Taler Systems S.A.

Taxable **A**nonymous **L**ibre **E**lectronic **R**eserves

Christian Grothoff & Leon Schumacher

Instant Independent One-Click Payments

August 24, 2017

"I think one of the big things that we need to do, is we need to get a way from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity."

–Edward Snowden, IETF 93 (2015)

Agenda

1. Unique Sales Propositions
2. The Problem
3. What is Taler?
4. Operating Model
5. The Market
6. Competitors
7. About Us
8. Use Cases
9. Partners
10. Next steps
11. Risks

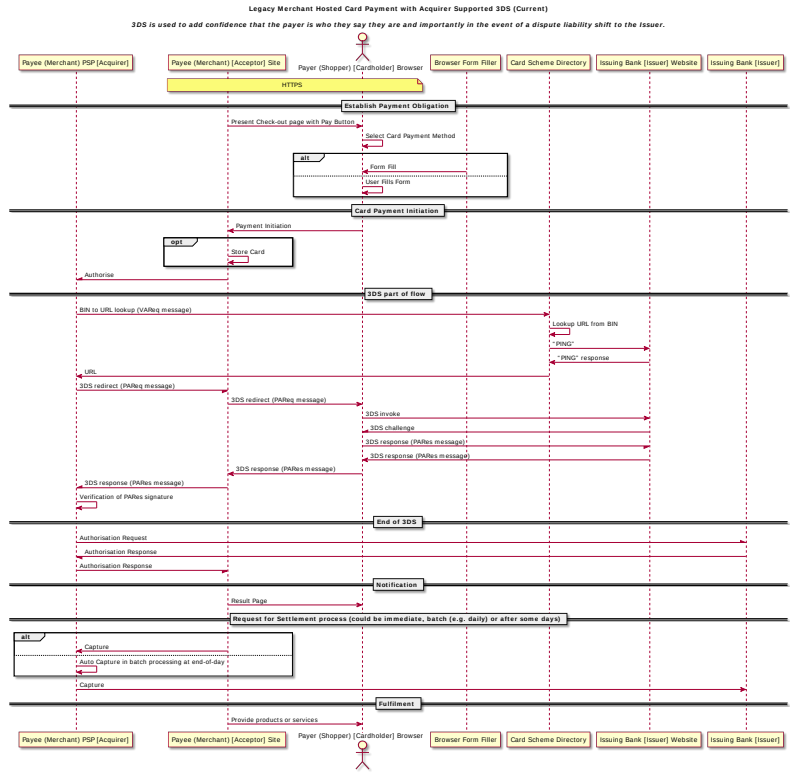
1. Unique Sales Propositions (USPs)

- Instant One Click Payments
- Privacy for spender from payment system provider
- No Fraud (compared to credit card online payments)
- No authentication needed for payment
- Micropayments possible
- Low transaction costs
- Open
- Scalable
- Transparent

2.1. The Problem

3D secure ("verified by visa") is a nightmare:

- Complicated process
- Shifts liability to consumer
- Significant latency
- Can refuse valid requests
- Legal vendors excluded
- No privacy for buyers



Cryptographers' paper on 3DS:

"Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication"

Online credit card payments will be replaced, but with what?

2.2. The Problem

- Global tech companies push oligopolies
- Privacy and federated finance are at risk
- 30% fees are conceivable
- Economic sovereingity is in danger

2.3. The Problem

European alternatives are low-tech:

European regulation requires high-tech:

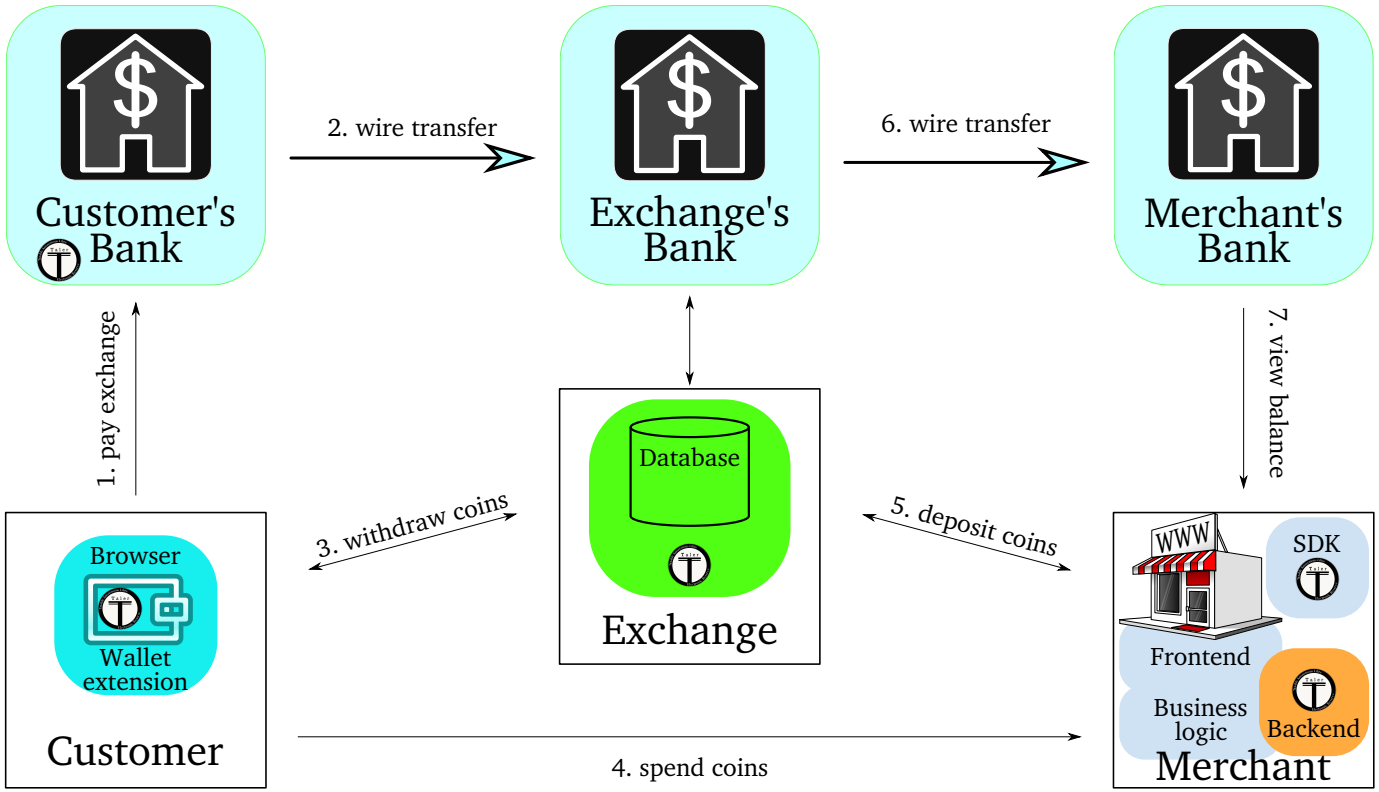
AML, KYC, **GDPR**

3.1. What is Taler?

Taler is an electronic instant payment system.

- Pay in existing currencies (i.e. EUR, USD)
- Uses electronic coins stored in wallets on customer's device

3.2. What is Taler?



⇒ Convenient, taxable, privacy-enhancing, & resource friendly!

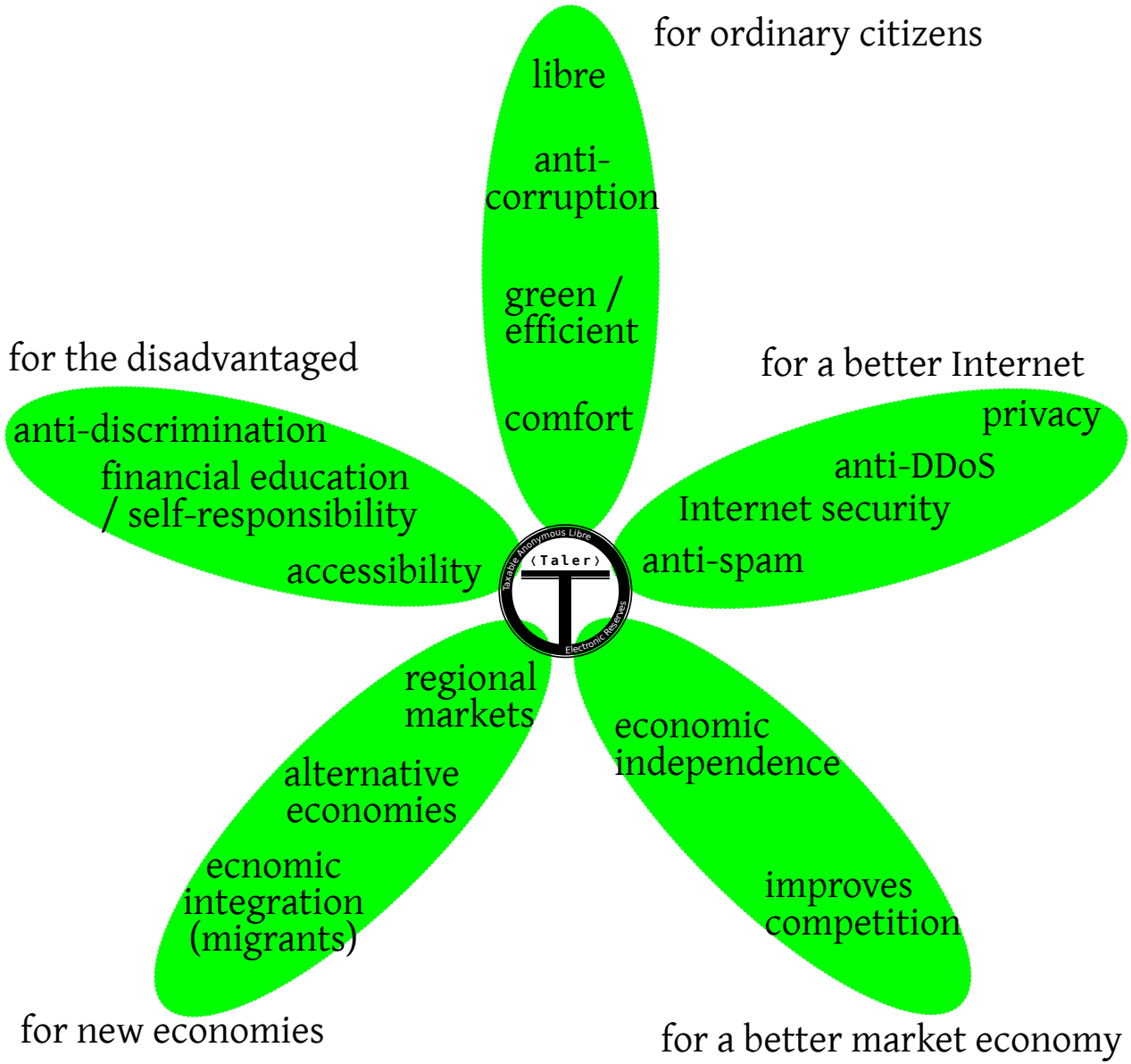
4.1. Advantages of Taler

- All operations provide cryptographically secured, mathematical proofs for courts & auditors
- Customer can remain anonymous
  - retain civil liberties in increasingly cash-less world
  - eliminates costly customer authentication
  - no credit card number theft possible
  - merchants do not need to operate expensive certified equipment & processes (PCI DSS, etc.)
  - Taler can give change and refunds, even to anonymous customers
- Merchants are identifiable in each payment they receive
  - bad for illegal business
  - no tax evasion

4.2. Advantages of Taler

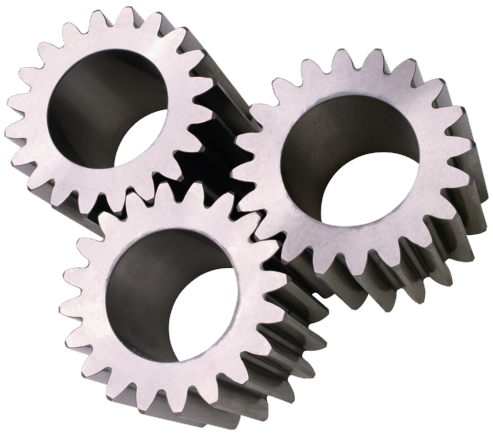
- Payments in existing currencies, does not introduce any new currency
  - financial stability, no risks from currency fluctuation
  - payment system, not speculative investment
- Scalable, fast protocol implementation
  - low transaction costs (in terms of computation at high volume)
- Open standard protocol without patents with free reference implementations
  - low barrier to entry for new merchants
  - governments may adopt as part of digital sovereignty agenda

5. Social Impact of Taler



6. Operating Model

Taler Systems S.A.



Exclusivity

Fees & Invest

Financial Services

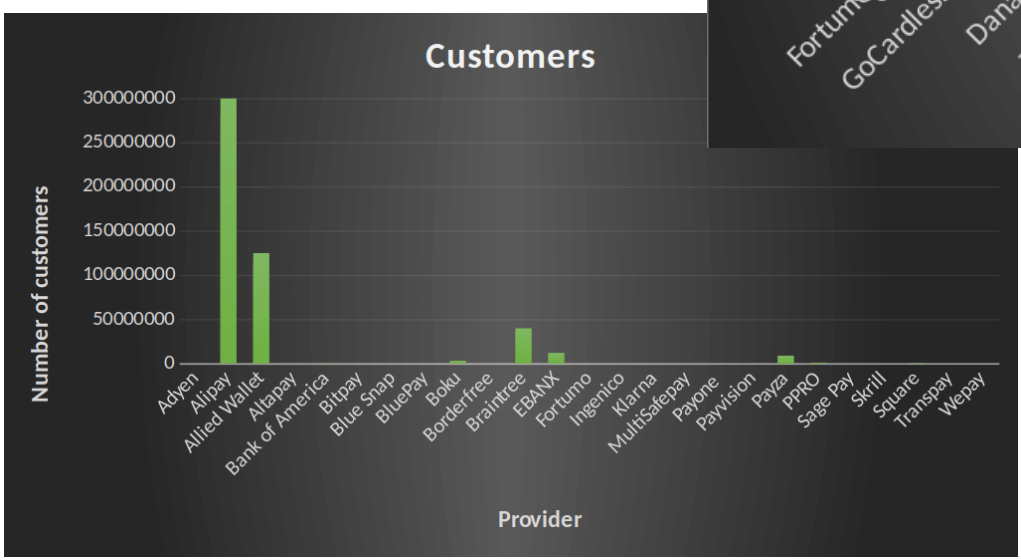
Partner

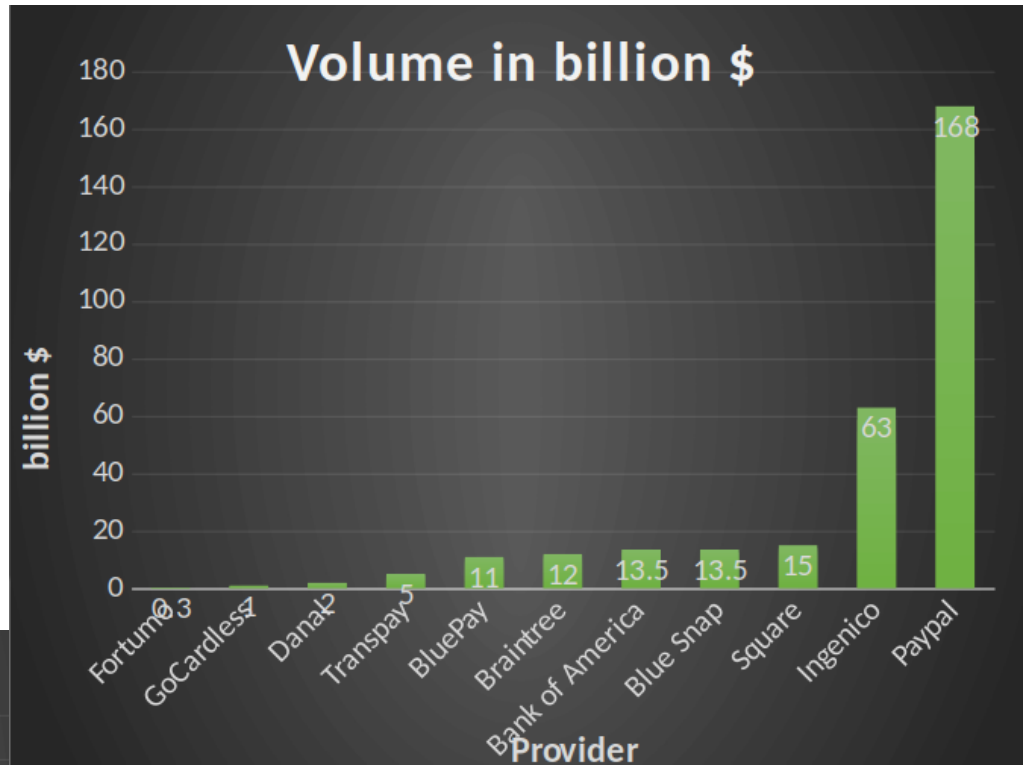
Operations Company
(currency exchange)

Low exchange fee
(0.5% for example)

Customer Wallet

7. The Market


Customers
Number of customers
300000000
250000000
200000000
150000000
100000000
50000000
0
Adyen
Alipay
Allied Wallet
Altapay
Bank of America
Bitpay
Blue Snap
BluePay
Boku
BorderFree
Braintree
EBANX
Fortumo
Ingenico
Klarna
MultiSafepay
Payone
Payvision
Payza
PPRO
Sage Pay
Skrill
Square
Transpay
Wepay
Provider


Volume in billion $
billion $
180
160
140
120
100
80
60
40
20
0
0.3
1
2
5
11
12
13.5
13.5
15
63
168
Fortumo
GoCardless
Dana
Transpay
BluePay
Braintree
Bank of America
Blue Snap
Square
Ingenico
Paypal
Provider

8. Competitor comparison

	Cash	Bitcoin	Zerocoin	Creditcard	GNU Taler
Online	−−−	++	++	+	+++
Offline	+++	−−	−−	+	−−
Trans. cost	+	−−−	−−−	−	++
Speed	+	−−−	−−−	o	++
Taxation	−	−−	−−−	+++	+++
Payer-anon	++	o	++	−−−	+++
Payee-anon	++	o	++	−−−	−−−
Security	−	o	o	−−	++
Conversion	+++	−−−	−−−	+++	+++
Libre	−	+++	+++	− − −	+++

9. Payment solutions - Pricing

Provider	**Pricing**
Alipay	2,0% - 3,0%
Allied Wallet	1,95% + $ 0,20
Amazon Payments	2,9% + $ 0,30
Avangate	4,9% + $ 2,50
Billpro	2,1% + 3,5% fee
BitGold Inc.	1% fee on every purchase
Bitpay (Bitcoin)	0%
Checkout.com	2,95% - 3,95% + £0,15
Coinify (Bitcoin)	0%
eComCharge	3,5% + 0,35 €
GoCardless	1% up to a maximum of £2
Western Union	Variable — From 5% up

10. Why now and why us?

Why now?

- Chaum's original patents[1] from 1996-1999 have expired
- Increased awareness of issue of privacy in payment systems
  - Contemporary payment systems fail on privacy
  - Cash is disappearing
  - Alternatives urgently needed
- Cryptocurrencies threaten control over money supply and tax base of governments

Why us?

- solved (technical) problem of unlinkability
- designed a modern, open standards based version
- technical expertise to really build it:
  - 15 years of research in network security and privacy
  - Founder of GNUnet and related projects
- good contacts: free software movement, press, academics

[1] USPTO 5878140, 5781631, 5712913

9. Team & Advisory Board

Leon Schumacher
co-founder

Dr. Christian Grothoff
co-founder

Dr. Jeff Burdges
PostDoc

Dr. Christina Onete
PostDoc

Florian Dold
PhD Student

Prof. Mikhail Atallah
Cryptographer, co-founder Arxan Technologies Inc.

Prof. Roberto Di Cosmo
Director IRILL

Greg Framke
CIO Manulife,
former COO Etrade

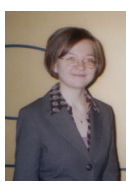
Ante Gulam
Global Head of Information Security — CISO
MetaPack Group

Dr. Richard Stallman
Founder of the
Free Software movement

Chris Pagett
former Group Head Security/
Fraud/Geo Risk HSBC

Prof. Alex Pentland
MIT Media Lab







10. Use Case: Consumers

Why would a consumer adopt Taler?

- Convenient: pay with one click instantly
- Guaranteed: no rejection by false-positives in fraud detection
- Secure: like cash, except no counterfeits
- Privacy-preserving: payment requires no personal information
- Stable: no currency fluctuations, pay in traditional currencies
- Free software: no hidden "gadgets", third parties can verify

11. Use Case: Merchants

Why would a merchant implement Taler?

- Instant payments: transactions at Web-speed
- Secure: signed contracts, no legitimate customer rejected by fraud detection
- Free software: competitive pricing and support
- Low fees: efficient protocol + no fraud = low costs
- Flexible: any currency, any amount
- Ethical: no fluctuation risk, no pyramid scheme, not suitable for illegal business
- Legal: complies with Regulation (EU) 2016/679 (GDPR)[2]

[2] Requires privacy by design and data minimization for all data processing in Europe after 25.5.2018.

12.1 Use Cases — Potential Niches for launch

1. Non-bankable / unbanked people
    - Children
    - Refugees / Displaced population
    - Developing markets (Africa)
2. Instant One Click Web purchases
    - Newspaper articles (see Spiegel's LaterPay)
    - Platform provider with exposure risk (see Spotify)
3. Niche Markets
    - Entertainment & Media
    - Tor users (when privacy is required)
4. Micropayments
    - Gaming (in-game payments)
    - Eliminate spam (require payment to display unsolicited e-mails)

12.2 Use Cases — Potential Niches for launch: Anti-Spam

p≡p provides authenticated encryption for e-mail:

- Free software
- Easy to use opportunistic encryption
- Available for Outlook, Android, Enigmail
- Committed strategic partner

Attach Taler payment to secure e-mail communication channel:

- Avoids two-sided market: peer-to-peer payments (this is how PayPal launched)
- If unsolicited sender (i.e. not in address book), hide messages from user automatically request payment from sender
- Sender can attach Taler payment to be moved to inbox
- Receiver can grant refund to sender
  (Taler still collects applicable transaction fees)

13. Use Cases — Used in financial model

- Newspaper articles (ex. Spiegel)
- Platform provider with exposure risk (ex. Spotify)
- Entertainment & Media
- Tor users

14. Partners

Research and development:

Business development:

Merchants:

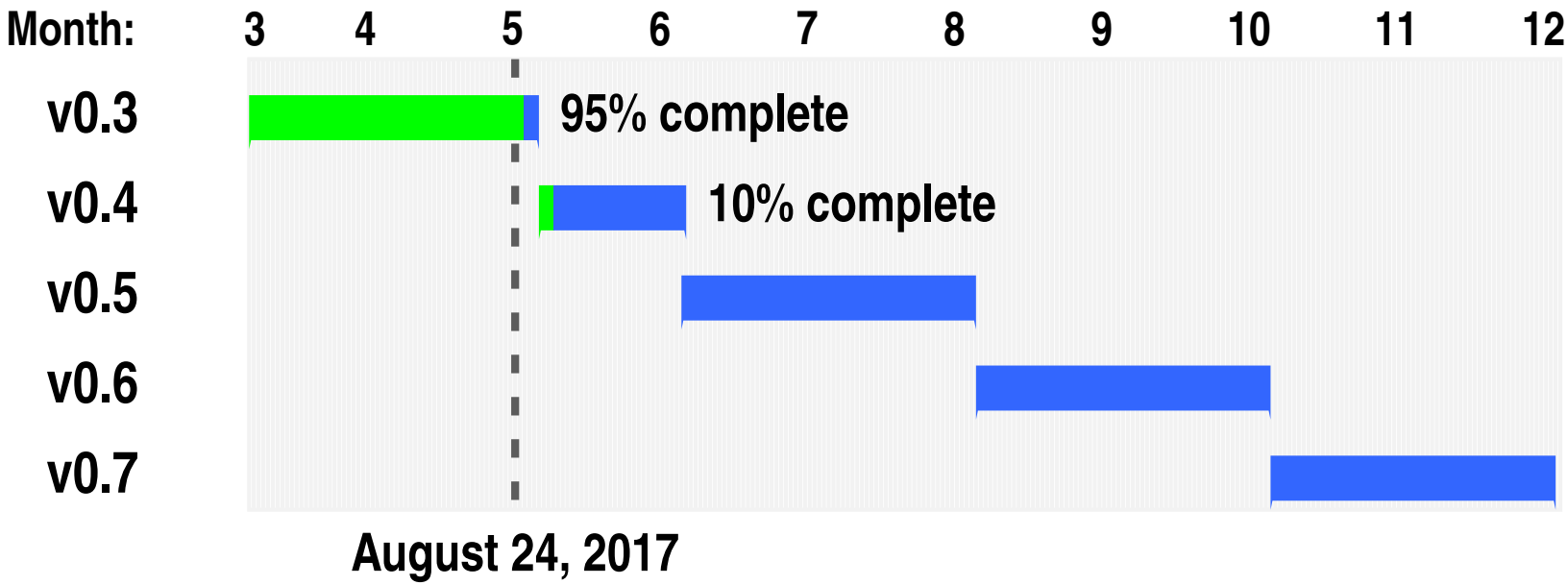
15. Strategic partners for distribution

2+ million daily users (in discussions)

p≡p

(in discussions)

16. Next steps in development and timeline



Development details can be found under:
https://gnunet.org/bugs/roadmap_page.php
Demo of real system: https://demo.taler.net/

Resources: Currently development is funded until late 2017

17. Efforts needed to reach v0.7

1.	Support refunds from merchant	-	2 PM
2.	Support refunds from (bankrupt) PSP	-	2 PM
3.	X.509 integration of merchant keys	-	1 PM
4.	Performance tuning	-	4 PM
5.	Extensive testing incl. fault injection	-	6 PM
6.	Documentation, minor features	-	6 PM

21 PM $\times$ 6k/month € = 126k €

Budget envelope: 150-200k €

PSP = Payment Service Provider / Exchange

PM = Person month

18. Efforts for other critical elements

1.	Wallet backup and cross-device synchronization	-	4 PM
2.	Wallet App for Android	-	18 PM
3.	Wallet App for iOS	-	18 PM
4.	Translation of user interfaces	-	3 PM
5.	External security audit	-	100k €

43 PM $\times$ 6k/month €	=	256k €
External audit	=	100k €
Budget envelope:		**360-400k €**

19. Extra efforts needed for refugee scenario[3]

1.	Shop App for Android	-	12 PM
2.	Shop App for iOS	-	12 PM
3.	Simplify exchange installation	-	2 PM
4.	Stand-alone basic-income bank	-	6 PM
5.	Translate Taler operator manuals	-	2 PM
6.	Network-challenged backup procedures	-	3 PM

27 PM $\times$ 6k/month €	=	222k €
Budget envelope:		**250-280k €**

[3] Optional special case

20. Sizing of Seed Round

1.	Development / Programming	600k €
2.	GoToMarket and Partner Sign-up	350k €
3.	Integration efforts with merchants	225k €
4.	Administrative & Overhead	325k €

Size of seed round (until 12/2018):	1.5m €
Time line:	Q4 2017
(Special optional refugee addition	300k €)

21. Next steps

1. Complete solution in v0.5 (alpha)
2. Complete first seed fouding round for 1.5-2m €
3. Integrate with one or more distribution channels (Tor browser, Mozilla browser, p≡p, . . .)
4. Launch successfully in one of the niches
   - Newspapers
   - Entertainment & Media
   - Gaming
   - Platform provider under threat from ApplePay, GooglePay, Amazon, . . .

22. Main Risks

1. Technical risk — resolved
2. Cryptographic risk — resolved
3. Distribution on customer side challenging
4. Distribution on merchant side challenging
5. Regulator does not approve
6. System hacked (by internal admin staff)

23. Risk Mitigation

1. Technical risk — resolved
2. Cryptographic risk — resolved
3. Distribution on customer side challenging
   Partner with reach on consumer end
4. Distribution on merchant side challenging
   Partner with platform merchant, or
   Partner with large financial service player
   Focus on e-commerce
5. Regulator does not approve
   Initial reviews by specialists see no issues
   Partner with large financial service player
6. System hacked (by internal admin staff)
   Automated reporting shows maximum exposure
   Audits conducted regularly
   Vetting of admin personnel

24. Business risks and measures

Risk	**Impact**	**Countermeasure**
Usability too low	few users, insufficient income	usability testing
Exchange data loss	financial damage	backups
Exchange compromise	financial damage	limit loss by key rotation
Exchange offline	reputation loss	redundant operation
Compliance issues	illegal to operate	work with regulators
No bank license	illegal to operate	work with banks

25. Recent Press

09-2015

- https://bitcoinmagazine.com/21901/bitcoin-governments-without-privacy-taxes/
- http://www.heise.de/tp/artikel/46/46089/1.html

06-2016

- http://www.theregister.co.uk/2016/06/06/gnu_cryptocurrency_aims_at_the_mainstream_economy_not_the_black_market/
- http://www.golem.de/news/halbanonymes-bezahlsystem-gnu-taler-soll-kryptowaehrungen-gerechter-machen-1606-121323.html
- http://www.heise.de/newsticker/meldung/GNU-Taler-Open-Source-Protokoll-fuer-Zahlungen-in-Version-0-0-0-erschienen-3228525.html

08-2016

- https://www.theguardian.com/technology/2016/sep/01/online-publishers-readers-ad-block-surveillance-donate-anonymously

02-2017

- http://hackerpublicradio.org/eps.php?id=2222

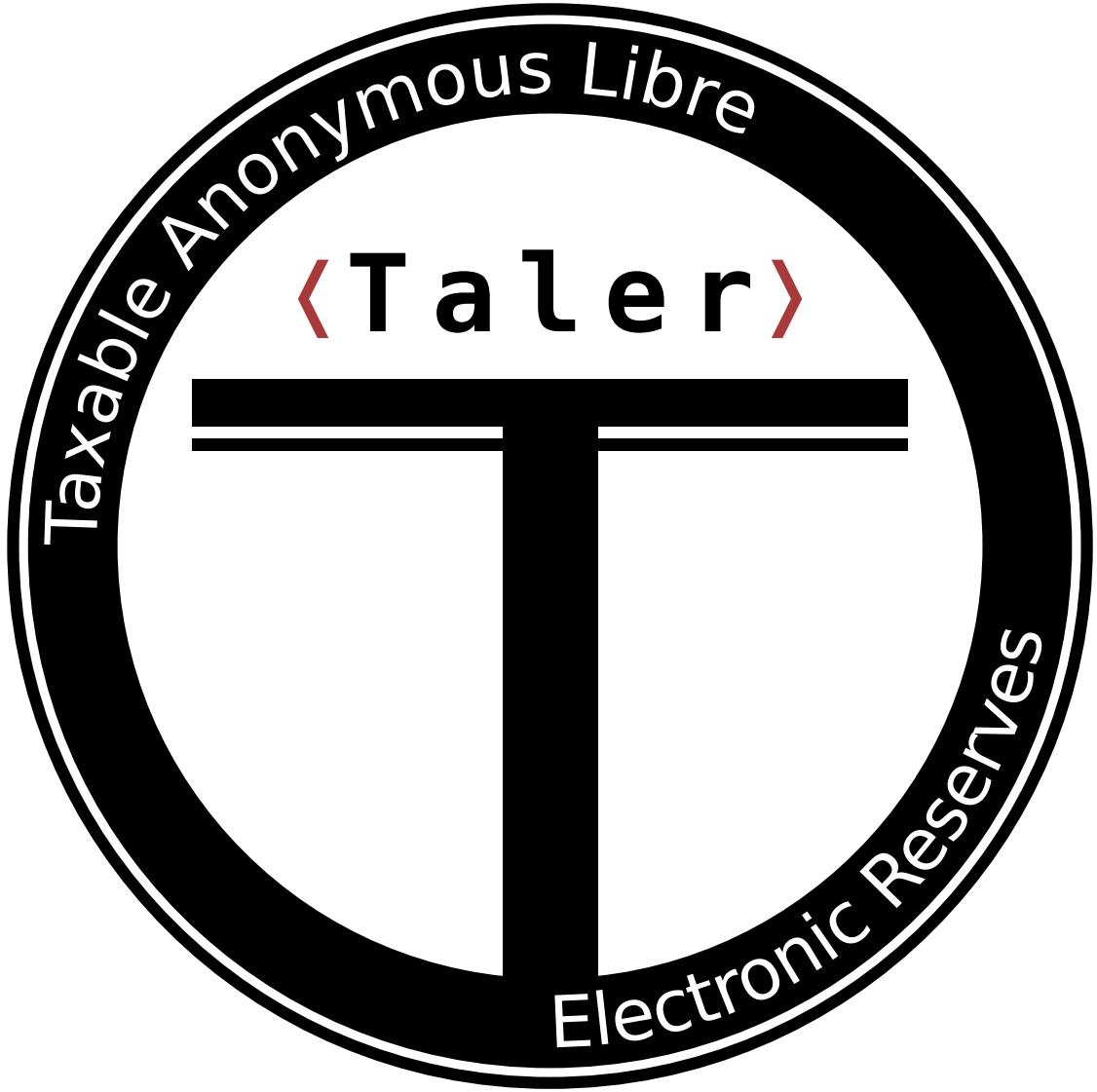
Complete list at `https://taler.net/press`

Contact details

Leon Schumacher
leon@taler.net
+41-79-865-9365

Dr. Christian Grothoff
christian@taler.net
+33-2-99-84-71-45

https://www.taler.net/


Taxable Anonymous Libre
⟨Taler⟩
Electronic Reserves

Potential Synergies between Taler and Blockchains

What can Blockchains do for Taler?

Taler cannot cryptographically prove the **timing** of transactions. Using a blockchain for **timestamping** would allow GNU Taler to provide hard proof of **when** a payment happened.

What can Taler do for Blockchains?

Blockchains have inherently high transaction **costs** and little **privacy**. Taler can operate as a **side-chain**, providing enhanced privacy and **performance** for crypto currencies.