Digital Money

Martin Summer

Oesterreichische Nationalbank

“Do we need central bank digital currency? Economics, Technology and Psychology”, SUERF Milano 07.06. 2018
Overview of the Talk

Introduction

What is money?

What are cryptocurrencies?

Cryptocurrencies: The future of money?

Conclusions
Introduction

- This talk is based on a joint paper (in progress) with Paul Pichler and Alexander Schierlinger-Brandmayr from the University of Vienna.

- The aim is to discuss the issue of cryptocurrencies in the broader context of contemporary monetary arrangements and payment technology to provide some background for the key question of this conference “Do we need central bank digital currency?”
Two faces of money

- Paper money and coins
- Deposit money

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Debit</th>
<th>Credit</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan. 1, 20X3</td>
<td>Balance forward</td>
<td>$25,000</td>
<td></td>
<td>25,000</td>
</tr>
<tr>
<td>Jan. 1, 20X3</td>
<td>Journal page 1</td>
<td></td>
<td>$2,000</td>
<td>23,000</td>
</tr>
<tr>
<td>Jan. 4, 20X3</td>
<td>Journal page 1</td>
<td>4,000</td>
<td></td>
<td>27,000</td>
</tr>
<tr>
<td>Jan. 8, 20X3</td>
<td>Journal page 1</td>
<td></td>
<td>500</td>
<td>26,500</td>
</tr>
<tr>
<td>Jan. 18, 20X3</td>
<td>Journal page 2</td>
<td>4,800</td>
<td></td>
<td>31,300</td>
</tr>
<tr>
<td>Jan. 25, 20X3</td>
<td>Journal page 2</td>
<td></td>
<td>5,000</td>
<td>26,300</td>
</tr>
</tbody>
</table>
Important aspects

- Both forms of money are based on **trust**. Trust in the central bank and the state underwriting the currency, trust in the banking system to be able to fulfill its promises.

- It is a **hybrid, hierarchical** system in which bank notes and coins are at the top. They are the contents of all debts in particular of the promises embedded in deposit money.
Important aspects

- The system has a **high degree of centralisation and coordination** and an **implicit incentive structure**: Banks have for example an incentive to maintain the integrity of accounts to prevent runs.

- Bank notes and coins have a physical representation, deposit money has not. Deposit money is **digital money** (but not cryptocurrency).
Recurring Themes

- Trust
- Security against forgery and attacks
- The role of a central authority
What are cryptocurrencies?

- Privately issued **virtual value units** which are convertible to actual currencies at a flexible exchange rate.
- While the value units are often referred to as “coins” in analogy to bank notes and coins they are conceptually more closely related to deposit money.
- Cryptocurrencies are **digitally held** in so called **wallets**.
What are cryptocurrencies?

- Agents exchanging cryptocurrencies are represented as addresses in a computer network, which do not reveal the real identity of the person behind it.

- Transactions are authorized and verified using modern cryptographic techniques and the integrity of transactions is collectively verified in a decentralized network of independent agents called “miners”.

- Miners verify transactions, batch them into blocks and append them to a register of all blocks of verified transactions that have ever happened in the network, the blockchain.
Why has this concept created widespread fascination?

- While the cryptography is sophisticated and sounds magical to non-experts, it is – technologically speaking – entirely standard.
- The innovation is in the way transactions are publicly recorded, to maintain a public ledger of all transactions, called the blockchain.
Why has this concept created widespread fascination?

- This creates a system of value exchange that functions with the deliberate exclusion of any central authority.
- This has created excitement because it is a concept of a decentralized, anonymous, self verifying and reliable register that works.
- Will this technology change the face of money yet once again?
The current payment system in the EU

- 122 billion **transactions** (2016 3856 T/sec)
  - 60 billion card payments: 2.9 billion Euro.
  - 54 billion retail payments, mainly bank transfers: 41.8 billion Euro
- Based on deposit money
- Financial intermediaries as **trusted third parties**.
  - Banks
  - Credit card companies
  - Central banks
SEPA instant payments (from 2018)

- Real time payments (max. 10 sec)
  - Real time clearing
  - Settlement in central bank money
- Multichannel
  - Person to Person
  - Point of sale
  - Online
- 24/7/365
Payments in deposit money with intermediation

- Fast (99% in real time)
- Secure
  - Transactions are final
  - Intermediaries are liable if abuse or attacks occur
- Privacy
  - Protected by bank secrecy law
  - Transaction history and accounts cannot be publicly accessed.
- The infrastructure is technologically up to date and highly efficient.
**Impressments in payment system by cryptocurrencies?**

- Payments in cryptocurrencies are **slower**, because the public blockchain needs a consensus protocol which is slow.
- Have a **low transaction capacity**. Otherwise the storage requirements for the blockchain would grow too rapidly.
- The proof concepts needed for the consensus protocol are **ressource intensive and wasteful** and impose **high externalalities** on society.
- From a payments perspective cryptocurrencies are **highly inefficient** compared to the infrastructure in place.
Opportunities and limits of blockchain technology

“... There are many reasons to be cautious about bitcoin. My scepticism does not concern blockchain, the technology behind bitcoin. This distributed ledger technology is a welcome innovation with useful applications, including fast, automatic execution of smart contracts.”

Jean Tirole, Financial Times 30.11.2017
The key innovation of the bitcoin blockchain

• What is really new in the bitcoin blockchain is its **public** and **entirely decentralized** character.
  • It is open source
  • Everybody can participate in the consensus protocol and gets compensated for this work.
  • No trusted third parties or central authorities, high degree of anonymity

• These seem **decisive success factors** for
  • The establishment of a crypto-IT community
  • R&D on blockchain based apps by startups
  • Attractiveness for illegal transactions
The public consensus protocol: The example of Bitcoin

A clever system of technology and economic incentives ensures that all participants despite of their individually different goals reach a consensus on the state of the transaction register.

- Successful miners are compensated by new bitcoins (plus transaction fees)
- It is easy for every miner to check the integrity of transactions in his block and in all other past blocks by cryptographic methods.
- If successive miners consider a block as invalid its creator looses his compensation ex-post automatically and the transactions in his block are deleted.
- This provides strong incentives for behaving honestly.
The public consensus protocol needs a cryptocurrency

- Only if miners are compensated in the cryptocurrency they can be *sanctioned* in a *swift and simple* way for dishonest behavior. Mining rewards *disappear automatically* if misbehavior is detected by others.
- Even with *high concentration of power* among miners the incentives are still there.
- If miners would steal coins in a coordinated effort to manipulate the public consensus protocol *trust in the protocol* – and hence in the cryptocurrency – would *collapse* and the stolen coins would automatically lose their value.
Limits of public blockchains

- Miners can not be compensated in currency because it cannot be seized ex-post and thus the economic incentives do not work.
- As soon as property rights in assets with high intrinsic value are documented in a legally binding form in the blockchain there are massive manipulation incentives, for instance so called 51% attacks.
- Even if the cryptocurrency looses its value the attacker has secured his property rights in a highly valuable real asset.
The exclusion of trusted third parties is expensive

Eric Budish in a recent paper analyzes the **economic limits of a public blockchain**:

- Bitcoin mining can be best understood as a **rent-seeking competition** in which the equilibrium amount of computational power devoted to maintaining the network is pinned down by a zero profit condition.

- Incentives for honest behavior by miners require that the **equilibrium per block-payments** to miners for running the blockchain must be large relative to a **one-off benefit** of attacking it.

- For most businesses as well as for the public sector **distributed databases with trusted third parties** seem to be a much **cheaper and more efficient** option than the high costs required to provide trust in the protocol of a public block chain.
Public blockchains...

- Do not make much sense if separated from cryptocurrencies
- Are not particularly useful beyond cryptocurrencies and trade in digital items
- It is unlikely that the public blockchain will be useful for transaction volumes beyond relatively modest value.
Cryptocurrencies and central banks

• In the public discussion about central bank issued digital currencies it is **often unclear what is exactly proposed**.
• Proposals range from real-time securities settlement up to blockchain based electronic cash for citizens.
• Still others hope for a technological change in money that facilitates the implementation of negative interest rates if macroeconomic stabilisation requires to do so.
Central bank deposit money for citizens

- If digital money means that citizens should have access to central bank money via accounts at the central bank this would of course be a major structural change in monetary arrangements.
- From a *technological perspective* this has nothing to do with cryptocurrencies and could be implemented entirely with the payment systems technology in place.
- The concepts and ideas implemented in cryptocurrencies - in particular the public blockchain and its consensus protocol - are *irrelevant* for this discussion.
Central bank issued digital cash

- Should a central bank decide to issue **digital forms of cash** this would be a different matter.
- It is, however **hard to see a compelling reason** why central banks should do so.
- Nobody has yet made a **convincing case** that the still widespread use of cash can be interpreted as a **market failure** that needs to be addressed by public policy intervention.
- Note also that central bank issued digital cash would run completely counter to the spirit of cryptocurrencies: The **elimination of a trusted third party from monetary arrangements** is its key idea and the reason why the particular consensus protocol of the public blockchain is needed.
Conclusions

• From a perspective of the payment system cryptocurrencies are **not needed** and are not particularly **well suited**. The incumbent systems are at the moment vastly superior and it is very unlikely that this will change in the foreseeable future.

• For the economic role of cryptocurrencies useful applications of public blockchains are the **decisive factor for success**.

• There are lots of ideas but **no convincing cases are there yet**. There seem to be **considerable intrinsic limits** to such developments. The deliberate exclusion of trusted third parties – while possible– is highly **expensive and wasteful**.
**Do we need central bank digital currency?**

**Most probably not** for the reasons given in this talk and for other deeper reasons which I did not mention in my presentation but which we might touch in the discussion.