Multi-Layered Security

Critical Enabler for Enterprise and CBDC

Ryan Lackey, Chief Security Officer, Tezos Foundation
<ryan.lackey@tezos.com> - Zug, Switzerland

Why are Enterprise and CBDC Applications Unique?

Largest-scale application of digital currency technology

While cryptocurrency payments are already a big market, they're dwarfed by conventional payment systems in transaction numbers and value. CBDC will be the largest scale payments application of cryptocurrency, and thus unique due to scale

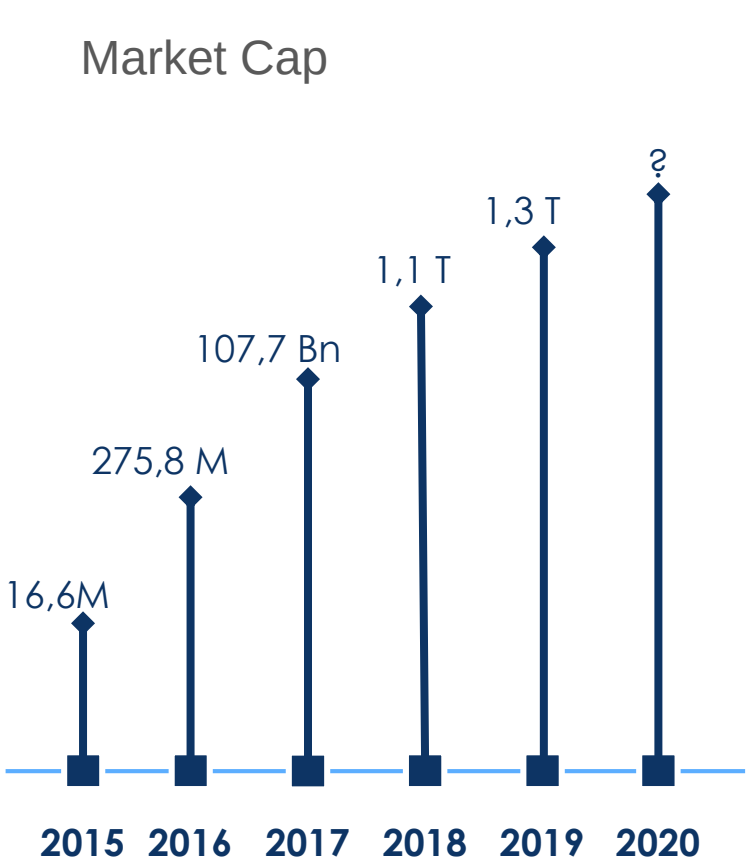
Extreme risks if anything goes wrong

- **Regulatory:** Front-loaded regulatory compliance, but also consequences in any failure
- **Reputational:** Trust is the ultimate currency of central banks
- **Total system size:** Large systems attract well-resourced attackers
- **Political:** National adversaries may seek to sabotage systems

Broad adoption

Bringing cryptocurrency to the broad market means user experience, security, and per-user costs must be optimized

Scale of Stablecoins



Stablecoin	USD
USDT (Omni)	2,865,716,915
USDT (ETH)	400,057,493
USDT (Tron)	37,902,010
USDCы	359,073,390
TUSD	243,230,996
PAX	185,393,508
DAI	81,355,756
EURT	55,828,306
EURS	35,706,863
GUSD	22,903,779
TGBP	1,374,541
Total	**4,288,543,557**

- **Spot trading**
  1.3 Trillions volume on 1000 trading pairs
- **Investment gateway**
  100 regulated US based VC participated in crowdsales
- **E-comm payments**
  Access to 1,7 billions unbanked population
- **Bridge to US Stocks Market**
  Access to regulated tokenized securities
- **Cross border tool**
  Instant, cheap & traceable remittance operations
- **Financial derivatives**
  Most liquid access to build financial derivative instruments

CBDC Choices

Public vs. Private Blockchain Choice

Public and private blockchains have unique characteristics. Ultimately this is the most fundamental decision in building a CBDC.

Security and Technical Model

- **Privacy:** transaction privacy
- **Participants:** central bank, commercial banks, merchants, and users
- **Support:** vendors and ecosystem.
- **Performance:** system scale exceeds existing blockchain applications

Life-cycle Management

Long product lifecycles relative to technology lifecycles. Need technology solutions for a multi-decade lifecycle.

Private vs. Public Blockchains

Private	Public
Inherent privacy	Innovation
Control	Interoperability
Traditional or default model	Cost efficiency
Single point of vendor contact	Many potential vendors
Security (DoS, “Big Red Button”, existing tools)	Many potential applications
Performance	Scalability

Tradeoffs Between Private and Public

Private blockchain: Easier but less scalable or broadly innovative

Easier for proof of concept, but ultimately less potential maximum benefit if successful.

Public blockchain: Harder engineering challenges but can scale if successful

Arguably faster innovation, but generally technically insufficient (performance and security) for CBDC needs

Balance

Neither solution is really ideal, today or long-term.

Public vs. Private? No, Public + Private = Hybrid

Private blockchain: Easier but less scalable or broadly innovative

Easier for proof of concept, but ultimately less potential maximum benefit if successful.

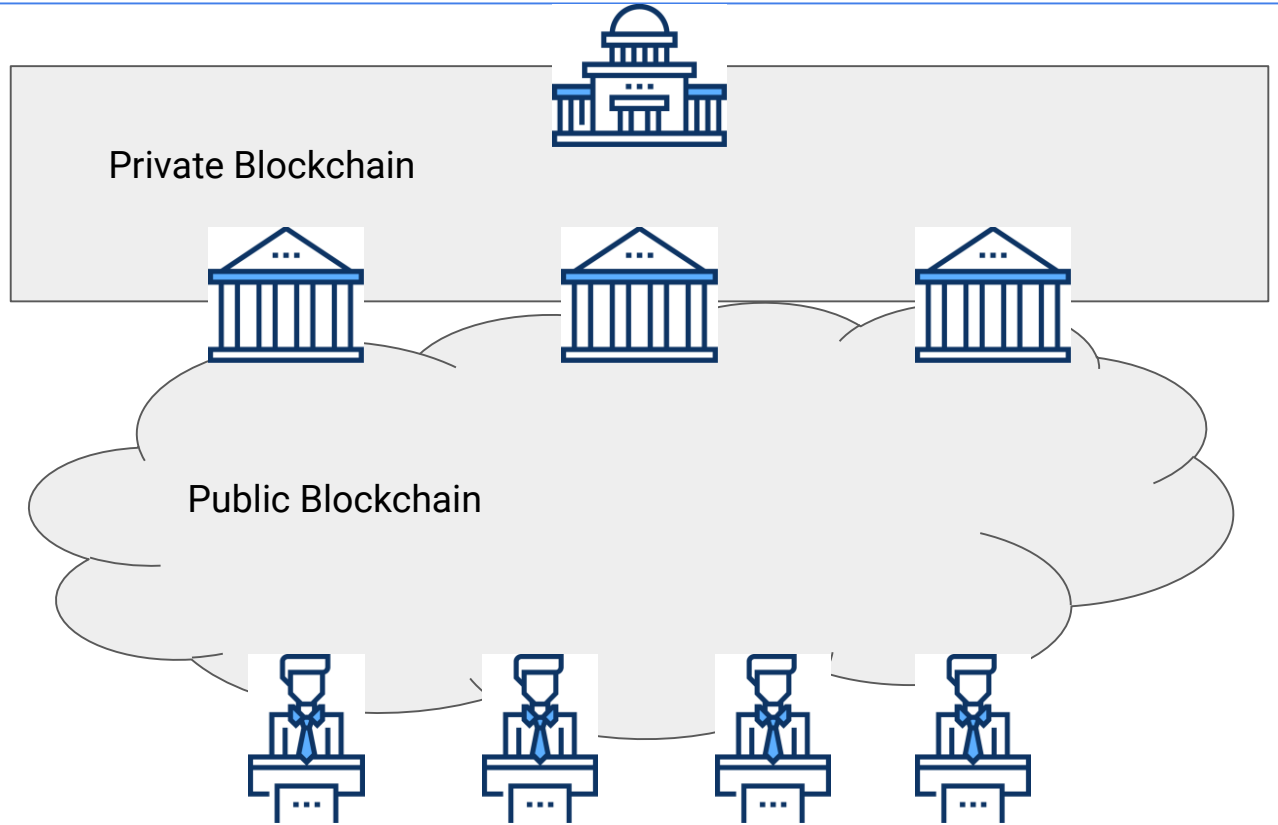
Public blockchain: Harder engineering challenges but can scale if successful

Arguably faster innovation, but generally technically insufficient (performance and security) for CBDC needs

Hybrid

- Core operated by central bank has performance, security, robustness, and control of a private system
- Public-facing systems on public blockchains have scalability, innovation, and flexibility of public system
- Costs at scale are similar to public blockchain systems
- Allows the best functionality of each type of system where it works best

Hybrid Solution



Security and Technical Considerations

Privacy

Default model of blockchains is for transactions to be public to the entire world. Incompatible with existing privacy regulation, user expectation, or good system design. Advanced technology like zk-SNARKs can provide end-user privacy while retaining central bank control and regulatory compliance.

Verifiability

Systems are inherently complex and have multiple interoperating components, with failure potentially leading to serious lost of funds, trust, or safety. Only formally verifiable systems can be trusted.

Life-cycle and Governance

Due to long deployment, adoption, and broad adoption timescales, and cost of switching systems, system must be in place for a long period. Must be comfortable with a system for decades, so it must be able to grow and adapt. Open-source systems can be good, but how are decisions made?

Conclusion and Next Steps

1) Ultimately, **hybrid** public/private solutions seem best suited for CBDC
2) **Privacy**, formal **verifiability**, and **open-source** systems with clear **governance** make sense
3) Many technical and implementation choices to make

Contact

`ryan.lackey@tezos.com`	Ryan Lackey, Tezos Foundation
`https://www.tezos.com/`	Tezos Blockchain