The Future of Money and Payments
BUSGEN102
Course Syllabus

Darrell Duffie

Graduate School of Business
Stanford University

Winter Quarter 2024

This version: April 4, 2024

Course assistants: James Eklund and Austin Bennett

In its exploration of the future of money and payments, this course focuses on technology and public policy. Money and payments have long been dominated by physical cash and by bank-railed payments. We will investigate ongoing improvements and disruptions of these conventional approaches with new technologies, including fast payment systems, central bank digital currencies, and applications of cryptography such as blockchain-based digital ledgers, stablecoins, zero-knowledge proofs, smart-contract settlement, and automated market making. Policy concerns include financial inclusion, efficiency, disruption of banking, privacy, anti-money laundering, financial stability, and monetary policy transmission.

Grading is based on frequent homework assignments (50%) and quizzes (50%). There is no final exam. This syllabus is a live course document that will be updated on a rolling basis during the quarter.

1 Introduction

We begin with an overview of the future of money and payments. How will Alice pay Bob? Over the past few centuries, the most popular way for Alice to pay has changed from physical cash — such as coins and paper currency — to a transfer from her bank account to Bob's bank account. In the near future, there could be significant use of blockchain-based payment arrangements such as stablecoins, which are already actively used in cryptocurrency markets and are beginning to be used for cross-border business payments, wholesale finance, peer-to-peer

payments, and some fringe applications such as money laundering, ransomware, and sanctions avoidance. Central bank digital currencies (CBDCs), now under development around the world, may eventually come into common use. The introduction of CBDCs is controversial, especially in the United States, where CBDC research and development is lagging over concerns about the potential for loss of privacy and disruption of banking. Paper money is falling out of common use in some countries such as Sweden. In the United States, consumers now make payments with cash with a frequency of about 18%, down significantly over the past few years.

References:

Required reading:
U.S. Department of the Treasury (2022). *The Future of Money and Payments*. United States Treasury Department, September. Section II, pages 3-18.

Optional reading:
Board of Governors of the Federal Reserve System (2022b). *Money and Payments: The US Dollar in the Age of Digital Transformation*. Federal Reserve Board, January.

Sveriges Riksbank (2022). *Payments Report*. Sveriges Riksbank (central bank of Sweden), December.

2 Simple elements of blockchain payments

A cryptocurrency is a fungible asset that can be transferred on a blockchain ledger. We will cover the basic elements of blockchain ledgers and transfers. The leading example of a cryptocurrency is Bitcoin, which was invented in 2009 and remains the largest cryptocurrency in terms of total market value. Large quantities of energy are required to validate transfers of Bitcoin because of its computationally intensive proof-of-work consensus protocol (Biais et al., 2019). In any case, Bitcoin is not effective as a broad-application payment scheme because of its high price volatility and the significant latency for conducting Bitcoin transfers. Typically, Alice and Bob don't want to wait several minutes or more for the verification of a payment. Moreover, if Alice is buying a new home from Bob, the change in value of Bitcoin between the inception and completion of the payment for the home could involve substantial price risk to her or Bob. While sometimes used to make payments, Bitcoin is more often purchased as a speculative investment.

A stablecoin is a cryptocurrency whose price is intended to be stable relative to some common numéraire such as US dollars. Alice could pay Bob by assigning some of her stablecoins to him on a blockchain ledger. Not all stablecoins, however, actually have a stable value. See for example, Securies and Exchange Commission (2023).

Alice could also pay Bob by transferring stablecoins to him by some "off-chain" method, for example by sending a message to a custodian that records her claims to stablecoins in some other form of account, which may or may not be a blockchain ledger. Alice can ask her custodian to transfer some amount of this ownership claim to Bob's custodial account. As a payment scheme, however, this off-chain approach may have few of the advantages of blockchain technology. In some cases, Alice might as well have asked her custodian to pay Bob in units of a conventional asset such as bank deposits. Some off-chain payments are made with transfers on an auxiliary blockchain that records positions on the underlying blockchain, typically relying on a third party to make the transfers, again sacrificing some of the security and privacy advantages of blockchain transfers. The majority of cryptocurrency transfers are currently off-chain, mainly because of the significant fees and latency of on-chain transfers. Bob and Alice may be trading cryptocurrencies for purely speculative purposes rather than because of the features of blockchain technology. In that case, they may be willing to trust a third party or suffer some loss of privacy.

A ledger on which cryptocurrency positions are recorded can be "permissionless," as for the case of Bitcoin and for Paypal's stablecoin, PYUSD, thus requiring no trusted third party to validate transfers or the creation and destruction of units. Or a cryptocurrency could be permissioned, as proposed by Fnality for wholesale financial applications of stablecoins such as the settlement of trades of securities and foreign exchange.

Rather than exploring investment in cryptocurrencies, this course focuses instead on real-economy payment-and-settlement applications of stablecoins that take advantage of round-the-clock global access and smart contracting. These features can protect privacy, facilitate the programmability of payments, and reduce default risk. For example, when Alice buys euros from Bob, she could use a smart contract that cryptographically assigns dollar stablecoins to Bob, contingent on the event that he has likewise cryptographically assigned his euro stablecoins to Alice. With this, neither Alice nor Bob is at risk of sending a payment and not receiving a payment from their counterparty. This swap can be immediate or programmed for future settlement, potentially contingent on some other events that can be verified on the blockchain.

Stablecoins have raised concerns over consumer protection, financial stability, and money laundering (President's Working Group, 2021). Although many developed-market economies have established or are well on the way to establishing a legislative and regulatory framework for digital assets that encompasses cryptocurrencies, the US Congress has not yet made progress in this direction. Instead, the Securities and Exchange Commission (SEC) has pursued violations of US federal securities laws for cases in which the SEC believes that the cryptocurrencies involved are securities, in the legal sense of the term. Alleged violations include failure to register cryptocurrencies (including certain stablecoins) as securities, failure to register cryptocurrency trading platforms as securities exchanges, and failure to disclose risks to investors. The SEC has not suggested that Bitcoin is a security, probably because Bitcoin does not appear to meet the Howey Test of whether a financial instrument is a security (Securities

and Exchange Commission, 2022). Until new US legislation clarifies regulations regarding digital assets such as stablecoins, the development of some new US payment and settlement businesses and technologies may be delayed.

In a series of homework assignments on blockchain payments, you will learn how to:

- Create your own cryptocurrency wallet.
- Interact with smart contracts.
- Swap digital currency tokens with your classmates.
- Trade digital currencies on an automated market maker.

Over the course of these assignments, we will use Metamask as our wallet software and the Sepolia Ethereum blockchain as our test environment.

References:

Required:

Zulfikar Ramzan (2012a). *Cryptographic hash functions*. Kahn Academy, YouTube video.

Zulfikar Ramzan (2012b). *Digital signatures: High-level description*. Kahn Academy, YouTube video.

3Blue1Brown (2017). *But how does Bitcoin actually work?* YouTube video.

Optional:

Satoshi Nakamoto (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. White paper, bitcoin.org.

Valery Buterin (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. White paper, ethereum.org.

Hayden Adams, River Keefer, et al. (2021). *Uniswap v3 Core*. Uniswap, March.

Agostino Capponi and Ruizhe Jia (2024). *Liquidity Provision on Blockchain-based Decentralized Exchanges*. January.

Chainlink (2023b). *What Is a Smart Contract*. Chainlink, May.

Hong Kong Monetary Authority (2023). *Conclusion of Discussion Paper on Crypto-assets and Stablecoins*. HKMA, January.

President's Working Group (2021). *President's Working Group on Financial Markets and the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency Report on Stablecoins*. US Department of the Treasury, November.

Securies and Exchange Commission (2023). *Complaint: Securities and Exchange Commission v. Terraform Labs Pte. Ltd.* Southern District of New York, July.

Jed Rakoff (2023). *Opinion and order: Securities and Exchange Commission v. Terraform Labs Pte. Ltd.* Southern District of New York, December.

Securities and Exchange Commission (2022). *Framework for "Investment Contract" Analysis of Digital Assets*. Securities and Exchange Commission.

Bruno Biais et al. (2019). "The blockchain folk theorem". In: *The Review of Financial Studies* 32.5, pp. 1662–1715.

Fahad Saleh (2020). "Blockchain without Waste: Proof-of-Stake". In: *The Review of Financial Studies* 34.3, pp. 1156–1190.

Financial Stability Oversight Council (2022). *Report on Digital Asset Financial Stability Risks and Regulation*. US Department of the Treasury, October.

Ron Rivest, Adi Shamir, and Leonard Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2, pp. 120–126.

US Department of the Treasury (2023b). *Illicit Finance Risk Assessment of Decentralized Finance*. US Department of the Treasury, April.

3 Bank-railed payments

Whether measured by frequency or volume, the majority of payments are made by reducing the balance of Alice's bank account in favor of Bob's bank account. The money used for these payments is bank deposits, which are a form of debt owed to Alice and Bob by their respective banks, A and B. To pay Bob \$8, Alice sends a message to Bank A that it now owes her \$8 less and instructs her bank to arrange for an \$8 increase in Bob's account balance. The message can be sent by a credit or debit card, a paper check, a Zelle transfer, or a wire transfer, among other means. The payment is normally made via an intermediate sequence of compensating account transfers that can involve multiple banks and other payment service providers. For example, some time after getting a message from Visa about Alice's card payment request, Bank A can message the central bank (the Federal Reserve for US dollar payments) to reduce the account balance

of Bank A at the central bank by \$8 and increase the balance of Bank B at the central bank by \$8. Having also gotten the message, Bank B increases Bob's balance at Bank B by \$8. This payment sequence, which can happen quickly or slowly depending on the setting, involves three different forms of money denominated in US dollars: deposits at Bank A, deposits at Bank B, and deposits at the central bank. Banks A and B may profit from payment fees and from the opportunity to make loans to others with the funds that are left on deposit with them. Banks tend to offer depositors a much lower rate of interest than the banks themselves achieve by lending to others.

A cross-border payment involves two currencies. For example, Alice can pay dollars and ask that Bob receives euros. In that case, one of the intervening banks along the payment chain, called a correspondent bank, typically converts the dollars to euros by debiting and crediting the accounts of affiliate banks that have a Federal Reserve account and an account at a Eurosystem central bank, respectively. The correspondent bank can also determine the price at which Alice's dollars are exchanged for euros. Currently, bank-railed cross-border payments tend to be slow and costly, leaving a significant opening for new payment technologies.

As opposed to bank-railed payments, "e-money" transfer schemes such as Paypal, Venmo, WeChat Pay, and Alipay do not transfer bank deposits. How e-money customer funds are "backed" by assets varies across these schemes. Backing assets can include Treasury bills, deposits at third-party banks, and deposits at the central bank, among other assets. Some e-money services such as Wise and Revolut are best known for their cross-border payment services. As distinct from e-money services, "overlay" digital wallets such as Apple Pay and GooglePay typically act only as a messenger and a "digital wallet" that facilitates bank-railed payments (typically card payments) or e-money payments.

The first common use of bank-railed payments was probably at the "giro banks" of Venice in the early 14th century (Mueller and Lane, 2020). In 2021, bank-railed payments of US commercial bank deposits totaled \$128 trillion, based on Federal Reserve Board data. According to a San Francisco Fed survey, in 2022 about 73% of US consumer payments (by number of events) were bank railed, including credit card, debit card, and automated clearing house (ACH) transfers. Only about one percent of payments were made by e-money services. Virtually all US business-to-business payments are bank-railed. On top of payments in commercial bank deposits, on an average day there are over \$4 trillion of interbank payments of central bank deposits. These interbank payments are made on the Fedwire payment system.

In our coverage of bank-railed payments, we will emphasize the distinction between real-time gross settlement (RTGS) payment systems such as Fedwire and deferred net settlement payment systems such as ACH, which batch payments. Batching allows a bank to pay only the net of its outgoing payments over its incoming payments during the batching period, thus reducing the amount of central-bank balances that the bank needs at the beginning of a day to cover its payment obligations on that day. On the other hand, deferred net settlement involves delays and the risk that the payment might not ever be made because

the payer defaults before the batching time. RTGS avoids these costly delays, but requires larger initial balances.

Bank-railed payments can also be made with "tokenized deposits," which are bank deposits recorded on a blockchain ledger in order to take advantage of features such as round-the-clock transfers and smart contracting.

References:

Required reading:

Stripe (2023). *How credit card transaction processing works: A quick guide*. Stripe, August.

Tom Sullivan (2022). *What is an ACH Transfer? All about ACH bank transfers*. Plaid, December.

Rodney Garratt and Hyun Shin (Apr. 2023). "Stablecoins versus tokenised deposits: implications for the singleness of money". In: *BIS Bulletin* 113.

Gokce Ozcan et al. (Mar. 2023). "Deposit Tokens: A Foundation for Stable Digital Money". In: *Oliver Wyman and J.P. Morgan*.

Corporate Finance Institute (n.d.[b]). *SWIFT*. CFI Team.

Corporate Finance Institute (n.d.[a]). *Nostro Account*. CFI Team.

Optional reading:

Bank for International Settlements (2023a). *Blueprint for the future monetary system: improving the old, enabling the new*. BIS Annual Economic Report, Chapter 3, June.

Bank for International Settlements (2023). *Project Nexus: Enabling Instant Cross-border Payments*. BIS Innovation Hub, March.

Christopher J. Bechler, Szu-chi Huang, and Joshua I. Morris (July 2023). "Purchase Justafiability Drives Payment Choice: Consumers Pay with Card to Remember and Cash to Forget". In: *Journal of the Association for Consumer Research*.

Board of Governors of the Federal Reserve System (2022a). *Federal Reserve Payments Study*. Federal Reserve Board.

Emily Cubides and Shaun O'Brien (2023). *2023 Findings from the Diary of Consumer Payment Choice*. Federal Reserve Bank of San Francisco, May.

FNA (2023). *CHIPS Review*. FNA, January.

Reinhold Mueller and Frederic Chapin Lane (2020). *Money and Banking in Medieval and Renaissance Venice: Volume I: Coins and Moneys of Account*. Baltimore: Johns Hopkins University Press.

Regulated Liability Network (2022). *Digital Sovereign Currency*. Regulated Liability, November.

William Roberds and Francois R. Velde (2016). "Early Public Banks I: Ledger-Money Banks". In: *Money in the Western Legal Tradition: Middle Ages to Bretton Woods*. Ed. by David Fox and Wolfgang Ernst. Oxford University Press.

Jonathan Rose (2023). *Fedwire*. Federal Reserve History, August.

David L. Stearns (Jan. 2011). *Electronic Value Exchange: Origins of the VISA Electronic Payment System (History of Computing)*. 2011th ed. Springer.

Stripe (2023). *How credit card transaction processing works: A quick guide*. Stripe, August.

Tom Sullivan (2022). *What is an ACH Transfer? All about ACH bank transfers*. Plaid, December.

World Bank (2021b). *Global Findex Data*.

4 Central Bank Digital Currencies

Alice and Bob could potentially have digital deposit accounts at the central bank. In that case, Alice could pay Bob by transferring $8 from her account at the central bank to Bob's account at the central bank. This form of deposit is called a central bank digital currency (CBDC). One can view a CBDC as a digital-ledger-based extension of paper currency. A CBDC may or may not be based on a blockchain.

Although commercial banks routinely pay each other with digital central bank deposits, the term "CBDC" is reserved for cases in which the digital central bank money can also be used by consumers and merchants, or is held on a blockchain ledger. A widely used CBDC, whether or not based on blockchain technology, is called a "retail" CBDC. Most central banks are exploring a retail CBDC whose account and payment services will be provided by private-sector service providers such as banks.

A blockchain-based CBDC that is used primarily for payments between banks and other financial-services firms is known as a wholesale CBDC. Most central banks are also exploring wholesale CBDCs. Applications for wholesale

CBDCs include the settlement of transactions involving securities and foreign exchange. For example, Bank A could use a smart contract to cryptographically assign $500 million of wholesale CBDC to Bank B, contingent on the event that Bank B has paid for these dollars by likewise assigning digital euros to Bank A.

No large developed-market economy has put a CBDC into common use, but almost all central banks are working on CBDC technology. China was the first large country to pilot a CBDC, called eCNY, but adoption of eCNY has been slow. The European Central Bank is aiming to release a retail CBDC — the digital euro — within a few years. The US is behind most countries in CBDC exploration because of sharply divided policy views about the potential usefulness of a digital dollar, the extent to which it could disrupt conventional banks, and the degree to which it could curtail privacy. We will analyze each of these potential concerns.

References:

Required reading:

Bank of England and His Majesty's Treasury (2023). *The Digital Pound: A New Form of Money for Households and Businesses?* BoE and HM Treasury, February. Section D.1, "The platform model and public-private partnership," pages 50-66.

Optional reading:

Bank for International Settlements (2023b). *Project Rosalind: Building API prototypes for retail CBDC ecosystem innovation*. BIS Innovation Hub, June.

Bank for International Settlements and Hong Kong Monetary Authority (Oct. 2022). "Project Aurum: A Prototype for Two-tier Central Bank Digital Currency". In: *BIS Innovation Hub and HKMA*.

Bank of Canada (2023). *A Digital Canadian Dollar: What we heard 2020-23 and what comes next*. Bank of Canada.

Sally Chen et al. (2022). *CBDCs in Emerging Market Economies*. BIS Paper 123, April.

European Central Bank (2023). *A stocktake on the digital euro*. ECB, October.

Federal Reserve Bank of New York and Monetary Authority of Singapore (2023). *Project Cedar Phase II x Ubin+*. Federal Reserve Bank of New York and Monetary Authority of Singapore, May.

House of Commons Treasury Committee (2023). *The digital pound: still a solution in search of a problem?* House of Commons Treasury Committee, December.

Neha Narula, Lana Swartz, and Julie Frizzo-Barker (Jan. 2023). "CBDC: Expanding Financial Inclusion or Deepening the Divide?" In: *Digital Currency Initiative*.

Anders Ögren (2022). *Replacing bank money with base money: Lessons for CBDCs from the ending of private banknotes in Sweden*. Uppsala Papers in Economic History, Working Paper 2022-03, October.

Gabriel Soderberg et al. (2023). *How Should Central Banks Explore Central Bank Digital Currrency*. International Monetary Fund, Fintech Note 2023-008, September.

Alexandra Sutton-Lalani et al. (2023). *Redefining Financial Inclusion for a Digital Age: Implications for a Central Bank Digital Currency*. Bank of Canada, Staff Discussion Paper 2023-22, October.

5 Fast payment systems

A fast payment system is a broadly accessible RTGS bank-railed payment system that runs around the clock. This allows Alice to pay Bob instantly, 24 $\times 7 \times 365$, if their respective banks have given them interoperable access to the fast payment system. The World Bank's Project Fast Tracker shows extensive development of fast payment systems around the world.

In terms of adoption and impact on their economies, Brazil's Pix and India's Unified Payment Interface (UPI) are notably successful fast payment systems. Their wide adoption and heavy use are due in part to the effectiveness of their alias resolution services, by which Alice can easily target a payment to nearly anyone in the economy by using a simple common alias for the payee, such as Bob's phone number, which can be stored on Alice's phone for repeated later use. Alias resolution services and the common use of QR and other merchant bar codes have led to extremely high penetration for these fast payment systems, much in the manner that the e-money services WeChat Pay and Alipay have been almost universally adopted in China's cities. Beyond the interoperability benefits of an economy-wide alias resolution service, factors behind the high penetration of Pix and UPI include the common use of mobile phones, regulations that require banks to provide basic low-cost bank accounts to any adult, and, in the case of Pix, a regulation that requires all large banks to give their customers access to Pix on an app meeting common standards. Because of

these regulations, most Brazilian adults were using Pix within two years of its appearance. No other fast payment system achieved such rapid and ubiquitous adoption. According to research studies, Pix and UPI have advanced financial inclusion, credit provision, and economic growth.

The US has two fast payment systems, RTP and FedNow, but neither has yet achieved broad-spread adoption. RTP, a private-sector service available to only a subset of US banks, has achieved relatively high transaction volumes for specific services, mainly business related. FedNow, operated by the Fed, became available to any bank in 2023. By January 2024, 400 banks had enrolled in FedNow, although relatively few of the largest banks have joined. Neither RTP nor FedNow has a broad-based alias resolution service. Whether and how these US fast payment services are provided by a bank to its customers has been left up to the bank to decide, without much of a regulatory nudge. The Monetary Control Act, moreover, does not allow the Fed to subsidize FedNow.

The fast payment systems of two or more countries can be linked, allowing Alice to make fast and inexpensive cross-border payments to Bob through correspondent banks that are members of their respective fast payment systems (World Bank, 2021a; Committee for Payments and Market Infrastructure, 2022; Committee for Payments and Market Infrastructure, 2023). Singapore has already linked its fast payment systems with those of several other countries. IXB is a planned fast-payment link between the US and Europe.

References:

Required reading:

Peter Conti-Brown and David A. Wishnick (2020). "Private Markets, Public Options, and the Payment System". In: *Yale Journal on Regulation* 37. Section II, pages 391-405.

Bank for International Settlements (2023). *Project Nexus: Enabling Instant Cross-border Payments*. BIS Innovation Hub, March. Section 1, Executive Summary.

Federal Reserve Bank Services (2021). *How the FedNow Service works*. Youtube, February.

World Bank (2023). *The future of fast payments*. World Bank Group Focus Note, October. Chapter 2, Background.

Optional reading:

Angelo Duarte et al. (2022). *Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix*. BIS Bulletin, 52, March.

Tamana Singh Dubey and Amiyatosh Purnanadam (2023). *Can Cashless Payments Spur Economic Growth?* University of Michigan, Stephen M. Ross School of Business, November.

Committee for Payments and Market Infrastructure (2022). *Interlinking payment systems and the role of application programming interfaces: A framework for cross-border payments*. Interim report to the G20, Bank for International Settlements and Committee for Payments and Market Infrastructure, July.

Committee for Payments and Market Infrastructure (2023). *Linking fast payment systems across borders: Considerations for governance and oversight*. Interim report to the G20, Bank for International Settlements and Committee for Payments and Market Infrastructure, October.

World Bank (2021a). *Cross-border fast payments*. World Bank Group Focus Note, September.

6 Financial applications of smart contracting

Smart contracting is beginning to be used for financial applications such as trade execution and settlement. Automated market makers (AMMs) provide algorithmic market making services from a liquidity pool of two or more tokenized assets, at terms of trade set by a mathematical formula known as a bonding curve. Liquidity providers commit "deposits" of the tokenized assets to be exchanged on an AMM, and profit from trading fees. We focus mainly in lectures and homework on the Uniswap AMM.

Turning to trade settlement, we compare blockchain smart-contract settlement with various traditional approaches, such as bilateral settlement, payment-versus-payment, delivery-versus-payment, and central clearing. Central clearing and smart-contract settlement reduce counterparty default risk. These approaches can be chosen with settlement lags that reduce needed initial inventories of cash and traded assets by allowing market participants to trade before acquiring the needed assets and cash, and through the effect of netting purchases against sales. However, longer settlement lags increase counterparty risk and require longer commitments of assets and of space on intermediary balance sheets. Smart-contract settlement can be conducted with short or long settlement lags, but reduces the fungibility of money and assets and may therefore require greater quantities of assets and money to manage payments and settlements.

References:

Required reading:

Dennis McLaughlin (2023). "The trade-off between shorter settlement times and multilateral netting benefits in deferred net settlement". In: *Journal of Financial Market Infrastructures* 11.1, pp. 1–17. Sections 1, 2, 3, 5, 6, 7.

Hayden Adams, Noah Zinsmeister, et al. (2021). *Uniswap v3 Core*. uniswap.org whitepaper, March. Sections 1 and 2.

Optional reading:

Bank for International Settlements and Monetary Authority of Singapore (June 2023). "Project Guardian: Enabling Open and Interoperable Networks". In.

Bank for International Settlements (2023c). *Project Mariana: Cross-border exchange of wholesale CBDCs using automated market-makers*. BIS Innovation Hub, September.

Morten Bech et al. (2020). *On the future of securities settlement*. BIS Quarterly Review, March.

Shaun Byck and Ronald Heijmans (Jan. 2021). "How much liquidity would a liquidity-saving mechanism save if a liquidity-saving mechanism could save liquidity? A simulation approach for Canada's large-value payment system". In: *Journal of Financial Market Infrastructures*.

DTCC, Clearstream, and Euroclear (2023). *Advancing the Digital Asset Era, Together*. September.

Michael Egorov and Curve Finance (2021). *Automatic market-making with dynamic peg*. June.

Gordon Liao and Dan Robinson (2022). *The Dominance of Uniswap v3 Liquidity*. May.

Giulia Secco (Dec. 2021). "The importance of Fnality's Universal Payment Leg". In: *FNALITY*.

Stuart D. Levi and Alex B. Lipton (May 2018). "An Introduction to Smart Contracts and Their Potential and Inherent Limitations". In: *Skadden*.

Regulated Liability Network (2022). *Digital Sovereign Currency*. Regulated Liability, November.

7 Payment privacy and legality

How can the authorities be confident that Alice's payment to Bob is legal, while at the same time protecting their privacy? Growth in the volume of US suspicious payment activity reports (SARs) provided to the government, concerns over government access to CBDC payment data, and some US Supreme Court cases have led commenters to raise concerns over the privacy of payments.

In the area of payments, protections of privacy afforded under the Fourth Amendment of the US constitution have become thin, according to Van Valkenburgh (2019). In 2023, financial institutions sent the US government roughly 4 million SARs about their payments. Some leading politicians, among others, have suggested that central bank digital currencies will cause an excessive loss of privacy.

The European Data Protection Board (2023) has recommended tighter policies in favor of data privacy for the digital euro, saying that the European Central Bank and payment service providers should do more to protect privacy than is required by currently proposed regulations. They "strongly recommend to introduce a 'privacy threshold' for online transactions, under which neither offline nor online low-value transactions are traced for purposes of anti-money laundering (AML) and for combating the financing of terrorism (CFT)."

Separately, the European Commission has proposed new access for government designees to web-based information All EU citizens will be offered the possibility to have an EU Digital Identity Wallet to access public and private online services in full security and protection of personal data all over Europe. This law, still to be ratified by the European Parliament, generated a letter of protest from over 500 scientists and NGOs, regarding the risk that the designation of data recipients is not well controlled and could lead to a significant loss of privacy.

Zero-knowledge proof (ZKP) is a cryptographic method for validating a fact for others without revealing the fact itself (Goldwasser, Micali, and Rackoff, 1985; Feige, Fiat, and Shamir, 1987). For example, Alice could use ZKP to prove to Bob that she has made a payment to him on a public ledger, without the need to reveal any confidential information about herself (such as her account details or identity documentation) and without the need to reveal information about the payment to others. Alice could also use ZKP to validate publicly that the payment meets some standard of legality, for example that the payer, payee, and certain other parameters of the payment meet stipulated anti-money-laundering criteria (Ben-Sasson et al., 2014).

References:

Required reading:

US Department of the Treasury (2023a). *Finance Risk Assessment of Decentralized Finance*. US Department of the Treasury, April. pages 1-7.

Peter Van Valkenburgh (2019). *Electronic Cash, Decentralized Exchange, and the Constitution*. Coin Center, March. Section III "Electronic Cash, Decentralized Exchange, and the Fourth Amendment."

Video on Zero Knowledge Proof, Amit Sahai, Computer Scientist Explains One Concept in 5 Levels of Difficulty," *Wired*, 2022.

Optional reading:

Bank for International Settlements (2023d). *Project Tourbillon: exploring privacy, security and scalability for CBDCs*. Bank for International Settlements, November.

Christopher J. Bechler, Szu-chi Huang, and Joshua I. Morris (July 2023). "Purchase Justafiability Drives Payment Choice: Consumers Pay with Card to Remember and Cash to Forget". In: *Journal of the Association for Consumer Research*.

Eli Ben-Sasson et al. (Nov. 2014). "Zerocash: Decentralized anonymous payments from bitcoin". In: *Proceedings - IEEE Symposium on Security and Privacy*. Institute of Electrical and Electronics Engineers Inc., pp. 459–474.

Chainlink (2023a). *Zero-Knowledge Proof: Applications and Use Cases*. Chainlink, November.

European Data Protection Board (2023). *Joint Opinion on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro*. European Data Protection Board, October.

Federal Deposit Insurance Corporation (2003). *"Suspicious Activity Report"*. Washington DC.

Uriel Feige, Amos Fiat, and Adi Shamir (1987). "Zero Knowledge Proofs of Identity". In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pp. 210–217.

Nick Maxwell (2024a). "Paper 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk". In: *Future of Financial Intelligence Sharing (FFIS) research programme*. Payment Systems Policy Discussion Series.

Nick Maxwell (2024b). "The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design". In: *Future of Financial Intelligence Sharing (FFIS) research programme*. Payment Systems Policy

Discussion Series.

S Goldwasser, S Micali, and C Rackoff (1985). "The Knowledge Complexity of Interactive Proof-Systems". In: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC '85. Providence, Rhode Island, USA: Association for Computing Machinery, pp. 291–304.

Nadia Pocher and Andreas Veneris (2021). *Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme*. January.

Zachary Warmbrodt (Feb. 2024). "Conservatives rally against CBDC". in: *Politico*.

Michalopoulos Panagiotis et al. (2024). *Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT*. working paper, University of Toronto, to appear.