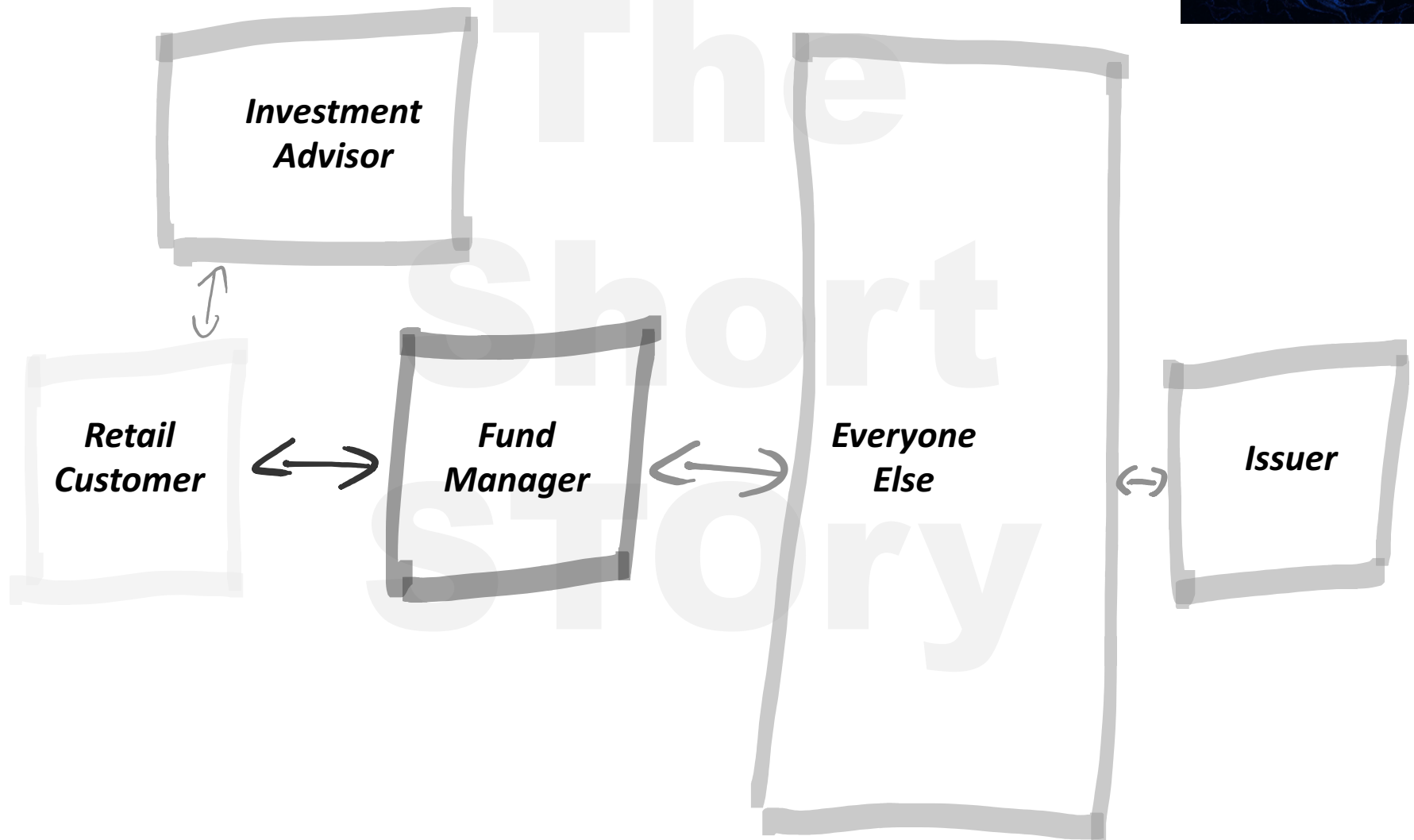
Public Key Infrastructure will ultimately lead to a vertical breakup of the entire financial services value chain, especially in fund management and custody!

The financial services value chain



- **Issuer.** Another customer of the system.
- **Depository.** Holds the golden record of security ownership and executes corporate actions.
- **Custodian.** Hold securities on behalf of a client, and deals with reporting etc.
- **Clearing house.** Deals with the settlement of transactions
- **Market.** Provides a platform for buyers and sellers.
- **Fund manager.** Has discretionary portfolio management authority on behalf of the customer.
- **Investment advisor.** Provides advice to the investor, but does not have authority to trade on their behalf.
- **Investor.** The main customer of the system.

Today's main entry point for retail customers are fund managers



Why are fund managers the main entry point?



- **Cognitive load.** It is not mentally efficient for a retail investor to take granular decisions about a diversified investment portfolio
 - But: (“robo”) investment advisors can help with this; so why don’t they?
- **Custody.** Within the current system, custody for retail customers only works economically if they pool their investments into vehicles with a homogenous portfolio, aka “funds”
 - How do private keys change that?

What is different about private keys compared to current system?



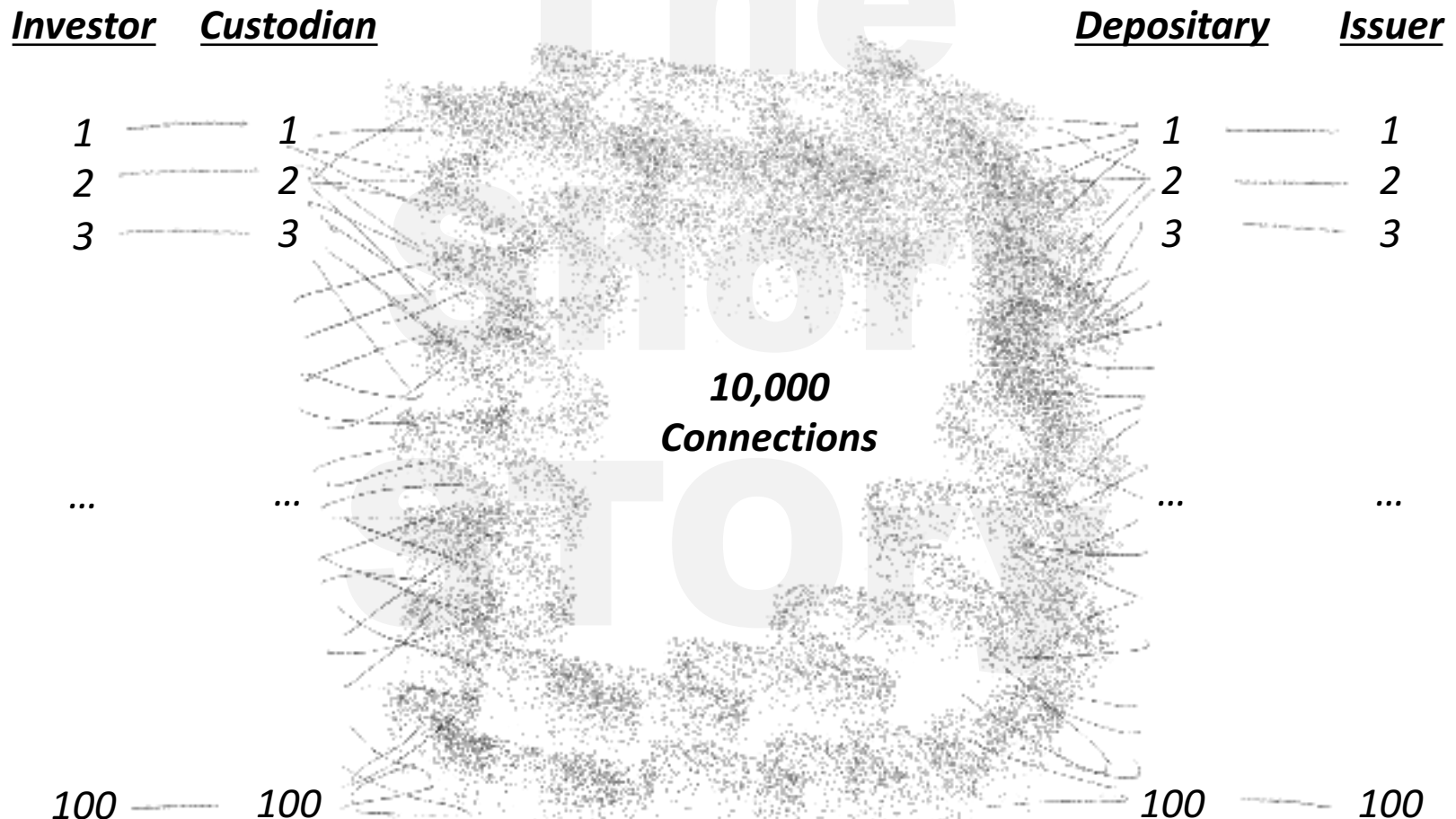
Symmetric Keys

- Shared secret between every pair of two interacting participants
- When multiple parties are involved requires either bilateral relationships or forwarding of trust

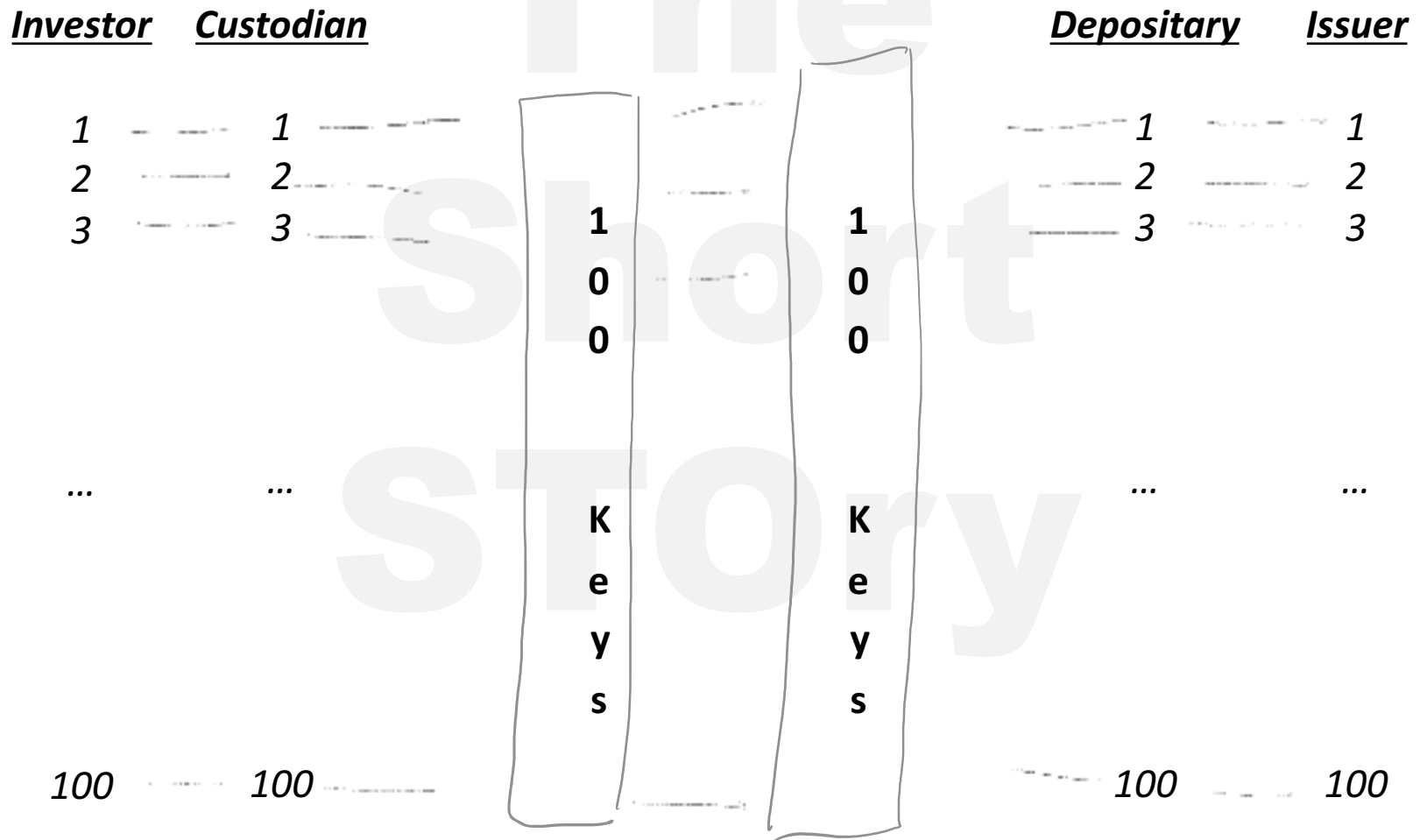
Public Private Keys

- One single key per participant, closely tied to their identity
- Does not require delegation of trust; every participant can independently verify authenticity

Traditional “symmetric key” system



Modern system based on public key infrastructure

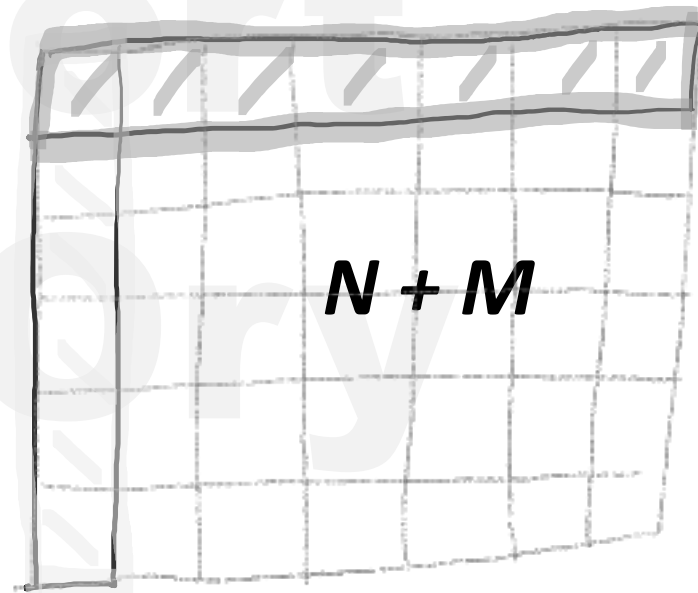
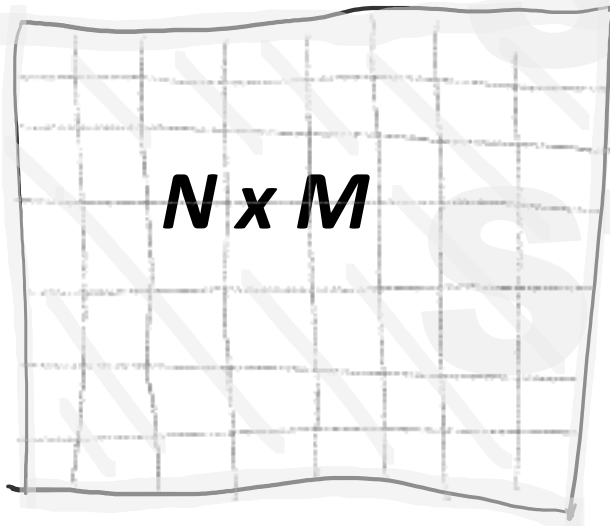


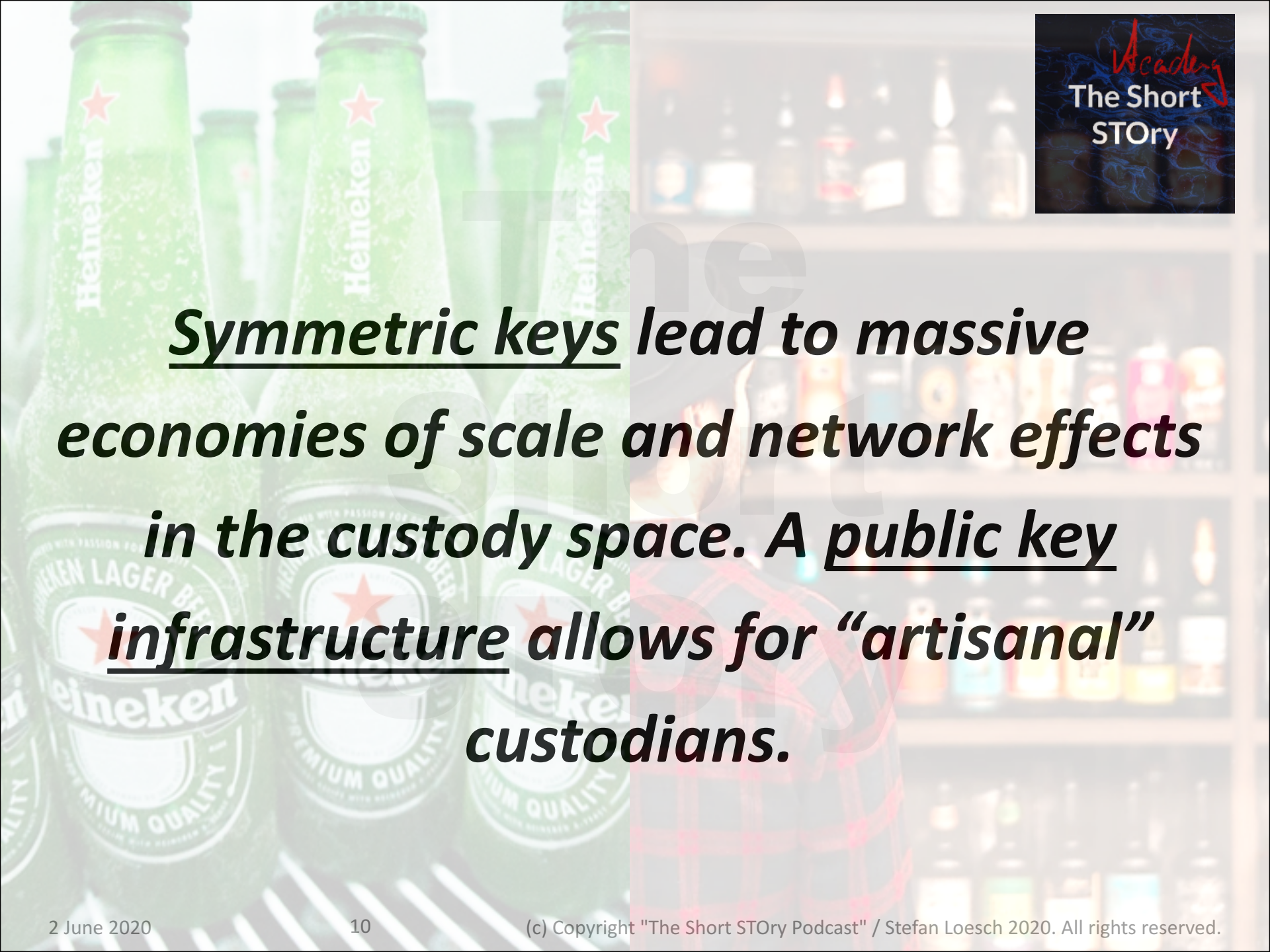
PKI much more efficient at large number of participants



Symmetric Keys

Public Key Infrastructure



The background of the slide is a composite image. On the left, there are several green Heineken beer bottles with white labels and red stars. On the right, there is a blurred image of a bar shelf filled with various bottles. The text is overlaid on this background.

Symmetric keys lead to massive economies of scale and network effects in the custody space. A public key infrastructure allows for “artisanal” custodians.

Once artisanal custody becomes possible there is no need for managers to run massive homogenous portfolios, and they can operate under a (robo) advisory model instead ... but this is for another day

Conclusion



- Public key infrastructure reduces the complexity from n -times- m to n -plus- m ; this allows for a massive increase in the number of custodians n
- This is particularly important in a cross-border setting (large m) and allows retail investors for interesting cross-border investment opportunities*
- Ability to custody more granular portfolios in turn allows to move from a pooled-investment model to a (robo) investment advisory model

**regulations are still a problem*





The Short TEMPLATES STOrY

LOGO TO COPY



The Short STOrY

