SWEN 422 Lecture 9
Digital Money 2

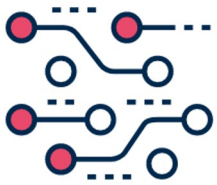
Dr Jennifer Ferreira

27 March 2024

Agenda

- Review of previous lecture
- Equity and ethical issues
- Digital transactions
- Transaction-related challenges

Bank of England



96% of money is held electronically (bank deposits)

4% of money is held physically in the form of cash (banknotes and coins)

Reserve Bank of New Zealand

~$452 billion in bank deposits and ~$8.6 billion in banknotes - 2023

Video: Where does money come from?

Who has the authority to ***issue*** (digital) money?

- Bank NEW ZEALAND $, BRITISH £, JAPANESE ¥
  - Government (e.g. Central banks, Reserve Bank of New Zealand)
  - Commercial (e.g. ANZ, Westpac, etc.)

Sovereign currency

- Private (non-bank) Bitcoin Bristol Pound Green Dollar
  - Corporation
  - Society
  - Community
  - Games

E.g. cryptocurrencies, community currencies, complementary currencies, local currencies, in-game currencies, etc.

Robux

Digital money interfaces

Earliest interface - ATMs

Developed in the UK? US? in 1960s

“Sleepless tellers” - Tillie the teller

Ergonomics (Hatta & Liyama, 1991)

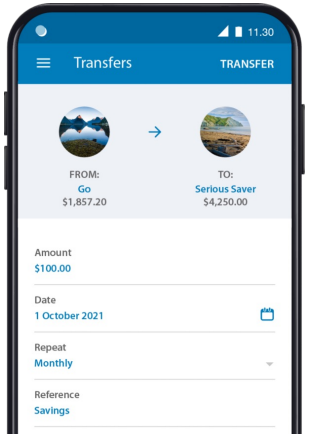
Menu design to reduce card re-insertions (Curran & King, 2008)

A brief history of the ATM (Batiz-Lazo 2015)

More recent interfaces

- Mobile money & payments

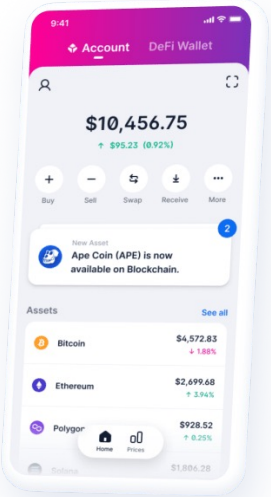
[Mobile Money and Payment: a literature review based on academic and practitioner – oriented publications (2001 - 2011)]



https://www.anz.co.nz/banking-with-anz/ways-to-bank/gomoney/

- Programmable money

[Programmable money: next-generation blockchain-based conditional payments]



https://www.blockchain.com/wallet

HCI and Digital Money Research

Why?

1. Evidence that existing tools do not meet people's needs
2. Design and innovation is being driven by commercial interests
3. Equity and ethical issues that need to be explored



HCI and Digital Money Research

Goals:

1. Critique and improve the design of current financial interactions
2. Uncover everyday practices and design tools that support them
3. Discover new ways of interacting with money and financial services

Equity & Ethical issues

Digital Equity

“a digital divide exists when a group’s access to digital technologies and resources differs along one or more dimensions of social, economic, cultural, or national identity.”

Problems of access and knowledge lead to exclusion from physical, intellectual, digital, social, economic, cultural, and/or national life, resulting in gaps between those that have access and those that do not.

Equality - each person receives an equal share of resources despite what they already have, or don’t have.

Equity - resources are shared based on what each person needs in order to adequately level the playing field.

Ethics

Ethics is about making the best possible decisions concerning people, resources and the environment.

System of principles and values that helps us make those decisions.

- NZ Institute of IT Professionals Code of Ethics
- ACM Code of Ethics
- IEEE Code of Ethics

Ethical values e.g., integrity, honesty, trustworthiness, responsibility

Equity & ethical issues

Covid-19

Cryptocurrencies

Cashless society

Central Bank Digital Currencies

(Financial) Literacy

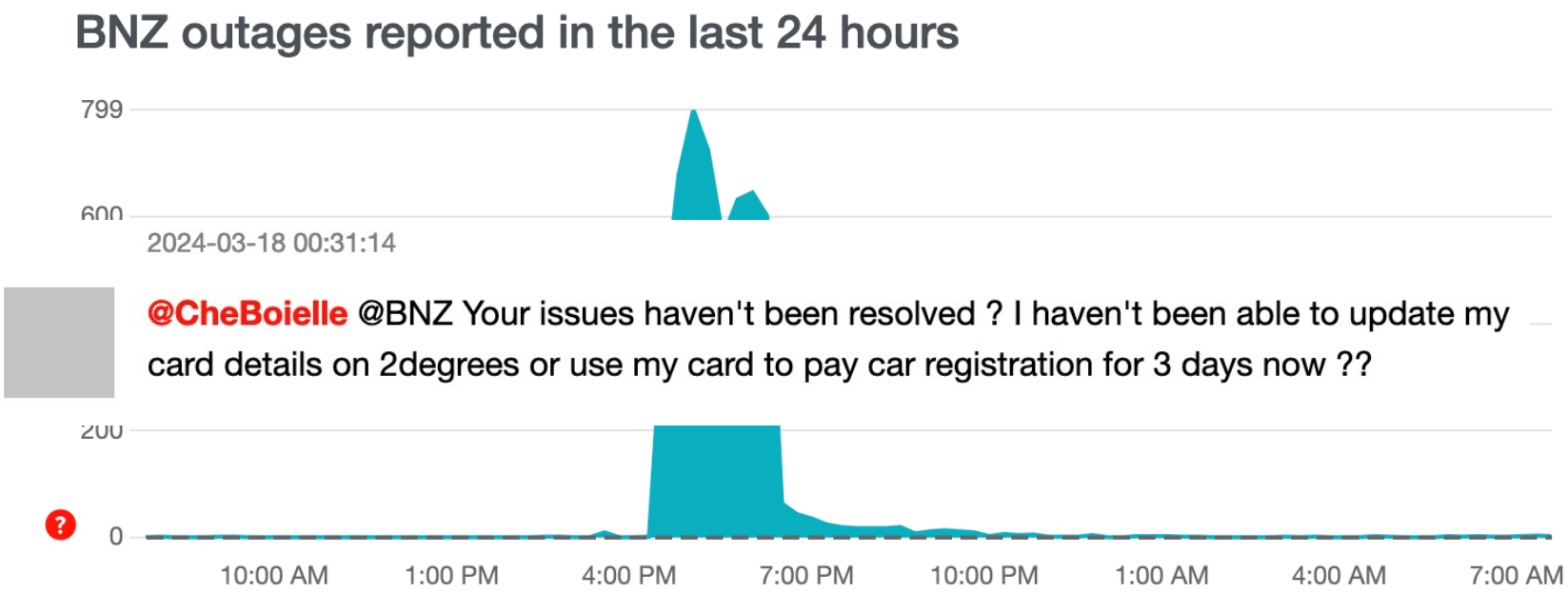
Poverty

2 Billion Unbanked (2017)

Aging population

DDos attack 3 September 2021

BNZ “systems issue” 26 March 2024



https://downdetector.co.nz/status/bnz/ on Wed 27 March AM

2024-03-26 03:49:52

@Chenstarz @BNZ Hi. BNZ customer here. Great App. I sent a couple payments over the weekend on the 17th Sunday March from my ANZ to my BNZ in the morning. It’s Monday afternoon. Not arrived yet. Is there a known issue for over the weekend on getting payments ?

Equity & ethical questions

For any system:

Who benefits and who gets left behind?

Whose life is made easier and whose is made more difficult?

Are we satisfied with the status quo? Or can we think of ways to do better?

Equity & Inclusion

Woldmariam, M. F., Ghinea, G., Atnafu, S., & Grønli, T. M. (2014, June). **Mobile money system design for illiterate users in rural Ethiopia**. In International Conference of Design, User Experience, and Usability (pp. 482-491). Springer, Cham.

Al-Muwil, A., Weerakkody, V., El-haddadeh, R. et al. **Balancing Digital-By-Default with Inclusion: A Study of the Factors Influencing E-Inclusion in the UK.** Inf Syst Front 21, 635–659 (2019). https://doi-org.helicon.vuw.ac.nz/10.1007/s10796-019-09914-0

Kaushik Ghosh, Tapan S. Parikh, and Apala Lahiri Chavan. 2003. **Design considerations for a financial management system for rural, semi-literate users**. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems* (*CHI EA '03*). Association for Computing Machinery, New York, NY, USA, 824–825. DOI:https://doi-org.helicon.vuw.ac.nz/10.1145/765891.766014

Tandon, U., Siri, L., Mehra, A., & O'Neill, J. (2019). **Designing a financial management smartphone app for users with mixed literacies**. Proceedings of the Tenth International Conference on Information and Communication Technologies and Development, 1–5. https://doi.org/10.1145/3287098.3287131

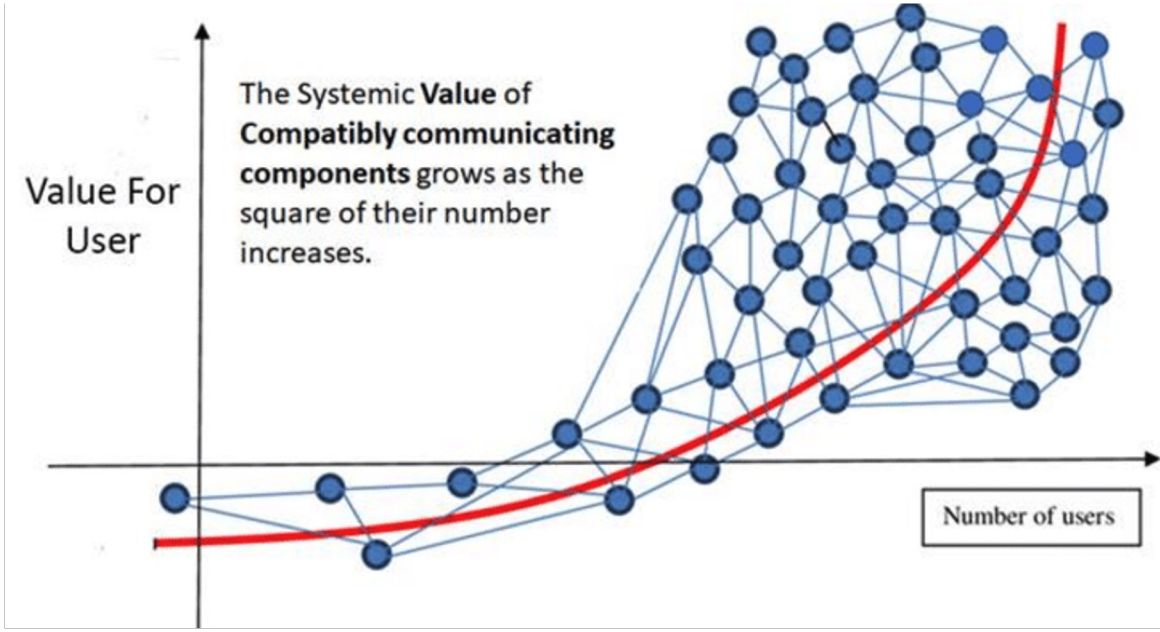
Bátiz-Lazo B., Haigh T., Stearns D.L. (2016) **Origins of the Modern Concept of a Cashless Society**, 1950s–1970s. In: Batiz-Lazo B., Efthymiou L. (eds) The Book of Payments. Palgrave Macmillan, London. https://doi.org/10.1057/978-1-137-60231-2_10

Digital Transactions

Network effects and Metcalfe's Law

Money requires a network effect: "everyone's using it because everyone's using it."

Metcalfe's Law: The value of a network increases with the square of the number of participants (n^2).



Using digital money

Money is worthless to the complete loner. There must be other entities to *transact* with.

Transaction

- transfer of value, exchange of goods, services, or funds.

To be useful in transactions, digital money must be securely stored, circulated, and accounted for.

Can you write a basic algorithm for a transaction?

Mechanics of a transaction

Goal: economic exchange between transactors (payer & payee)

Mechanics of a transaction

Goal: economic exchange between transactors (payer & payee)

Procedure:

1. Payer transfers required amount to payee

Mechanics of a transaction

Goal: economic exchange between transactors (payer & payee)

Pre condition:

1. Payer & payee are known
2. Payer & payee agree on the required amount
3. Payer holds the required amount

Procedure:

1. Payer transfers required amount to payee

Mechanics of a transaction

Goal: economic exchange between transactors (payer & payee)

Pre condition:

1. Payer & payee are known
2. Payer & payee agree on the required amount
3. Payer holds the required amount

Procedure:

1. Payer transfers required amount to payee

Post condition:

1. Payee holds the amount transferred
2. Payer holds an amount minus the amount transferred

Mechanics of a transaction

Goal: economic exchange between transactors (payer & payee)

Pre condition:

1. Payer & payee are known
2. Payer & payee agree on the required amount
3. Payer holds the required amount

Procedure:

1. Payer transfers required amount to payee

Post condition:

1. Payee holds the amount transferred
2. Payer holds an amount minus the amount transferred

Modified by:

- Money material
- Where money is stored
- Location of payee & payer
- Instruments involved in identification, transfer, verification of amounts
- Safety & security
- Motivations for transaction
- Tracking
- Other rules

Transaction-related challenges

1. **Identity verification**
2. Double-spending
3. Record-keeping
4. **Secure transfer & storage**
5. Real-time, offline digital exchanges

1.Identity verification

Are payer and payee who they say they are?

Financial institutions are beholden to KYC compliance

Biometrics - For example PayByFace, Selfie Pay (now Smile to Pay?), JP Morgan pilot.

BUT...Mastercard partnership to capture biometrics of 30 million individuals in Africa

AND...Ali Pay Didn't Ask First-Time Users for Consent

Self-sovereign identity (SSI) - https://selfkey.org/ - (Mühle, A., Grüner, A., Gayvoronskaya, T. & Meinel, C. (2018) A survey on essential components of a self-sovereign identity, *Computer Science Review*, 30, pp 80-86).

Other ideas on identity verification

- **Keystroke characteristics** (Umphress, D. & Williams, G. (1985) Identity verification through keyboard characteristics, *International Journal of Man-Machine Studies* 23(3), pp 263-273)
- **Mouse dynamics** (Feher, C., Elovici, Y., Moskovitch, R,. Rokach, L., Schclar, A. (2012) User identity verification via mouse dynamics, *Information Sciences*, 201, pp 19-36)
- **Shape and geometry of hands** (Sharma, S., Dubey, S. R., Singh, S. K., Saxena, R. & Singh, R. K. (2015) Identity verification using shape and geometry of human hands, *Expert Systems with Applications*, 42(2), pp 821-832)
- **Hand vibrations** (New Scientist)
- **ECG waveforms** (Shen, T. W., Tompkins, W. J. & Hu, Y. H. (2002) One-lead ECG for identity verification. In: *Proceedings of the Second Joint 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society* pp. 62-63)

Striving for anonymous digital money (akin to cash)

https://www.chaum.com/ecash/

Blind signatures for untraceable payments (1982)

David Chaum's Elixxir platform - Video

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system – Paper

Privacy coins – Monero, Dash, Zcash

4. Secure transfer and storage

Where there is money there must be security (Castle, et al., 2016) - in storage and in transit

Mobile Banking - Reaves, B., Bowers, J., Scaife, N., Bates, A., Bhartiya, A., Traynor, P. & Butler, K.R.B. (2017) Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications. ACM Trans. Priv. Secur. 20, 3, Article 11 (August 2017), 31 pages.

Mobile Money - Castle, S., Pervaiz, F., Weld, G., Roesner, F. & Anderson, R. (2016) Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In Proceedings of the 7th Annual Symposium on Computing for Development (ACM DEV '16). Association for Computing Machinery, New York, NY, USA, Article 4, 1–10.

NFC Payments - N. E. Madhoun, F. Guenane and G. Pujolle (2016) "An online security protocol for NFC payment: Formally analyzed by the scyther tool," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ) pp. 1-7.

4. Secure transfer and storage

Where there is money there must be security (Castle, et al., 2016) - in storage and in transit

Ethereum - Atzei, N., Bartoletti, M. & Cimoli, T. "A survey of attacks on ethereum smart contracts (sok)." In International Conference on Principles of Security and Trust, pp. 164-186. Springer, Berlin, Heidelberg, 2017.

Bitcoin - Conti, M., Kumar, E.S., Lal, C. & Ruj, S. (2018) "A Survey on Security and Privacy Issues of Bitcoin," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter.

Y. S. Tsiounis. Efficient Electronic Cash: New Notions and Techniques. PhD thesis, 1997

American banking app Dave says a data breach at third party provider Waydev has exposed the personal information of its 7.5 million users.

https://www.finextra.com/newsarticle/36286/banking-app-dave-hit-by-data-breach

Heartland Payment Systems, provider of credit and debit processing, payment and check management services, disclosed it has been the victim of a data breach

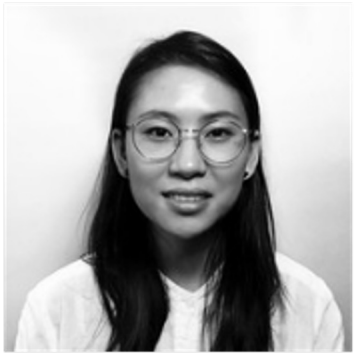
https://www.csoonline.com/article/2123599/heartland---largest-data-breach-ever-.html

A software engineer in Seattle hacked into a server holding customer information for Capital One and obtained the personal data of over 100 million people, federal prosecutors said on Monday, in one of the largest thefts of data from a bank.

https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

venmo Payments are public by default

Millions of Venmo transactions scraped in warning over privacy settings



https://www.linkedin.com/in/hangdothiduc/en

https://twitter.com/bltjetpack

venmo Payments are public by default

Researcher discovers Venmo exposes 'an alarming amount' of personal data in public API

https://www.linkedin.com/in/hangdothiduc/en

https://twitter.com/bltjetpack