Digital Economy and Blockchain

To Distribute and Share

David LEE Kuo Chuen

Chairman, Global FinTech Institute

Professor, Singapore University of Social Sciences

Digital Economy and Blockchain

- Governments are looking towards a distributed and share digital economy
  - AI and Data Analytics based economy without constraints will lead to Winner-Takes-All and Surveillance Capitalism
  - A Blockchain or Distributed Ledger based digital economy provides a token economy with financial inclusion and privacy protection
- Future Trends that regulators and investors will need to pay attention
  - Central Bank Digital Currency
  - Smart Contracts
  - Inclusive Blockchains
  - DeFi
  - Privacy Protection

CBDC

Most Distributed Ledger Technology-based Central Bank Digital Currencies (CBDCs) are digital fiat currencies:

That are Issued and regulated by a trusted central monetary authority

Each unit of CBDC may be represented by a unique serial number stored in a robust cryptography to prevent imitation

Act as a store of value, medium of exchange and an official unit of account

BUSINESS DESIGN

RETAIL

Transactions are mainly among the general public

Increase Financial inclusion

WHOLESALE

Transactions are mainly between institutions for the purchase and sale of financial assets

Enhance Security Settlements & Improve Efficiency

PROS

FAST AND EFFICIENT
May bypass intermediaries, directly linked to central banks

FOSTERS ECONOMIC GROWTH ALONGSIDE DIGITAL INNOVATION
Creates an appealing crypto ecosystem boosts economic activity and digital innovation

AFFORDABLE
Lower cost of third-party trust, thus cheaper for consumers and merchants

COMPETITIVE
Foster competition among private sector intermediaries, set standards for security and innovation

FINANCIAL INCLUSION
Enable the unbanked to access financial services

INCREASES EFFECTIVENESS OF MONETARY POLICIES
Allows the control of digital money supply, introducing interest bearing CBDCs will allow monetary policy to break below the effective lower bound

CONS

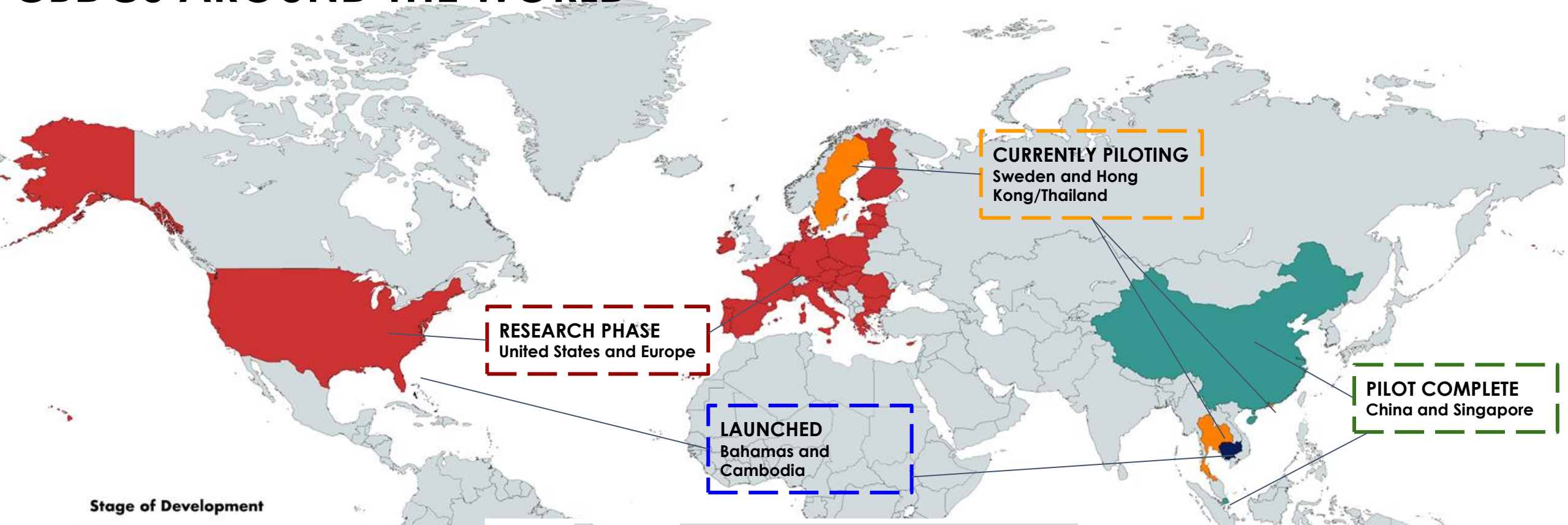
STRUCTURAL DISINTERMEDIATION OF BANKS
Lesser deposits, shrinkage of commercial loans
→ threat to sustainability of banks

INCREASED FINANCIAL RISK
Risk of bank runs since transfers to CBDC accounts
can be done with no restrictions if time and geography

DATA PRIVACY & CYBERSECURITY RISKS
Central banks are able to monitor all CBDC transactions (depending on jurisdiction)

Cyber threats due to CBDC model being open to many users, providing multiple point of attacks

CBDCS AROUND THE WORLD



		BUSINESS DESIGN	
		Wholesale	Retail
LEDGER DESIGN	Token based	Hong Kong & Thailand Singapore	Sweden
	Account based	Europe US Bahamas	Europe US Cambodia China Bahamas Sweden

The Multiple (mCBDC) Bridge project is a DLT project to support multi-currency cross-border payments by HKMA, BoT, DCI of PBOC and Central Bank of UAE.

CBDC slides prepared by: Adeline Tan Mei Chin Ang Yun Xuan, Charmayne Tay, Khoo Tze Yang Rayson, Koh Qian Siang Gordon, Teo Hui Kit Karl, Yeo Wee How Adrian

SINGAPORE

From PROJECT UBIN To PARTIOR

KEY SPECIFICATIONS

1. Partnership with a consortium of technology companies and world largest financial institutions like JPM, BoA and Credit Suisse
2. Tokenized fiat currency on distributed ledger

MOTIVATIONS

- The company Partior, will leverage blockchain technology and digitise commercial bank money, with the aim of reducing current frictions and time delays in cross-border payments, trade and currency settlements.
- Temasek+DBS+JP Morgan: **To Distribute and Share!**

Although the eventual goal is to shape future commercial solutions that leverage DLT and tokenised fiat (which would include CBDCs), the project's impact on the financial system will only be seen in the years to come

A BRIEF TIMELINE

Phase 1
Explored the use of a tokenized Singapore CBDC with blockchain technology to conduct inter-bank payments

Phase 2
Explored the use of DLT for Real-Time Gross Settlement (RTGS) functions, with a focus on liquidity savings mechanisms

Phase 3
Developed Delivery vs Payment capabilities for settling tokenised assets across different blockchain platforms

Phase 4
Tested and assessed cross-border payments with DLT systems under various alternatives models

Phase 5
Tested a prototype blockchain network for a multi-currency payments model in terms of interoperability and explored its value for wholesale banking purposes.

FUTURE

DBS, J.P. Morgan and Temasek are leading the development of a digital multi-currency payments network, with pilot trials starting in 2021, to enhance transparency, traceability and immediacy of cross-border wholesale banking transactions.

CHINA

AT THE FOREFRONT OF RETAIL CBDCs

DCEP

PILOT PHASE

KEY SPECIFICATIONS

1. Instant transaction
2. Offline usability
3. Use without bank account
4. Likely interoperable with WeChat Pay and Alipay
5. Capable processing 300,000 transaction per second

MOTIVATIONS

- **Maintaining sovereignty and control over digital currencies and curbing demand for private cryptocurrencies**
- **Improve payment efficiency and liquidity**
- **Promoting financial inclusion**
- **Drive internationalisation of the RMB by increasing ease of use overseas**
- **Using Bitcoin UTXO methods in tracing coins.**

A BRIEF TIMELINE

2016

China Ministry of Industry and Information Technology issued a white paper on China technology and Application Development , the first time blockchain technology is included in the 13th Five-Year Plan

2017

The People's Bank of China officially established the Digital Currency Research Institute and promoted the application of new technologies such as blockchain and artificial intelligence

2019

The People's bank of China promoted the development of China's legal digital currency as one of the eight key task in 2nd half of 2019

2020

Conducted test in four cities across China, with the most recent trial in Shenzhen. Announced plans to launch DCEP in 2020

CAMBODIA

BAKONG

LAUNCHED

KEY SPECIFICATIONS

1. Fiat-backed, representative of tokenized commercial bank deposits denominated in either Cambodian Riel or US Dollars, thereby reducing liquidity risk
2. **Permissioned append-only blockchain, with core infrastructure maintained by NBC**
3. Byzantine fault-tolerant consensus is also used to validate transactions

MOTIVATIONS

- **Financial and corporate inclusion**
- Create real-time gross settlement system
- Promotes use of local currency, thereby trying to de-dollarize an economy which still heavily reliant on the daily use of the U.S. dollar
- **Reduces and mitigates risks related to counterparty and therefore lowers the barrier of entry for new FinTech players into the payment system.**

Key goal of National Bank of Cambodia (NBC) has always been financial inclusion.
→ 100% smartphone penetration byt only 22% of population above 15 y.o have a bank account

A BRIEF TIMELINE

2017
Initially established with the government aiming to tap into the increasing number of internet users in the country

Reached 9.7 Mil people and 14.8 Mil mobile internet subscribers

Bankong's transaction time stands around 3-5 seconds and its throughput at nearly 2,000 transactions per second

28 OCT 2020

Promises scalability at acceptable costs

BENEFITS

- Free of charge transactions, businesses save costs on developing their own payment network
- Increased network effect encourages financial institutions to develop new services for the largely unbanked

FUTURE PLANS

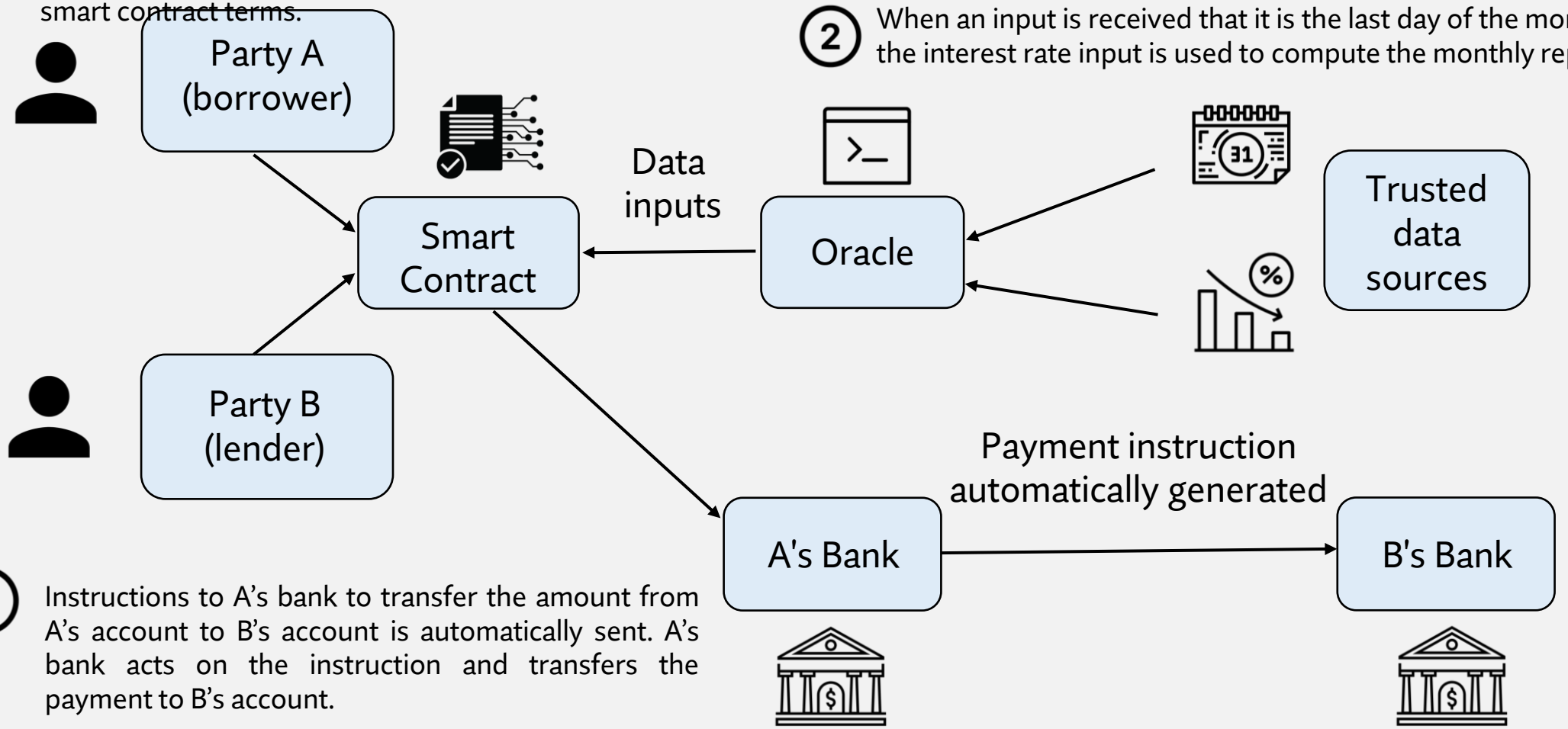
- Eventually plans to allow cross-border payments to serve domestic workers abroad (Maybank is one)
- Plan to continually scale up network and create a financially-inclusive ecosystem

Smart Contract

A blockchain oracle is a third-party data service that provides smart contracts with information from the outside world. Smart Contract reduces the cost of trusted third party and facilitates Corporate Inclusion!

① For example, when 2 parties enter a smart loan contract, it is programmed to receive inputs from oracles and automatically create payment instructions based on those inputs, according to the smart contract terms.

② When an input is received that it is the last day of the month, the interest rate input is used to compute the monthly repayment.



③ Instructions to A's bank to transfer the amount from A's account to B's account is automatically sent. A's bank acts on the instruction and transfers the payment to B's account.

Benefits and Current Applications

Main Benefits of Migrating to Smart Contracts

Speed and Accuracy

- Time saved not processing or reconciling manually-filled paperwork
- Computer code is often more exact than the legalese found in traditional contracts

Trust

- Automatic execution of transactions following predetermined rules
- Encrypted transaction records are shared across participants, ensuring indisputability

Security

- Encrypted blockchain transaction records on a distributed ledger are difficult to hack
- The slightest alteration results in changes in the entire chain, as each individual record is directly connected to its precedent

Savings

- Participants' trust in the visible data and underlying technology for execution of transactions results in disintermediation,
- Mitigates need for third party validation of an agreement's terms since it is built into the code

Current Applications Beyond Payments

Trade Finance

Blockchain technology will lead to over $20 billion worth of savings per year by 2022, with the bulk stemming from the automation of presently labour-intensive approval workflows and clearing calculations that are currently error-prone and time-consuming.

Healthcare

Legacy healthcare systems globally are currently more vulnerable to cyber-attacks than blockchain-based counterparts, which facilitate the secure encryption and safekeeping of patient medical records in large databases, while restricting access to only permitted entities.

Limitations and Challenges

Limitations of smart contracts

Enforceability of complex contracts

Smart contracts focus on executing the agreed terms and may not identify what could go wrong. Complex contracts may require many pages of contract terms irrelevant to the execution stage and are inappropriate for coding. This makes complex smart contracts hard to enforce when unexpected situations occur. A smart may be more or less than a legal contract and need experienced code auditors.

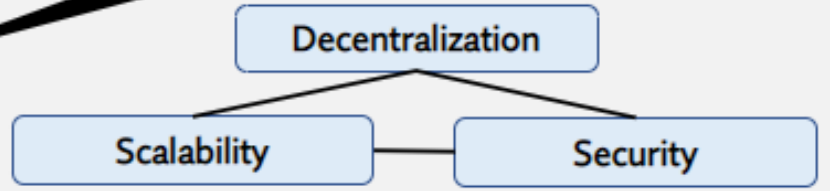
Non-superfluous knowledge of intermediaries

Varying interpretations of contract law on the blockchain when applied across different geographies may result in enforceability issues, ultimately requiring oversight from third parties with legal expertise, thereby contradicting smart contracts' intermediary-free nature.

The 'SIS' Challenges of Blockchain

Scalability	**The rate at which transactions are processed.** Ability to process higher volumes of transactions more quickly would serve more users, but speed comes with its trade-offs.
Interoperability	**The ability to exchange data across blockchain platforms.** Data-sharing may be facilitated with or without a trust third-party, the involvement of which requires off-chain authority.
Sustainability	**Environmentally sustainable and long-term project viability.** The energy-intensive nature of mining is environmentally-unfriendly, while blockchain projects require dedicated funding and development for long-term sustainability.

The Blockchain Trilemma



Example of Desired Feature	Selected Characteristics	Trade-off
Large-scale Decentralized Trust	Decentralization, Security	Scalability
Behaviour 'policing'	Security, Scalability	Decentralization

What are the latest technology to solve the SIS?

Ethereum – keeps a record of both coins and codes!

Ethereum Ecosystem

VALUE PROPOSITION

No Monopoly of Data

Peer-to-Peer Transactions

Data Owned only by Creator

KEY FUNCTIONS

Smart Contracts

Ethereum Virtual Machine (EVM)

Blockchain Validation

USE CASES

Trading as a digital currency (Ether)

Non-fungible Tokens (NFTs)

DeFI/ DApps

Token Launches (ICOs)

Decentralized Autonomous Organizations

Stablecoins

Ethereum Blockchain

- Uses GHOST Protocol and Ethash
- Supports complex transactions
- Stores granularity of information

Smart Contracts

- Turing Complete
- Uses Solidity
- Charges Gas fees
- ERC-20 token standard for DApps

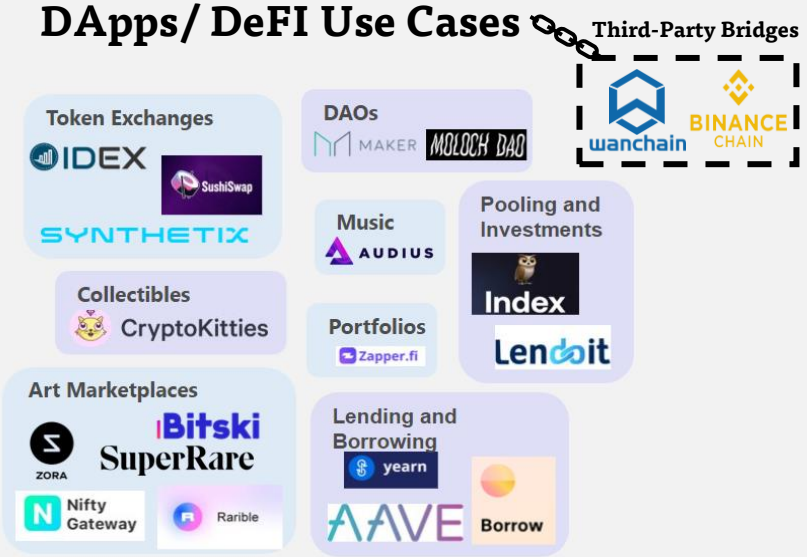
NFTs

- Adopts token standards ERC-721 and ERC-1155
- Fuelled by Ethereum's age and broad adoption
- Compatible with Ethereum's ecosystem

Functionalities of Ethereum's Smart Contract

- Receive, hold, and send Ether/ tokens
- Execute functions from any other contract/robot
- Create any kind of transaction in the Ethereum blockchain
- Allow tokens to run on Ethereum's wallet and blockchain without full fledged infrastructure

DApps/ DeFI Use Cases



Ethereum 2.0 Developments

- **Vision: Scalability, Security, Sustainability**
- **Introduction of Sharding to increase efficiency**
- **Proof of Stake Consensus Protocol**

Cardano and many others

Key Features

Ambitious Project still Underway

Peer Reviewed Protocol Development

First Provably Secure Proof of Stake Protocol

Ease of Smart Contract Creation

Development closely watched, Revolutionary if successful

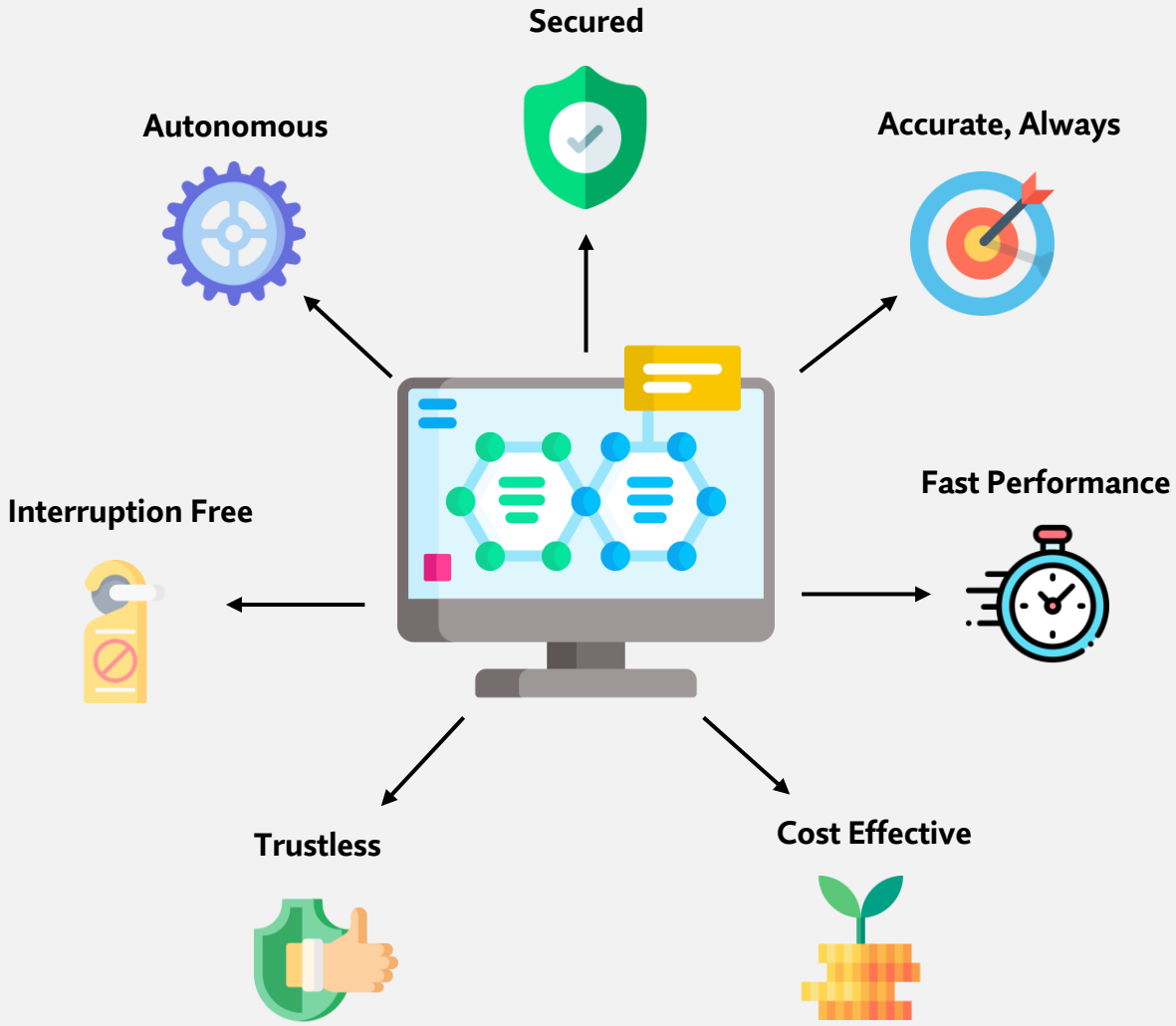
5 Phase Development Stages

Key Features sorted according to SIS

Scalability	Interoperability	Sustainability
PoS Ouroboros Ouroboros Hydra delivered 1000 TPS	**KMZ Sidechains** Scaling & Interoperability Possibilities	**PoS Ouroboros** Goal: Improve PoW Security at fraction of cost
Plutus Platform (Smart Contract Platform) – SDK enabling smart contract authors to easily write SCs	**Multi Currency Ledger** Enable new natively supported tokens. Ease Integration of SC & DApps involving Multiple Cryptos	**Peer Reviewed Development** Community, Transparency, High Assurance Code
Marlowe – Allows non technical people to develop SCs	**Dev Friendly Support**	**Hard Fork Combinator** Smooth Transitions between Updates

Use Cases

Smart Contracts Benefits



Smart Contracts Use Cases


Record Storing


Trading Activities


Supply Chains


Mortgage


Real Estate Market


Employment Arrangements


Copyright Protection


Healthcare Services

Government Voting


Insurance Claims


Internet-of-Things

Smart Contract slides prepared by: Chan Chun Hou, Daryl Lee Zheng Jie, Lei Yuchong, Tan Jun Yu Leonard, Tay Ruo Fan, Yeo Tze Hern

Inclusive Blockchains

Chloe Tan | Chong Wei Xian | Christine Seng | Claudia Tan | Liaw Wen Kiat | Joel Ng | Tan Tu Jin

Sentinel Chain: Tokenising Livestock

Company Profile

Sentinel Chain

Founded by **Singaporean** innovator Roy Lai

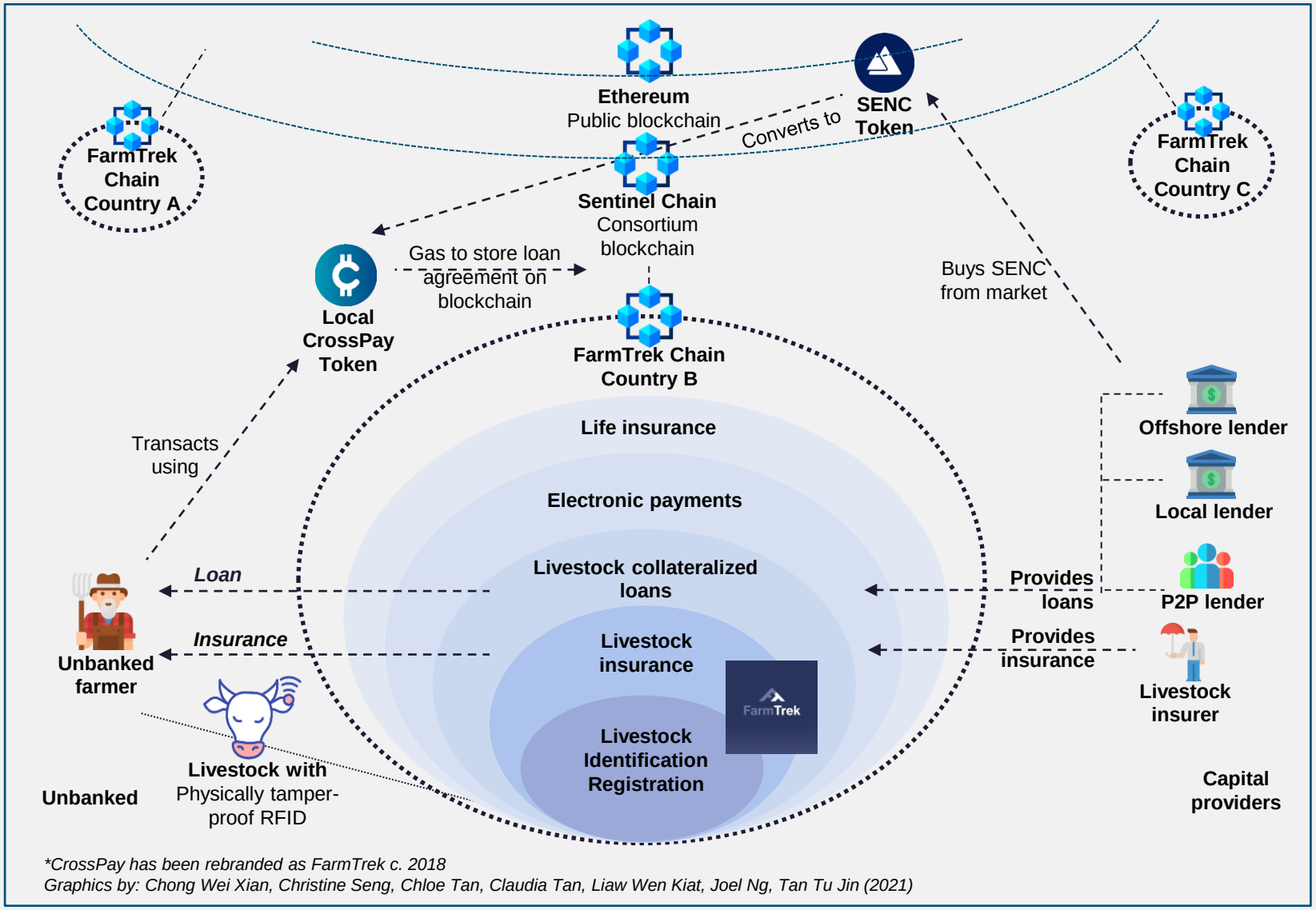
A **blockchain-based international marketplace** for cross-border financial services that will be the world's first platform to accept the use of livestock as collateral.

Financial inclusion for 570 million agricultural small-holders, majority living on > US$2 a day

By allowing farmers to **tokenise and collaterialise their livestock** via the Sentinel Chain ecosystem

Has begun operations and is now live in **Myanmar**, where with a **cattle population** is the largest in SEA. It aims to expand out from Bangladesh and India

The Ecosystem: How it works



**CrossPay has been rebranded as FarmTrek c. 2018*

Graphics by: Chong Wei Xian, Christine Seng, Chloe Tan, Claudia Tan, Liaw Wen Kiat, Joel Ng, Tan Tu Jin (2021)

MeshBox: Tokenising Communication (Internet & WiFi) and Storage

Company Profile

Description

A Singapore-based decentralized open source IoT hardware, leveraging blockchain technology to reward network operators with cryptocurrency

Target Developing Countries

Africa, Asia, and Latin America

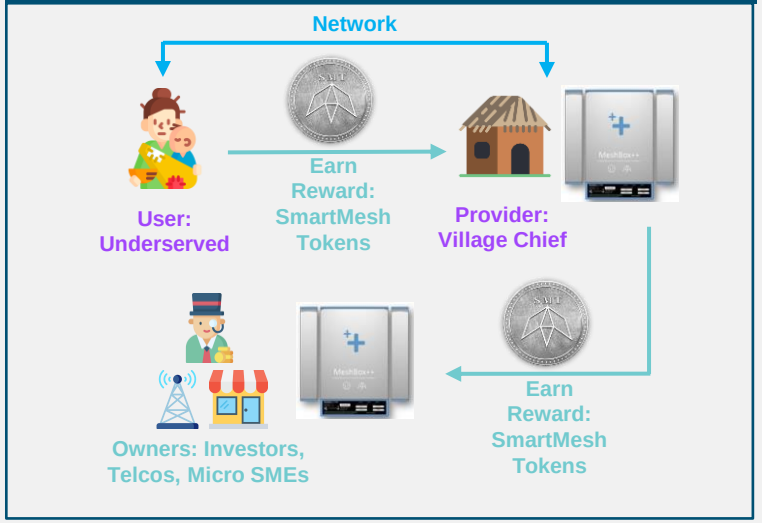
How it creates inclusive FinTech?

Acts as a router to solve the need for cyber-physical infrastructure

MeshBox vs Traditional Tech

- **Cost-Effective vs Expensive**
- **Lightweight vs Heavy Tech**
- **Peer-to-Peer vs Machine-to-Machine Communications**
- **Distributed vs Decentralized**

MeshBox: How it works



Pain Points/Challenges

Need for cyber-physical infrastructure in LDCs

- LDCs have poor cyber-physical infrastructure and from energy poverty, resulting in limited internet penetration
- Traditional telcos wireless network provider comes at a high cost

Thus, connects unconnected individuals

- Reduces the barriers of entry experienced with basic access to advanced technology
- Allows the underserved to have access and participate in FinTech solutions

Solution

Blockchain & SmartMesh Token

- For a shared return on investment
- Operators help a community by investing in deployment of a MeshBox, SMT Tokens are rewarded

Operate w/o Ground Lines & Power Supply

- Deployed in any community and serve as central node of a local mesh network regardless of telecom accessibility

Users Can Extend Idle Broadband

- Users can earn rewards by contributing idle broadband, extending Mesh networks, and transmitting data packet

While Simultaneously Achieving…

Inclusivity

- Cyber-physical infrastructure provides access to FinTech solutions
- For underserved areas w/o access Eg. remote areas, farms, fishing ports

Social Entrepreneurship

- Dignity and sustainable livelihood to the masses
- People become service providers by selling Internet of Value services to neighbours
- ROI kept within community

AID:Tech – Tokenising Identity

Company Profile

An Irish-based Fintech firm that leverages upon digital ID and blockchain technology to provide identity-focused solutions for the undocumented and unbanked

Pain Points/Challenges

Corruption

As much as 30% of global donations are siphoned off due to corruption

Undocumented

Formal delivery of aid only extends to legally identified recipients

Solution

Digital Identity through Blockchain

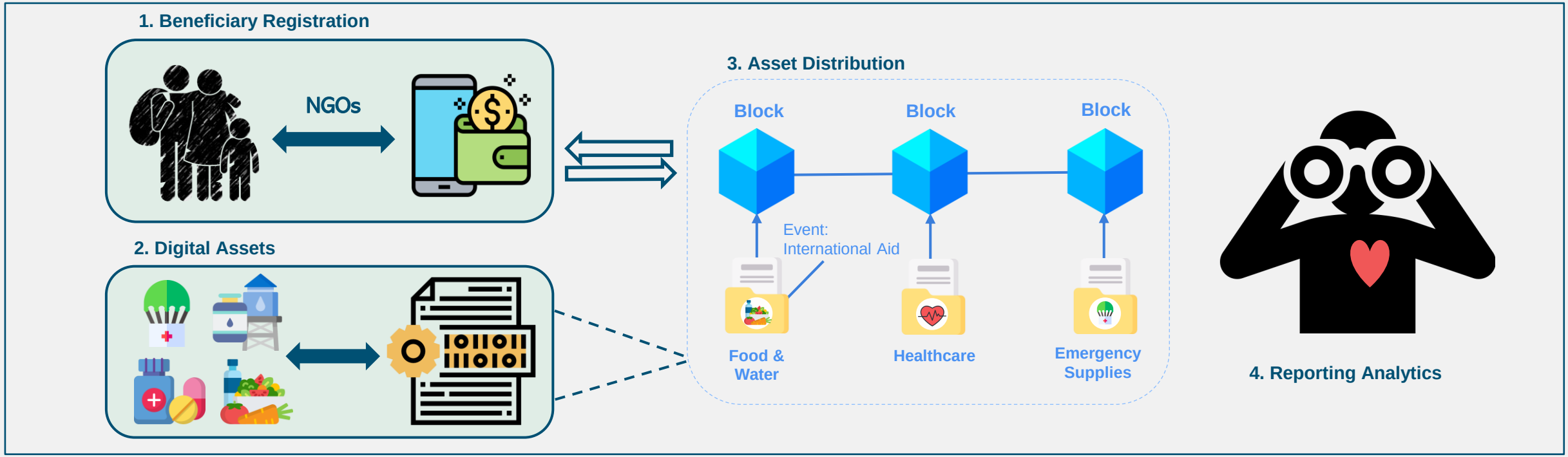
- Employed to improve aid transparency and efficiency
- Traceable flow of information ensures that undocumented obtain goods and services directly

Trial: Syrian War Refugees

Disrupts Traditional Foreign Aid Donation Model

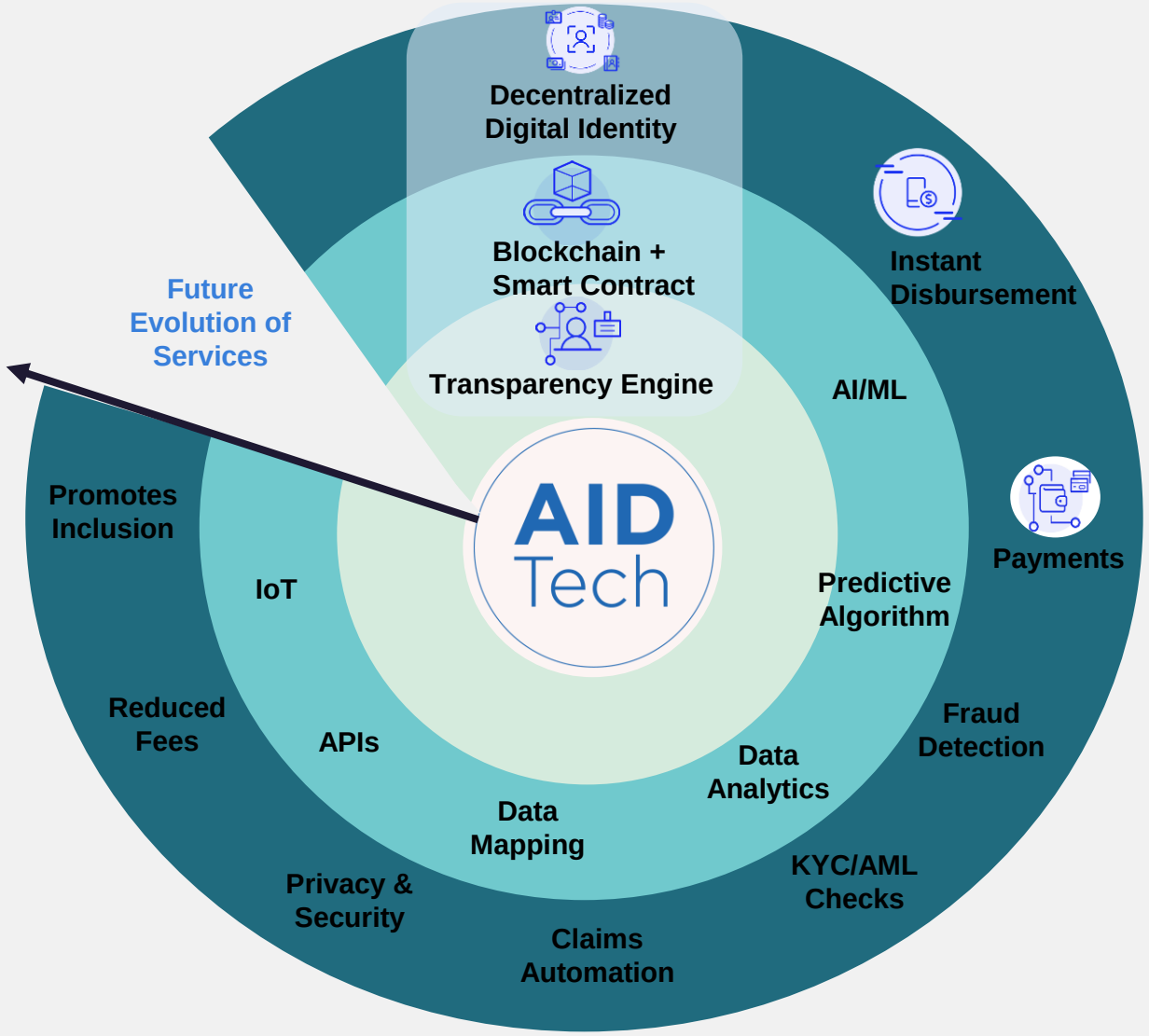
- Construction of a digital platform – data capture and management tool, electronic vouchers embedded with QR codes are given to the refugees

Transparency as a Service, business model explains how AID:Tech works



Evaluation of AID:Tech

Onion Analysis



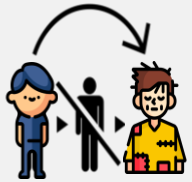
6Ds

Digitisation

There is digitisation of good & services as well the identity of the beneficiaries

Data Privacy Protection

Blockchain technology helps donors and beneficiaries transact through the platform without exposing their private data

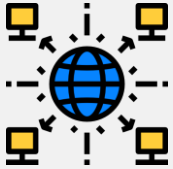


Disintermediation

TraceDonate leverages on blockchain to send donations directly to beneficiaries. This will help bypass potential corruption

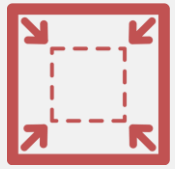
Democratisation

Displaced families are able to access much needed financial services despite being without a legal identity or actual cash-in-hand



Decentralisation

Governance of fund flow is relegated to the blockchain instead of through a few third parties



Diminish

The role of TTPs like NGOs would be diminished over as the work is being done more and more by the users in the blockchain

$5.2
TRILLION PER YR

> In Indonesia, 74% of Micro, Small and Medium Enterprises (MSMEs) and 71% of middle to lower income individuals have no formal access to credit. In total, MSMEs in developing markets have an unmet financing need of $5.2 trillion a year.

INTRO TO DEFI LENDING

- DeFi Crypto Lending uses cryptocurrencies and smart contracts to provide peer-to-peer financing, eliminating the need for trusted third parties such as banks.
- As smart contracts are the foundation for decentralized finance, most Defi applications are built on the Ethereum Blockchain.

Source: International Finance Corporation, Central Bureau of Statistics, Ministry of Cooperative and MSME, Central Bank of Indonesia

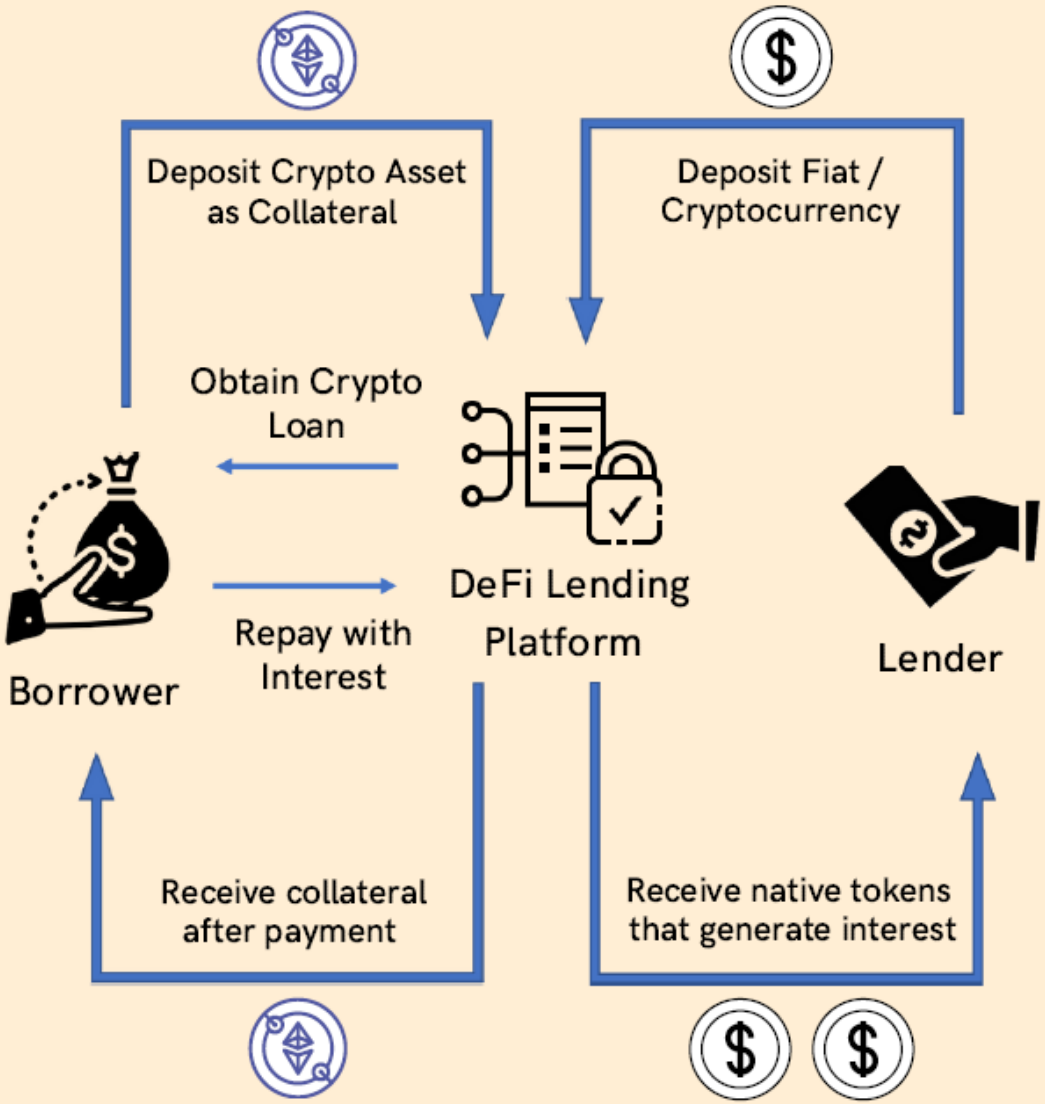
DeFi slides are prepared by:
Chua Le Xuan Andrea, Daniel Lam Chin Kiat, Dio Lim Kang Kai, Kenneth Leng Jing Rui, Lai Kai Ming, Ngiam Kee Yong Joel, Ryan Tan Wei Young

HOW IT WORKS

MECHANISM

- Lenders deposit fiat or cryptocurrency using a smart contract and earn interest on the platform's native token in return
- Borrowers obtain loans by depositing crypto assets as collateral at a specified Loan-to-Value (LTV) ratio
- The blockchain utilises smart contracts, which automatically executes transactions

So what happens when the crypto prices change?



If prices fall (LTV rises), (1) top up more crypto assets (2) pay back some of the loan and interest
If prices rise (LTV falls), (1) request for additional loans (2) redeem some of the collateralized asset

Source: LeewayHertz

BENEFITS OF DEFI LENDING

Eliminates the need for traditional KYC protocol

Open, permissionless and round-the-clock access

Transactions are immutable and lending decisions are set by algorithms

Greater access to credit for those lacking credit history or funds

Greater access to credit for those in rural areas

Increases transparency and eliminates preferential treatment

FINANCIAL INCLUSION

Much Harder to Launder Money, Reaching the Underserved, Eliminate Rent-Seeking Behaviour

Source: Research Gate

CASE STUDY - AAVE

Different protocols have innovated on the underlying P2P lending through novel offerings.

offered flash loans, where users can borrow an unlimited amount of funds

Up to $2b of flash loans was processed in a single month

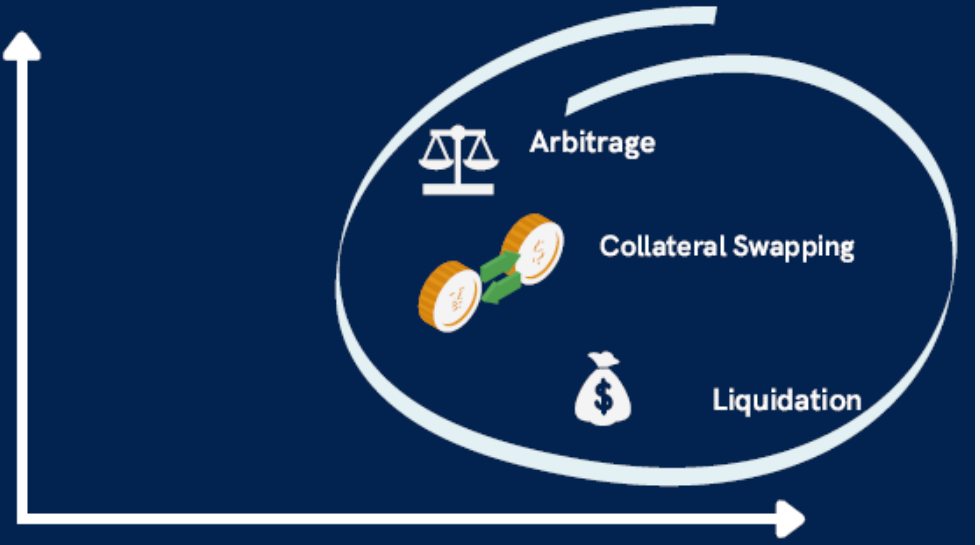
Unlike other P2P currency which require collateral, flash loans do not require any

Not perfected but ongoing experiments for governments to harness

Source: Medium, Aave

WHAT PROMPTED AAVE'S RISE?

Categoring of use-cases of Flash Loans by Aave



Use Case	Why Aave User's Value it
Arbitrage	Taking advantage of the price difference between various decentralized exchage
Collateral Swapping	Defi Users can switch the collateral they have used on a multi-collateral lending app
Liquidity	Defi users can use flash loans to receive access to funds readily, and accessibly

Delving Deeper: The Need for Privacy & How Privacy Coins work

Why Privacy?

1. Commoditisation of user data by Tech Giants such as Google, Facebook & Microsoft
2. Alarming rate at which such firms experience attacks by hackers
3. Even if a user has nothing to hide, they are still entitled to their privacy

How do Privacy Coins ensure privacy?

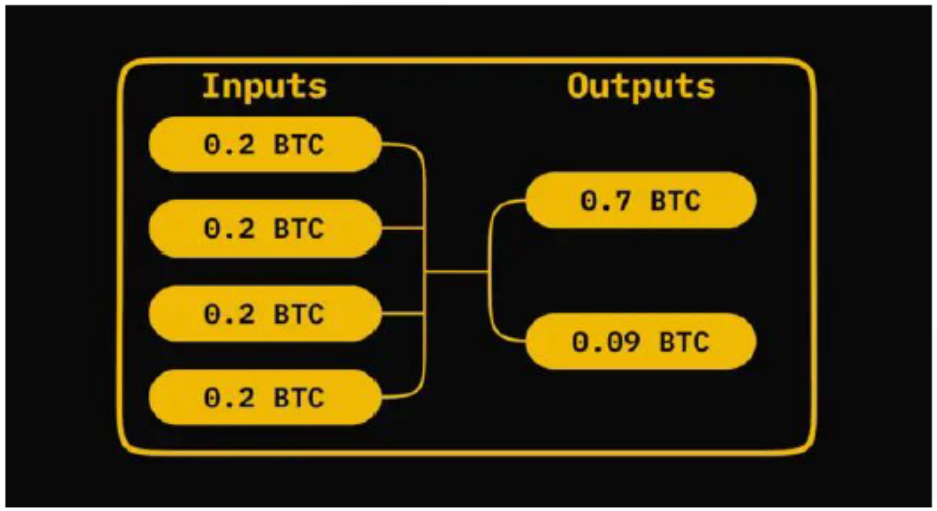
Privacy Coins **obfuscate transaction details and wallet addresses** using cryptography, protecting the privacy of end-users while still allowing for **proof-of-work.**

Example: CoinJoin

Initially proposed in 2013 by Bitcoin developer, Gregory Maxwell, to address traceability issues associated with Bitcoin's public ledger.

In essence, a CoinJoin involves the combination of inputs by multiple users into a single transaction.

Serves as a Black Box to mix funds



Jan 2014
1. **Dash** — PrivateSend

April 2014
2. **Monero** — Ring Signatures and Stealth Addresses

2017
3. **Zcash** — Zero-knowledge Proofs

Crypton.

FUTURE OF PRIVACY COINS

Developments in Technology

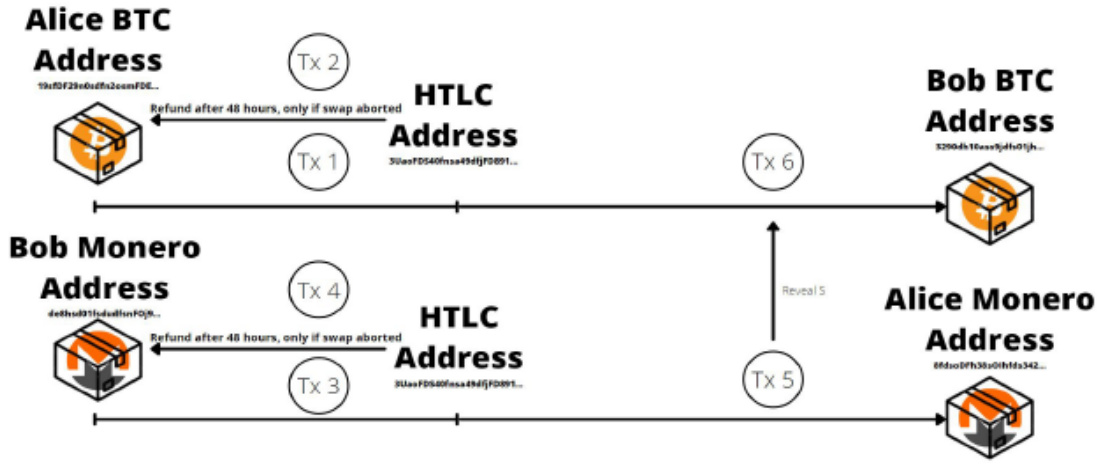
The potential for Privacy Coins is limitless. Developments in **Atomic Swaps** allow for the leverage of more liquid cryptocurrencies to utilise Privacy Coins.

Further developments in mainstream Cryptocurrencies with added privacy functionality such as **Incognito** may lead to increased competition with established Privacy Coins.

01 Atomic Swaps

Peer to peer exchange of cryptocurrencies without going through a third party.

Requires the use of HTLC (Hashed Timelock Contracts)



02 Incognito

A Crypto network that delivers the option to shield any cryptocurrency and allow them to function like privacy coins.

FUTURE OF PRIVACY COINS

Conclusion

ECB Says Public Values Privacy Above All for Digital Euro
By Carolynn Look
April 14, 2021, 5:52 PM GMT+8 Updated on April 15, 2021, 2:23 AM GMT+8

Privacy coins will unfortunately continue to face opposition and challenges.

South Korean regulator to ban privacy coins in 2021

Coingeek, 6 Nov 2020

Privacy-preserving crypto communities should educate regulators about the value privacy coins brings

France Declares War on Crypto Anonymity, Cites 'Terrorism' in KYC Mandate

Coindesk, 10 Dec 2020

The optimal spot will most likely lie somewhere between the radical transparency of public blockchains and the full anonymity provided by privacy chains.

IRS Will Pay Up To $625,000 If You Can Crack Monero, Other Privacy Coins

Forbes ,17 Sept 2020

Always remember to do good! :)

These are experiments that the government can harness for privacy protection as what Project Ubin has done!

Privacy coins slides prepared by:
Blondelle Kong, Foo Sek Jian Darren, Jerome Chong Hao Wen, Mun Yu Teng Natalie, Seah Yong Xian, Donovan, Shaun Phang Rong Jun

Digital Economy and Blockchain:

The Partners
The Purpose

- Harness not Fear
  - Global FinTech Institute
    - Working with regulators and professionals
    - Partnering with universities
  - Chartered FinTech Professional (CFtP) Qualification
    - Promotes the field of Fintech and professionalism in the Fintech industry
    - Provides a pathway for professionals in other industries who aspire to make a career in Fintech.

- It is all about Distributing and Sharing
  - To lower the cost of trusted third party with new form of business models
  - To prevent rent-seeking
  - To include the excluded corporates and individuals
  - To serve the underserved
  - To protect privacy
  - To have stable and sustainable growth
  - To share the fruits