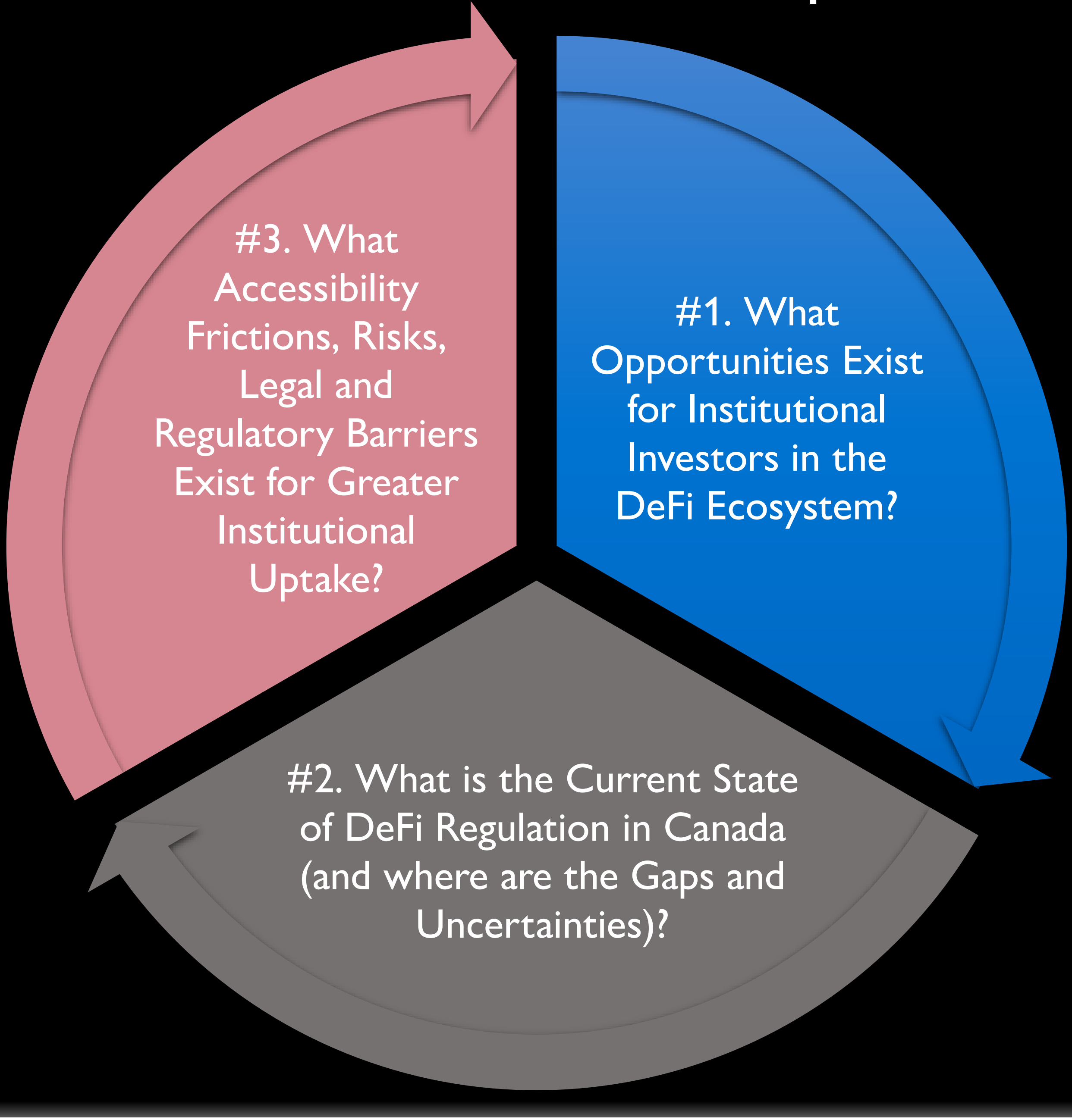
UNIVERSITY OF CALGARY

Legal and Regulatory Barriers Preventing Institutional Investors From DeFi Opportunities

Dr. Ryan Clements
Presentation to Canadian Investment Review
April 6, 2022

Presentation Roadmap

UNIVERSITY OF CALGARY

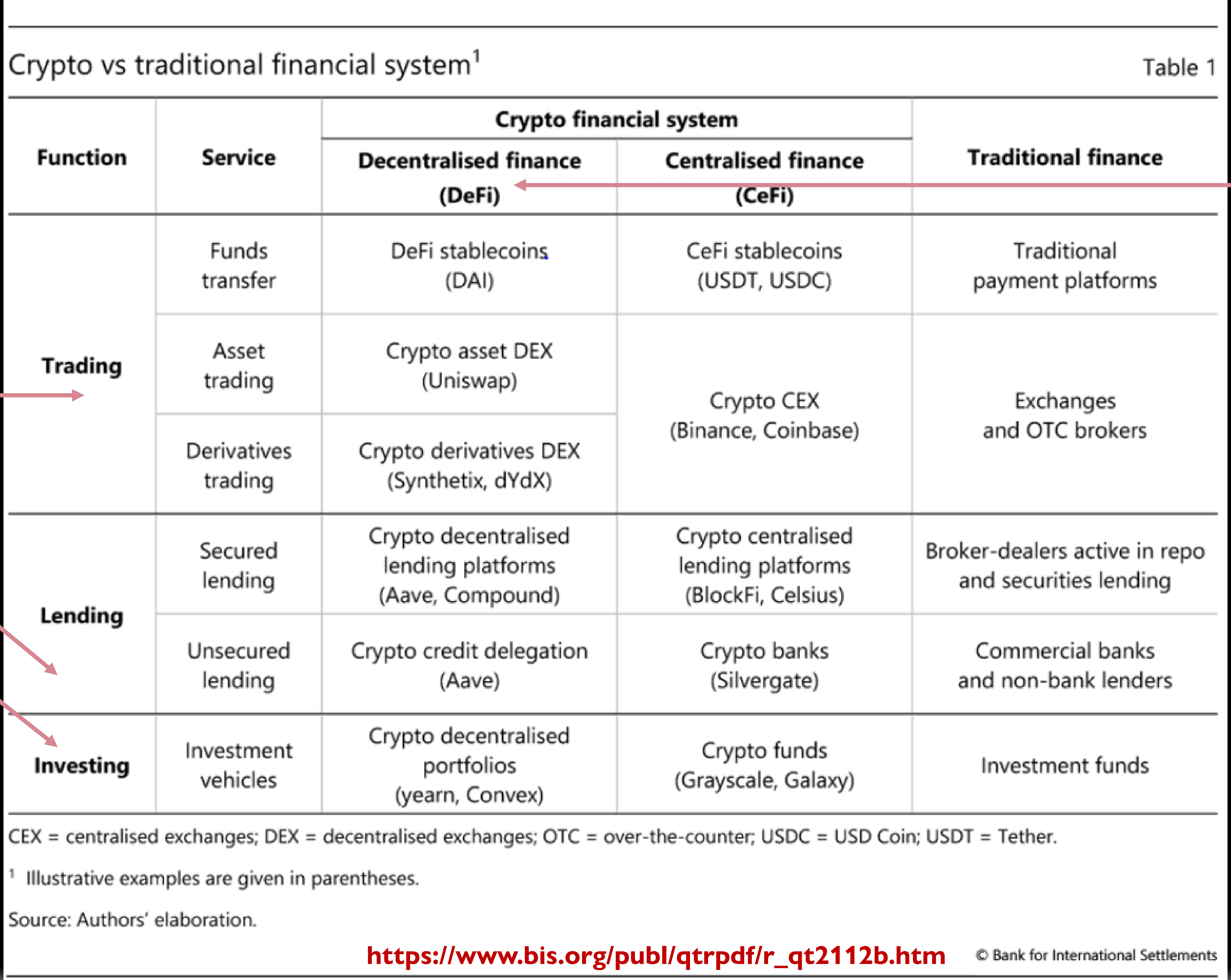


#1. What Opportunities Exist for Institutional Investors in the DeFi Ecosystem?

#2. What is the Current State of DeFi Regulation in Canada (and where are the Gaps and Uncertainties)?

#3. What Accessibility Frictions, Risks, Legal and Regulatory Barriers Exist for Greater Institutional Uptake?

#2. Income earning opportunities through DeFi ecosystem participation: Yield farming, staking (proof-of-stake consensus), liquidity pools, automated market makers, collateralization, stablecoins



Crypto vs traditional financial system[1]

Table 1

Function	Service	Crypto financial system		Traditional finance
		Decentralised finance (DeFi)	Centralised finance (CeFi)	
Trading	Funds transfer	DeFi stablecoins (DAI)	CeFi stablecoins (USDT, USDC)	Traditional payment platforms
	Asset trading	Crypto asset DEX (Uniswap)	Crypto CEX (Binance, Coinbase)	Exchanges and OTC brokers
	Derivatives trading	Crypto derivatives DEX (Synthetix, dYdX)		
Lending	Secured lending	Crypto decentralised lending platforms (Aave, Compound)	Crypto centralised lending platforms (BlockFi, Celsius)	Broker-dealers active in repo and securities lending
	Unsecured lending	Crypto credit delegation (Aave)	Crypto banks (Silvergate)	Commercial banks and non-bank lenders
Investing	Investment vehicles	Crypto decentralised portfolios (yearn, Convex)	Crypto funds (Grayscale, Galaxy)	Investment funds

CEX = centralised exchanges; DEX = decentralised exchanges; OTC = over-the-counter; USDC = USD Coin; USDT = Tether.

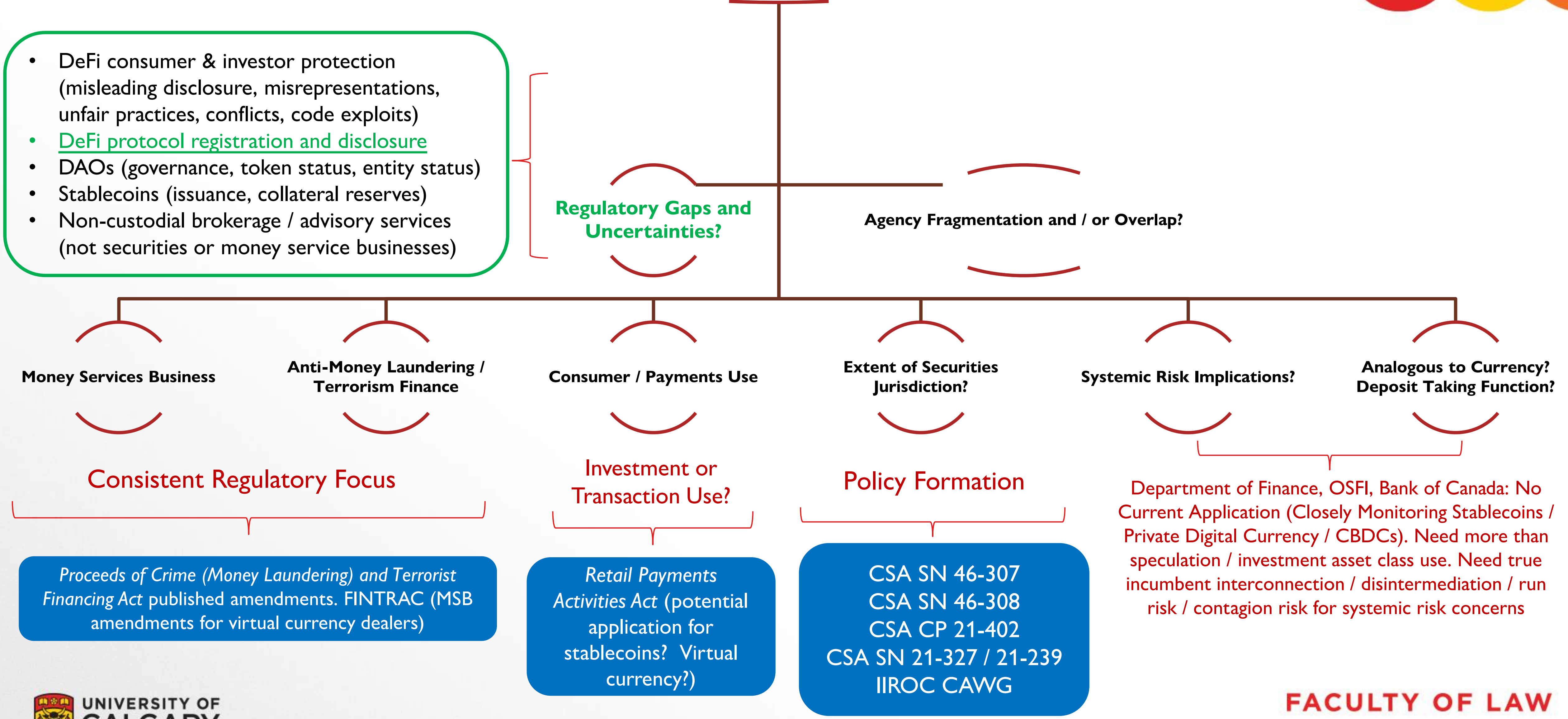
[1] Illustrative examples are given in parentheses.

Source: Authors' elaboration.

https://www.bis.org/publ/qtrpdf/r_qt2112b.htm

#1 Direct participation: Proprietary trading, lending, investment vehicle holdings (crypto decentralized portfolios)

Canadian Regulation of Crypto-Assets



- DeFi consumer & investor protection (misleading disclosure, misrepresentations, unfair practices, conflicts, code exploits)
- DeFi protocol registration and disclosure
- DAOs (governance, token status, entity status)
- Stablecoins (issuance, collateral reserves)
- Non-custodial brokerage / advisory services (not securities or money service businesses)

Regulatory Gaps and Uncertainties?

Agency Fragmentation and / or Overlap?

Money Services Business

Anti-Money Laundering / Terrorism Finance

Consumer / Payments Use

Extent of Securities Jurisdiction?

Systemic Risk Implications?

Analogous to Currency? Deposit Taking Function?

Consistent Regulatory Focus

Proceeds of Crime (Money Laundering) and Terrorist Financing Act published amendments. FINTRAC (MSB amendments for virtual currency dealers)

Investment or Transaction Use?

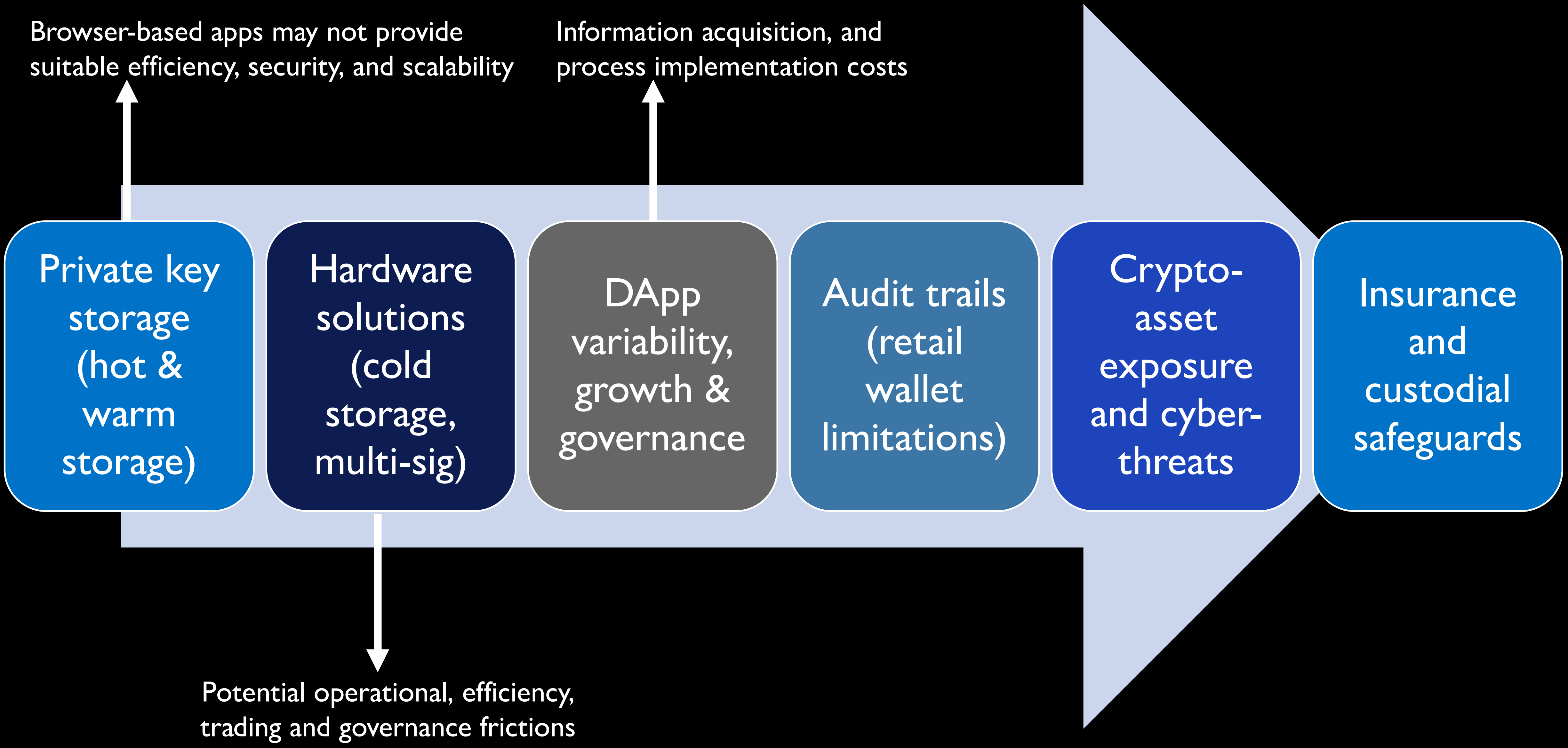
Retail Payments Activities Act (potential application for stablecoins? Virtual currency?)

Policy Formation

CSA SN 46-307
CSA SN 46-308
CSA CP 21-402
CSA SN 21-327 / 21-239
IIROC CAWG

Department of Finance, OSFI, Bank of Canada: No Current Application (Closely Monitoring Stablecoins / Private Digital Currency / CBDCs). Need more than speculation / investment asset class use. Need true incumbent interconnection / disintermediation / run risk / contagion risk for systemic risk concerns

Considerations For Institutional Investors in DeFi (Informing Policy Formation)



Browser-based apps may not provide suitable efficiency, security, and scalability

Information acquisition, and process implementation costs

Private key storage (hot & warm storage)

Hardware solutions (cold storage, multi-sig)

DApp variability, growth & governance

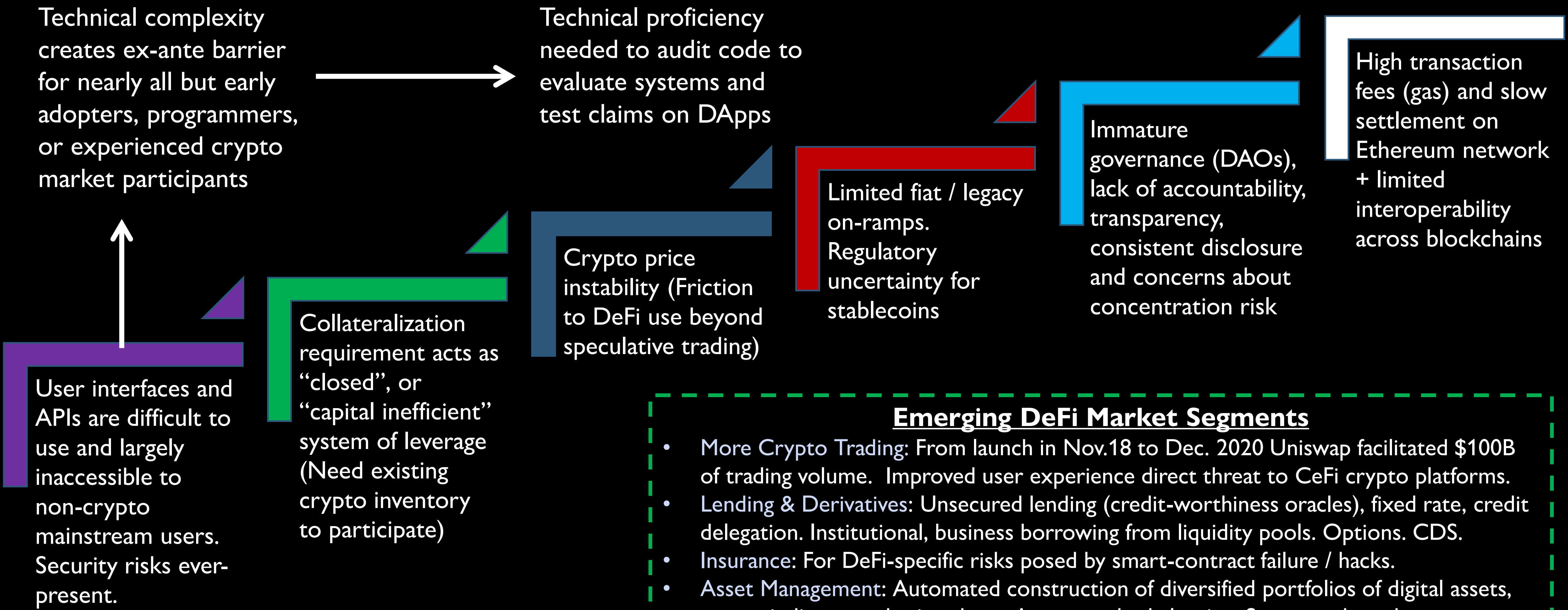
Audit trails (retail wallet limitations)

Crypto-asset exposure and cyber-threats

Insurance and custodial safeguards

Potential operational, efficiency, trading and governance frictions

Frictions to Wide Institutional DeFi Adoption



User interfaces and APIs are difficult to use and largely inaccessible to non-crypto mainstream users. Security risks ever-present.

Technical complexity creates ex-ante barrier for nearly all but early adopters, programmers, or experienced crypto market participants

Technical proficiency needed to audit code to evaluate systems and test claims on DApps

Collateralization requirement acts as “closed”, or “capital inefficient” system of leverage (Need existing crypto inventory to participate)

Crypto price instability (Friction to DeFi use beyond speculative trading)

Limited fiat / legacy on-ramps. Regulatory uncertainty for stablecoins

Immature governance (DAOs), lack of accountability, transparency, consistent disclosure and concerns about concentration risk

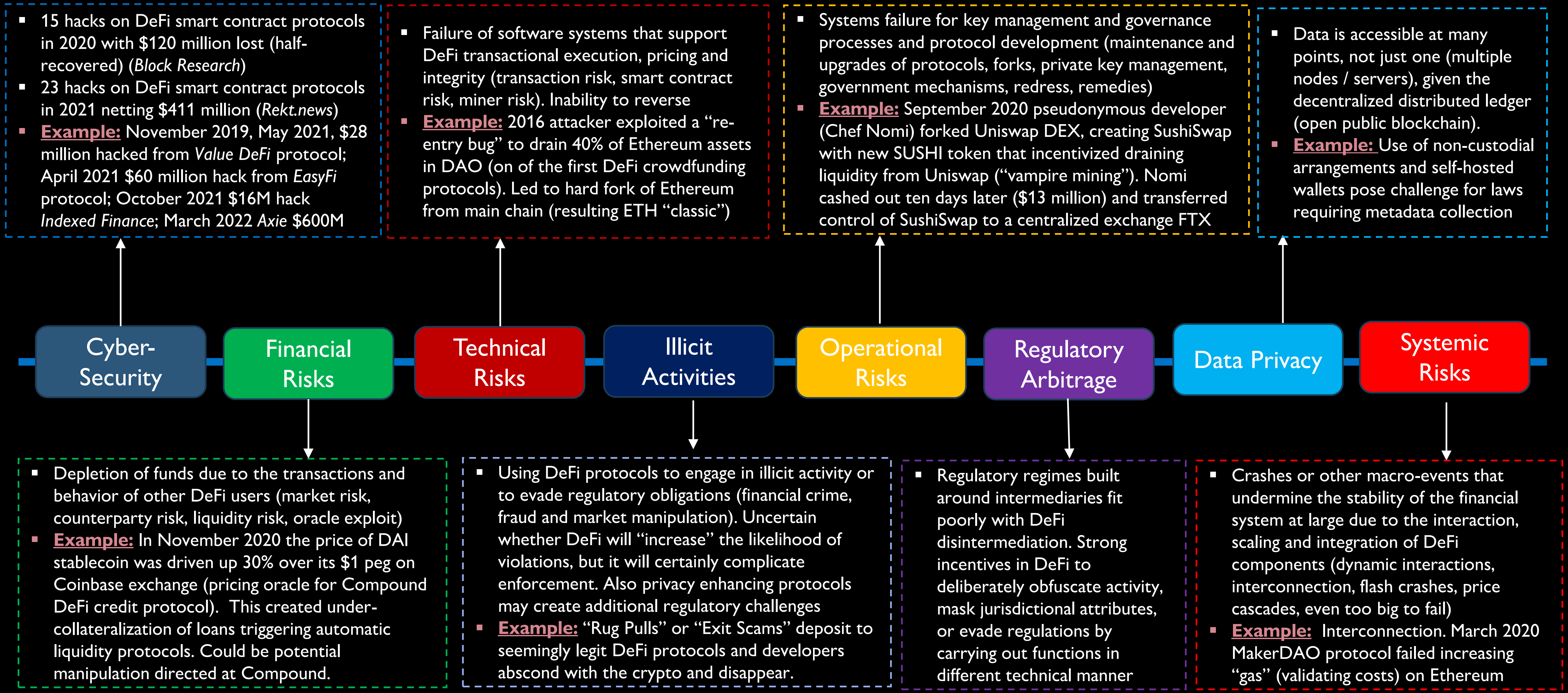
High transaction fees (gas) and slow settlement on Ethereum network + limited interoperability across blockchains

Emerging DeFi Market Segments

- More Crypto Trading: From launch in Nov.18 to Dec. 2020 Uniswap facilitated $100B of trading volume. Improved user experience direct threat to CeFi crypto platforms.
- Lending & Derivatives: Unsecured lending (credit-worthiness oracles), fixed rate, credit delegation. Institutional, business borrowing from liquidity pools. Options. CDS.
- Insurance: For DeFi-specific risks posed by smart-contract failure / hacks.
- Asset Management: Automated construction of diversified portfolios of digital assets, crypto indices, synthetic tokens. Automated rebalancing. Structured products.
- Aggregators (Money “Legos”): Mediate activity across services in base categories (stablecoins, DEX, lending, derivatives, insurance, asset management). Optimize returns while reducing complexity. Enhanced governance and usability.

DeFi Regulatory Considerations for Policy Formation

UNIVERSITY OF CALGARY



Cyber-Security

- 15 hacks on DeFi smart contract protocols in 2020 with $120 million lost (half-recovered) (*Block Research*)
- 23 hacks on DeFi smart contract protocols in 2021 netting $411 million (*Rekt.news*)
- Example: November 2019, May 2021, $28 million hacked from *Value DeFi* protocol; April 2021 $60 million hack from *EasyFi* protocol; October 2021 $16M hack *Indexed Finance*; March 2022 *Axie* $600M

Financial Risks

- Depletion of funds due to the transactions and behavior of other DeFi users (market risk, counterparty risk, liquidity risk, oracle exploit)
- Example: In November 2020 the price of DAI stablecoin was driven up 30% over its $1 peg on Coinbase exchange (pricing oracle for Compound DeFi credit protocol). This created under-collateralization of loans triggering automatic liquidity protocols. Could be potential manipulation directed at Compound.

Technical Risks

- Failure of software systems that support DeFi transactional execution, pricing and integrity (transaction risk, smart contract risk, miner risk). Inability to reverse
- Example: 2016 attacker exploited a "re-entry bug" to drain 40% of Ethereum assets in DAO (on of the first DeFi crowdfunding protocols). Led to hard fork of Ethereum from main chain (resulting ETH "classic")

Illicit Activities

- Using DeFi protocols to engage in illicit activity or to evade regulatory obligations (financial crime, fraud and market manipulation). Uncertain whether DeFi will "increase" the likelihood of violations, but it will certainly complicate enforcement. Also privacy enhancing protocols may create additional regulatory challenges
- Example: "Rug Pulls" or "Exit Scams" deposit to seemingly legit DeFi protocols and developers abscond with the crypto and disappear.

Operational Risks

- Systems failure for key management and governance processes and protocol development (maintenance and upgrades of protocols, forks, private key management, government mechanisms, redress, remedies)
- Example: September 2020 pseudonymous developer (Chef Nomi) forked Uniswap DEX, creating SushiSwap with new SUSHI token that incentivized draining liquidity from Uniswap ("vampire mining"). Nomi cashed out ten days later ($13 million) and transferred control of SushiSwap to a centralized exchange FTX

Regulatory Arbitrage

- Regulatory regimes built around intermediaries fit poorly with DeFi disintermediation. Strong incentives in DeFi to deliberately obfuscate activity, mask jurisdictional attributes, or evade regulations by carrying out functions in different technical manner

Data Privacy

- Data is accessible at many points, not just one (multiple nodes / servers), given the decentralized distributed ledger (open public blockchain).
- Example: Use of non-custodial arrangements and self-hosted wallets pose challenge for laws requiring metadata collection

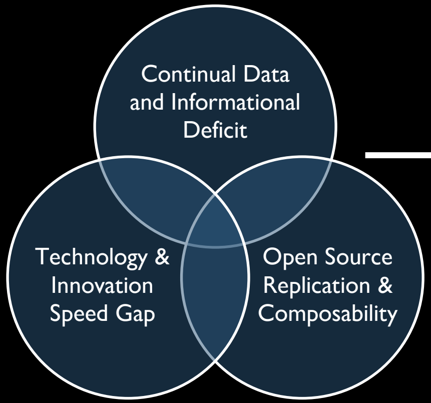
Systemic Risks

- Crashes or other macro-events that undermine the stability of the financial system at large due to the interaction, scaling and integration of DeFi components (dynamic interactions, interconnection, flash crashes, price cascades, even too big to fail)
- Example: Interconnection. March 2020 MakerDAO protocol failed increasing "gas" (validating costs) on Ethereum

Sources: World Economic Forum, "Policy-Maker Toolkit" (2021); Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, "Decentralized Finance (DeFi)" (March 2020) IIEL Issue Brief 02/2020, European Banking Institute Working Paper Series 59/2020; Lewis Cohen, Angela Angelovska-Wilson & Greg Strong, "Decentralized Finance: Have Digital Assets and Open Blockchain Networks Found Their 'Killer App'? (2021) online: Global Legal Insights, Blockchain & Cryptocurrency Regulation 2021

Challenges Regulating DeFi

UNIVERSITY OF CALGARY


Continual Data and Informational Deficit
Technology & Innovation Speed Gap
Open Source Replication & Composability

Which courts and law apply to an unincorporated distributed ledger system, with an automating, self-governed software protocol operating on it, used in multiple jurisdictions where the substantive claim to jurisdiction can be based on entirely different concepts – contract, tort, joint venture or partnership law, antitrust, blockchain specific legislation in some jurisdictions?

Open, programmable, global, public blockchains have no regulator truly in charge.

Jurisdiction

Not clear that the securities regulator has legal jurisdiction over DeFi non-custodial products and services using decentralized crypto-assets (especially if no “crypto-contract” is created by a DApp)

Anonymity

The decentralized, non-custodial, composable nature of DeFi makes it difficult to identify a responsible party. Further, DeFi users remain largely anonymous (little KYC / AML on DApps)

Arbitrage & Enforcement

Significant challenges. Enforcement measures will likely be directed towards largely anonymous DeFi participants, extra-jurisdictional software developers, or attempts to block sites & DApps through ISP / App stores

Copycats & Forks

Widespread use of open-source code allows participants to view, verify and copy protocols to create independent, derivative or competitive services. Programmability allows for infinite dynamic extensions

Redress of Disputes

Once smart contract is executed, the ouput cannot be modified or reversed just because an individual actor, or a governmental authority, orders it to be. Complexities for judicial or administrative orders. Easy of exchange on DEX