nChain
Data without question

DR CRAIG WRIGHT – CHIEF SCIENTIST – NCHAIN GROUP

Bitcoin, IPv6, and the Future of the Internet

Global Forum, Oman – 18.10.22

nChain

- Introduction – Identities and Digital Signatures in Bitcoin
- Bitcoin as Electronic Cash: Directly From One Party to Another…
- Security in a World of Bitcoin and IPv6
- Use Cases – Controlling the Performance of a Contract

Introduction
Identities and Digital Signatures in Bitcoin

Introduction

Identities and Digital Signatures in Bitcoin

1. In the privacy model introduced with Bitcoin, identities remain a part of its solution
2. For high-value transactions, identity can be provided through certificate authorities and public key infrastructure
3. Bitcoin requires anti-money laundering (AML) provisions—AML enforcement means that large-value transactions require reporting and intermediaries
4. Digital signatures require a digital signature algorithm such as ECDSA and an ability to exchange identity
5. While every transaction retains full traceability, the cost of monitoring all users globally is prohibitive—retaining privacy for honest users

Bitcoin as Electronic Cash:
Directly From One Party to Another...

Peer-to-peer

No security issues,
like man in the middle

Diffie-Hellman protocol

Alice and Bob communicate
securely and privately.

Alice

Bob

Peer-to-peer exchange

Alice sends Bob a cheque.

Alice

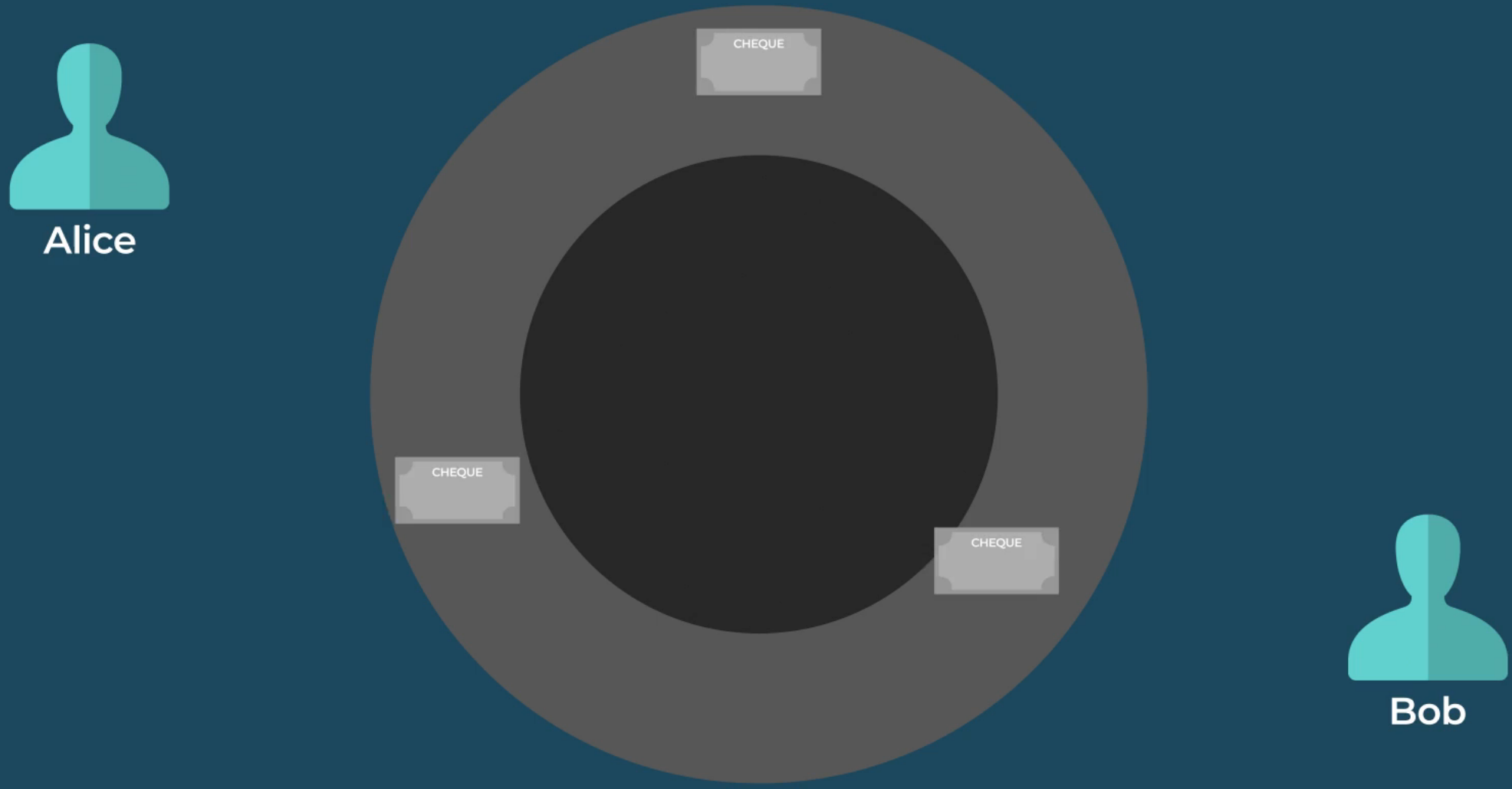
Bob

Peer-to-peer exchange

Negotiations going back and forth between two parties.

Peer-to-peer
happening everywhere

BTC is not P2P



Security in a World of Bitcoin and IPv6

Security in a world of IPv6 and Bitcoin

The growth of network systems will drive applications and uses beyond light bulbs with web and IP addressing…

- Disposable communication tablets (including $1 devices)
- Milk, coke cans, and other products in supermarkets with IP addresses and RFID tags for merchandising and stock control

Exchange of all things: Anytime, anywhere

IPv6 brings security to a mobile network.

In the domain world, Windows and other existing operating systems allow the integration and simple deployment of secure server and client-trust models.

Security in a world of IPv6 and Bitcoin

IoT and the Mobile Experience

In case the user loses a tablet or other device, they are not actually connected to the system and files, preventing the loss of data.

With the right set-up, the location of the user no longer matters, providing a truly mobile experience in accordance with IPv6.

Using flags in IPv6 and Bitcoin, we can directly and efficiently integrate payment services.

A well-defined cloud and IPv6 system can be far more secure than the traditional shell-firewall model.

With IPv6 jumbo blocks and Bitcoin payment channels, we have a path to an on-demand Internet of value.

Use Cases
Controlling the Performance of a Contract

Licensing computer software, music, and digital artwork

Distributed hash table (DHT)
Stores Alice's public key and a hash of Alice's hardware string

Bob (software vendor)
Populates the DHT with software licence, a hash of the encrypted executable and the URL for the software download

Alice (end user)
Can sign transaction on the blockchain
Can query whether the licence is valid
Can revoke licence

Oracle (trusted third party)
Signs transactions when a user-provided expression evaluates to true
Employs a DHT
Can revoke licence

Use Cases

- Security: Access control
- Monetisation: Automated payments

Blockchain technology can be used to facilitate an inexpensive, secure, and transparent procedure for the purchase, integrity, and licensing of proprietary software.

Consumers benefit from continuous integrity and transparency.

Software vendors can ensure that the conditions associated with their **license** are adhered to on a continuous and cost-effective basis.

The software vendors could enhance their reputation and increase their trustworthiness by being seen to be transparent.

The immutable record of transactions between the software vendors and consumers could be valuable for both audits and cases of dispute resolution.

THANK YOU

Q&A

nChain

Data without question

Contact us

Switzerland
Grafenauweg 6,
6300 Zug,
Switzerland

United Kingdom
30 Market Place,
London W1W 8AP
United Kingdom

contact@nchain.com