Internet-Scale Payment Systems Ecosystem & Challenges

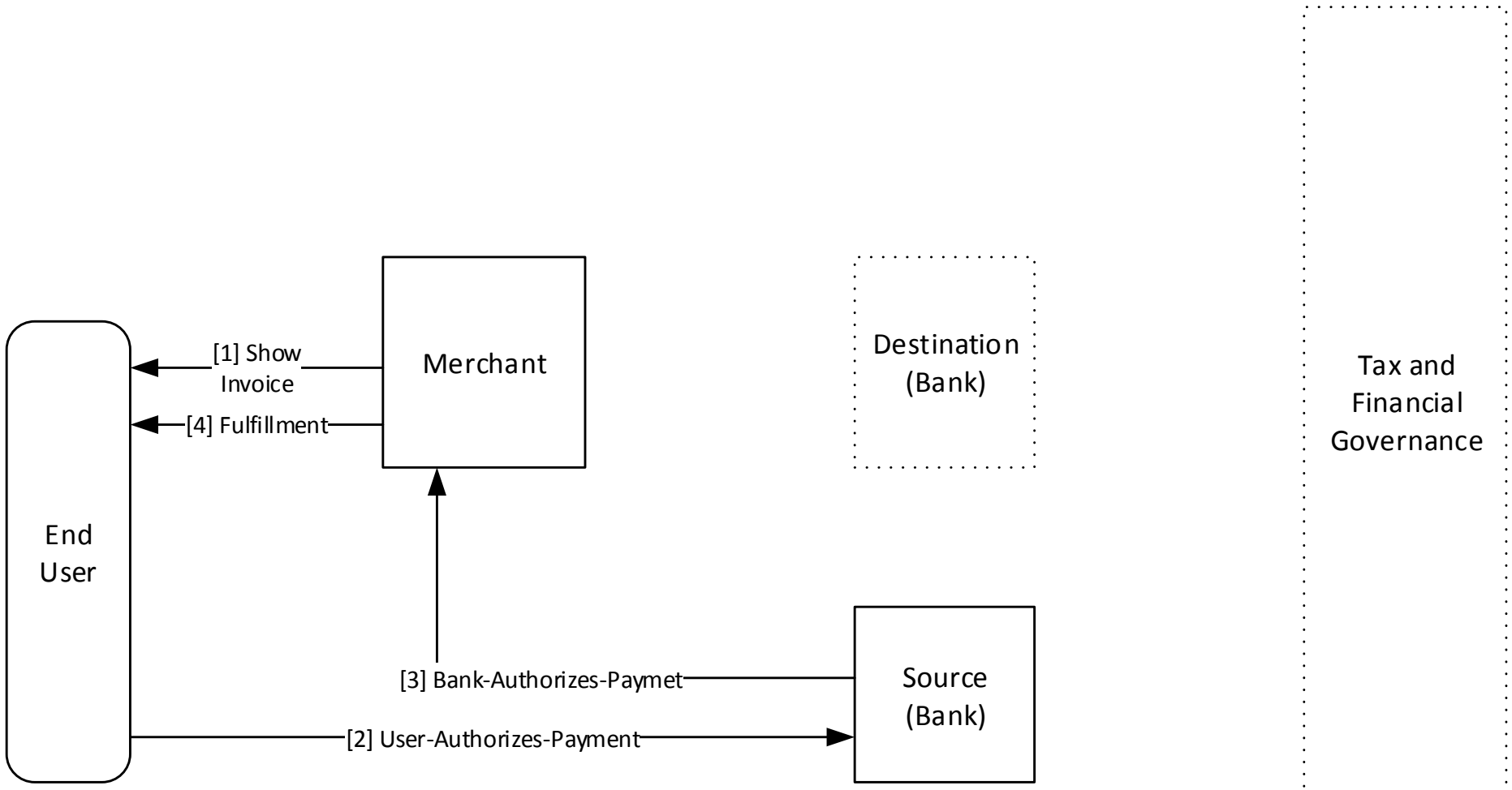
Malcolm Pearson

malcolmp@microsoft.com

Agenda

- Abstract Payment Flow
- Key Payment Challenges
- Payment Scenarios
- Payment Instrument Flows
  - Mobile
  - Kiosk
  - vCurrency
  - eWallet
  - Cards
  - Bank Transfer
- Needs for Standardization

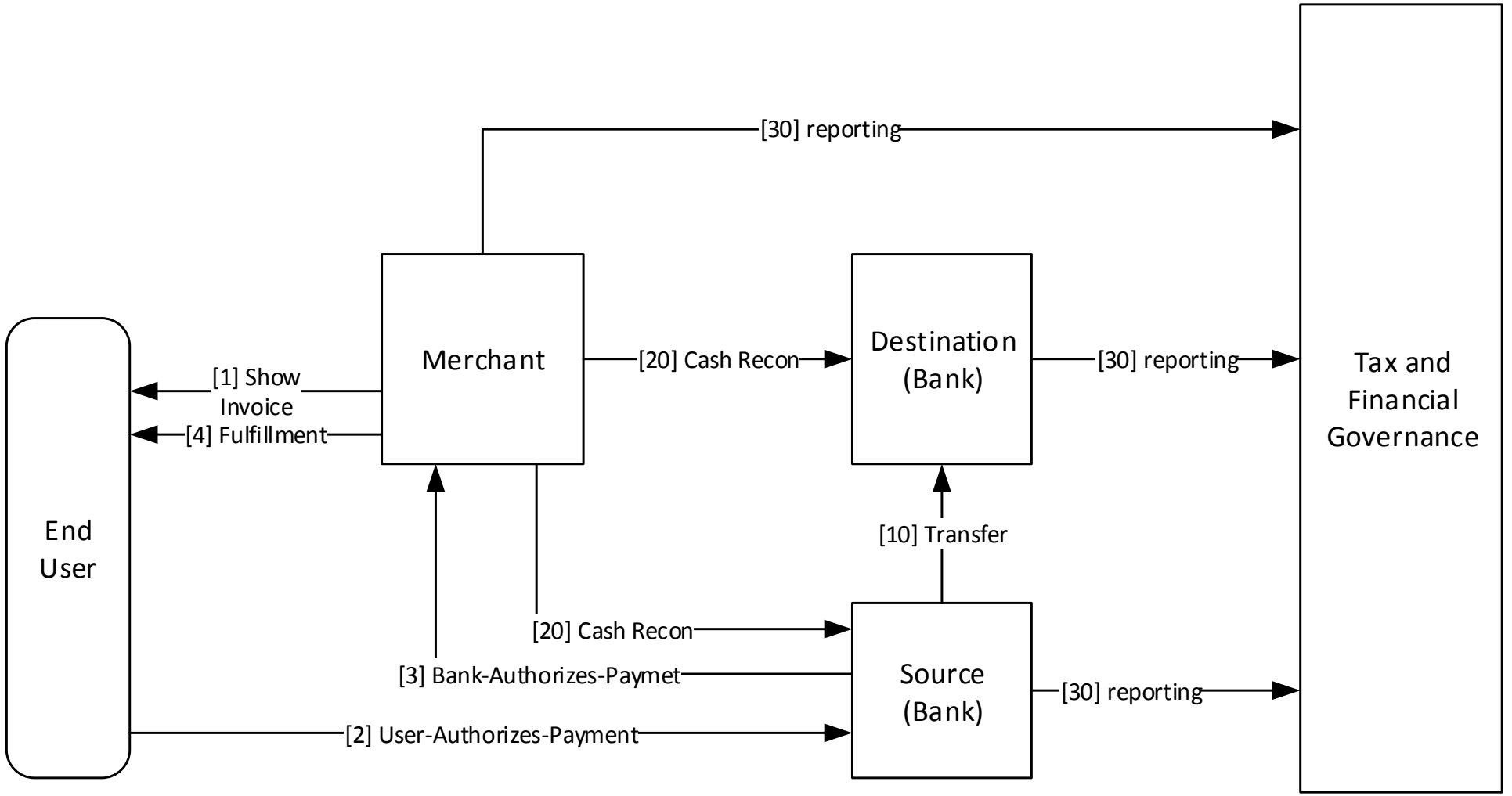
Abstract Payment Flow- Online



Notes

- Network of many sources, merchants and payment instruments.
- Conceptually, source responsible for following user intent
- Destinations & merchants may cascade

Abstract Payment Flow- Full



Back-end issues

- Cash reconciliation
- Tax reporting
- Financials

Key Payment Challenges

Area	Notes
Network	• Many Countries and Currencies • Many Sources, Payment Instruments and Flows
Security vs. Convenience	Merchant Concerns • Merchant expresses pricing • Many pricing models • Integrated merchant experience Payment Source Concerns • User agrees to pricing • Payment sources follow user's instruction
Business	• Already a long and rich history, many entrenched players
Emerging Markets	• Anticipating Different Cultural Norms • Economic impact of cash-oriented commerce

Payment Scenarios

Scenario	**Notes**
Purchase physical Goods Online	• Relatively asynchronous payment flow permitted due to delays in physical delivery
Purchase Digital Goods	• Subscriptions to be used over a long period of time allow time and authorization • Immediate use items (consumed in a game) cannot be taken back by merchant and cannot interrupt end user flow
Subscriptions. Payment Agreement Complexity	• Agreement to pay on a schedule • Usage based subscriptions have variable pricing
Purchasing goods from physical stores. Roaming between mobile, tablet, TV and PC.	• Users expect continuity between online, mobile and physical store experiences
Consumer to consumer payments	• Gifting, sharing costs, informal payments
Returns and disputes	• Connecting payment and fulfillment
Securing payment material	• Target, Bitcoin
Backend	• Cash reconciliation • Tax and Financial Reporting

Payment Mechanism Flows

Cash Kiosks & Retail centers

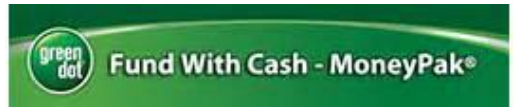
Bank Transfer

Mobile Billing


Others


eWallets

Cash Cards



Cards

Mobile Billing

Mobile Billing

Pay via Mobile – Auth* via SMS

Leverage pervasive mobile billing networks

Merchant Website, Online

- User selects product
- Website generates price
- User select mobile account via phone #

On User's Mobile Device

- Receive single-use SMS challenge
- Respond on phone
- Respond on Merchant Website

Merchant Website, Online

- User purchase is fulfilled

Pay via Mobile – Auth* via Mobile Network

Leverage pervasive mobile billing networks

On User's Mobile Device

- User selects product
- Merchant generates price
- User selects to pay with "this" mobile account

Mobile operator validates

- Trust user identity due to mobile network transport or SIM
- Trusts purchase description due to marketplace app on device
- Validates and reserves funds

Purchase fulfilled

- Mobile or otherwise

Pay via Mobile – QR Code, auth via Mobile

Leverage pervasive mobile billing networks, transfer payment devices

Merchant Website, Online
- User selects product
- Website generates price
- Website generates QR code

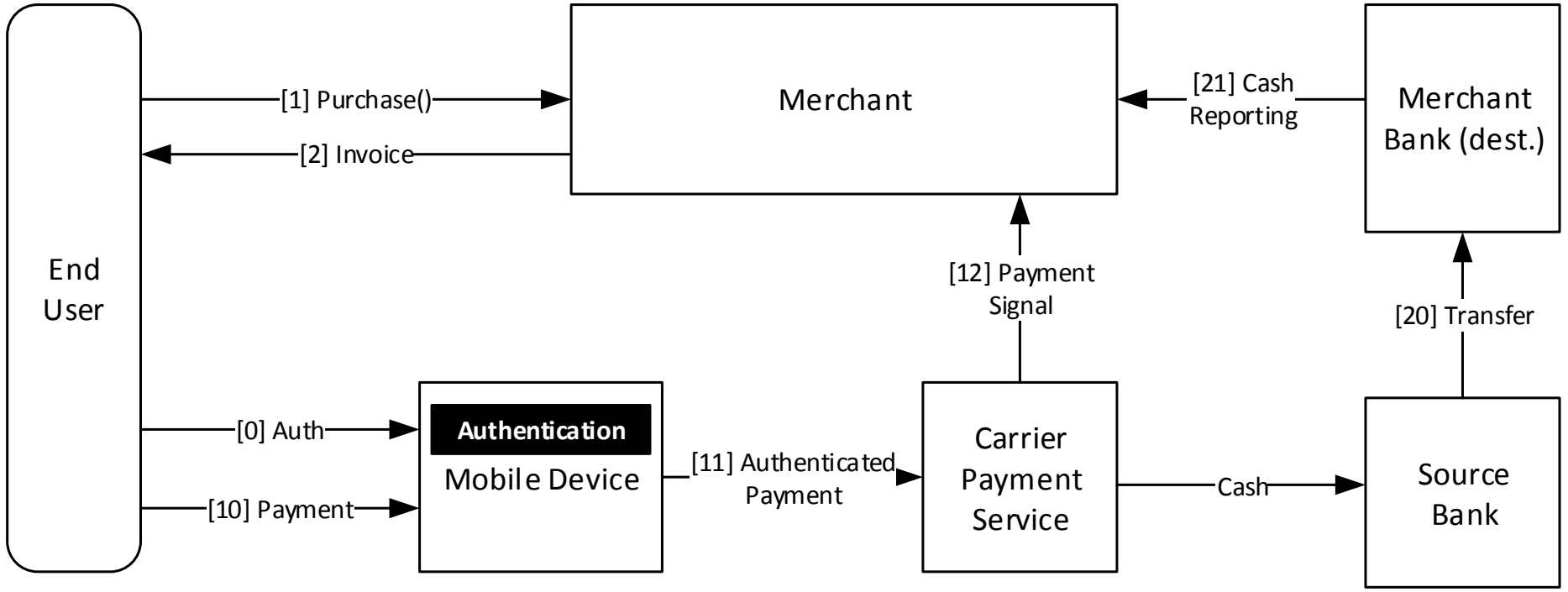
On User's Mobile Device
- Purchase details retrieved via QR code
- Purchase details forwarded to Mobile Operator

Mobile operator validates
- Trust user identity due to mobile network transport or SIM
- Trusts purchase description due to marketplace app on device
- Validates and reserves funds

Merchant Website, Online
- User purchase is fulfilled

Also applies to physical goods and inter-personal payments of gifts

Mobile Flows



Strength: Low fraud
Challenge: Regionally specific solutions, cost, flexibility
Need: Payment Federation

Phase	**Steps**
Invoicing	1…2
Payment	10…12
Reconciliation	20, 21

Mobile Device as Payment Instrument Wallet

Approach	**Notes**
Conventional Card Wallet	• Susceptible to similar fraud problems as conventional cards
Authentication Mechanism	• Device receives invoice • Device verifies user's consent • Device generates secure statement of user-payment authorization • Bank must generate source authorization to verify and reserve funds

Ideal Mobile Solution Technical Elements

Element	**Notes**
End User Authentication	• Possession of mobile device + ??? • Leverages Mobile Operator Network or SIM security
User Payment Authorization	• Performed within mobile device • TPM
Source Payment Authorization	• Mobile operator verifies funds availability • Need for common format to express Source payment Authorization
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources

Cash Kiosks and Retail Centers

Cash Kiosks & Retail centers	

Online + Retail Centers Example: Boleto

Merchant Website, Online

- User selects product
- Website generates price
- User selects and prints Boleto

Boleto de Cobrança

Microsoft

Recibo do Sacado

Cedente	Agência/Código Cedente	Vencimento
MICROSOFT DO BRASIL IMPORTACAO E COMERCIO DE SOFTWARE E VIDEO GAMES LTDA. CNPJ: 04.712.500/0001-07	001/0095945015	23/03/2014
Sacado	Número do Documento: SP00V46WPTPS	Nosso Número: 00000009648-2
Espécie: R$ / Quantidade / (x) Valor	(=) Valor do Documento: 100,00	(-) Desconto
Demonstrativo:	(+) Outros Acréscimos	(=) Valor Cobrado
AdCenter Account Id = 2639409		

Autenticação Mecânica

Corte Aqui

citibank 745-5 74593.60009 95945.015006 00000.964825 5 60110000010000

Local de Pagamento: Até o vencimento pagável em qualquer banco do sistema de compensação					Vencimento: 23/03/2014
Cedente: MICROSOFT DO BRASIL IMPORTACAO E COMERCIO DE SOFTWARE E VIDEO GAMES LTDA. CNPJ: 04.712.500/0001-07					Agência/Código Cedente: 001/0095945015
Data Documento: 21/02/2014	Número do Documento: SP00V46WPTPS	Espécie Doc.: RC	Aceite: N	Data Processamento: 21/02/2014	Nosso Número: 00000009648-2
Uso do Banco	Carteira: 600	Espécie: R$	Quantidade	(x) Valor	(=) Valor do Documento: 100,00
Instruções (texto de responsabilidade do cedente)					(-) Desconto
					(+) Mora/Multa
					(+) Outros Acréscimos
					(=) Valor Cobrado

Sacado
, One Microsoft Way, Sao Paulo, SP Sao Paulo SP 01010-125
Sacador/Avalista

Ficha de Compensação

Autenticação Mecânica

At Retail Center [Merchant 2]

- User presents Boleto and cash to cashier
- Cashier accepts cash and scans Boleto to record payment

Merchant Website, Online

- User purchase is fulfilled

Online + Retail Centers Example: ChinaUnicom

At Retail Center Kiosk
[not ChinaUnicom]

- User selects product and price
- User selects and prints Payment Slip

Cell # 12093847
Topup: 456 RMB
Time Date
QR Code

At Retail Center Counter

- User presents slip and cash to cashier
- Cashier accepts cash and scans slip to record payment

On cellphone

- Balanced topped up
- Available for other payments

Online + Retail Centers
Example: Qiwi

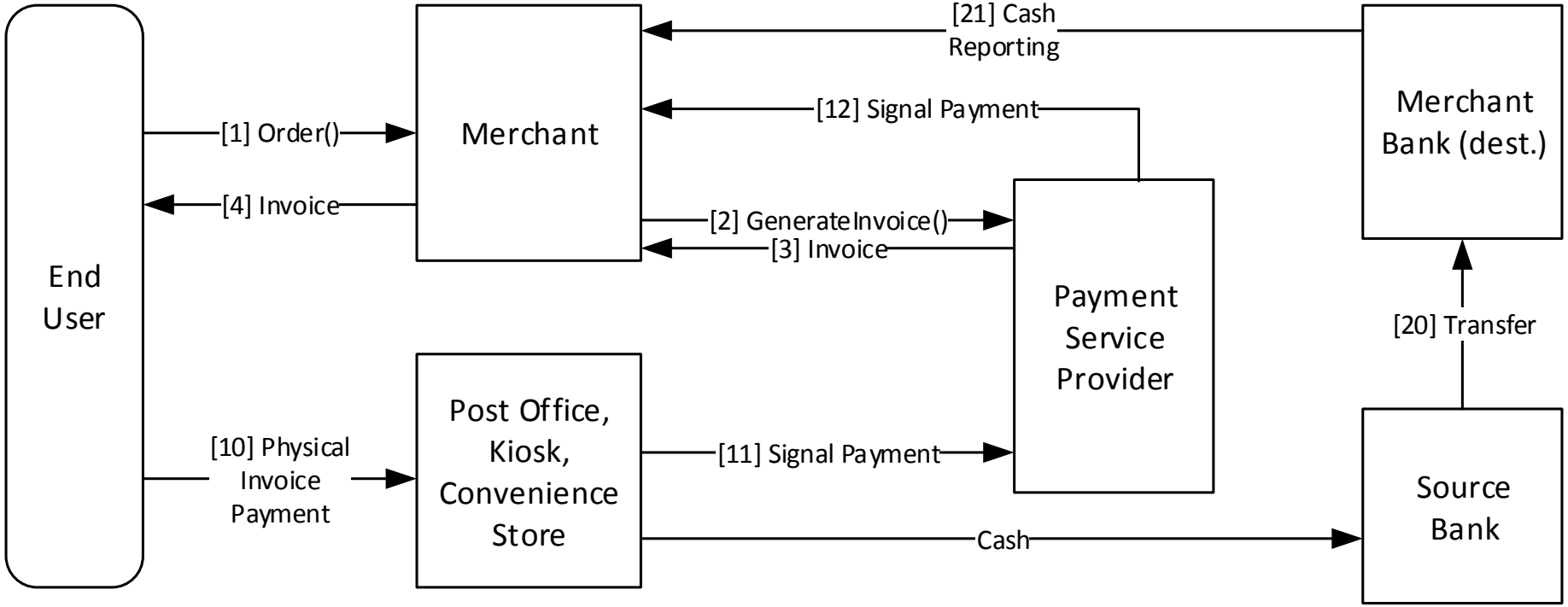
At Retail Center Kiosk

- User selects account to pay into
- User selects price
- Deposits cash

Merchant Website, Online

- User purchase is fulfilled

Invoice Cash Kiosk Flows



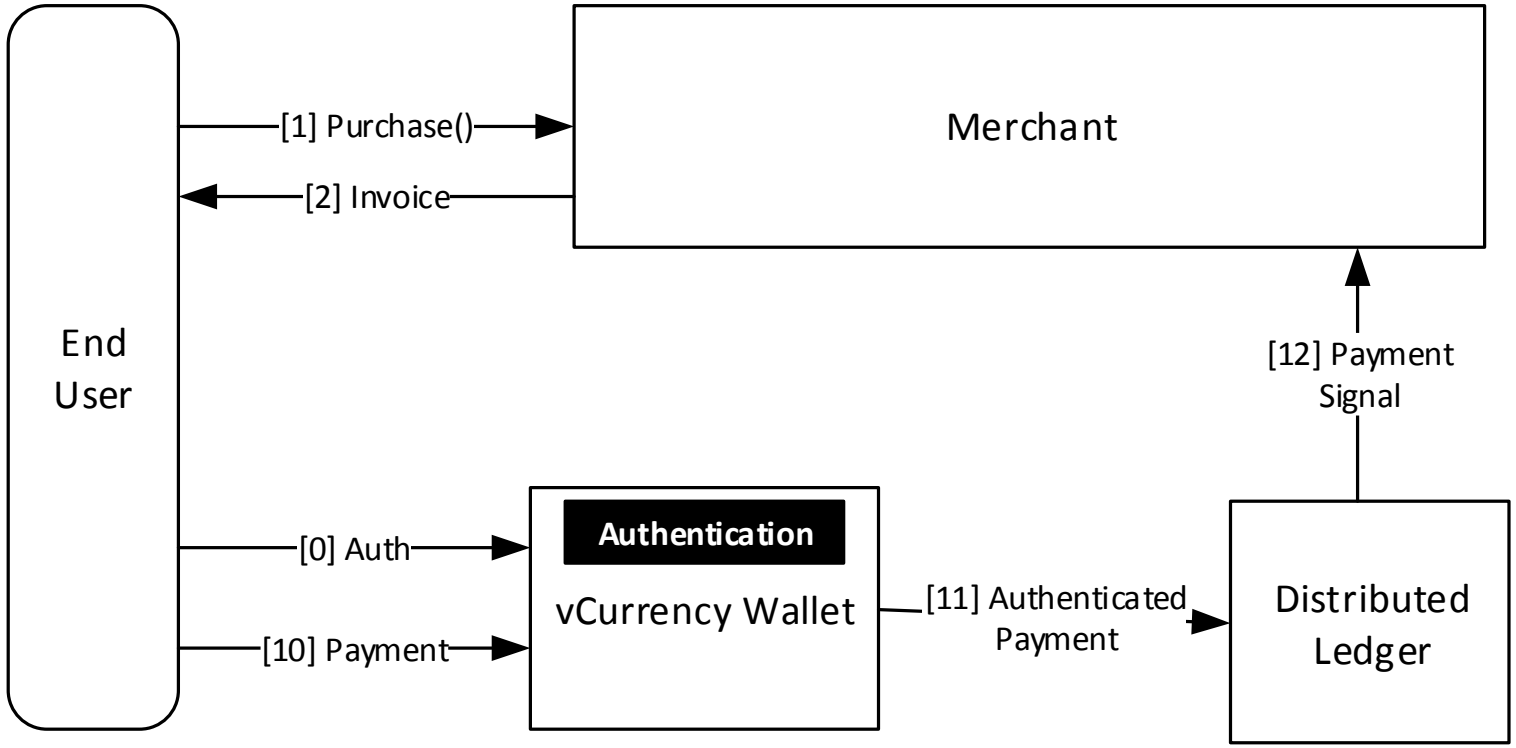
Phase	**Steps**
Invoicing	1…4
Payment	10…12
Reconciliation	20, 21

Strength: Low fraud
Challenge: Some methods are not automated, Async
Need: Common encoding, network of sources

Ideal Kiosk Solution Technical Elements

Element	**Notes**
End User Authentication	• Not an issue because cash is presented
User Payment Authorization	• Not an issue because cash is presented
Source Payment Authorization	• Kiosk or cashier verifies cash presented • Variable quality identifying payment targets. Boleto is rigorous. Qiwi is highly dependent on user correctly typing payment account ID. • Need for common format to express Source payment Authorization
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources

Virtual Currency Flows



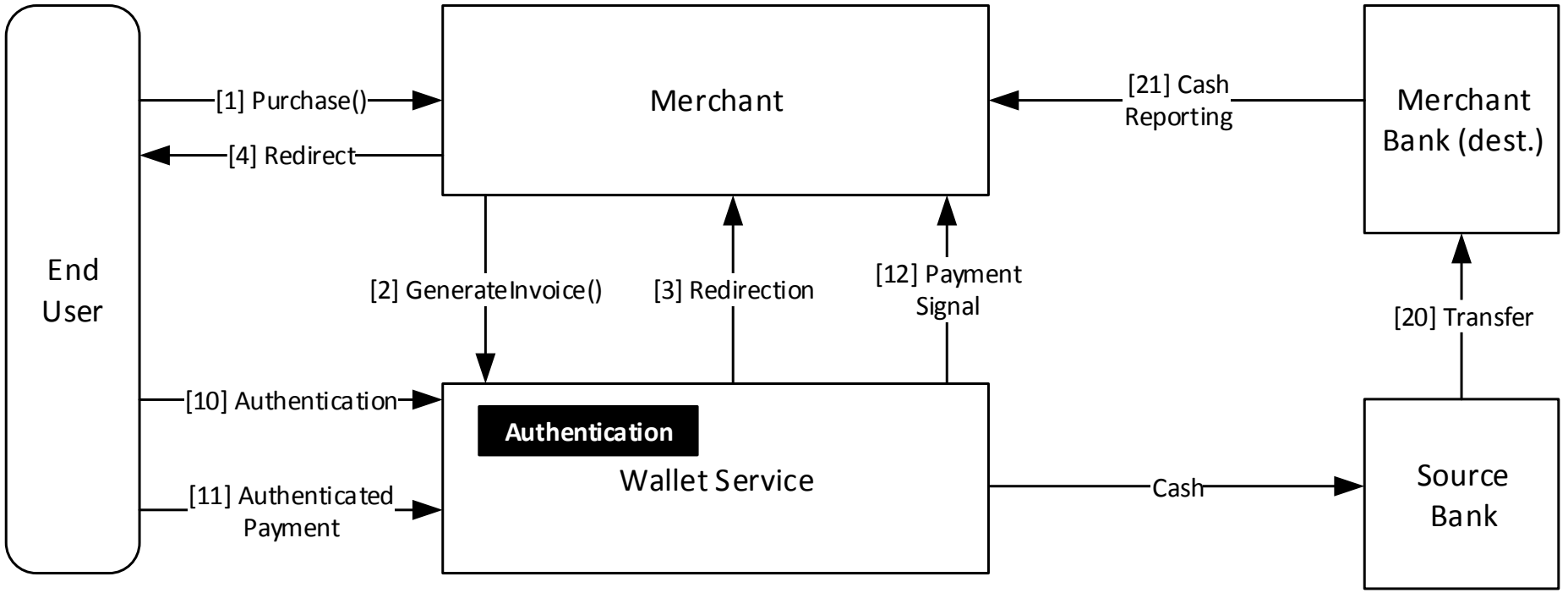
Phase	Steps
Invoicing	1…2
Payment	10…12

Strength: Low fraud
Challenge: Adoption, Governmental Support
Need: Business guarantees and Reporting

eWallets

- eWallet performs similar function to source bank
  - Holds balances
  - Authenticate user payment authorization
  - Generate source payment authorization
- Combine with other strategies to fund eWallet balance
  - Kiosk
  - Mobile
  - Conventional credit card
  - ACH

Wallet Flows



Strength: Low fraud
Challenge: Regionally specific solutions, Abrupt UX
Need: Payment and Authentication Federation

Phase	**Steps**
Invoicing	1…4
Payment	10…12
Reconciliation	20, 21

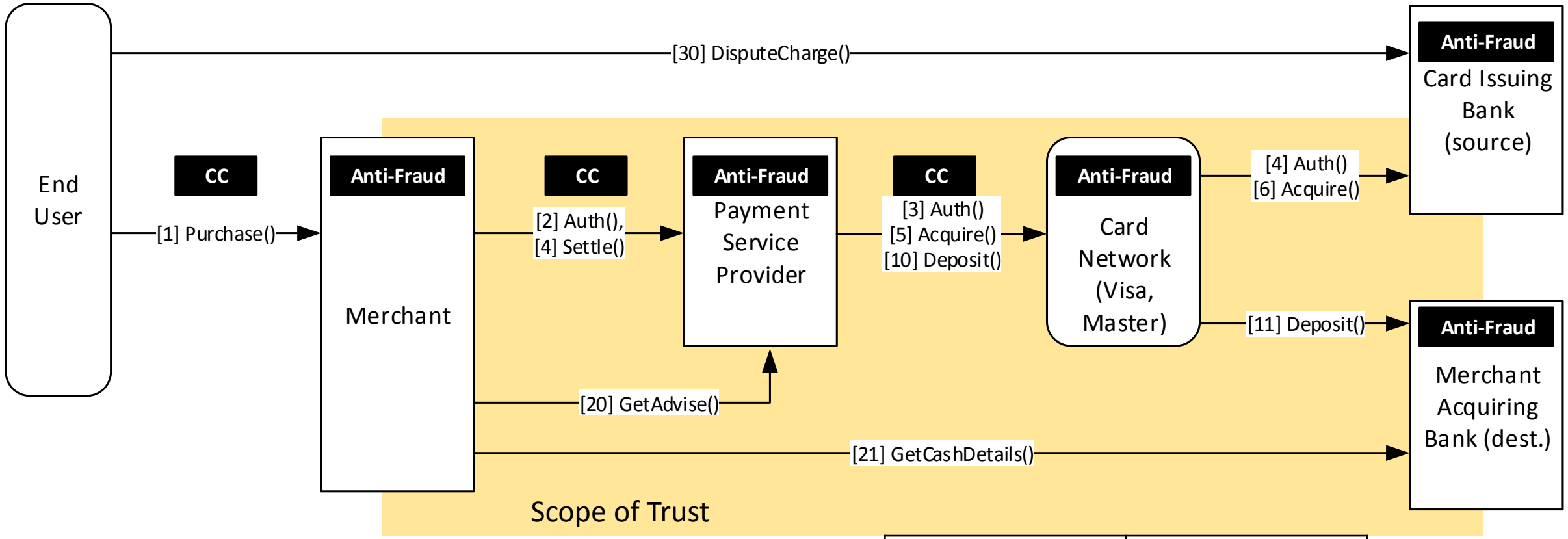
Ideal Wallet Solution Technical Elements

Element	**Notes**
End User Authentication	• Typically implemented by the wallet provider
User Payment Authorization	• Performed within wallet provider
Source Payment Authorization	• Wallet provider verifies funds availability • Need for common format to express Source payment Authorization
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources

Credit Cards

General Purpose	
Local	
Other	

Online Credit Card Flows - Actual

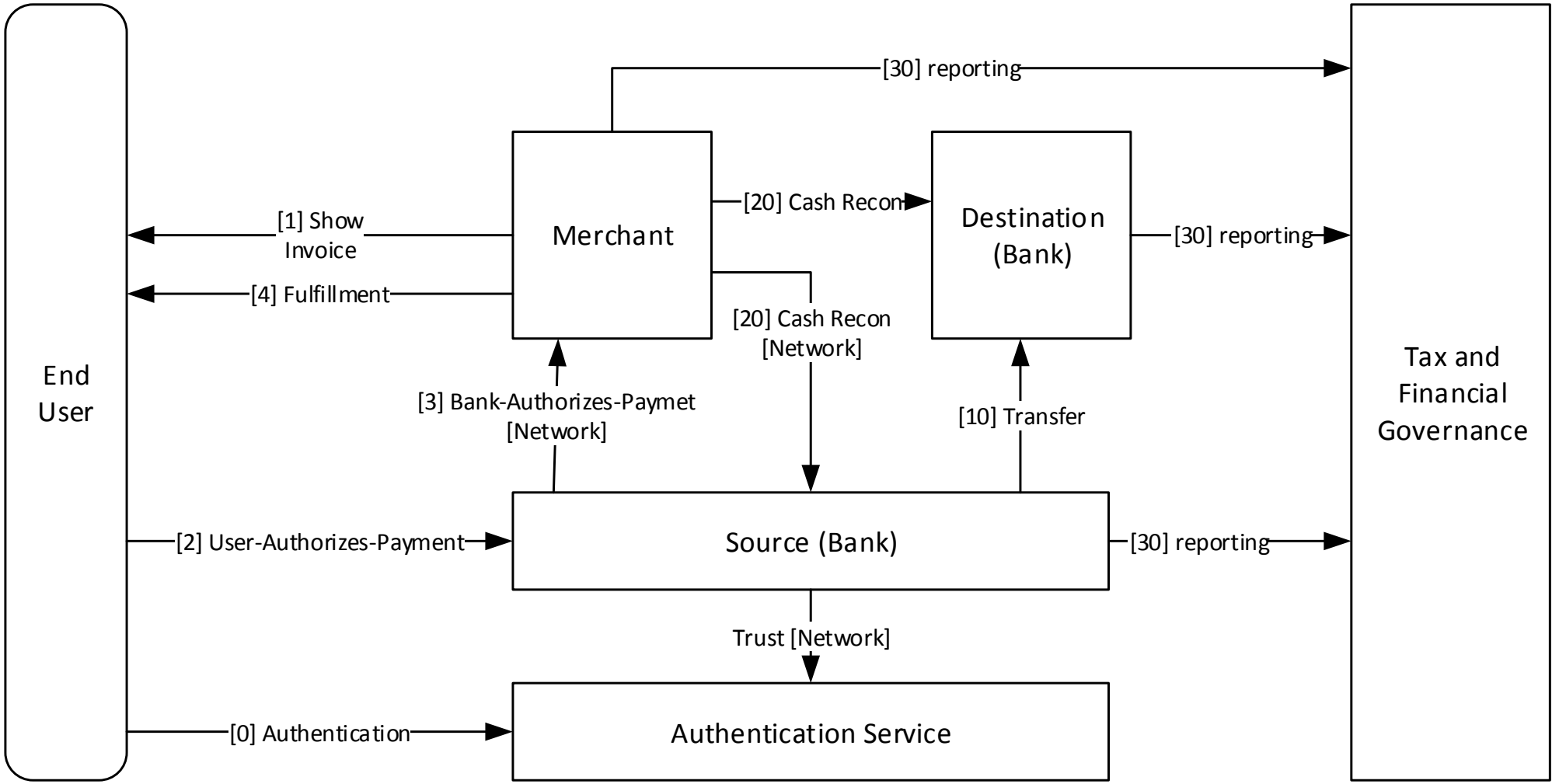


Strength: Broad North American adoption, smooth UX
Challenge: Anti-Fraud and Dispute complexity & Cost
Need: Secure payment instructions

Phase	**Steps**
Purchase	1…6
Cash to merchant	10, 11
Reconciliation	20, 21
Dispute	30+

Ideal Banked Technical Solution

principle: minimize scope of trust



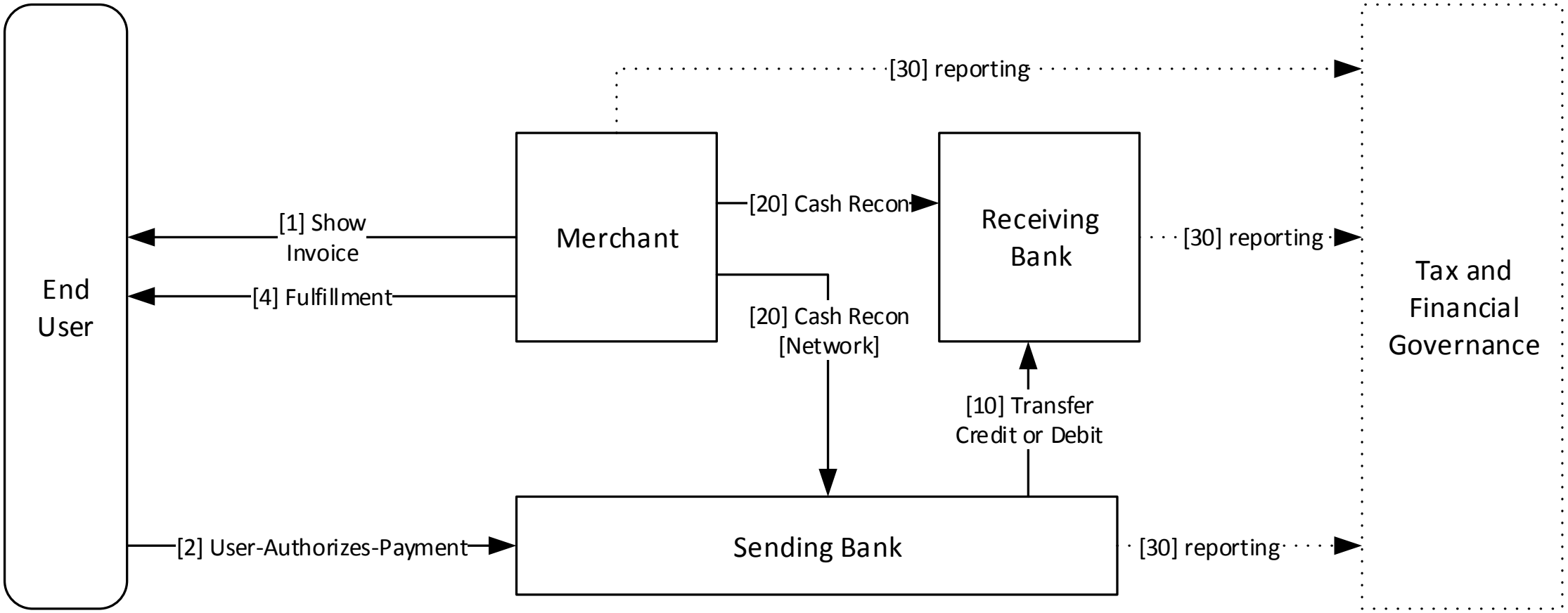
Ideal Banked Solution Technical Elements

Element	**Notes**
End User Authentication	• Secure channel between end user and authentication service prevents replay • Authentication service could be delegated outside the bank, but must be trusted • Many banks have invested significantly in their own solutions already
User Payment Authorization	• User states intent to make a payment (authorize). • Authorization specifies source, target merchant, invoice, quantity and time • Statement is tied back to secure authentication of the user • A single authorization statement could authorize multiple payments
Source [Bank] Payment Authorization	• Bank verifies validity of Payment Authorization, tied back to End User • Bank verifies and reserves availability of funds through credit or debit • Bank produces trustable statement of funds availability • Merchant may fulfill as soon as Source Payment Authorization is available
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources

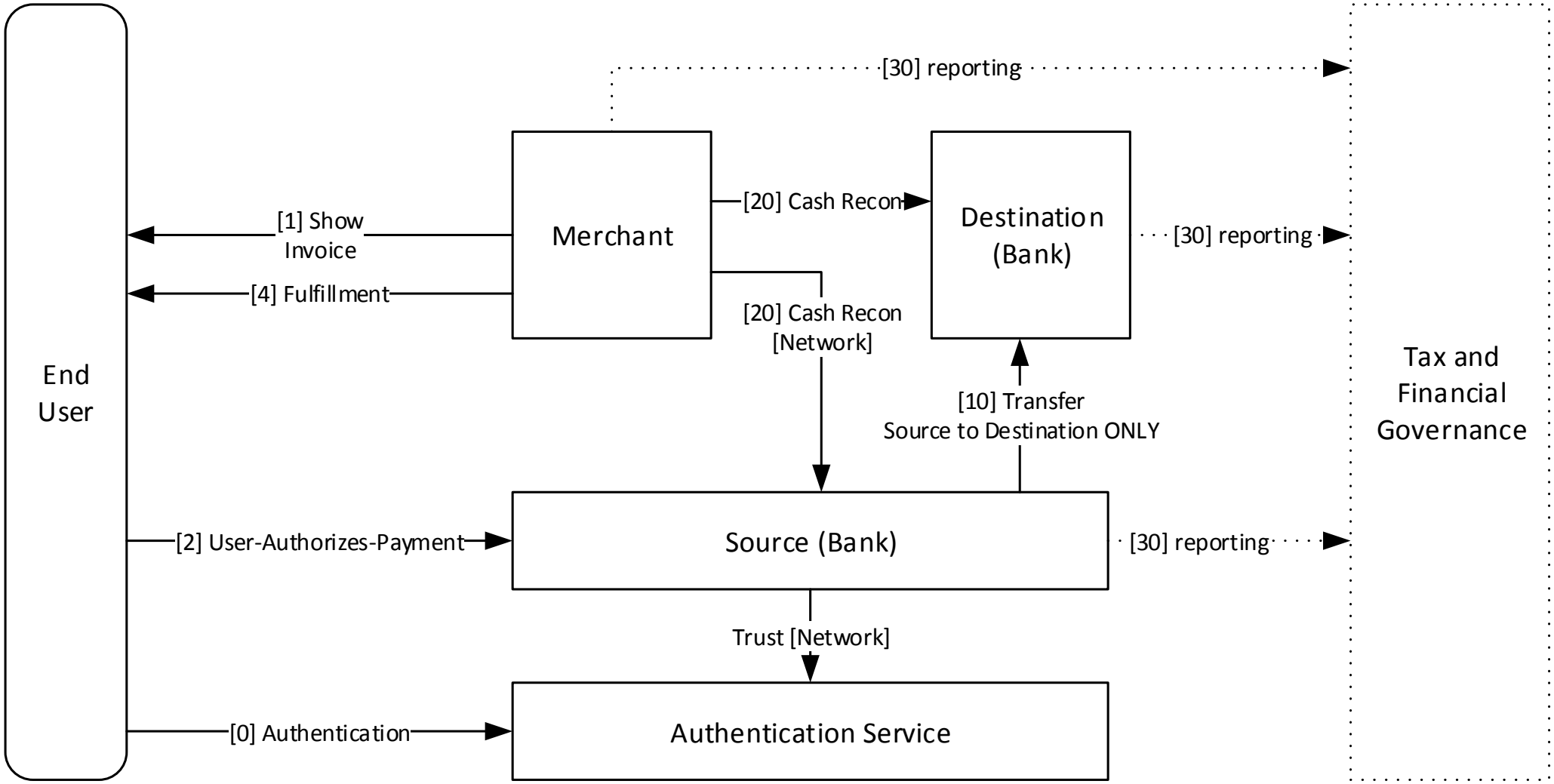
Bank Transfer

- Batch implementation
- Low transaction cost
- Two way transactions
  - Push – secure, like Kiosk Scenarios
  - Pull – trusts merchant, like North American Credit Card. Similar fraud risk, but currently less exploited because less accessible.
- Ideal flow applies
  - Automated push based on secure authorization

Bank Transfer Current



Ideal Bank Transfer



Ideal Bank Transfer Solution Technical Elements

Element	**Notes**
End User Authentication	• Secure channel between end user and authentication service prevents replay • Same requirements as credit card
User Payment Authorization	• Same requirements as credit card
Source [Bank] Payment Authorization	• Bank verifies validity of Payment Authorization, tied back to End User • Bank verifies and reserves availability of funds through credit or debit • Bank produces trustable statement of funds availability • Payment processing may still be batched
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources

Ideal Payment Solution: Secure Network

Element	**Notes**
Invoice	• States target of funds • Ties prices with product to be delivered
End User Authentication	• Secure channel between end user and authentication service prevents replay • Authentication service could be delegated outside the bank, but must be trusted • Many banks have invested significantly in their own solutions already
User Payment Authorization	• User states intent to make a payment. Statement tied back to authenticated user • Authorization specifies source, target merchant, invoice, quantity and time • A single authorization statement could authorize multiple payments • Experience integrated with merchant.
Source [Bank] Payment Authorization	• Bank verifies validity of Payment Authorization, tied back to End User • Bank verifies and reserves availability of funds through credit or debit • Bank produces trustable statement of funds availability • Merchant may fulfill as soon as Source Payment Authorization is available
Merchant to Source Network	• Facilitates Merchant's ability to scale to trust multiple payment sources
Cash Reconciliation	• Matches multiple user payments into single bank deposits from sources
Reporting	• Transaction details from source banks, target banks and merchant • Used in financial reporting and taxation