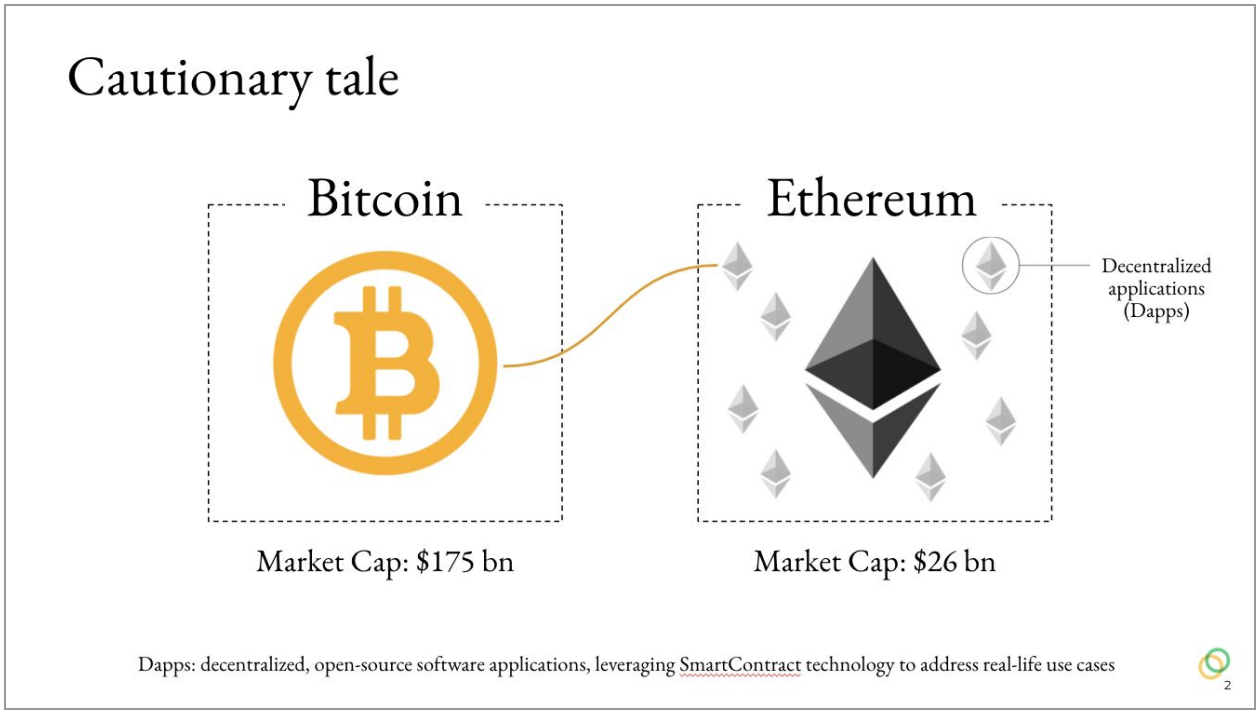
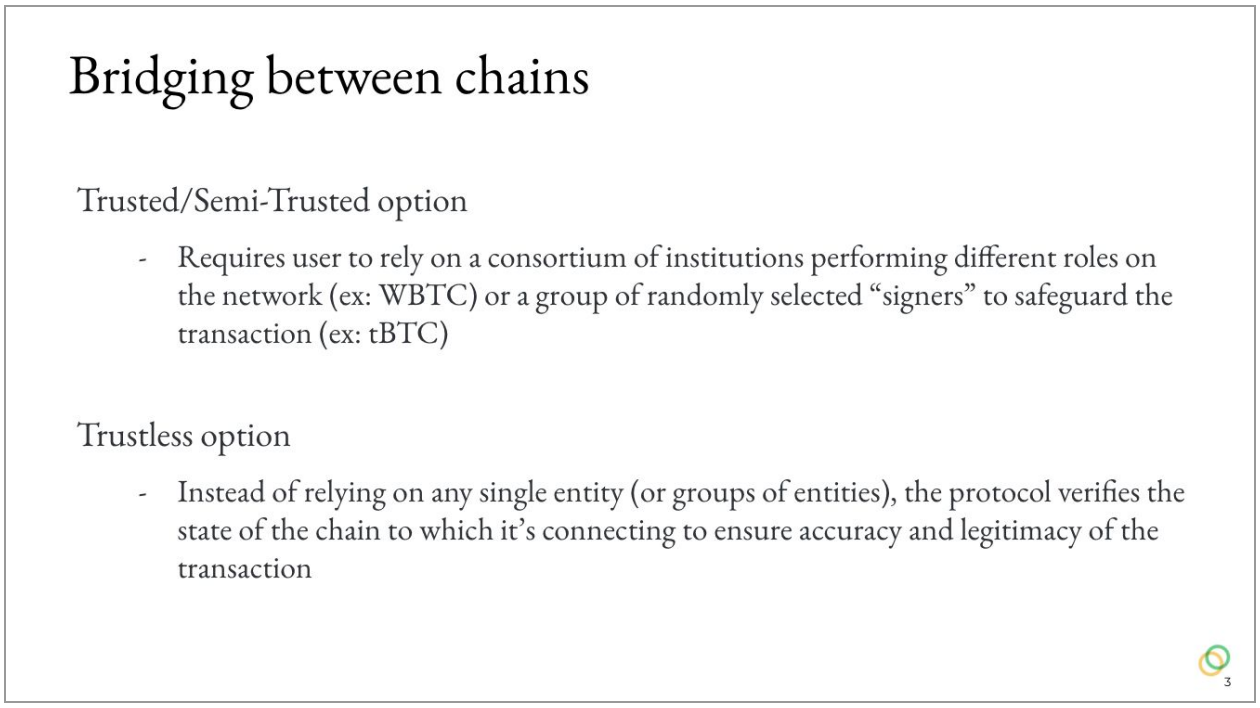
- Focus: interoperability, a topic that is gaining urgency within the CBDC universe
- OMFIF report on Retail CBDC:
  - 60% concerned interoperability would encumber progress on CBDC issuance
  - 43% admitted current focus is strictly domestic
- Divergence in CBDC standards could limit potential
- Interoperability: building bridges between blockchains

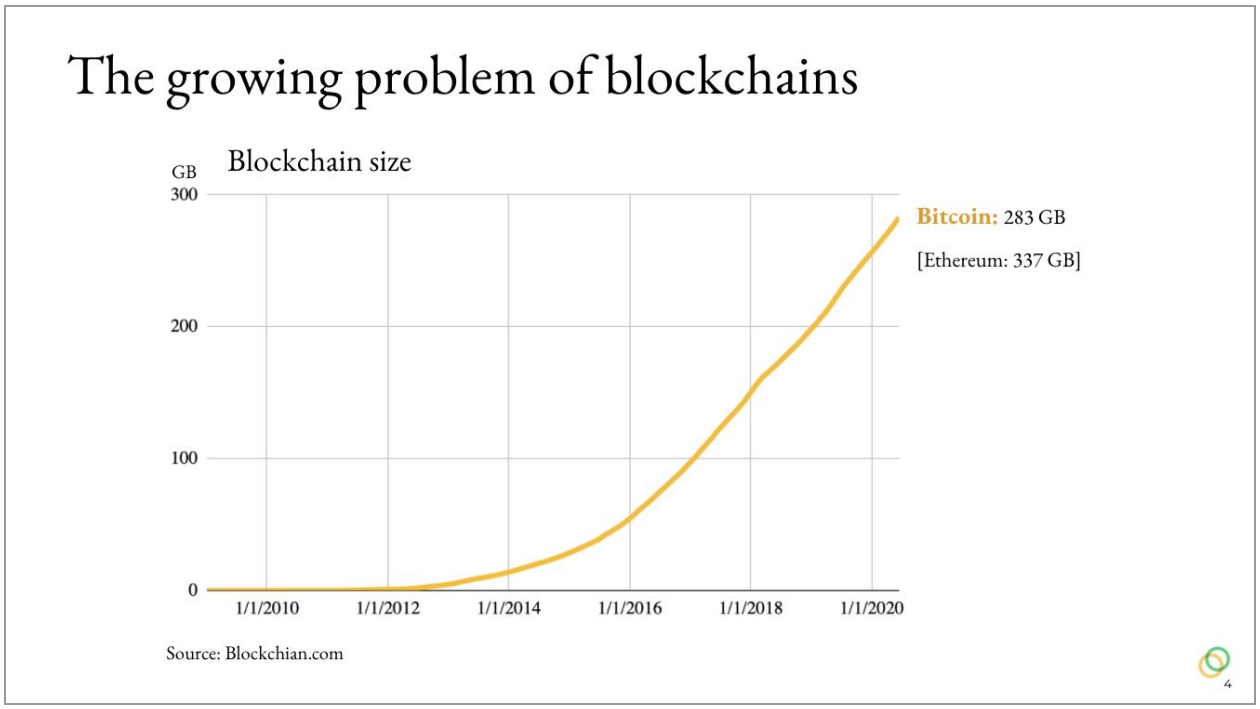


- Bitcoin vs Ethereum
  - Bitcoin: $175 billion market cap
  - Ethereum: $26 billion market cap
- Ethereum -- decentralized applications
  - Leveraging Smart Contracts
  - Address real-life use cases

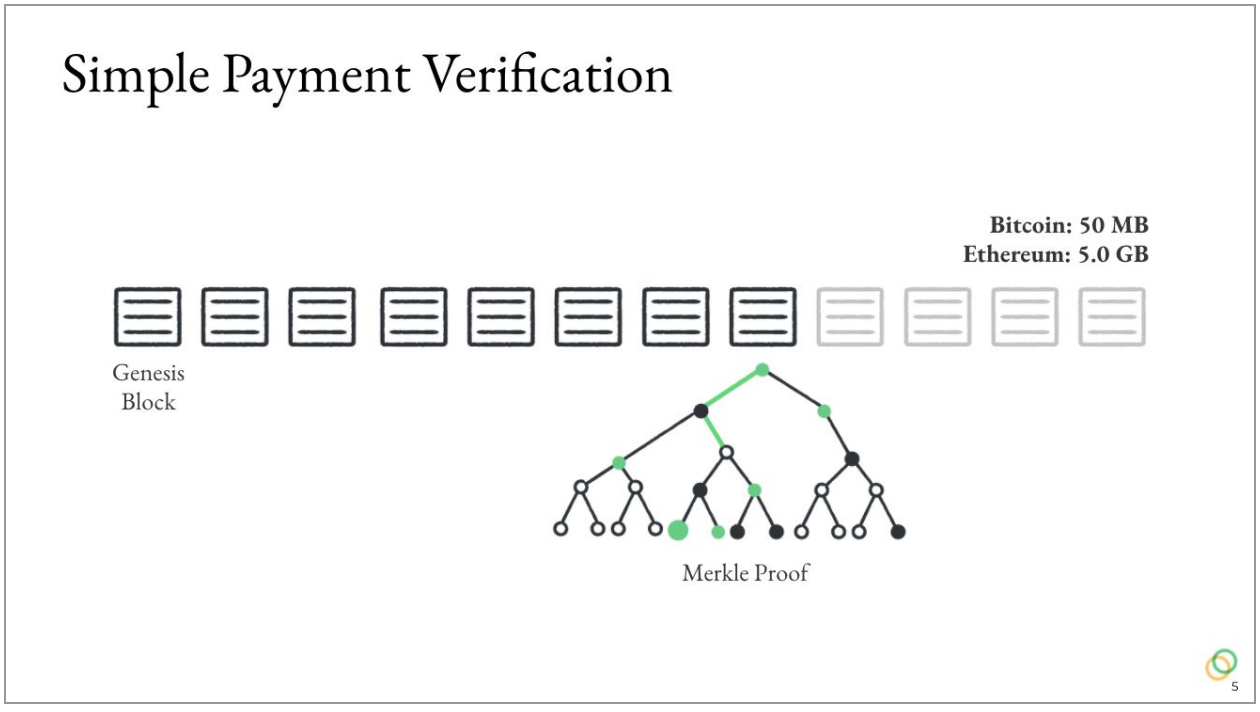
- Bitcoin holders that want to use Ethereum dapps need a bridge between the two blockchains



- Essentially two options when bridging between blockchains: trusted and trustless
- Trusted
  - User essentially exchanges Bitcoin for ERC20 tokens on Ethereum
  - Implicitly relying on a small group to verify tokens are valid
  - Examples:
    - WBTC
      - "wrapped bitcoin", which relies on consortium of institutions performing different roles to essentially "wrap" Bitcoin for use on Ethereum
    - tBTC
      - working to allow people to use Bitcoin in Ethereum dapps by using a group of randomly selected "signers" to safeguard the transaction
- Trustless
  - protocol will verify state of the chain to which it's connecting to ensure the accuracy and legitimacy of the transaction -- do not need to trust anyone

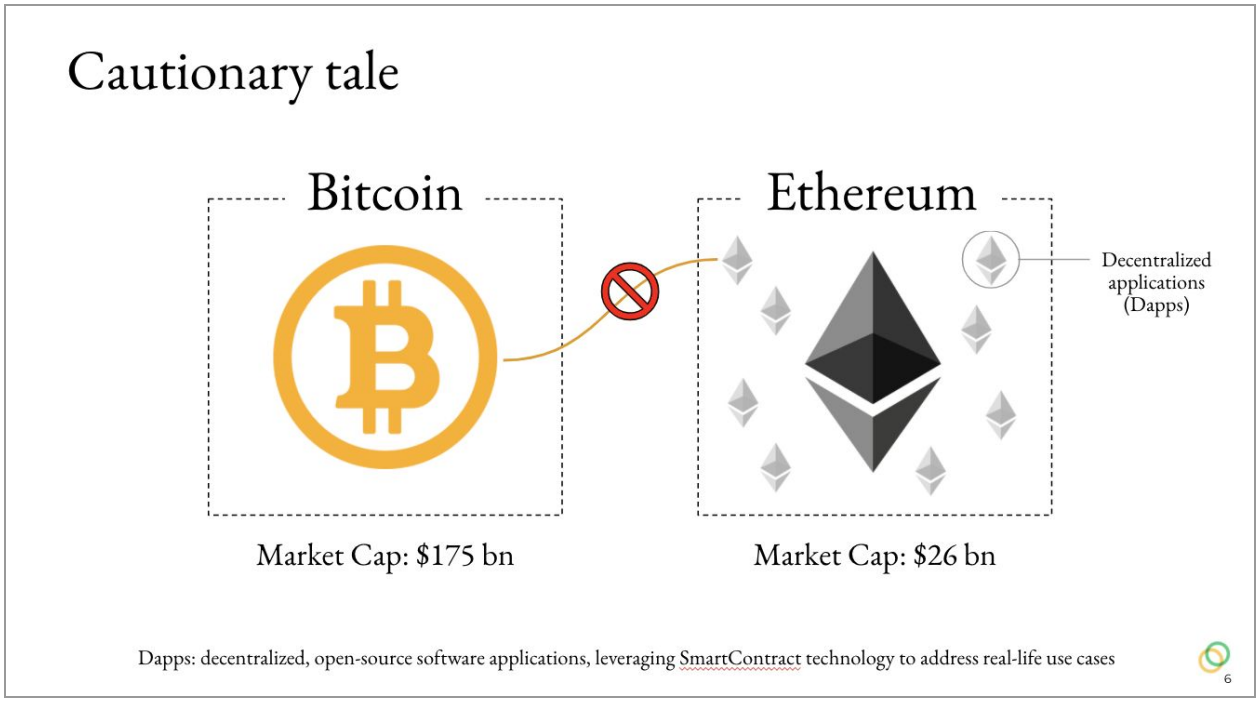


- Steady growth in blockchain size makes it harder for resource constrained devices to do a full sync, and thus verify the state of the chain
    - Bitcoin: 280 GBs
    - Ethereum: 340 GBs
- Creating a bridge essentially replicates one chain onto the other, effectively doubling the size to more than 600 GBs
- SmartContracts are resource-constrained and expensive -- you simply can't do that much computation nor can you store that much data
- Effectively impossible to bridge from one chain to another using a full sync



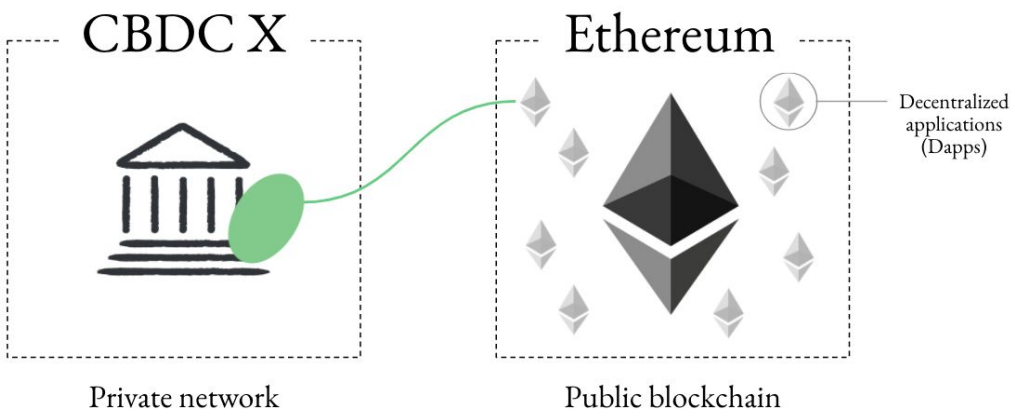
- Original Bitcoin whitepaper there is a description of a "Simple Payment Verification" technique

    - SPV: how light clients can sync with the chain by downloading only the headers of a chain
    - Assuming no “51% attack” scenario, SPV suggests light client can verify latest header it’s presented with is, in fact, part of the longest chain.
    - Light client can then request transaction data from full nodes and use the latest header for verifying any Merkle proofs the full node sends with the data
- Unfortunately amount of header data necessary is still massive
    - Bitcoin: 50 MB
    - Ethereum: 5.0 GB



- Still too much data needed using SPV to create trustless bridge between two chains
- BTC Relay project tried to sync Bitcoin chain on Ethereum, but became cost prohibitive
- Last write to BTC Relay Smart contract was almost 2 years ago
- Example illustrates relevance for CBDC

Bridging from Private to Public

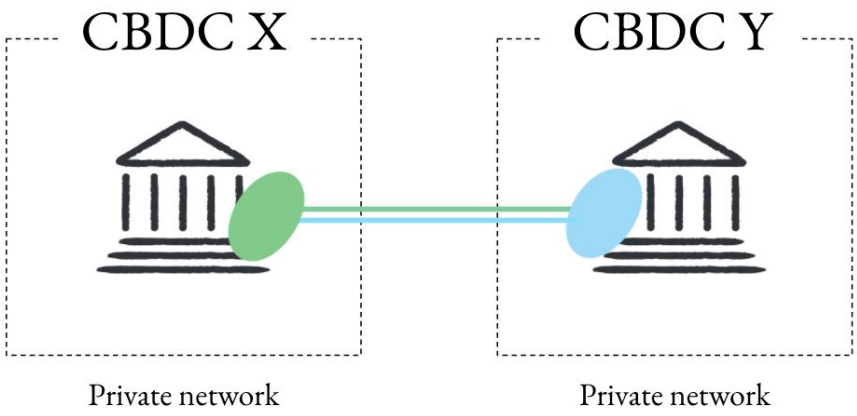


Dapps: decentralized, open-source software applications, leveraging SmartContract technology to address real-life use cases

7

- Highly likely most central banks are envisioning CBDC on a private network
  - May or may not utilize blockchain technology
- Also likely that these private networks will not produce significant amount of decentralized applications focused on real-life use cases
- Like Bitcoin, CBDC users will need a bridge to public blockchains like Ethereum to access dapps

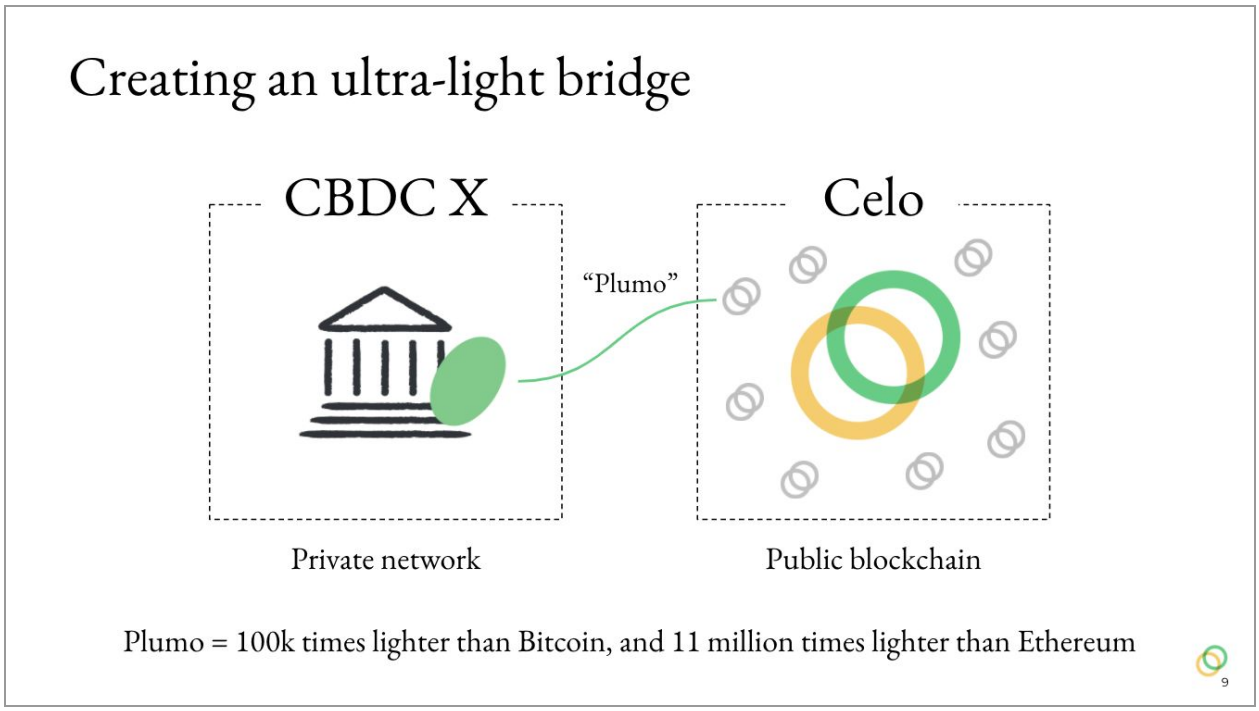
Bridging from Private to Private



Dapps: decentralized, open-source software applications, leveraging SmartContract technology to address real-life use cases

8

- Another likely scenario is to build a bridge between CBDC of various countries
- You could try and build a trusted bridge, but there are likely limits to the amount of trust between countries
- In order to build trustless bridge for resource-constrained devices must ensure data requirements are as light as possible



- To solve the data issue for bridges, the team working on Celo developed an open-sourced light client called Plumo
- Innovations in the light client focused on:
    - Epoch-based synching
    - BLS signature aggregation
    - Use of SNARKs
- Plumo reduces data requirements to verify blockchain states down to a single 500 byte proof
    - 100k times lighter than Bitcoin
    - 11 million times lighter than Ethereum
- As we think about building bridges for CBDC we need to be vigilant about the data requirements for these bridges
- Developing best practices and industry standards around the use of epoch-based synching, BLS signature aggregation and the use of certain elliptic curves in SNARKs may be a helpful place to start