Distributed Ledger Technology (DLT)

And Where this Innovation is Moving

William K. Santiago (@williamsantiago)
Certified Bitcoin Professional (CBP ID (8eea71))

PrivKey LLC

Agenda

- Introduction
- Blockchain Introduction
- Permissionless & Permissioned Blockchain
- Why Blockchain?
- Challenges Blockchains Brings
- Classes of Tokens
- Digital Payments
- Smart POS
- Digital Settlement Payments Benefits
- Example
- Where this Innovation is Moving

PrivKey LLC

Introduction

Since the introduction of the Internet 35 years ago and the use of it for commercial purposes in over 25 years, there has always been a challenge posed by the **need to establish trust** while transacting on the Internet.

This has been addressed by the use of legacy third party services and **centralized databases**.

This **challenge** was **solved** by the Bitcoin (innovation) protocol (Blockchain) in 2008.

Now we have new applied variations of this innovation which will explore.

PrivKey LLC

Blockchain Introduction

- A blockchain is a **<u>digital ledger</u>** that keeps a record of all transactions taking place on a peer-to-peer network
- A blockchain is a set of blocks containing information that are connected between each other using **<u>cryptographic techniques</u>**
- The information is **<u>unalterable</u>** and is shared for all nodes participating in a system based on the Bitcoin protocol (Innovation)
- A full copy of a blockchain contains every transaction ever executed

PrivKey LLC

Permissionless & Permissioned Blockchain

- **Permissionless** blockchain is an open model innovation that **no 3rd party** is in control of transactions and is open, global, trustless and decentralized

- **Permissioned** blockchain is controlled by a **federation** or group of permitted members that establish consensus for control over transactions

PrivKey LLC

Permissionless Blockchain (Bitcoin)

- Censor resistance (no oppression)
- Immutability (no fraud)
- Openness (no barriers)
- Transparent (no lies)
- Global (no borders)
- Trustless (no laws only laws of mathematics)
- Deflation (no inflation, scarcity)
- Accountability (no cheating)
- Decentralization (no centralization)

PrivKey LLC

Permissioned Blockchain

- Censor resistance (outside the federation)
- Immutability (no fraud, only as strong as federation)
- Openness (permitted by federation)
- Transparent (provided by federation)
- Global (stipulated by federation)
- Accountability (regulated federation)

PrivKey LLC

Why Blockchain?

- Persistent Immutability
  - Having records and data decentralized, and deployed on a blockchain makes it virtually impossible for any one party to tamper with data or records
- Security
  - To get the full picture, hackers will need to hack not just the current block, but also every block before it. This is not only technically almost impossible, but it is costly, thereby reducing the incentive for malicious activities
- Redundancy ((DLT) Distributed Ledger Technology)
- Overhead/Cost Reduction (Programmable money with distributed consensus) Smart Contracts!
- Accountability/Transparency (Censorship resistant)

PrivKey LLC

Challenges Blockchains Brings

- **Scalability**
  - For most computer systems (e.g., a database or search engine), "scalability" refers to the system's capability to handle a growing amount of work, or to scale
- **Governance**
  - All organizations and software development projects need a way to agree on and to finalise each decision along the roadmap. Most organizations are centralized and have a leadership team. Strategies for governing a **fully decentralized** and **federated** blockchain have been developed and address different challenges
- **Interoperability**
  - The ability to share information across various blockchains systems or networks

PrivKey LLC

Classes of Tokens

Each class derives value differently:

- **<u>Currency Tokens</u>**—Tokens like Bitcoin, Monero, Litecoin, etc.
- **<u>Utility Tokens</u>**—Tokens that allow you to essentially use or perform an activity on a network, such as ETH. On the Ethereum network you would need to spend Ether (aka gas), to run a smart contract, etc.
- **<u>Asset Tokens</u>**—Tokens that represent an actual asset or product
- **<u>Equity Tokens</u>**—Tokens that basically act like a share, and gives you some kind of voting right or consensus participation. Securities!

PrivKey LLC
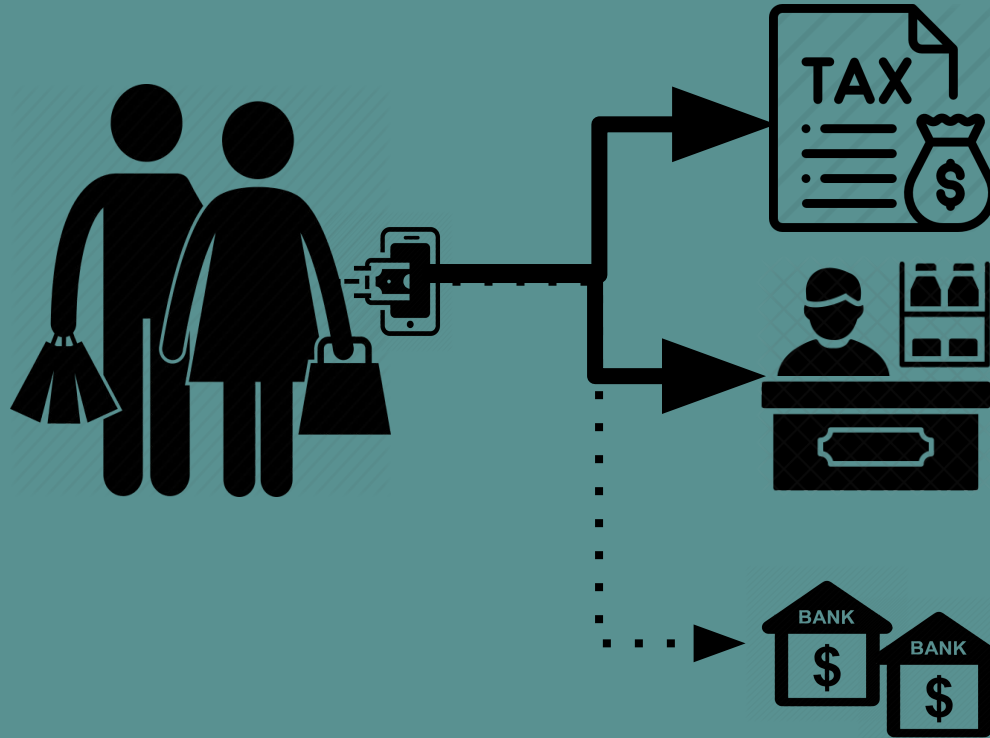
Digital Payments

Tax payment and transaction data **automatically** paid to the tax authority

Merchant **immediately** receives payment in their digital account

Data records about the transaction are **automatically submitted** to the merchant's bank, customers bank

PrivKey LLC

Smart POS

Customizable

Direct Tax Collection

Portable

Direct Reporting to Central Bank

Camera / Scanner Fingerprint

Direct reporting to Treasury

All-in-One POS Terminal, QR-code, scanner; NFC

Multiple Settlement per Transaction

Credit/Debit Card MSR, IC Readers

Real-time sales monitoring & data centralization

PrivKey LLC

Digital Settlement Payments Provides Significant Benefits to Economy

Free Movement of Capital

Reduced Transaction Costs

Faster and Convenient Transfers

Digital Finance Network Effect

Improved Financial Inclusion

PrivKey LLC

Where this Innovation is Moving

- **Payment Platforms**
  How would you like to pay for that, sir?" **cash**, a **cheque** or a **plastic card**.
  Go to Beijing, however, and you will see few transactions in those forms.
  People pay with their phones, using systems created by the two biggest
  Chinese tech companies, Alibaba (Alipay) and Tencent (WeChat Pay).
  From taxis in Tokyo to the Harvard gift shop in Cambridge, Massachusetts.

- **Chinese Growth** due to:
  Right timing, Regulation design to protect banks and credit companies and
  Everyone else not motivated to do so and expansion of Chinese fintech.

- **America** will start to compete at the digital payment level to maintain dominance
  A shortcut would be Libra, the digital currency proposed by Facebook, well
  positioned with its 2.4bn active users

PrivKey LLC

Where this Innovation is Moving (Cont.)

- **Security Tokenizations**

  Placing the distribution, trading, governance and capital distribution of securities onto public blockchains

  Benefits: cost reduction, increase accessibility, improve transparency and integrated compliant financial products

- **Central Bank Digital Currency (CBDC), "Stable Coins"**

  Digital currency issued by central banks of the world.

- **Blockchain Identity**

  Decentralized Identities(DIDs): DIDs are fully under the control of the DID subject, **independent from any centralized registry**, identity provider, or certificate authority. Only possible because of **Cryptography**

- **Smart Contract**

  Security to vet smart contracts that can potentially be automating decisions and executing high value outcomes in lieu of people
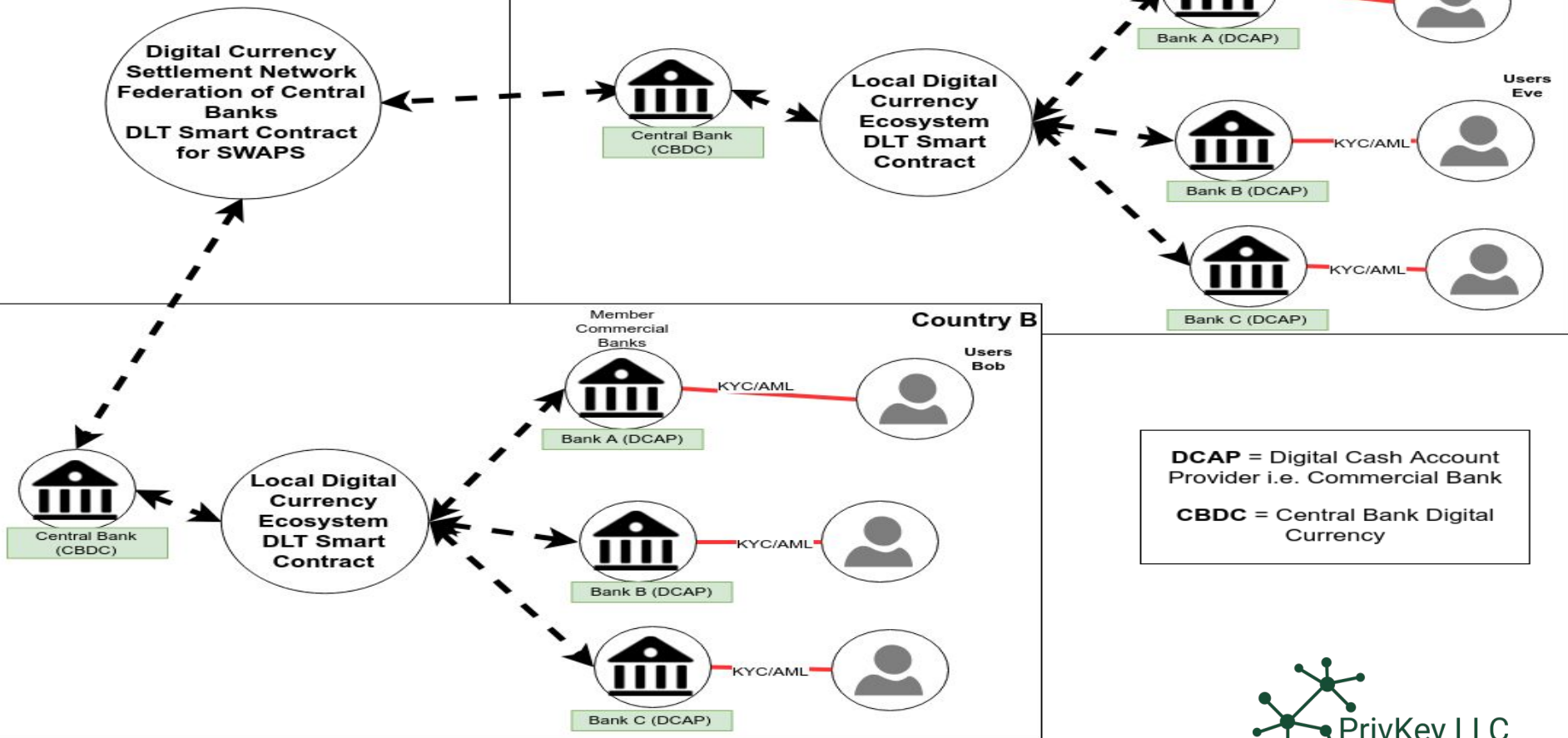
PrivKey LLC

"People will carry verifiable digital equivalents of the paper and plastic documents ("credentials") they have today, issued by the same organizations and authorities. They will be able to control whom they share them with and when they share them, just like you can with paper and plastic today. But unlike paper and plastic, these digital credentials come with cryptographic superpowers that preserve privacy and enable instant verification of their authenticity."
-- everym

"Fiat banks have buried routing deep in their backend via SWIFT, leaving users in blissful ignorance of its complexity. Fiat and banks have had years, decades, centuries to streamline their UX and move the complexity of the system into the backend." -- Roy Sheinfeld

PrivKey LLC

21st Century Blockchain DLT Use Case Payment Settlement

Country A

Member Commercial Banks

Users Alice

Digital Currency Settlement Network Federation of Central Banks DLT Smart Contract for SWAPS

Central Bank (CBDC)

Local Digital Currency Ecosystem DLT Smart Contract

Bank A (DCAP) — KYC/AML

Users Eve

Bank B (DCAP) — KYC/AML

Bank C (DCAP) — KYC/AML

Country B

Member Commercial Banks

Users Bob

Central Bank (CBDC)

Local Digital Currency Ecosystem DLT Smart Contract

Bank A (DCAP) — KYC/AML

Bank B (DCAP) — KYC/AML

Bank C (DCAP) — KYC/AML

DCAP = Digital Cash Account Provider i.e. Commercial Bank

CBDC = Central Bank Digital Currency

PrivKey LLC

Text

Q & A

PrivKey LLC